

係長セキュリティから社長セキュリティへ： 日本的経営と情報セキュリティ

林 紘一郎*

概要

内閣官房情報セキュリティ対策推進室の設置から11年、本学の設立から7年目に入り、「情報セキュリティ」という概念自体は、世間に受け入れられたようである。しかし言葉を理解することと、それを実践することとは、まったく別物である。リスクを評価する際に「統制環境」が大切だというのが、わが国企業に情報セキュリティが定着するには、「日本的経営」という環境にマッチした施策を工夫する必要がある。そこで最も大切な要素は、ボトム・アップを中心にしてきた「日本的経営」の伝統の中に、トップ・ダウンが不可欠な情報セキュリティ施策を、不適合を起さぬように埋め込むことであろう。標語的にいえば、「係長セキュリティ」にとどまっている現状を打破して、「社長セキュリティ」への転換(止揚)が求められる。本稿では、企業ガバナンスの日米比較等を通して「日本的経営」の特徴を洗い出し、転換に必要な留意点を抽出するとともに、トップ経営者に理解を訴える。

1 はじめに

1999年1月、複数の中央官庁ウェブ・サイトのトップページが、不正に書き換えられるという事件があり、それを契機に情報セキュリティへの関心が高まった。政府は、翌春内閣官房情報セキュリティ対策推進室(2005年に情報セキュリティセンターNISCと改称)を設置し、公的機関を中心にした対策を強化した。また関係省庁を含めて、重要インフラ10分野ほか民間の情報セキュリティ対策についても、年度計画や数多くのガイドラインを発出して、セキュリティ・レベルの向上に努めている。

この間、2005年の個人情報保護法の全面施行や、2009年3月期から義務づけられた財務報告を中心にした内部統制制度の法制化など、新しい制度の導入もあった。これらに促されて、情報セキュリティという概念やその重要性については、(一部に「行き過ぎ」が懸念されるほど)十分に浸透したようである。当大学院も、創立当初は「そもそも情報セキュリティとは」という切り口から、説明を始めねばならなかったが、現在ではそれは昔話になった感がある。

しかし言葉を理解することと、それを実践することとは、まったく別物である。リスクを評価する際に「統制環境」が大切だというのが、わが国企業に情報セキュリティが定着するには、わが国企業の統制環境の代表的要素である「日本的企業風土」に合った施策が、不可欠

* 情報セキュリティ大学院大学学長・教授

である。その際参照点とすべきは、一般的な「日本的経営」論のほか、伊丹敬之氏の指摘する「人本主義」であろう(伊丹 [1987][2000] など)。企業統治の日米比較等を通して、「日本的経営」の特徴の洗い出しに成功しているからである。

そこで「人本主義」としての日本企業が、「資本主義」を旨とするグローバル市場で生き残るには、どうした良いのか。最も大切な要素は、ボトム・アップを中心にしてきた「日本的経営」の伝統の中に、トップ・ダウンが不可欠な情報セキュリティ施策を、不適合を起さぬように埋め込むことであろう。標語的にいえば、「係長セキュリティ」にとどまっている現状を打破して、「社長セキュリティ」への転換(あるいは両者を止揚すること)が求められる。

なお、本稿は私一人の独創によるものではなく、共同研究の成果を私が代表して報告するものである。私たちの研究チームは²、科学技術振興機構から助成を頂き、「企業における情報セキュリティの実効性あるガバナンス制度の在り方」というテーマで、2006年から3年半の間研究してきた。その最終成果は報告書として公表済みである³が、その中に主として経営層向けの提言として、以下の「Awareness 提言」がある。

認識1. (リスク・テカーとしての企業)

企業はリスク・テカーであり、リスクを低減したり、ヘッジしたり、移転したりすることは出来るが、それをゼロにすることはできない。

認識2. (業務のシステム依存)

企業活動の大部分は、コンピュータとネットワーク・システムに支えられており、そのリスク対策が情報セキュリティであるから、これは経営の根幹に触れる問題である。

認識3. (経営者自身に課せられた最適化問題)

情報セキュリティがリスク対策である以上、それは全社的に費用対効果を最適化すべきものであり、他の経営意思決定と何ら異なるものではない(専門家に任せておいて済むものではない)。

認識4. (ガバナンス制度間の整合性)

情報セキュリティ対策は、経営全般のガバナンスと責任のあり方(内部統制、コンプライアンス、品質管理、環境適応、企業の社会的責任)などと整合的、かつ統制の取れたものでなければならない。

認識5. (企業ごとの特色)

情報セキュリティ対策は、企業を取り巻く環境や、長年にわたって培われた企業文化と不可分のものであるから、他から移植して済むものではなく、自ら生み出さねばならない(わが国全体としてみれば、「日本的経営の特色」との整合性が必要である)。

これらは見慣れた提言で、ことさら新しいものは何もない、と思われよう。そのように受け止めてくださる方は、それで十分である。しかし、日本の経営者の多くが、そのように答えて

¹ この標語は、本学教授板倉征男氏が最初に命名したもので、本稿で論ずるように「係長クラスが情報セキュリティ対策を一生懸命やっているが、その意図がトップには届いていない」状況を指している。

² チームのメンバーは以下の通りで、この場を借りてご協力に感謝する。代表: 林紘一郎、総括班: 大井正浩、岡村久道、国領二郎、苗村憲司、田中英彦、法制度班: 石井夏生利、岡田仁志、城所岩生、佐藤慶浩、鈴木正朝、新保史生、早貸淳子、湯浅懇道、経営管理班: 内田勝也、柿崎環、加賀谷哲之、中尾宏、藤本正代、山川智彦。技術班: 江崎浩、門林雄基、小林克志、砂原秀樹、辻秀典、起草委員: 田川義博。

³ http://www.ristex.jp/examin/infosociety/governance/pdf/fin_hayashikou.pdf

くれるとは思えない。そこで本稿では、上記報告書のうち経営学的分析を中心に紹介⁴、併せて提言の背景や、その後得られた知見についても付言することで、われわれが何を考えて報告書をまとめたのかを明らかにしたい。

まず第2章で、そもそも情報セキュリティを担う主体として、なぜ企業を取り上げるのかを論ずる。第3章では、日本的経営の特色とされる諸点を、通説とされる見方を中心に列挙し、第4章では参照点として有効な、人本主義の指摘に耳を傾ける。第5章では、話題を科学的管理法や標準化の動きに転じ、日本の経営者の間では、こうした動きを理解する層と、まったく理解できない(理解したくない)層に、分断されていることを指摘する。第6章では、以上の分析を総括した上で、転換に必要な留意点を摘出するとともに、主としてトップ経営者の理解を訴える。

2 なぜ企業を取り上げるのか

なぜ企業を対象にして「情報セキュリティ」を論ずるのだろうか？ 提言を理解するには、その背景になっている思想を理解していただく必要がある。このスタンスが違ってしまうと、その後の理解も進まないのだから、これは重要なスターティング・ポイントである。

どうやら世間の大部分は、「企業」というものを誤解しているようである。企業に勤めている人は企業を当たり前存在だと思ひ、時には自己と同一視しているが、一方企業不祥事などを追いかけている人は、企業を悪の代表のように考えている。このように理解が分断してしまつて、企業というのを正しい意味で捉えるのが、意外に難しい。

私自身にとつても、会社人間であつたときは、やはり企業を正当化する傾向があつた。例えば、マスメディアの批判にさらされている最中に、「自社を客観視して、別の視点から見る」ことは、なかなか難しかった。しかし会社を離れて十数年たつてみると、良いところも悪いところもある程度見えてきた。

そこで改めて、なぜ企業を取り上げるのか、情報セキュリティのガバナンス問題を考えるときに企業が主体であるし、主体にならざるを得ない理由を、「企業の存在の大きさ」「リスク・テーカーとしての企業」「責任の主体としての企業」の3つの側面から取り上げてみよう。

2.1 企業の存在の大きさ

まず第1の「企業の存在の大きさ」については、これを4つに分けることができる。1つは現代資本主義社会における、「存在の大きさ」という面である。社会におけるビジネス活動の比重が、どんどん大きくなつていく。官から民へというスローガンに促されて、従来官がやっていた業務を民営化したり独立行政法人化すれば、民の方のウェイトが高まってくる。民の活動の担い手は、法人、中でも大部分は株式会社であろう。奥村宏氏の一連の著作では、こうした時代を「法人資本主義」と呼んでいる(奥村 [1975][1991][2006] など)。

第2点は、「情報量の大きさ」である。情報セキュリティは、情報処理と裏腹の関係にある。情報爆発という言葉があるように、経済・社会活動における情報量の増大がまずあり、それに連れて「情報処理装置としての企業」が、中心的役割を担うようになってくる。

⁴ 報告書には、経済学と法学のアプローチも含まれているが、これらは別の機会に訴求することにしたい。

確かに、情報は政府にも集まっているし、政府の情報の方が重要で、多様性に富んでいるという面もある。しかし政府が情報を扱うときには、法の下でやらなければならないので、用途が制限されたり自由度が制限されて、民のように自由闊達に使うことはできない。また個人も情報処理の主体であり、ましてや集合知とか Web2.0 という環境の中では、個人の役割は大きい。しかし法人の情報量を凌駕するということは、あまり考えにくい。そうすると勢い、法人に注目した施策というものを考えることになる⁵。

企業の大きさの3点目として、グループ経営、アウトソーシング、クラウドコンピューティングのように、「多様化・複雑化」しているという面がある。企業経営そのものがネットワーク型になり、バリューチェーンが広く長くなっていることとも、連動している。企業の扱う情報から派生する問題の影響度も、従来のようにあるスタティックな範囲で管理すれば良いという問題ではなく、一旦漏洩すると連鎖的にあちこちに広がる、まさにウィルスのような格好になっていく。

この点について浅井 [2007] は、情報セキュリティを取り巻く環境の変化として、次の5点を指摘している。取引先との情報共有を前提にしたビジネス、客先からの厳しいセキュリティ要望、インターネット環境での情報伝達・共有方法の激変、e ビジネスの進展による新しいリスク、社内からの経営情報の漏洩リスク(p.36)。これらの指摘は、報告書で述べた「動態的ガバナンス」にもつながるのではないと思われる。

企業の存在の大きさの4点目として、以上のことと裏腹で、「企業市民としての責任」が求められている。つまり、コンプライアンスや内部統制が、声高に叫ばれるのは、結局企業の存在が大きくて、無視できないということと裏表の関係になっている。しかし、法令を適切に遵守することは良いことだが、場合によってそれが行き過ぎることも問題にされている。

例えば、郷原 [2007]⁶は、コンプライアンスが行き過ぎると、本来の業務運営さえまならなくなると言い、さらに菊澤 [2007] のように逆に「命令違反」を煽る主張まである。これらは、行き過ぎの弊害を指摘する限りでは正しいが、逸脱行為そのものまで是認する主旨ではなからう。こうした反語的表現が出てくる背景には、次節で述べる「企業はリスク・テーカーである」という認識が、日本企業のトップに希薄である、という焦りがあるものと推測される(この点は、2.3 で再論する)。

以上小項目としての4点ばかりが、企業の存在が大きいが故にセキュリティのガバナンスを考える上で、まず企業を取り上げなければならない理由である。しかし全く別の面から考えると、「そもそも企業ってなんだろう」という論点があり得る。

2.2 リスク・テーカーとしての企業

世の中にはいろいろなプレーヤーがいる。例えば政府は通常はリスクを取らないで、「安全の方が大切」という保守主義で運営されるが、「税金の無駄使い」を避けるためには、そのような慎重さも必要である。個人もリスクが取れるほどの資金がない。コロンブスがアメリカへ船出する時に、スペイン女王からお金をもらったのは例外で、通常リスク・マネーは必

⁵ 実はこの2点目が、科学技術振興機構に助成金を申請するときに最初に訴えた点だが、だんだんそれ以外の点も分かってきて、ここでは幅広く論じている。

⁶ 英和辞典を引けば、compliance には「(バネのように)外部環境に柔軟に対応する」という意味であり(例えば、The American Heritage Dictionary of English Language)、このような誤解が生ずる余地はなきそうだが、日本では「法令順守」は硬直化しているようである。因みに、BS 標準をグローバル・スタンダード化しようとするイギリス人は、「融通無碍」が特質の一つだという(渡辺 [2009])。

要だが手に入りにくいものである。そこで、株主は利益があれば配当に与ることができるが、失敗した場合も出資分を放棄すれば、それ以上の責任は負わなくて良い、という仕組みが生まれた。これが企業、すなわち今日の株式会社である。

当初の企業は「当座企業」といい、航海 1 回毎に精算する仕組みだったが、その後「継続企業」(going concern)として永続的に事業を営むことが志向された。そして、それを支える会計や監査の仕組み、さらには株主の有限責任制が考案されたことによって、今日の株式会社が誕生した。したがって株式会社は、発生史的には「ベンチャー」であり、リスク・テーカーであったと考えることができる。

企業がリスク・テーカーだというのは、バーンスタイン [2001] などに極めて明瞭に説明されていて、定説になっている。ところが、日本企業はリスク・テーカーといえるだろうか。必ずしもそうではなく、逆に risk averse(リスクを避ける)傾向が強い。他方、アメリカ企業に見られるように、あまりにもリスク・テークが過ぎた強欲資本主義が良い、ともいえなくなっている。どの辺のリスク・テークが適切かが問題になるが、少なくとも企業という存在自体は、一義的にはリスク・テーカーだと考えられる。

2 点目はそこから派生して、リスク・テークする(低減・受容)以外に、リスクを回避したり移転したりする技術も、同時に生み出さなくてはならない。テーク & テークでは破綻してしまうからである。そうすると移転されたリスクとか、回避されたリスクは、どこに行くのか。ゼロになるわけではないから、2次的リスク 3 次的リスクというように、必然的に拡がりを持つことになる。

科学技術の発展も似たようなところがある。近代化の初期の段階では「技術は必ず善をもたらす」というように歓迎する向きもあったが、現在においては新しい技術が新しいリスクを生むかもしれない。ベック [1988] が指摘した「再帰的近代」という言葉があるように、自分の製品やサービスの外部効果(特に、負の効果)が自分に帰ってくることもある。金融業において、この点をまざまざと思い出させてくれたのが、サブプライム・ローン問題ではなかったらうか⁷。

金融業におけるセキュリタイゼーションとは、長期にわたらないと回収できないような資金コストを、証券化して他に移転する方法で、早期に回収できる手段として考案されたものである。買い取った会社は、証券である利点を生かして別の人に売るか、専門業者に引き取ってもらうかして、リスクを回避する。したがって、本来セキュリタイゼーションというのは、セキュリティを確保するための手段であり、セキュリティが高まると思われていた。

ところが、無記名の証券が早いスピードで転々流通するようになると、一体今誰が持っているのか分からない。さらに残念なことに、一番最初に証券化して買い取る人は、次に売ればいいので、市場が整っていて自由に売ることができる限りリスクの評価が甘くなる、というモラル・ハザードが生じかねない。一番目の買い手のハザードは、二番目以降の買い手についても言えるから、どこで、誰が、どのくらいのリスクを保有しているかが分からなくなる。アメリカのサブプライム・ローンでは、正にそういうことが連鎖的に起きた。

市場全体がバブルっぽく膨らみ、住宅価格が上がっているうちは、そうした欠陥は、全部吸収されて目立たない。ところが、一旦金利が上がって住宅価格が下がると、今度は逆の方に行ってしまう。早く資金を回収しようと思って、取り付け騒ぎのようなことが起こり、そ

⁷ この点については、金融情報システムセンターの機関紙に駄文(林 [2009a])を書かせていただいた際、何冊かの本を読んで非常に勉強になった。特に池尾・池田[2009] はサブプライムの背景から始まって、非常によく書いてある。

の連鎖によって激変が起きた。これが前述の「再帰的近代」の、非常に良い例になっている。

2.3 責任の主体としての企業

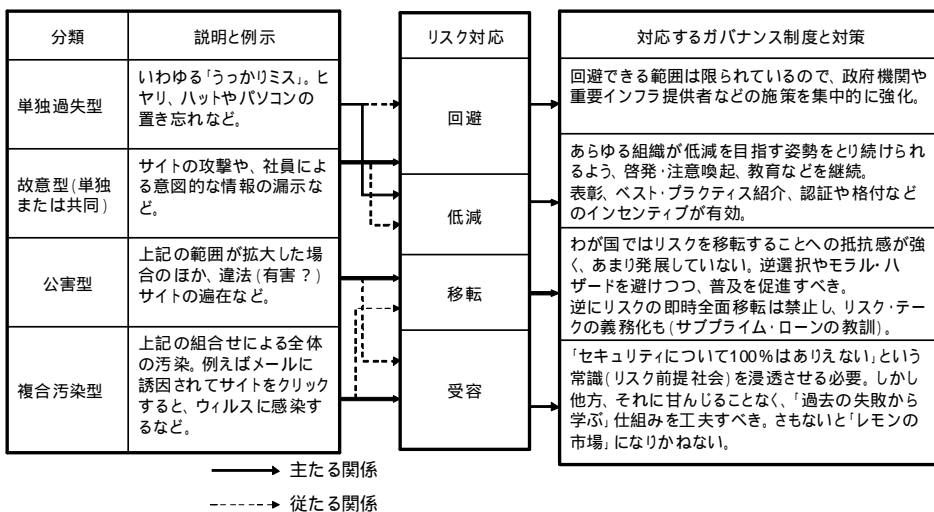
さて、「企業の社会的責任」が重視されるようになって、法体系はすぐに追いついてこない。現在の日本法においては、責任の第一の主体は個人(自然人)で、法人が責任を負うのは、その監督責任に限定されるのが建前になっている。これを、市民相互の関係である民事事案と、社会秩序の維持と関係する刑事事案の両面から見ていこう。

まず民事の事案においては、故意や過失で他人の権利や利益を侵害すると、それを賠償する責任が生ずる(民法 709 条)が、その主体は行為者すなわち個人である。当該個人を雇っている法人は、事業執行上のことであれば「使用者責任」を負うが(同 715 条 1 項)、「相当の注意」を払っていれば免責される(同但し書き)。刑事の事案においては、この原則はさらに徹底しており、処罰されるのは行為者(個人)であって、法人に責任が及ぶのは「両罰規定」として、その旨が法に特に規定されている場合(例えば、労働基準法 117 条以下など)に限るとされてきた。

しかし、公害に代表されるように企業活動そのものが他人の権利を侵害したり、製造物責任のように、働いている労働者の行為というよりも、企業そのものの行為と見た方が常識に合致するような事例が、多く見られるようになった。そこで、民事の事案においては、法人そのものが責任の主体であることが、珍しくなくなっている。刑事の事案については、通説はなお「法人責任論」に対して懐疑的といわれるが、それを真正面から主張する見方も出始めている。

以上の文脈を、情報セキュリティに当てはめると、どのような見取り図が描けるだろうか。責任を論ずるには、前述の通り「リスク・テカー」である企業にとって、どのような対応があり得るのかを見定める必要がある。そこで図表 1. は、セキュリティの専門家が「インシデント」と呼んでいる事件や事故と、リスクの取り方、さらにガバナンスの基本となる事項を対応させたものである。ここでは、インシデントを単独過失型、故意型、公害型、複合汚染型の 4 つに分け、一方リスクの取り方を、回避・低減・移転・受容の 4 つに分けている。

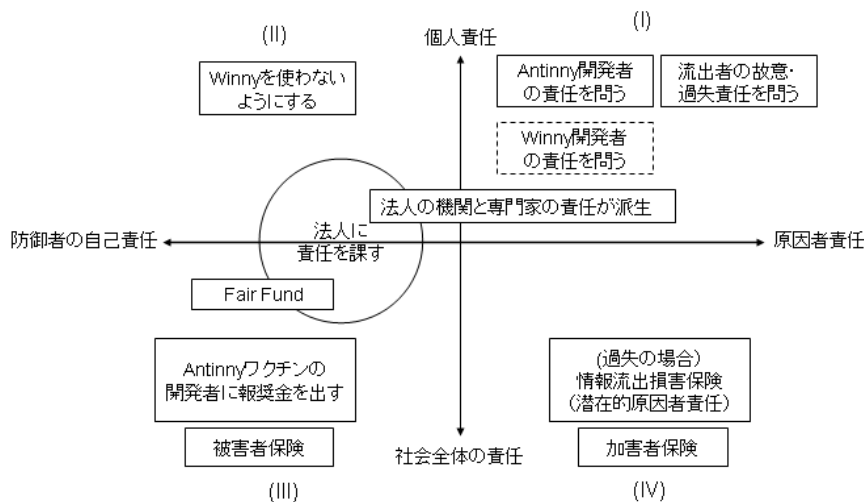
図表 1. インシデントとリスクとガバナンスの対応



この図から分かることは、情報セキュリティのインシデントは、かつて故意や悪意があっても、典型的な愉快犯であったものが、インターネット全体を汚染し、あわよくば一儲けしようといった知能犯や、場合によってはゲーム感覚的行為に、移行しつつあることである。そこでリスク対応も、インシデントの A タイプにはこれ、B タイプにはこちら、といったように 1 対 1 で対応することができず、主たる関係と従たる関係が入り乱れる結果となっている。

このことを責任論の面から図示したのが、図表 2. である。この図の横軸は、原因者が責任を負うのか、被害者が自己責任で防御を迫られるのかを示し、縦軸は個人の責任なのか、社会全体で責任を負うべきかを分けている。近代法の建前は、() の領域にある原因者の個人責任であり、これは今でも責任論の第 1 原則になっている。例えば、情報の流出事故が起これば、流出させた個人を特定して、その責任を問う。

図表 2. 責任のあり方



この原則に従えば、一時情報漏洩の主原因とまで言われた P2P ソフトの代表例である Winny と、そのウイルスである Antinny については、Antinny 開発者を逮捕してウイルス作成罪(その法制化前は、著作権侵害なりの別罪)に問うのが王道であろう。ところが、匿名を隠れ蓑に活動する犯人を捕まえるのが至難の技であるため、警察は Winny の開発者に著作権侵害の幫助の罪を着せようとした。これはもともと「無理筋」であるため、主として技術者の間から「革新的なソフトの開発などに萎縮効果が及ぶ」ことが懸念されていたが、高裁では無罪の判決が下された⁸。

このように()の領域が有効に機能しないとすれば、その他の領域の適用を考えねばならない。時の政府は、「Winny を使わないように」と呼びかけることで事態の収拾を図ろうとしたが、それは()の領域に属する。また、「Antinny ワクチンの開発者に報奨金を出す」など、インセンティブを与える方法(III)もある。こうした報奨金方式は、日本ではなじみが薄いだが、アメリカでは広く行なわれている。また、加害者が掛けるにせよ被害者が掛けるにせよ、保険が用意されていれば、事業活動等に伴うリスクを、「移転」という方法で避ける

⁸ 2009 年 10 月、大阪高等裁判所は一審判決を破棄し無罪を言い渡したが、検察側が上告中。

ことができる(IIIとIV)。

このように、近代法が想定していた「行為者 = 個人責任」だけに固執していると、情報セキュリティを維持できないことが、広く認識されつつある。図の左側に「法人に責任を課す」という円を入れたのは、そのような意味である。ただし、行為者が罰せられず法人だけが責任を負うという制度も、これまでの慣行になじまない⁹。その際には、法人の機関や専門家の責任も、併せて検討せざるを得ないことになる¹⁰。

しかし、こう言ったからといって、sanction の有効性¹¹を追求するあまり「厳罰化」を求めている訳ではない、ことに留意していただきたい。例えば、個人情報保護法の施行以来、情報漏洩に対する社会的意識が高まった。それ自体は遵法精神の向上として評価すべき面もあるが、困ったことは「厳罰化」が追及される一方で、責任の所在が曖昧なままの「責任の希釈化」が、同時並行的に進んだことである(林・鈴木 [2008])。責任のあり方は、過大でも過小でもいけない。適切なレベルを維持する必要がある。

この面からは、「失敗学」的な発想(畑村 [2000])で、「事故の責任追及」よりも「再発防止」に資するため、例えば捜査よりも事故調査を優先させ、一定の条件を満たせば「事故調査に協力する限りで責任は問わない」という免責条項を新設することも、検討されてしかるべきだろう。最近では裁判も、被害者や遺族の感情に、より配慮するようになった。そのこと自体は必然の流れであるが、被害感情をも超えて公益に資する「情報」を入手し活用することに、もっと努力が傾注されて良い(村上 [1998])し、個々人の過失よりもシステムとしての不完全さに、より注目すべきであろう(デッカー [2009])。

2.4 企業のガバナンス

リスク・テーカーである会社は、リスクに対してどのような対応を取ったら良いのだろうか。ここでまず問題になるのは、企業がリスク対策をとるのは誰のためか。つまり会社は誰に責任を負っているのか、突き詰めて言えば、会社は一体誰のものかということである。

日本的には、会社はステーク・ホルダー全体のものであり、労働者だとか債権者だとか多くのプレーヤーを考慮に入れる考え方が根強い。これは「ステーク・ホルダー資本主義」とで呼ぶべき考え方で、日本ばかりでなくヨーロッパ大陸系の諸国では、そうした発想が広まっている。法的には、これらの国々は「大陸法系」(あるいは制定法系)の諸国と呼ばれる。

他方、アングロサクソンの国々(法的にはコモン・ローの諸国)では、会社は「株主」のもので、それ以外のプレイヤーはすべて「利害関係者」に過ぎない。これらの諸国ではproperty(財産権)は経済社会の基礎になる、基本概念である¹²。会社もpropertyの一種で、その権利を持つ人が多数いると、アンチ・コモンスの悲劇が避けられないから、会社は

⁹ 現行の個人情報保護法においては、安全管理義務違反を犯した企業に対して主務大臣の改善命令が出て、それにもなお従わない場合に初めて、刑事罰が課せられる可能性がある(個人情報保護法20条, 34条, 56条など)。このように限定的な措置(間接罰)であるにもかかわらず(あるいは限定的であるが故に?)、企業人の間からは漏えいの主体である個人に対して、直ちに刑事罰を加える方式(直罰方式)を望む向きが多い。

¹⁰ ISMSの審査員など、情報セキュリティの専門家を対象にするセミナーの都度、「ISMSの認証取得企業と未所得企業に、同じデータベースの個人情報へのアクセスを許してシステム開発をさせたところ、両者ともに同じような規模の情報漏えいを起こした。この場合、両者の責任の度合いは、前者がより重い。差がない。後者がより重い、のいずれであるべきか?」という調査をしたことがある。われわれの予測に反して、の比率が相対的に高かったことは、専門家の責任についても言えそうである(林・鈴木)2008)。

¹¹ sanctionは通例「罰」に近いマイナスのイメージがあるかと思われるが、ここでは報奨金のようなプラスの仕組みも含めて考えている。

¹² 英米法におけるproperty概念の整理については、林 [2010] 参照。

株主だけのものである、と割り切る傾向が強い(株主資本主義)。

どのような環境でも、どちらかが一方的に正しくて、他は完全に間違いである、とまで言い切ることはできないだろう。しかし東西冷戦を制したのが、所有権という property を重視する「資本主義」であったことは否定できない。また、Legal Origin Theory (LOT) が指摘するように、ここ 20 年ほどの経済パフォーマンスは、制定法の国々よりもコモン・ローの国々が優れていたことも否定できないだろう¹³。

このように考えてくると、「ステーク・ホルダー資本主義」も、「株主資本主義」も共に理論としては成り立つが、第一原理はやはり「株主資本主義」だということになる。実際のビジネス経験においても、例えば 50:50 の出資比率のジョイント・ベンチャーが旨く行かなかったり¹⁴、共同 CEO の両者の関係が微妙になってしまうことは、広く視察されている。一義的な責任を負うのは、一人でなければならないのである。したがって、いかなる場合にも、この第一原理がなくなるということはない。

そうするとここには、経済学のいう「プリンシパル・エージェント問題」が、最もプリミティブな形で現れる。つまり、主人(プリンシパル)である株主がエージェントである経営者に、「最も自分の意向に沿うように経営してもらいたい」と考えても、それは常に達成されるとは限らない。何故ならエージェントには、プリンシパルの支配をなるべく逃れて、自分の思うように経営したいという動機が常に働く。それに対して株主は、経営の情報を常時持っているとは限らないから、日常の意思決定はかなり任せないといけないので、管理に限界がある。

一方で意思決定を任せながら、他方で「ここだけは必ず締めなければいけない」という点を締める、というのがガバナンスの問題だが、これは往々にして失敗することが多い。リスク・テーカーである企業全体として見ても、リスクを正しく評価して過不足なくリスクをテークするかというと、必ずしもそうならないかもしれない、という問題が内在している。

小さな企業で、特に創業当初であれば、会社を作った人たち = 出資者 = 経営者であることが多く、組織自体の全体が割と見渡せる。もしそこに組織の目的と逸脱した行為を取るような人がいれば、直ちに見つけて sanction を加えることは可能である。しかし現代の企業のように、組織が大きくなって歴史も長くなると、組織がそれ独自の文化を持つようになり、個人と組織の行動目的がぴったり合うのは、なかなか難しくなってくる。

組織の中には、いろんなことを考える個人がいるわけだから、個人の行為で組織の方針から逸脱するものが出てくる。と同時に、個人個人で判断すれば、合理的な判断ができて逸脱しないかもしれないが、何故か体制に従うと組織全体として逸脱するという、所謂会社ぐるみの犯罪とか、不祥事がたくさん出てくる。

同じ科学技術振興機構の助成による、岡本グループの研究(岡本・今野[2006] など「組織の社会技術」5 分冊が出版されている)では、そうした逸脱行為を主として個人の良心との葛藤という面から調べて、いかなる心理現象だと見るのがいいのか、逸脱を防ぐための組織構造や風土は如何にあるべきか、ということ論じている。

しかし最近の研究は、多分それをさらに超えているのではないか。というのは、岡本グループの研究における責任の主体は、やはり個人にあり、近代の責任能力を持った独立し

¹³ 主導者はハーバードのシュライファー教授であるが、共同研究者との著作によって LOT を論証している。例えば、La Porta, et al. [2008] 参照。

¹⁴ 京セラの創設者稲盛和夫氏は、50:50 では経営が旨く行かないことを実感的に身に付けていたようで、DDI がトヨタ系の TWL と合併する最、マジョリティ取得にこだわったようである(渋沢 [2010])。

た個人という発想は、そこで貫かれている¹⁵。ところが本間 [2007] の研究による「組織性逸脱行為」では、その組織に属していると逸脱を逸脱だと感ずる感覚さえ鈍くなってしまふ、という側面を見出している。現在問題視されている企業不祥事を見ると、どうやらこちらの方が当たっているのではないかと思われる(リーズン [1999])¹⁶。

そうすると、法人がリスクを取って利益を上げるためには、極端に行くと「なんでもあり」ということになりかねない。金さえ儲かれば、法に触れない限りなんでもするというようなことが横行する危険性がある。都合が悪い情報を隠したり、自分達しか知らない情報で儲けたり(インサイダー取引)しかねない。これはまさに、情報セキュリティを考える上では無視できない論点である。極端なことをいえば、この点だけを取り上げて、企業における情報セキュリティの在り方、そのガバナンスの仕組みとこのことを、考えなければならないということになる。

そんなことをいうなら、組織を見捨てたらいいではないか。法人に代わる、もっと倫理観が貫かれるような組織形態を考えたらということは、頭の体操としてはあり得る。しかし、近代社会以降の長い歴史の中で、株式会社を超える良い仕組みとこのことは見出されていない、というのが正しい。

市場という制度についてよく言われるように、市場が常に最良の方法とは限らない。市場はあくまで次善の方策かもしれないが、それを上回る良い仕組みを考えてご覧といわれると、行き詰まってしまう。それと同じように、株式会社を超える良い制度を考えてご覧といわれると、行き詰まってしまうのではないか。そのあたりが難儀だということになってくる。

ここで、公益通報者保護法について触れておきたい。日本の企業では、異質なものは排除される傾向があったため、組織性逸脱行為が蔓延しているとしても、誰もそれを指摘しないということになりかねない¹⁷。一人一人見ればいい人なのに、全体としてみればなんだかおかしいことになっている。やはり個人にも良心があるのだから、その一人の良心を聞く道はないのかということとは、当然考えてしかなるべきだと思う。

それを促すために、社内に専門の窓口を設けて解決を図る。そして、いろんな手を尽くしても駄目な時は、最後の手段としてマスメディアに訴えるなり、外部に訴える道を開くということは、無いよりは良いに決まっている。しかし先ほどのような空気が変わらないで、この制度だけが行なわれると、事後的に誰が訴えたのかということがはっきりした時は、やはり不利益な処遇になるということはあるだろうと思う。

アメリカでさえ、ボーグルの本で読むと、内部通報者 300 人のうち 207 人はその後退職しているという(ボーグル [2008] p.71)。不利益処分を企業から受けることは許されないから、解雇ではないと思うが、やはり内部の軋轢等で耐えられないということもあるのではないか。ドライと言われるアメリカでさえこのような状態だから、日本の場合もっとドロドロしたものにならざるを得ない(奥山・村山・横山 [2008])。

人情的には世話になっている会社を告発するのは忍びないけれど、「大義のためには

¹⁵ もっとも岡本も、逸脱が広範囲になれば「無責任の構造に至ってしまうことを懸念しているが、それは意識的な個のリーダーシップで克服可能と見ているようである(岡本 [2001])。

¹⁶ 最近の企業不祥事においては、「悪いことをしていると知りつつ止められない」というケースよりも、「会社に忠実なあまり、ついで線を超えてしまふ」というケースの方が多く見られる。このような「善意過失」を促すような企業風土が生じた場合には、個人の責任を追及するよりも、組織改革を優先させなければならない。

¹⁷ 聖書に「良きサマリア人」の逸話もあり、ボランティア精神が日本よりは強いと想定されるアメリカで、1964年に起きたキティ・ジェノヴェーゼ事件は、この点を考える上で示唆に富む。深夜3時に仕事からアパートに帰った彼女が暴漢に襲われ助けを求めたにもかかわらず、警察に通報があったのは35分後の3度目の襲撃の後(既に死亡していた)で、叫び声を聞いた人は38人にのぼるとされる。この経験から、「冷たい隣人」「傍観者効果」などの概念が生まれた。

身を捨てても」という行動が、確保される仕組みを考えなければいけない。そのことが、ひいては(多分長期的には)、企業にとっても役に立つはずだと思う。

3 日本の経営論

「わが国企業には独特の風土がある」という議論が、80年代に盛んに行なわれた。それは、単一言語単一民族の宿命かもしれない。アメリカのような多民族国家で暮らすと、国の中に宗教や言語や出自の違う人がいる。そこで自ずと、他の人は随分違うが、それは個性なのだから当たり前だと思うようになる。それに対して日本では、国土の中で多様性を実感できないためか、日本人論とか日本社会論が好きなようである。

ただ、80年代にその論争が強くなったのは、別の理由もある。世界経済の中で日本企業が「一人勝ち」状態になっており、21世紀は日本の世紀だとか、「Japan as No.1」とか煽られた、ということにも関係がある。強いには何か理由があるのだろう、というように皆考えるからである。

また、それを逆手にとって「日本異質論」という批判があったことも、忘れることができない。「確かに日本は強いかもしれない。しかしそれはアンフェアなやり方で強いだけじゃないか」とか、「欧米流のグローバル・スタンダードからすると日本は外れている」というような意味で捉えられたこともあった。しかし「失われた10年」なり「20年」を経た現在では、日本的経営論の中には真実もあるが神話的部分もあるというように、割と客観視されるようになったかと思われる。

そこで以下では、このように客観視できる状態での「日本的経営」の特色を抽出し、それが情報セキュリティとどのようにかわるのかを、検討してみたい。

3.1 いわゆる3種の神器

日本企業の特徴が、終身雇用、年功序列賃金、企業別組合という、いわゆる三種の神器¹⁸に象徴されるという通説については、やや神話化された面がある。つまり、事実なのか神話なのか、あるいは事実だとすれば昔からの事実なのか、それとも最近になってのことなのか、というようなことが真剣に議論されることは稀であった。しかし小池 [2009] などの批判あるいは研究によって、一部の神話が突き崩されつつある。

そのような例を幾つか挙げると、第一に終身雇用である。日本では「昔から終身雇用だった」という風に何となく信じていたが、実は歴史を遡れば比較的新しいことで、1920年代の不況の時に、「熟練労働者を温存するにはどうしたらよいか」と考えた企業が、採用し始めた。それが戦争に突入して加速されたことによって、その後の経路を決めたのだという(岡崎・奥野 [1993])。

つまり終身雇用というのは、現在の日本の大企業を見る限り間違いではないが、それは昔からあったことではなく、せいぜい50~60年前のことであったということである。一方これに対比される、アメリカ企業の雇用形態については、大変な誤解がある。というのは、アメリ

¹⁸ これは日本人が古くから意識していたのではなく、アベグレン [1958] などの研究によって、いわば「外部から発見された」。同様のことは、トヨタ生産方式における「JIT(Just In Time)」「Kaizen」などにも言える。トヨタがこうした概念を広めたというより、ハーバード・ビジネス・スクールによって発見された、という方が事実に近い。どうやら日本人は、概念を作って売り込む才能に乏しいようである。この点については、6.1で再論する。

力の大企業も実は、ほとんど終身雇用だからである。GMを見れば分かる通り、経営破綻のかなりの原因が、非常にリッチな退職後プランにある。

私が長い間お付き合いしていた AT&T でも、早期退職してニュージャージーの海や川の近くに住んで、釣りやゴルフ三昧している人たちがいる。私が NTT アメリカの社長をしていたとき、エンジニアを募集したら AT&T の Bell 研究所の OB で、しかも博士号を持っている人が来た。「博士号を持っている人にやってもらう仕事じゃない」と断ったけれど、「自分は週に2日か3日は体を動かしたいから」といってやって来た。early retirement しても、十分暮らしていけるようなペンションシステムを、公的年金のほかに用意していた証拠である。

終身雇用に近い状態でなければ、こんなことはやるはずもないし、企業にとって大きな負担になるはずもない。アメリカの大企業は、少なくとも黄金の50年代や60年代を経験してきた過程においては、多分終身雇用だったのではないか。そうすると、終身雇用が日本独特の仕組みであるというのは神話に過ぎない、ということになる。

2点目の年功序列賃金については、終身雇用が前提となるのであれば、経済合理性を持ったシステムではないかと思われる。何故なら、子供が小さいときには教育費用はそんなにかからないが、高学年になればなるほどお金がかかる。あるいは持ち家を持ったりすると同じことが言えるから、生活費保証ベースで年々給料が上がるのは合理的だからである。

終身の雇用が保証されている中では、若い時には自分の会社に対する貢献度よりも安い賃金を甘受する代わりに、将来的には貢献度を上回る高い賃金が約束されているとすれば、会社を離れるインセンティブはない。それは、個人にとっても会社にとっても、有利な方法である。

アメリカも実は終身雇用であったことを認めるにしても、年功序列の面ではアメリカに比べて、日本のユニークさが目立つかと思う。アメリカの場合は職務を決めると、それに対して賃金がだいたい固定するので、将来的にもそんなに上がっていかない。その代わりに、ボーナスとか昇給を決める際に、成果主義が合理的だということになって、アメリカは皆そうやっていると思われてきた。

しかし、これもまた小池 [2009] によると大きな間違いで¹⁹、人事考課についての驚くべき指摘がある。彼が親しい研究者や経営者に、例えば5段階評価の時に5や1といった極端な評価を、どのくらいのパーセンテージで付けるかという、それはごくごく少ない。圧倒的に中位に集中している、というような研究結果を小池氏自身も聞いたし、アメリカの論文にも出ている(小池 [2009] p.35)。

どんなに合理性に富んだ上司でも、「標準より上の方だけ、何パーセントを上限に付けていい」という仕組みならできるが、「上に5パーセント付ければ、下にも5パーセント付けなければならぬ」という仕組みをとった途端、下の方に付けるのを躊躇する。ということは、必然的に評価が中位に集中する訳で、これは日米にかかわらず人情としても当然ではないかと思われる。私もアメリカで人事評価をやる際、同じ事を実感している。

そうすると、アメリカは年功序列かもしれないけれど成果主義であったかという、そうとも

¹⁹ もっとも著者自身が以下のように告白していることから分かります。これらの指摘が学問的な検証に耐えられるものかどうかは、今のところ留保が必要かもしれない。「年来わたくしが世にいいたいことが心に残っている。それを書いた。つまり、証拠がやや足りないにもかかわらず、なおいいたい議論を集めている。」(pp.5-6)

言い切れない。それをあたかもアメリカは成果主義だと誤認して、日本はグローバル・スタンダードに立ち遅れているから、にわかに成果主義を導入すべきだというのは、愚の骨頂だったのではないかと思われる(城[2004]などを参照)。

3.2 人も調達対象か？

アメリカ人は、一般的には人・物・金(最近では情報も入るかもしれないが)といった経営資源は、「市場から調達できるもの」と考えている。お金は自己資金を別にすれば、借入れ等種々の方法で外から持ってくる資源である。物も勿論 make or buy で、自分で作ることもできるが、買ってくることもできる。自分で作るとしても部品まで作る人はいなくて、外から買ってくる。場合によって最近では fables になっていて、全部外から買ってくることも可能である。

このように金と物の調達については、市場を経由することがいわば当たり前のことなのだが、問題は人である。アメリカ人は、どうやら人も市場で調達できているので、本当に長期に雇用したい限られた人材は、終身雇用で採用して社内の転勤(社内労働市場)で対処するかも知れないけれど、そうでない大勢は job description を書いて、それに合った人をその都度雇っていく、という発想がかなり強い。

この点では日本企業は明らかに違っていて、原則として人は調達する資産ではない。人という資産は、長期的視点で採用してトレーニングして「熟練」を生み出して、そうして内部に維持するものだと、こういうふうになっている。これはどちらが良いとか悪いとかいう問題ではなくて、考え方の違いではないかと思われる。

アメリカにいとレイオフがしょっちゅうあって、不況の時のクッションになっている。働いている人たちも、不況になれば若い人が先にレイオフされるのを当然と思っている。ここで若いというのは実年齢ではなく、その会社に何年いるかということである。seniority という制度があって、勤続年数の長い人ほど保護されており、労働組合もそれを是認し、むしろ推進しているように見える。

一方、日本は不況になって支出削減をする時にどうするかというと、4つの順番が決まっている。まず1番目に在庫を取り崩す、2点目として労働時間を減らす、3番目にパートや臨時工を減らす、4番目にいよいよ常用労働者の雇用を調整する、というのが暗黙のルールになっている(篠塚・石原 [1977])。そういう意味では、日本は人を大事にする企業だと言え、これが次の章で取り上げる「人本主義」の原点でもある。しかし実は、そこで人といっているのは、正規社員に限られている。

そこで次節で述べる、企業別労働組合は、実は「企業別正規社員労働組合」であって、同じ企業に3年ぐらいいは勤務するにしても、非正規社員を積極的に組合員に取り込もうとはしなかった。従って現在のような大不況が訪れた時には、正規社員と非正規社員の間に変な格差が生じて、いわゆる労・労問題(労使が対立しているのではなく、労と労が対立している)という不思議な構図になっている。つまり、労働者を守るはずの労働組合が、ある面では労働者の敵になってしまっている。

これは、日本全体にある程度蔓延している病かもしれない。例えば野口 [1995] が、日本の中央官庁というのは「1940年体制」で、戦争にどう備えるかということに照準を合わせた仕組みになっている。だから一つの目標に向かって多数の省庁が突進する時にはいい

かもしれないが、解くのが非常に難しい問題が生じて省庁間の調整が必要になったり、あるいは市場そのものがもうあまり成長しない場合には、こういう仕組みは有効に機能しない、と言っている。正規社員・非正規社員の問題は、ひょっとすると日本に致命傷になるような問題かもしれない。

3.3 企業別組合の神話性

日本企業の三種の神器の最後の「企業別労働組合」というのは、わが国の特色だと言われている、事実そうかもしれない。なぜなら、他の国では職能別組合というのが普通であるのに対して、日本の組合員は組合員である前に、特定の会社の社員であるからである。組合員の方に、「あなたはどこの方ですか」と聞いたら、間違いなく「私は何々社のものです」という。そこで「組合には入っておられますか」と聞くと、「わが社の労働組合がありますから、(当然)入っています」とこうなる。

それに対して、特に労働組合の発生の地であるイギリスなどにおいては、「あなたはどこに属してますか」と聞くと「私は何とか職能組合の組合員です」と答える。そこで、「今どこで働いていますか」という問いを出さないと、会社の名前が出てこない。そういうことになっていると典型的には言われているが、それが正しいかどうか私には分からない。

しかし小池 [2009] の身を挺した研究によると、事実は以下のようなことらしい。ある職場に 5 つの職能別組合がある、とする。そうすると我々が日本で習った暗黙の了解によれば、使用者は 5 つの組合と個別に交渉しなくてはいけない。それは大変で、どの順で交渉するかということ自体も問題になる。私は NTT に長くいたが、NTT は伝統的に第 2 組合を作らないという方針で来たので、このような問題は発生しなかった。それは相手が対決型の組合ではなかったからである。

それに対して旧国鉄という組織では、対決型の組合を持っていたために、会社側が促進して第 2 組合を作った。できてしまって困ったのは、どちらと先に話をつけるかということで、これは「話し合いをつけ易い方が先」、つまり第 2 組合からというのが、当たり前である。しかし、第 2 組合と手を握っていることが第 1 組合に分かれれば話が壊れるので、手を握っていないように見せながら、何とか相手を説得しなければいけない。また、例えば妥結の前後関係だとか、主席交渉員として誰が出るかなども、大変に神経を使う。

そういう日本人から見ると、いくつも労働組合があると、どこから先に交渉するのか心配になる。ところで小池氏の方法論は、サッカー好きを生かして、サッカーチームが強くて町ぐるみで応援しているところの大学に留学する。そしてサッカーを通じて組合の役員と親しくなって、「実際のところどうなっているのか」ということを、聞き取り調査している。

その彼の言っているところによれば、組合が 5 つあったとすると、もちろん個別に交渉しなければいけない事項は個別に交渉するが、そうでない事項については代表交渉員を決める。それは通常一番大きな組合があればそことやり、他の人はそこに委任して²⁰代表者と交渉するので、結局職能別組合があっても共通事項については、企業別労働組合あるいは工場別労働組合と同じことだというのである(小池 [2009] pp.188-189)。

そうすると、企業別組合は日本の特色でこんな例はどこにもない、とって日本異質論

²⁰ ここから先は証拠がないので本当かしらと思うが、その代表者の賃金は会社持ちである。それは日本の法によれば直ちに「不当労働行為」となるので、そんなことがあるのかとクエスチョンマークを付けておこう。

を煽るというのいかなものかということにもなる。要は日本的経営というのは、確かに特徴的な点があることは事実だけれども、それを絶対視しないことが大事ではないかという感じを抱く。そういう目で、日本には日本の流儀がありますよという風に見ていくのであれば、それはそれで有効な方法かと思う。

4 人本主義

前章の論点は、人本主義の議論へとつながっていく。日本的経営論には神話的部分が付随していたが、それらを消去してもなお、日本の特色があることは否定できない。西欧の会社組織が資本を中心にした集まりであり、まさに「資本」主義であるのに対して、日本企業は人を中心にして集まっているという意味で「人本」主義だということが、ある程度妥当するのではないと思われる(伊丹[1987])。

しかし、このような仕組みはグローバル化する環境の中で、今後も維持可能なのだろうか。他方サブプライム問題が発端になって、「(強欲)資本主義」も是正を迫られているとすれば、今後の会社組織はどう変化していくのだろうか、またどうあるべきだろうか。情報セキュリティという切り口から、分析を深めてみよう。

4.1 人本主義の特色

人本主義の提唱者である伊丹氏自身は、その特色を以下の表のようにまとめている(伊丹 [1987] p.51)。

図表 3. 人本主義対資本主義

	人本主義企業	資本主義企業
企業概念	従業員主権	株主主権
シェアリング概念	分散シェアリング	一元的シェアリング
市場概念	組織的市場	自由市場

「企業概念」と「市場概念」について追加すべき事項はないが、「シェアリング概念」については、若干の補足が必要かもしれない。従来の伝統的な会社概念では、「市場情報と技術情報をもった企業家が企業の所有者であり、意思決定を行ない、賃金などを市場価格で支払ったあとの付加価値は自分がすべてを占有する。つまり、情報、付加価値、意思決定の3つのシェアリングは、(中略)一人に集中したパターンとなっている。」

これに対して日本企業の場合には、「3つの変数のシェアリングのパターンを互いに微妙に違えて、『みんなにそれぞれ花をもたせている』こと(非相似)、1つの変数のシェアリングがどこかに集中している度合いが低い(非集中)、この2つの点で、『分散』シェアリングなのである」(伊丹 [1987] pp.53-55)。

こうした分析は、前章で述べたような3種の神器という「現象」に着目した見方を超えて、その背後にある「原理」に迫るという意味で、よりメタな分析といえよう。しかし、さらにメタレベルで考えると、人・物・金のすべてを自由に調達可能な資産であると見るのではなく、人だけは他の資源とは別だというメタ思考があることは、前述したとおりである。

このような観点から、人本主義と資本主義を私流に比較しなおしてみると、図表4. のようになる。ここでは、人という資源が他の資源とは別だという視点を強調するため、人資源に関係する仕組みを重点的に取り上げている。しかし「日本的経営」に多くの神話が伴っていたことから分かります、「人本主義」と「資本主義」に差があることは事実だが、場合に寄っては根拠が薄弱だったり神話に過ぎないものもある。両者の差は、世間で言われているほどには、大きくないとも言えそうである。

図表5. 人本主義と資本主義の特徴

論点	Governするのは誰か？	労働力は調達すべき資源か？	給与は職能給が望ましいか？	給与の業績連動部分を増やすべきか？	フリンジ・ベネフィットに金を掛けるべきか？
人本主義	株主(法的には社員)よりもコア従業員重視。人事は集権的	社内に蓄積されたノウハウや熟練が大切(長期)雇用保障	ローテーション人事などがあるので、職能給的にしかない。	ボーナスの査定などはよいが、連動部分をあまり多くすべきではない。	ある程度はかけるべき
資本主義	株主のみ。人事は事業部任せ(逆に、情報は集中)	技能向上は個人の責任。会社は労働者を市場で調達。レイオフ	Job descriptionに基づく職務給	連動部分やストック・オプションを増やすべし。	あまり意味がなく、その分を給与に反映させた方がよい
備考	コア従業員とは長期雇用にコミットした人	しかしアメリカでも大企業は終身雇用が多かった(例:GM)	アメリカでもコア従業員にjob descriptionはない	アメリカでも、実際の査定ではAとDは少ないという(小池)	わが国でも縮小の方向

いずれにせよ、私流に「人本主義」を解釈すれば、その核心は「企業は長期に在籍する人を中心にできているのだ」という見方に行き着くであろう。欧米流に、人・物・金全てが自由に調達し配分可能なものであると見れば、人もいつでも lay-off できると考えがちになる。一方日本のように、物と金は外部市場から調達可能だが、人だけは別だとすれば、「解雇の自由」もある程度制限されてしかるべきだ、というような風土になってくる。

その意味では、「解雇の自由」が著しく制限されている日本では²¹、伊丹流「人本主義」が当たっている面がある。しかし今日的には、それが正規社員に限定されているということは、大変大きな意味がある。前述のとおり、まず在庫を減らし、その次に勤務時間を減らし、それから派遣だとか短期制社員を減らし、いよいよ最後に本社員に手を入れるというような順序は、合理性を持っているかもしれないが、それ自体が差別的ということにならざるを得ないからである。

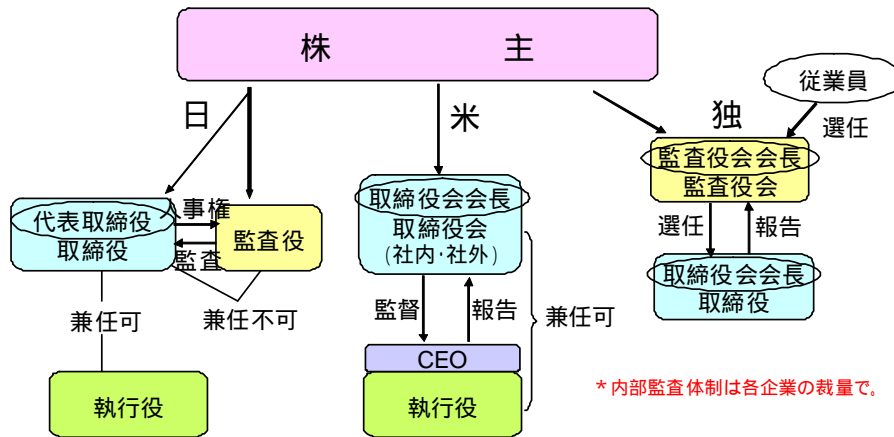
4.2 コーポレート・ガバナンス

以上の論点は、コーポレート・ガバナンスの国際比較をしてみると、さらに鮮明になってくる。図表5. は、日米独のガバナンス構造を比較するため、深尾・森田 [1997] の研究成

²¹ 試しに Google で「解雇の自由」を検索したところ、「もしかして『解雇の事由』?」というメッセージが返ってきた。ことほど左様に、わが国では「解雇の自由」は無いようである。

果を取り入れて私が作図したものである。彼らの研究によれば、会社のガバナンスの仕組みとして、(英)米型、ドイツ型、日本型の3つがそれぞれの特色をもって鼎立している。

図表 5. コーポレート・ガバナンスの3 類型



出典: 私のもともとのアイデアに、深尾光洋・森田康子(1997)『企業ガバナンス構造の国際比較』(日経新聞社)P. 62の指摘を加味

中央にある(英)米型では、会社の所有者である株主が取締役を選任し、会社の運営と執行役以下の従業者を監督させる。執行役のトップである CEO が取締役を兼ねることは許されるが、通常取締役は外部の出身者で占められ、内部昇進という慣行はない。これに対して左側の日本型では、株主は経営の責任を負う取締役と、それを監督する監査役を別々に任命する。取締役が執行役を兼ねることが許されるが、取締役と監査役を兼ねることはできない。また執行役を経て取締役に「昇進」するのが常態であり、代表取締役も取締役に「昇進」したものと理解されている。

ここで、わが国に特徴的なのが監査役である。監査役は株主総会で選任されるのだから、責任を負うのは株主に対してである。したがって仮に株主の利益に反する決定が行なわれるような場合は、社長の「お目付け役」として、是は是、非は非と面と向かって言えることが望まれる。しかし実際は、監査役候補者を含む議案書は社長以下の経営陣が作成するから、社長の推薦がなければ監査役になれないという、これまた「内部昇進」の究極の姿になっている。

他方、右側のドイツ型の特徴は、監査役会という組織が取締役会の上位の機関として位置づけられており、その構成が労使半々であることである(ただし、議長は使用者側から出すことになっており、賛否同数の場合は議長に決定権がある)。

これには同国に特有の「共同決定法」が色濃く影響している。この制度は当初は、労使双方が同数の代表を出す職場協議会を事業所単位に設置して、多数決によって重要事項を決定しなければならない、とされたことに端を発する。その後、同じ仕組みを会社全体に広めたのが、監査役会だと考えることができる。また、職場協議会の設置が必要な企業規模や、監査役会を設置する必要がある企業規模も、時代とともに拡大されてきている。

このドイツ型制度の利点としては、「1) 資本と労働のコンセンサス経営、労働争議の回避

が実現されること、2) 長期的観点から戦略決定がなされること」等が強調される、一方欠点としては、「1) 選出母体の利益代表という色合いが強く、監査役会にセクショナリズムが持ち込まれやすい、特に株主代表から選出される監査役会会長に特別議決権があり、株主寄りの決定がなされやすい、2) 迅速な意思決定や必要なリストラクチャリング・イノベーションが阻害され、ドイツ企業の国際競争力が低下する」等が指摘されている(『通商白書2003』)。

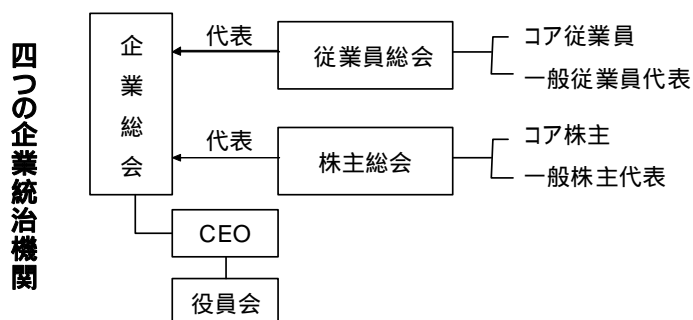
このようなドイツに特有の事情を除けば、アメリカはコモン・ローの国、日本とドイツが制定法の国であることを重視する、前述の LOT 理論が役立つのではないと思われる。アメリカが純粹の株主資本主義で、日本とドイツはステーク・ホルダーとして、監査役(日本)や従業員代表も参加する監査役会(ドイツ)など、株主の直接統制以外の仕組みを持っている。これが、コモン・ローと制定法の差に還元できるとすれば、理解しやすい。

しかし、このように割り切ることにも、問題がある。総じて言えば、日本はやはり資本が第一にありきというのではなく、資本を押しつけるとはいえないけれど、資本といわば同格のような形でステーク・ホルダーが並んでいる、というような形になっている²²。

そこで「人本主義」の始祖である伊丹氏は、その主旨を徹底するには、図表6.のように「株主総会」と並立する「従業員総会」と、両者をまとめる最高意思決定機関としての「企業総会」が必要ではないか、という問題提起をしている²³。この提言は、論点を明確にするためには優れているが、実効性は保証できない。前述のとおり、「両雄並び立たず」で、最終的な意思決定権(residual right)は、どちらか一方にしか与えられないからである²⁴。

図表6. 人本主義企業の機関設計(理念型)

- 企業を構成する2大要素は、カネとヒトであるのに、ガバナンスの仕組みの中にヒトは組み込まれていない、という認識から出発。
- 最高意思決定機関としての「企業総会」と、(コア)従業員の意見と代表する機関としての「従業員総会」、アメリカの「監査委員会」と「指名委員会」を兼ねた「経営者監査委員会」等を提案



(出典)伊丹敬之[2000]『日本型コーポレートガバナンス』日経

²² 以上の他、日本の場合にはメイン・バンク制と株式の持ち合いが、ガバナンス機能を代行してきた、との指摘もある。過去においては指摘は当たっているが、21世紀に入ってからはその構造は激変しているため、ここでは省略した。

²³ 実はこの提案の一部は形を変えて、既にわが国企業で実施済みと考えられるものもある。例えば、従業員持ち株会社は「意見を言う(voice)」場ではないが、「入退会自由(exit)」の仕組みとして、従業員の意向を反映する機能も持っている。なお、voiceとexitの概念は、Hirschman [1970]による。

²⁴ この点を抉りだしたのは、経済学における「契約理論」の功績である。

4.3 内部昇進と監査役制度

人本主義が原理主義的に守られている状態では、新卒採用で長期に勤務するのが最大の企業貢献になるので、中途採用は歓迎されない。しかも新卒で入ってずっと長い人が、内部で昇進に次ぐ昇進を重ねて、そのまま取締役になることが圧倒的に多い。そうすると他から血が入らないので、企業文化はしっかりと根付いており、しかも取締役になるような人は、その企業文化を最も優れて体現している人である、ということになる。

もし仮にここで、先ほどの組織性逸脱傾向が見られるとしても、役員がチェックを掛けるのは期待薄だ、ということにならざるを得ない。役員がチェックを掛けるのが無理だとすると、日本には監査役という独特の制度があるではないか、という論議が出てくる。監査役は閑散役と言われたり、あまり栄進とはいえないが、少なくとも役員に準じる立場に上り詰めるという意味では昇進である²⁵が、やはり社長に推挙されたという面もあって、社長をチェックするのは難しい。

しかし最近になって、色々な変化が生じてきたのも確かである。もともとアメリカ等の取締役会は、会社の執行役を監督する機関であるから、外部取締役が圧倒的に多い。日本では仮に外部取締役がいたとしても、取引関係が強い会社の役員であったり、場合によっては資本関係がある会社の役員であったりすることが多かった。しかし外部の血を入れるとすると、外部監査役の方が機能するのではないかという考え方が取られて、現在では上場大企業では外部監査役は半分以上いなければならない、という法制度になった。

こういう人達の中に例えば、資格を持っている弁護士や公認会計士が入っていると、この方たちは仮に会社と意見が対立して辞任したとしても、あるいは気まずい関係になったとしても、失業するわけではないのである種の強みを持っている。内部昇進の監査役だと、社長と対立して次に再任されなければ、多分子会社にも紹介してもらえないだろうから、失業の危機に会う。そういう人に比べれば、外部監査役の方が強みを持っている、ということはあるかも知れない。

事実例えば、社外監査役が活躍したケースとして、本学のセキュアシステム研究所の特別研究員をしている大森義夫氏がいる。彼は、荏原製作所の監査役になったところ不祥事が発生した。そこで「当該事案に関して監査役だけには情報を開示せよ」と請求したのに対して拒否されたことから、当該決算については監査役として承認しないという事態になった。一部では「もの言う監査役」ということが言われるようになって²⁶。

大森氏は、この件で有名になってしまったが、ライブドア事件があった後の監査役も勤め、そうした不祥事の際に、監査役の意見書をどのように書けば良いかについては、彼が書いたものがその後のある種のデフォルトになっているという。彼に限らず大物の監査役が次々と登場するようになると、日本の社会もちょっとは変わるだろうなという感じがする。また現に優良企業の間では、会社の役員(特に社長などを辞めた方)を「是非わが社の監査役(あるいは社外取締役)に」という風に、ハンティングする時代になっている。

²⁵ もっとも、ある部署の長が株主総会で監査役候補に挙げられると、その部が大祝賀会をやるかという、あまりそういうこともないようである。要は監査役というのは、「おめでとうございます」と言っても怒られることはないが、本人がおめでたいとは思っていない、という微妙な立場になっている。

²⁶ <http://www.asahi.com/business/topics/economy/OSK200904190063.html>

4.4 トップ・ダウン対ボトム・アップ

しかし日本的企業の特徴として最も顕著なのは、こうした組織論ではなく、むしろ意思決定のプロセスではないかと思われる。それはトップ・ダウン対ボトム・アップということで、一般的に表現可能である。私のビジネス経験²⁷を元に、深掘りしてみよう。

トップ・ダウンの代表例は、アメリカの会社である。私もアメリカ企業で、経営の一翼を担っていた経験からすると、取締役会というのは真の意思決定機関で、ここで短時間のうちに意思決定することが、いかに大変なことが良く分かった。また、電話会議の活用も含め、取締役会が如何に効率的に行なわれているかに感心した²⁸。

それに対して日本の企業の特徴は、やはりボトム・アップで物事を決めるということである。これには二つの仕組みが付随している。一つはまずほとんど全員参加型の「みんなの知恵」を生かすシステムであり、TQC 運動であるとか提案制度であるとか、工員の一人一人にいたるまでが経営改善を考える、という風土になって現れている。これは日本企業の強さの秘密でもある、という風に言われてきた。

もう一点は、中間管理層の充実である。アメリカでは、何事もトップ・ダウンで決めるので短時間で済むが、決めるための資料が不足していることに、いつも悩まされた。私が純粹アメリカ会社の取締役であったからかもしれないが、日本であれば参謀役がいて、こういうことを調べてくれという大変たくさんの良い資料を集めてくれる。しかしアメリカの意思決定は、そうしたサポートなしでやっているような感じがする。つまり中間管理職に良い人はいない。そんなに良い人なら、すぐに取締役にしまったりする。

この二つのことが、日本企業の強さを支えてきたのだろうが、どうやらそれぞれに立ち行かなくなっている。まず皆の知恵を生かすのがよくて、トップはお神輿に乗っていれば良いという風潮は、右肩上がりの成長を続けている時には非常に良い仕組みであった。うちの社長はいい人だ。ニコニコと笑ってぼんと肩を叩くだけで、後は宴会の費用を持ってくれたりして、何も言わない。

確かに苦情を言われたり、要改善点を指摘されるのは嫌なことなので、自発性に任せて上手くいけばそれに越したことはない。しかし安定成長またはマイナス成長という時代には、大胆な構造改革をしなければならない。そうすると、いかにその後批判を受けようとも、いわば「小泉元首相的」にやるしかないのだから、日本のトップの何割がこういうことができるかという、甚だ心許ない。

この点はセキュリティを考える上でも、非常に大事なことはないかと思われる。なぜなら、セキュリティ施策は日常的な不断的努力の積み上げである。情報セキュリティという分野を一番最初にやったのは、次章で述べる JIS だとか ISO だとかやっている人達で、そういう人達が規格を作って「これを守ればなんとかなる」ということでやってきた。その人達の努力は多とするけれども、そのやり方だけでは経営陣になかなか届かない。

このように地道に努力はするがアピールの仕方が弱い人達と、大所高所の判断とセキュリティとの結びつきをあまり意識していない人達に分断されている現状は、やはりまずいのではないだろうか。これでは「係長セキュリティ」のままで終わってしまう。日本企業の今まで

²⁷ ニューヨーク州法人の社長、デラウェア法人の取締役、日本のベンチャー3社の監査役か顧問、といったところが、主たる源泉である。

²⁸ 私の場合はさらに英語の会話力という難点に加わっていたが、それが無いとしてもトップ・ダウンの意思決定は大変に難しいと思われる。

のセキュリティ対策というのは、こういうのは知っている人にやってもらわないと分からないということの良いことに、上司はほとんど手を入れていないのではないかと。トップはわからないということで、ほとんどお神輿だということで、果たして、セキュリティが守られるのか。

昔の、例えばウェブページが改ざんされないようにするとか、ウィルスをもたらさないようにするとか、そうした牧歌的なセキュリティの時代ではそれでよかったかもしれない。しかし今は、内部統制とかコンプライアンスだとか、そういうことも含めてセキュリティだと言い出している時代である。これはまさに経営陣が、自分の課題として取り組むべき問題だし、経営者にも経営学者にも、しかと認識していただく必要があると思う。そのためにも、やはりトップ・ダウンという要素を入れざるを得ない。

第2の特色である、中間管理者の数が多く、層も厚いということについても、見直しが必要である。確かに内部昇進を前提にするのであれば、油の載りきった30代40代のパフォーマンスの良い人に、将来の取締役候補として目一杯働いてもらうというのは、企業としても、個人のパフォーマンスの面でも良いことかと思われる。

しかしその人達が、例えば部長という職位に満足して、ずっと働いてくれるだろうか。取締役の数が昔に比べて少なくなっていて、せいぜい執行役になれるかどうかという時代に、今までどおり滅私奉公の企業戦士になってくれるかという点、そこは分からない。「それじゃあ報酬で報いるか」ということになるが、この点が今、日本企業のネックになっている。

先述のとおり、アメリカ企業でさえ成果主義の5段階評価のときに、5だとか1だとか、2シグマか3シグマの外の点数というのはつけにくいという状況がある。それは日本企業ではもっと顕著であり、大抜擢はなかなかできない。昔なら高卒が優秀でも、大卒に対してある種のエリート主義で大抜擢も貰ったが、今やほとんど大卒という中で、どうやって差をつけるのかということやはりなかなかつけにくい。

4.5 平等主義とスーパー・スター

これからの企業を考える場合、才能は多分「正規分布」だということを、しかと押えておく必要がある。つまり、非凡な才能を持った人も、きわめて才能に乏しい人もごくわずか、それ以外の人々が中央に山を作り、ずっとなだらかに分布している。それは才能をどんな風に分けるかにもよるが、例えばイチローのことだと思えば分かりやすい。たくさんの方が大リーグに行ったが、不幸にして恵まれないで帰ってきた人が一杯出てきている。つまり超エリート・プレーヤーというのは、そんなに多くない。

これは、ソフトウェア産業に今一番顕著に出ている。ソフトウェアは、多分超優秀なプログラマーが1人で百稼いで、残りの99人が全員で百稼いで、その会社の売上が二百という、そんな構図になっているのではないかと。そうすると百稼ぐ人には100あげないにしても70あげたり60あげたりしなければならないという時代が、近づくのではないかと。

つまり今後は、大変少数の大成功者と、大勢のほどほどの人という差異が出てくるのが、容認できるかどうかということになる。もしこれが容認できないとすれば、多分、人的セキュリティホールが(例えば不遇な社員が営業秘密を売る、といった例が)生ずる恐れがあると思われる²⁹。

²⁹ わが国では現在、社長の給料が新入社員の初任給の何倍までなら許容できるか、という議論が盛んである。金融庁が1億円以上の所得のある役員を開示するよう求め、予想外に多くの役員が「1億円プレーヤー」であることが判明したからである。しかし、NASDAQ 上場会社の役員であった経験からすれば、上場企業の役員報酬は、ストック・オプションも含め全て

なお、世間で成功したビジネスマンがよく使う言葉に「ほうれんそう」というのがある。ほう(報告)・れん(連絡)までは必要なことだと思うが、アメリカでは「そう(相談)」というのはいくらも聞いたことがない。もちろん上司が何を考えているかを探るという意味で、何気ない会話の中で言葉を見つけているのかも知れない。ところが日本の「そう」というのは文字通り相談であって、「ご相談に伺いました」とか「ご指導いただきたいと思ひまして、私迷っていて道が見つからないのです」などというのが「ウイ奴だ」ということになっている。

ゴマすりという軽蔑の対象かもしれないが、日本のビジネスマンは自然にゴマを搦っている。合議制や稟議制が主体だから、合意形成のときに異論を出す者は、あまり望まれていない。そうすると根回しとか称して、上司にある boundary, 上司がここから先に行くとは本気になって怒るとか、ここまでしかしなかつたら馬鹿にされるとか、そういうところを探り合っているのだと思う。それが「相談」になっている。

アメリカでは根回しはなく、むしろ異論を出して異論で説得できれば、そちらの方が褒められるので、「相談」は日本の特色ではないかと思われる。これが長続きするものであるかどうか、あるいは長続きすればいいのか、というのがよく分からない。

多分この手のことをやり続けると、先に日本の中間管理層は優秀だと言ったが、それも怪しくなってくる。中間管理者が部下から相談を受けると、決断はしないで上司に相談する。その上司はまた、決断をしないで社長に相談する、というようなことをやり続けると、無責任体制になってしまうのではないか。ベルリンの壁が崩壊した 1989 年以降の約 20 年ほどで総理大臣が 14 人も交代したという事実が、この悲劇を象徴しているように思えてならない。

4.6 再び監査について

以上に述べたところを総合して、私は「監査に対する理解が日本社会ではきわめて希薄ではないか」という懸念を持っている。私自身も複数社の監査役を経験し、監査役の悲哀も十分わかっているつもりで、経営者に少し頭を変えていただきたいと思う。

例えば私のように、対話型労働組合と長いことやってきた身からしても、労働組合があった方が無いか無い方が無いかといえば、無い方が気楽であることは確かである。しかしどんな優秀な人でも見落とししたり、自分の利益のために歪んだ眼鏡を掛けていたりすることは、大いにあり得ることである³⁰。

私はその意味で、対話型の労働組合は、自分を映す鏡であるという風に思っていた。私が知らなかったことを気づかせてくれたり、私が知らずに右の方に偏っていたのを直してくれたり、そういうことを何度も経験したことがある。従って私は、最もタフな経営者で労働組合の敵であったにもかかわらず、現在でも NTT の労働組合からお呼びがかかるという、非常に恵まれた境遇にある。

同じことが、監査役にも言える。あるいは労働組合よりも、もっと身近な存在として、監査役を考えることはできないか。それは言ってみれば「かかりつけのお医者さん」のようなものである。私の病歴を良く知っている、そして今腫瘍があるけれどそれはまだ良質だとか、いやいやそろそろ悪性になりかけているとか、今切った方が良いのではないかとか、そういうことを言ってくれる人だと考えれば、こんなに役立つ仕組みはない。

開示するのが、デフォルト規制であるべきだろう。

³⁰ タイガー・ウッズのような天才的ゴルファーでも、スイングを矯正するためにレッスン・プロを雇っているという事実は、「自分の欠点を自分で見つけ出すことは、ほとんど不可能に近い」ことを暗示しているように思われる。

ましてやそれが世界に例を見ない仕組みであるとすれば、これを活用しない手はない。しかし、どうやらそのように考える人は極めて少ない、というのが実情であるようだ。

5 標準化と日本的経営

継続反復的な業務を、誰がやっても同じようにでき、同じような品質を維持するために「標準化」というアイデアは、戦後品質管理の一環としてアメリカから輸入された考え方であろう。ところが、日本はデミング等に学んだことを自己流に改変して、製造業においては世界一の品質を実現した。1970年代の不況でこれを反省したアメリカは、製造業の復権を目指すのは当然として、さらに当時勃興しつつあったIT産業やサービス業においても達成すべく、BPR(Business Process Re-engineering)による業務の見直しや、そのためのソフトでの世界の覇権を目指している。

工学のアメリカに対して、理学で優位にあるイギリスも、工業規格を定めることが自国産業を優位に導くとの経験に立って、モノの規格から始まったISO(International Standardization Organization)の場を、サービス品質や経営品質をもカバーするフォーラムへと、政策的に転換する動きを主導している。イギリスの規格であるBS(British Standard)がそのままISO規格に採用されるケースが、多数見られるようになった。

対するわが国では、いわばグローバル・スタンダードになったこうした規格に、いち早くcomplyすることには熱心だが、その国際戦略的側面については無関心である。また、技術者はISOを良く知っているが、非理系の経営者(それが半数以上を占める)の間では、こうした手順の意味を知っている人がごく少ない、という分断現象が起きている。

本章では、こうした国際標準化の動きと日本的経営の視点から、情報セキュリティのあり方を考える。

5.1 ISO等の標準化

セキュリティの分野では、製品のセキュリティを定めたコモン・クライテリア(ISO15408)があり、これを追いかける形でISO17799ができ、それが27000シリーズになった。このような「技術標準」は、経営の中でどのように捉えられているのだろうか。さらには「日本的経営」の特色と両立しうるものなのか、あるいは、調整が必要となることになるのか。ここでは、そのような議論をしてみたい。

もともとISOは、製品の物理的規格や電気的規格を定めていたが、だんだんと、品質、プロセス、経営のやり方などに対象が広がっていった。特にISO9000シリーズで、品質問題一般に取り組んだころから、その傾向が顕著になった。ISO14000シリーズにおいては、環境問題と経営とをどのように扱うべきなのかという点に及び、さらにISO27000シリーズにおいてセキュリティの扱い方を決めた。これは単に、物の大きさや重量といった物理的特性を決めるのと違って、経営の根幹となる点をどのように扱ったら良いかという点にも、「標準化」の動きが及んだことを意味する。

ところで、かつては標準化といえば、国を代表する者が構成する公的標準化機関があり、そこに専門家が定期的に集まって、国際標準を決めるという方法(de jure standard)が一般的であった。ところが技術が発展して、変化の速度が早くなると、このようなゆったりし

た速度では対応できなくなる。特にソフト開発がからむ分野では、「一人勝ち現象」が一般的になるので、first mover にならないと「負け組み」になってしまう。

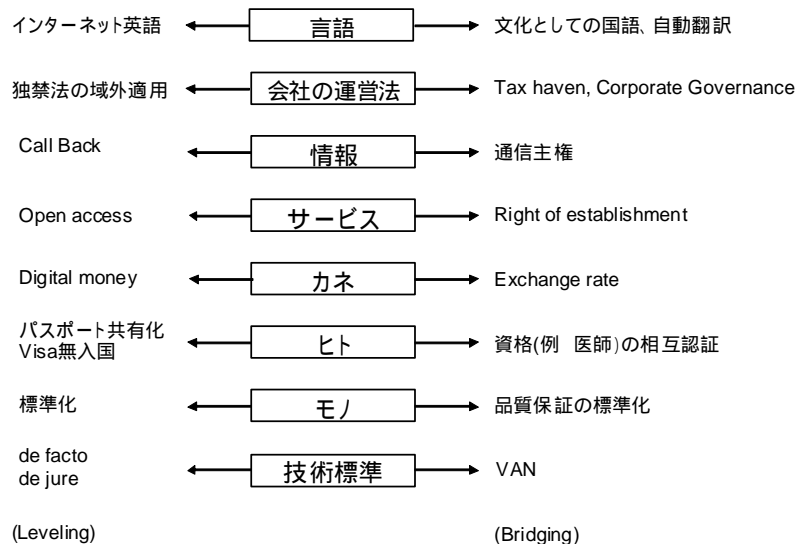
そこで、力のある企業が自社製品を「これが標準だ」と言って売り出し、初期に一定の市場を取ってしまうと、それが「事実上の標準」(de facto standard)になる、といった形態が一般化してきた。また、その中間にあって、予め標準を決めることを目的に任意団体を組織して、民間ベースで標準化活動をリードする形(フォーラム方式)も誕生している(山田[1999])。

また、ソフトウェアが絡むのであれば、ハードの場合のように厳密な「標準合わせ」をしなくても、「互換性」さえ保たれば相互接続や方式転換をすることもできる。ハードの場合を「レベル合わせ」(leveling)とすれば、ソフトは「橋かけ」(bridging)ということもできる。そして、これら広義の標準化にはレイヤがあることも分かってきた。

もちろん、標準化の原点は狭義の技術標準であるが、例えば「インターネットにおいては英語が標準言語になりつつある」という文章を、標準化問題とは別だという意味もないだろう。むしろ、こうした幅広い「標準」という概念に潜む共通項を摘出して、理解を深めた方が得策ではなかろうか。なぜなら、今や標準化は技術者だけの問題ではなく、標準化に先駆けた方が経済的にも優位に立てるし、標準化を無視すると「ガラパゴス化」、つまり世界の孤児になりかねないからである。

つまり、かつては「技術標準」という語が適切であったが、今や「グローバル・スタンダード」と呼ばねばならぬほど、その範囲と深さが進化してしまったのである。このような事態をより良く理解するためには、図表7. によって頭を整理してみるのが良いだろう。

図表7. グローバル・スタンダードの位相



出典:林紘一郎[1998]『ネットワークング 情報社会の経済学』NTT出版

結論的な諸点をまとめれば次のようになる(林[1998]の pp.125-126)。

- (1) 「グローバル・スタンダード」は複数ある。
- (2) それをまとめてグローバルに機能させる方法も、「平準化またはレベル合わせ」

(leveling) と「橋かけ」(bridging)の両面がある。

- (3) グローバル・スタンダードにはレイヤがある。ISO の 7 層モデルにも比すべきレイヤには、「技術標準」というハードに近いものから「言語」というソフト(文化)に近いものまで、何階層もある。
- (4) この各レイヤのうち、レベリングとブリッジングの両面が競い合っている代表例は、技術標準であろう。前者の例が標準化で、後者の代表は VAN である。そしてこの分類では、「事実上の標準」も「公的な標準」も前者のなかに包摂されてしまう。世間では両者の違いを対比的に強調する傾向があるが、それがすべてではないことを、この図は思い出させてくれる。
- (5) 伝統的な「モノ」の貿易は、規格や度量衡の統一などレベリングの知恵を多数生み出した。しかし品質保証については、世界統一の保証機関を設立するよりも、品質保証の手続きを標準化し、具体的な品質そのものはローカルに処理せざるを得ないので、ISO9000 や ISO14000 シリーズのようなブリッジングの手段を生み出した。
- (6) 今後最もグローバル・スタンダードが要請されるのが、金融の分野である。取引があつという間に国境を越えてしまうことが予測されるこの分野では、電子マネーに代表されるようなレベリングによって、グローバルな流通を確保することが期待される。しかし同時に現行の「為替交換」というブリッジング手段も、失くってしまうことは無いだろう。
- (7) 「サービス」貿易においも、open access というレベリング手段と、「設立権(right of establishment)」というブリッジング手段の両方が導入された。
- (8) 「情報」の国際間交流については、片や在来の「通信主権」を残置し、たとえば国際通話の料金は発信側の国に決定権があることを認めつつ、他方で「call back」のような国境の意味を無くすサービスも事実上の認知を得つつある。
- (9) 「ヒト」の移動が顕著になったグローバル経済では、各国別に付与されている資格(たとえば医師の免許)を他の国でどう扱うか、という問題が生ずる。世界統一の医師試験という考え方もなくはないが、今の所「相互認証」というブリッジングが有効である。
- (10) 現下の日本での最大の問題は、会社の運営方法、あるいはコーポレート・ガバナンスのあり方である。日本的な「法人資本主義」ないしは「会社第一主義」が、グローバルな視点からは受け入れられないことは明確になった。国力の強力なアメリカは、自国流の発想に基づく自国流独占禁止法を、他の国における行為にも適用しよう(域外適用)と試みている。ところが他方で、税金の安い国を求めて、企業が国家の枠組みを超えて移動しつつあり、電子マネーはこの動きを加速させずにはおかない。
- (11) こうした動きの頂点にあると思われるのが、文化と最も強く結びついている言語の問題である。片方でインターネットの中では、英語が事実上の標準となった。ところがもう一方では、フランスのように自国語に誇りを持っている人々を中心に、「多言語文化」を守る動きも活発化している。

5.2 ニューヨークからの発信と日本の対応

私がアメリカに滞在していた 1992 年から 95 年の経験からすると、前節の点を含めて技術と社会の関係については、日米に大変な温度差があるような気がする。

当時、日本側ではマルチメディア・フィーバーがあり、アメリカ側では「情報ハイウェイ」というスローガンが登場した。そして情報ハイウェイとは、結局はインターネットのことであった、というように変化していった。その過程で私は、インターネットや情報ハイウェイは、究極的にはホワイトカラーの生産性向上運動ではないかと思った。そこで私は、雑誌などを通じて「この本質を忘れないよう」日本側に警鐘を鳴らしたのだが、日本側の反応は、ほとんど皆無であった。

私が、民営化前後に電電公社総裁から初代 NTT 社長になった、真藤さんから頻りに言われていたのは、次のようなことであった。「ブルーカラーの生産性の向上で、日本は世界に誇るべきものを持っている。他国から教わった品質管理の手法を徹底的に日本化し、それを製造業に当てはめ自分の物にしている。これに対して、悪いのは白いシャツを着て、本社の冷暖房完備の部屋でふんぞり返っている連中だ。工場では、1 ミリや 1 円といった節約をしているときに、本社の方では何億円の浪費をしている」という批判であった。

私がアメリカに行って、インターネットが商用化されるプロセスを見てみると、ブルーカラーにも影響があるが、オフィスの働き方を大幅に変えるものではないか、という気がした。当時、経営学の方では、ビジネス・プロセス・リエンジニアリング(BPR)が喧伝されていた。そのことを、「情報ハイウェイとホワイトカラーの生産性」というテーマで朝日新聞に書いたが、ほとんど無視された。その原因として、おそらくハイテクに対する親近感の違いが、まずあると思われる³¹。

このことから分かることは、アメリカのエグゼクティブは、「自分で自分のことを管理している」ということである。この管理の過程で、どのようにすれば生産性が向上するのか、自分の時間をどのように有効に使うべきなのか、そして部下のホワイトカラーの従業員に、どのような仕事の割り振りをすれば生産性が上がるのかを常に考えている、ということが分かった。

日本に帰り NTT を辞めた後、「留守録普及会」の会長となり、このような事を宣伝したが、さっぱり駄目だった。それはどうしてかというと、90 年代半ば過ぎの「失われた 10 年」で様々なリストラなどをやったものの、日本のエグゼクティブは、三種の神器である「個室」「秘書」「車」を譲れない物であると思っていたということだろう。私に言わせれば、そんな物にこだわるのは、そもそもエグゼクティブの資格は無い、ということになる。土日であっても、自分で留守録を聴いて処理しないと駄目ではないか、このように思っていたが、なかなかそうはならなかった。

実は ISO のように技術標準を定めている人達の方が、経営者の関与が不可欠であることを十分認識している。前出したセキュリティ関連の要求事項には、すべて「経営者のコミットメント」が記述されているが、品質管理を標準化するさきがけとなった ISO9001 における該当事項を例示すれば、図表 8. のとおりである。

³¹ その当時、アメリカのエグゼクティブの間では、すでに「ボイスメール(留守録)」がかなり普及していた。飛行機の中で電話をかける人を見ていると、ほとんどが声を発していない。つまり、自分宛のボイスメールを聴いて、転送や消去をしていた。私があるアメリカのエグゼクティブに電話をしたところ、秘書が出てきて「ボスは不在」とのことだったが、その後が驚きだった。「あなたは、私にメモをとってほしいか、ボイスメールに吹き込むのがいいのか選択して下さい」と言われたからである。

図表8. 経営者のコミットメント

ISO9001

5.1 経営者のコミットメント

- a) 法令・規制要求事項を満たすことは当然のこととして、顧客要求事項を満たすことの重要性を組織内に周知する。
- b) 品質方針を設定する。
- c) 品質目標が設定されることを確実にする。
- d) マネジメントレビューを実施する。
- e) 資源が使用できることを確実にする。

日本のエグゼクティブは、システムや技術が絡むと、それは自分の守備範囲ではなく部下が宜しくやるものだ、ということにしたがる。せいぜい、チーフ・インフォメーション・オフィサー (CIO = Chief Information Officer) やチーフ・テクノロジー・オフィサー (CTO = Chief Technology Officer) がやることで、チーフ・エグゼクティブ・オフィサー (CEO = Chief Executive Officer) がやることではない、という発想があるのではないか。

また、中間管理者が立派であるから、秘書以外のサポート体制が充実している。私も学者になってみて初めて、自分がいかに恵まれていたのかが分かった。そこで、ITを活用すると、ホワイトカラーの働き方はどのようになるのか。そして生産性の中でも「エグゼクティブの生産性」が一番大切な問題である、ということに気が付いた次第である。

この点については、言いたいことが多数あるが、既に発表済みの諸論稿に譲ることしよう(林 [1994][1995][1998]など参照)。

5.3 技術標準を超える

技術標準のメリットとデメリットについては、アメリカの方がよく考えている。アメリカ発のグローバル・スタンダードである、「マニュアル的なもの」があり、「この方法が良いですよ」「この方法を利用した場合のベスト・プラクティスはこのようになっていますよ」という物はあった方が良く、ということはある程度言える。

しかし、私は技術標準については辛い経験があって、あまり信頼し過ぎるのはいかなものかという気がする。というのも、私は事務系であるにもかかわらず、NTT データの前身である「データ通信本部」という部署に4年間在職した。前半の2年は営業担当だったが、事務系のSEがいらないということになり、何も知らない私が後半の2年間はシステムの方へ転籍した。そして、今は無き「販売在庫管理サービス」を担当した。

その時、なるべくシステム設計を標準化して、同じタイプのユーザーは同じプログラムで対応し、生産性を向上させられないかと考えた。そのために NTT には、「標準実施方法」という手段があることを教えてもらった。「標準実施方法」のほか、工事が伴うものについては「工法」というものがあり、それらのドキュメントが棚に並んでいた。それは、ISMS(Information Security Management System)のように完全に体系化されていて、A から Z まで揃っていた。

私は、それを基にシステム設計の標準実施方法を書くことになったが、何も知らないもの

だから、「標準実施方法の書き方」という標準実施方法があることに気づかなかった。完全に事務系らしい方法で書いてしまったところ、これを監督する「技術局仕様課」という部署から、草案が真っ赤になって突き返され、その上に「Z の何番を先ず読みなさい」と書かれていた³²。

このような恨み辛み(?)があり、標準化というのはプラスとマイナスがあるということを強く感ずる。マニュアルのメリットの面から言えば、手順を標準(マニュアル)化し、それを守るように管理すれば、結果は自ずとついてくるという安心感が出る。これはこれで、ある程度までは当たっている。しかしその宿命として、ヒューマン・エラーや組織的逸脱行動を取り込みにくいというデメリットがあり、盲信は危険である。言い換えれば ISMS に代表される経営管理手法の本質(有効性と限界)は何か、を見極める必要があるということである。

また標準化をすれば、主流の所を取って、例外を切り捨てるということになるが、逆に例外が意外に重要である場合がある。例外をなるべく少なくしようとすると、様々な方法を書くことになり、これは「ベスト・プラクティス集」であるかもしれないが、「これが標準だ」と決めたことにはならないという面がある。このように、「あちらを立てれば、こちらが立たず」ということになる。

また、一本道を決めるわけだから、業態や企業規模によって対処策が多様にならざるを得ないのを、ある種一律に決めるということになる。つまり、カスタマイズが無いという前提で考えているということになる。ISMS については例えば、中小企業向けができないかと考えている方もいるが、あれだけ大量なものを一つ一つチェックしていくのは非常に困難である。

しかし、これらの欠点は、どのような仕事をしてでも発生する問題なので、決定的な欠陥とは言えないと思う。むしろ標準化、とくにプロセスの標準化の問題としては、次の二つの方が、大事ではないかと考える。

一つは、PDCA のモデルを使うという点である。これは、プロセスを制御して一回転するとまた次の段階に移るといって、永遠に繋がっているということである。そのように理解するのが正しいと思うが、これを裏返すと「完成版」というのはなかなか無いということになる。打ち止めということが無いわけで、あるとすればリスクとの関係で「この程度であれば受容してしまふ」ということが分かればそれで良い。しかし、その関数がなかなか分からないことが多いから、いきおい「たくさん書いてあると、たくさんやる」ということになってしまう。

二つ目に問題だと思ふのは、ISMS 等の本質は単なる「参照モデル」だと思ふが、「第三者評価認証制度」とセットとなって動き出すと、「経典」のようになってくるという点である。そして、経典になったとたんに手段と目的が逆転してしまい、「書いてあるからやらなければならない」という風潮になりかねないということがある³³。どのような分野であれ、経典に権威があればあるほど、このような逆転現象が生じがちである。

このような理解を元に技術標準を使うのであれば、日本では標準化の意義の理解が欠けていることから、むしろ現時点では ISMS 等を推奨しておいても良いという感じはしなくもない。しかし、それがセキュリティの狭義の手續論であれば良いが、セキュリティの概念が

³² 付随的なことかもしれないが、「基準」と「標準」は、手続き的な問題のようであり、標準化の限界を示す象徴のような気もする。「基準」は全国一律に守らなければならないもので、対する「標準」は自由裁量が認められるものである。作成者がうっかり「基準」と書いてしまって、後で地方組織から「これが何故基準なのか」と反撃を受けることがあった。ISO の場でも、shall と should を、基準と標準に近い語感で使い分けている。

³³ これは一般に「道具の法則」と呼ばれているものと同じである。「3 歳児にかなづちを与えると、彼は叩く対象を探し始める」というのが、その簡明な説明である。

だんだんと拡大解釈され、内部統制・コンプライアンスなどが、すべてセキュリティという感じになって、しかもそれが似たような方法で手順化されていくということになると、問題が多いと言わざるを得ない。

例えば、内部統制でいくと、「文書化」「見える化」をしなければならない、と言われる。また、「見える化3点セット」³⁴のようなことも言われ、それ独自としては非常に有効な手段であっても、ここでも手段と目的が逆転しがちである。また何でも「見える化」しなければならないとすると、逆に「見える化」することで安心してしまう。

本当は企業のトップが見て、「そこで打ち止め」ということを判断する必要がある。そうでないと、下の方へ行けば行くほど、係長が良かれと思ってやるセキュリティの施策「係長セキュリティ」が、それぞれごとに沢山出てきてしまう。そして、それらはすべて「良かれ」と思ってやっていることなので、「それは、やりすぎだ」と言うことが非常に難しいことになる。よって、だんだんと手順が目的となり、手順が肥大化し、それがどこまで多くなったのか分からない、ということになってしまう。

この点に関して、ISOでの標準化経験が長い飯塚 [2005] の指摘は貴重である。同氏は仲間と共同で『超ISO企業実践シリーズ』という普及書を企画し、その第1巻で次のように述べている。

「本書は、このシリーズの他の本に比較して“難しい”と思う。理屈っぽいとの批判は覚悟している。読者にある程度の抽象化能力、一般化能力を期待している。いわゆる単純明快な親切な本で、理屈はともかく明日から何をすれば良いかすぐ分かる本というわけにはいかない。ISO9000という時流に対して、その正体を見極め、品質管理における位置づけを真正面から論じ、その上でISO9000を経営ツールとして戦略的に活用しようとする方々に対し、思考の基礎を与えようとするものである。」(まえがき)。

そして「ISO9000を超える」という意味については、「私見では、以下の3つの意味があるように思える。」として、ISO9000の有効活用、ISO9001モデルからのステップ・アップ、競争優位のためのQMS(Quality Management System)の構築、の3つを挙げた上で、次のように述べる。

「 においては、組織が適用するQMSモデルそのものをISO9001の範囲に限定せず、積極的に上を目指し広げようとするものである。

においては、ISO9001より包括的なQMSモデルを参考にして、組織にとって有用と考えられることを実施していくことである。

においては、組織が対象にしているビジネスドメインにおける競争優位要因を明確にして、この能力を具現化するようなQMS構築をもくろむということである。」(p.12)。

結局のところ、飯塚氏の言わんとする「超える」とは、「道具の法則を超越する」ということに他ならない。ISOの権威者がこのような標語を掲げること自体が、「道具の法則」がいかに根強いものであるか、を暗示しているように思えてならない。

³⁴ 業務記述書、業務フロー、リスク・コントロール・マトリクスの3つの手段を指すのが一般的である。ただし、財務報告の信頼性確保の面からは、経営計画の作成、月次決算の実施、資金繰り表の作成を指す場合もある。

5.4 標準化と「経営判断の原則」

標準化や科学的管理法に対して、経営者はどのような心構えでやったらよいのか。経営者の責任が問われるときの会社法上のメルクマールは、「善良なる管理者の注意義務」というものである。そして、この注意義務を果たしたかどうかの判断基準の一つとして、「経営判断の原則」というものがある。

「右へ行くのか、左へ行くのか」という決断を迫られたとき、右の方に「違法性」があるのに右に行くというのは当然に駄目である。しかし、両方とも「適法」であるときに、右が良いのか左が良いのかを、事後的に第三者が決めるのはおかしい。これこそ、経営者としての「リスク・テーク」の原点で、両方とも適法であることを検討し、利害得失を知った上で「右だ」と言ったのなら、その限りにおいては経営者の判断を尊重してあげましようというのが「経営判断の原則」になる。この経営判断の範囲に入るとすれば、「善良なる管理者の注意義務」を果たしているということになる。

「経営判断の原則」にあてはまるような事態を考えると、そこに「標準」が働くとは思えない。「経営判断の原則」という領域に、標準マニュアルがあって、そのとおりにやれば良いということになれば、経営者は要らないということになる。そうすると、経営者がギリギリのリスクテークを判断する分野は標準化ができないし、また標準化すべきでもない、ということになる。

しかし、こちらを強調すると、先程の日本的経営者の像となってきた、「要するに、経験とカンだよ」という人がトップに立ったときに、これを論理的に説得することが不可能になってしまう。特に、日本の経営者は内部昇進なので、昔の営業部長が今の社長かもしれない。この場合、営業の案件は、ほとんどそのまま通るということが起きてしまう。「経験とカン」しかないとすれば、第三者が口を出すことができないからである。取締役購買部長が「これはおかしい」と言ったときに、その異議が通るのかというと、日本の会社では通り難いのではないだろうか。

ところで、標準ができるのは技術的な分野が多いから、文系的な分野、つまり、非技術の分野では標準などは無いのか、というと実はそうではない。「会計原則」を考えればすぐに分かるとおり、これが技術系の分野という人はいないと思うし、いかなるトップといえども、国際会計原則から外れたことをすることはできない。そのようなことをすれば、公認会計士などから非難されることになる。

そうすると、社長は会計原則を守ることを「当然だ」と考えるにもかかわらず、情報セキュリティの標準があったときに「そんなものは知らない」というアンバランスが、どこから生じているのかを検討する必要がある。私は、色々な経営者にこれを問うてみる必要があると考える。経営の核心というのはやはり「経営判断の原則」にあるのだから、最後は自分で決断をするしかない。ISMS が嫌いな人も、ISMS を読んだことがないよりは読んだ方が良いというのは、その通りだと思う。

ところで会計原則は、ISMS よりもっと遵守しなければならないもので、これには例外は無いのかという疑問が出てくる。私は無いと思っていたところ、稲盛 [1998] に出てきたのでびっくりした。事例は2つあるが、分かりやすい耐用年数の問題を紹介しよう。

「法定耐用年数」は、耐用年数表に書いてあり、これに従わないと税務当局が税務申告を認めてくれない。ところが、税法とは違った「管理会計」となると、社内のルールに従って

別のやり方でやっても良いことになる。しかし、差をつけると手間が大変だし、ミスの基にもなるので、通常の会社では、差をつけるということはやっていない³⁵。

ところが、稲盛氏は違った。例えば、A という設備は耐用年数が 15 年、B は 7 年だとする。そして京セラでは、A という機械を非常によく使用するが、B という機械はほどほどにし、使わないとする。この場合、稲盛流だと、A という機械も 7 年で償却することになってしまう。「A は、非常によく使用する自分の社の生命線のような設備である。よって、7 年ぐらいで摩耗するかもしれないし、物理的に取り替える必要がある」というのが社長の論理だった。

しかし財務部長は、当初頑なに反対をしたそうである。「残りの 8 年分は有税償却することになってしまう。そのような経営上不利なことを何故するのか」と主張した。しかし、社長は「やれ」と言った。そうすると何が起きたかという、職場の人は「これは 7 年で取り替えるのだが、財務部では 15 年の計算で減価償却している」と言われる。だから、普通の儲けでは減価償却の不足分が出てこないことなる。よって、もっと儲けるようにはどうしたらよいか、あるいは、製品コストを下げるにはどうしたらよいかということ、その機械を使用している人が考えることになる。そうすると、だんだんと 7 年で元を取れるようになってしまう、ということである。

まとめとして、次のようなことが言えると思う。まず、技術的なことであれ会計的なことであれ、あるいは営業もそうかもしれないが、標準的な手順として「プロセスはこのように管理をしたら良い」というノウハウというものが、色々な分野に在るだろう。このノウハウが「見える化」され、あるいは、「文書化」されるのであれば、それは知っておいた方が得ということになる。

しかし、そこで留まっていたのでは、経営者ではない。経営者は、それを知った上で、場合によってはそれを曲げてでも「こうやるのが正しい」ということを見つける人だろう。つまり、そこに「経営判断」があるということになる。一見、「こんなものは経営判断ではない」と思うところにも、「経営判断」は存在するということになりそうである。

6 日本的経営と情報セキュリティ

最終章では、マクロ的には「人本主義」としての日本企業が、「資本主義」を旨とするグローバル市場で生き残るには、どうした良いのか。そしてミクロ的には、ボトム・アップを中心にしてきた「日本的経営」の伝統の中に、トップ・ダウンが不可欠な情報セキュリティ施策を、不適合を起こさぬように埋め込むにはどうしたら良いのか、についてまとめておこう。標語的にいえば、「係長セキュリティ」にとどまっている現状を打破して、「社長セキュリティ」への転換(あるいは両者を止揚すること)を提唱することになる。

6.1 トヨタ式生産方式と技術標準

「技術標準はマニュアルか？」と問われれば、「マニュアルである」と言ってよい。そして最近では、日本でもマニュアルが好まれる、という傾向があるようだ。例えば、普段は学校できちんと挨拶をしない子供も、マックでアルバイトをしたら「いらっしゃいませ」と言えるの

³⁵ また、最終目的が、減価償却費を把握することにあれば、私のいた NTT では定率法の総合償却をやっていたので、償却の過不足が次年度に反映され、自動調整機能が働いて減価償却費はだんだんと調整されてしまう。したがって、あまり耐用年数にこだわるというのは、考えたことがなかった。

は、一体どういうことだろうか。若者はどうやら、マニュアルが好きなようだ。

また例えば、結婚相手を探すのに、今や「婚活マニュアル」というのができている。そのような面を見ると、日本人にもマニュアルが向いている、と理解すべきかもしれない。しかし企業ベースで考えると、例えばトヨタの生産方式は、社内ではマニュアルになっているのかもしれないが、口頭で伝承している部分が多いように思われる。それと同時に、当の本人達がこれを世界に誇るべき物だと思っていなかった、ということがある³⁶。

これに対して、アメリカ的な標準、マニュアル、コンセプトというのは、間違いなく彼ら自身の名前をつけて、世界に売り込んでくる。以下は、私の辛い思い出で少し長くなるが、お許しいただきたい。

NTT 東西に現在も課せられている「TELRIC (Total Element Long-Run Incremental Cost)」という概念がある。これは、ネットワーク相互間で接続をするときに、「どのような接続料を払うのが妥当か」という疑問に対し、「あらゆる要素を加味して、長期間にわたって、接続によってどれだけ費用が増すかということから、その部分だけを払えばよい」という、どちらかと言えば新規参入者に有利な方式である。

アメリカで FCC がスポンサーとなって、学者がこの方式を作ったときは、私は馬鹿にして、「こんなものを本当に実施する気か」と思ってしまった。ましてや、日本に押しつけてくることは考えもしなかったが、USTR(米通商代表)と手を組んで日本に押しつけてきた。このことが最初から分かっていたら、私は職責として、いち早く本社に対策を講ずるよう進言すべきだった。

実はボーモルという学者が、それより早く従来型のキャリアに有利な方式を考えていた (Efficient Component Pricing Rule=ECPR, Baumol & Sidak [1993])。ボーモルは、これをニュージーランドに売り込んだのに対して、FCC は「駄目だ」と言っていた。つまり、いったんある説を否定していたので、「TELRIC」だって相対的なものではないか、と思ってしまう。これは、私の NTT 在職中の、最も致命的な失敗の一つである。

ここから学んだことは、日本人がいかに「コンセプト」を作り、これを売り込むということが下手なのかということであった。日本は製造業でこそ世界に知られているが、サービス業などで世界を席卷しているのは、きわめて少ない³⁷。つまり、あるコンセプトなりビジネス・モデルを作り、それが汎用的だとして訴えていく力が弱いのではないかと思う。

標準化が有体物の物理的規格で終始していた時代はともかく、それが仕事の進め方や品質の保証方式にまで及んでくると、コンセプト作りと共通の要素を帯びてくる。そして、それが国の国際競争力を左右しかねないことになってくるし、「非関税障壁」として貿易摩擦の種になってくる。したがって先進国はこぞって、標準化のヘゲモニーを取るべく努力し、人を養成したり、予算を増やすことも厭わない (山田 [1997])。

これに対して日本はといえば、相変わらず「輸入学問」で満足して、自ら概念を構築したり、それをアピールすることが苦手である。後述する ISMS の認証取得企業数が世界一という事実は誇るべきだが、それが同時に「追従経済」をも意味していることを、忘れてはならない。

³⁶ 前出注 18. の後段を参照。

³⁷ アメリカの親会社を逆買収してしまったセブン・イレブン・ジャパンや、ユニクロは例外中の例外かと思われる。

6.2 ソフト産業における生産性向上

日本企業のもう 1 つの問題点は、製造業、特に輸出型製造業以外の分野の生産性が低いということであり、また、今後伸びるであろう「ソフト産業」の生産性向上のめどが立っていない、ということではなからうか。

ソフト産業については、「人月の神話」というのがある。ソフトの製作費は、企画や機能の良さで評価されるのではなく、結局それに何ヶ月かかったかによるという訳である。つまりソフト産業は、開発が下手であればある程多くのお金が貰えるという不思議な構図となっていて、それ以外の方法を誰も思いつかないというのはおかしい。欧米では、パッケージ・ソフトを買ってきてそのまま使うのに、わが国では小さな点でも「カスタマイズ」したがるというユーザー側の性向も、この不明瞭さに拍車をかけている。

この点について、NTTデータ社の前の社長であった浜口氏は、以下のように問題提起している(浜口 [2010])。「ITの純粋な技術部分の発展は、今後も世界規模のスピードで進んでいくことは確実です。ですから、われわれの生活をより良いものとしていくためにも、日本の社会全体が、積極的にITが持つ可能性を取り込み、そこで培った強みをもって国際的な展開を図っていかねばなりません。そしてこれには、ソフトウェアという仮想物が持ちあわせている少しばかりネガティブな『負』の部分を許容する寛大さが必要なのです。」(p.20)

それでは、「負」の部分とは何だろうか？ それに対して「寛大」に対処するとは、どういうことだろうか？ 少し長くなるが、関連部分を引用しよう。

「社会的に重要なシステムには、『ソフトウェア自体の品質』『運用の品質』そして『BCPと演習』の 3 点セットが欠かせません。そして、こうした事前の備えをどの程度まで行なうかはコストとの兼ね合いであり、システムの特長や用途別に応じた判断が必要になるのです。

ともかく、『ソフトには必ずバグが潜んでいる』『システムが止まってしまう可能性は決してゼロにはならない』といった認識が、ITを活用する企業にも、その先のシステムの利用者すなわち日本国民にも感覚として理解されることが、日本の社会がITの価値を最大限に活かす上で必要なことです。」(pp.74-75)

「世界を見渡せば、毎日どこかで、情報システムの故障が起きていると言っても言いすぎではありません。日本では金融取引所のシステムに不具合があると大きな騒ぎになりますが、海外の金融取引所のシステムは年に何回か止まっています。しかしこのような国々では、機会である以上コンピュータが故障するのは当たり前という認識があるのと、止まった際の備えが十分できているため、日本ほどの騒ぎにならないのです。」(pp.75-76)

「これこそが、まさにソフトウェアの持つ『負』の特徴なのですが、グローバル・スタンダードの考え方では、『多少の不便は受け入れつつ、それを上回るベネフィットのほうを高く評価しよう』というのが主流なのです。訴訟大国の米国で、ソフトウェアが製造物責任法(PL法)の適用対象外なのは、こうした背景が関係しているのかもしれませんが。あるいは、ソフトウェアはそもそも『製造物』に範疇には属さないという認識があるのかもしれませんが。」(p.77)

「企業を例にとれば、高品質の完璧な情報システムを手に入れるのが目的なのではなく、自社の事業としての生産性を向上させるなり、革新的なサービスを実現して業績を向上させることが真の目的のはずです。情報システムの品質を高めるのは、必ずしもそれを作る

側だけの役割ではありません。システム化する業務をきちんと整理・標準化する、複雑な作り込みは極力避ける、などの考え方次第でシステムの品質は格段によくなるものなのです。」(p.78)

「この問題が現象として如実に表れているのが、日本における企業向けパッケージソフトの利用の低さです。米国では、もう数十年も前から企業のパッケージソフト流通率は50%を超えています。一方日本では、20%以下と低レベルにとどまっています。なぜ、このような状態が続いているのでしょうか。(中略) 当時の米国のパッケージソフト販売会社の役員とディスカッションしたところ、主に売り込みに行くのは、まず経営者が交代した会社、そして経営を変えようとしている会社であることが分かりました。経営を変えるには、ビジネスのやり方も変える必要があるからです。しかし、『経営者や経営スタイルは変えられるとしても、現場のやり方はなかなか代わらないのでは』と聞くと、『それも一挙に変えてしまう。変えない従業員にはやめてもらう』という返答でした。」(pp.79-80)

ここには、本稿で主張してきた、リスクはゼロにはできないという認識、費用・便益分析によるリスクの受容、システム化と業務の見直し、目的と手段の関係、人は調達可能な資源か、といった論点が著者自身の経験を通じて、凝縮されて論じられている。他方で浜口氏は、企業経営者の視点から、「日本人の持つ『もてなし』や『こだわり』の精神に基づく“強み”をいかにサービスを軸とした視点でITに落とし込んで効率よくマネジメントするか」(p.70)に期待を残している。

しかし私は、最後の点については、悲観的である。結局、ソフトのグローバル化に逆らうことはできないから、日本もだんだんと「市場価格」で勝負するしかなくなる。さもないと、いわゆる「ガラパゴス化」がさらに進むことになってしまう。しかしその際、社員は次第に「イチロー型」と「その他大勢」に分かれて行かざるを得ないだろう。

そのようなことをしたら日本人の大反乱が起きる、という人もいる。しかし例えば、日本人の流動性がもう少し高く、英語のハンディを感じない人が増えてくれば「イチロー現象」が生じ、彼らはアメリカへ行くことになる。残った「その他大勢」の人達が立ち行くのかというと、彼らの給料はインドや中国に比べて非常に高いから、会社から見ればアウトソースした方が良く、ということになる。結局、両面から言って、長期間にわたって今の平等主義を維持するという事は難しい、ということになる。

では、どうすれば良いか。例えば、「生産性本部」は、製造業の生産性向上を推進していた。ところが、「社会経済生産性本部」となったとたんに、何の生産性のことが分からなくなってしまった。私は、ソフト産業の生産性、あるいはサービス産業の生産性を優先し、徹底的に改善しなければならないという気がしてならない。

そこを徹底的にやっていくと、結局は、「見える化」や「マニュアル化」の良い所と、それらの限界がもっと分かってくるのではないだろうか。日本の経営者の中には、そのことに気がついている人があまりにも少ないという感じがする。システム部門出身の社長がそれ程多くないということも、関連しているのかも知れない。

この点は、先に述べた「ホワイトカラーの生産性」と重なる部分が多いので、この辺にしておこう(林 [1994][1995][1998] 参照)。いずれにせよ、この分野の研究は未開発であり、研究を深めなければならない。

6.3 CIO, CISO と日本的経営

しかし、現実社会では、このような懸念とは逆に、日本企業は生産性の向上に熱心だし、サービス品質にも気を配っているように見える。例えば、日本の ISMS の取得企業数は、世界の中で突出してナンバーワンで、同じように日本版しかない「P マーク」の取得企業の数も順調に伸びている。

これは一体どういうことだろうか。現象だけ見ると、世界で最もセキュリティ・コンシャスな企業群が日本に出現しているようである。しかし、セキュリティ・インシデントが減ったかという点、必ずしもそうではない。このような矛盾した状況になっている。

これは、経営者が目覚めたか、あるいは、中間管理者が目覚めたかということではなく、最も端的には、「資格を持っていないと入札に参加させない」という指導があったことで、資格取得のインセンティブが生じたということであろう。加えて「横並び意識」や「勲章好き」ということもあるかもしれない。例えば、名刺に「ISMS 取得企業」と書くことが流行っている。

しかし他方で、グローバル・スタンダードだといっても、忌避されるものもある。その最たるものが、CIO や CTO ではないかと思われる。日本でも CEO と CFO (Chief Financial Officer) は、かなり普及してきたし、この人達の責任の度合いもかなり高くなっている。ところが、CIO は未だ認知度は低いし、さらに悪いことに、指名されると嫌がる人が多いのではないだろうか。

CIO がメディアに登場する時は、システムダウンや情報漏えいといった、謝る局面ばかりだからである。CFO であれば、もちろん不祥事があれば謝らなければならないが、例えば定期の決算の説明など出番はたくさんあり、褒められることもある。それに対して、CIO は褒められる出番は無く、貶される場面でしか出てこないという、あまりやりたくない役職である。CTO も、あまりなりたくないと聞く。まだ日本語で「技師長」と言ったほうが偉そうだからだろう。ましてや CISO (Chief Information Security Officer) となると、セキュリティが破られたときにお詫びに回るという立場に、ならざるを得ない。

なりたがるかなりたがらないかは別にして、そもそも日本では、このような機能別の役割分担は根付くのだろうか、という問題がある。CFO の独立性は強く、内部統制などが評価されることはあり得ると思われるが、それ以外の職務は日本的縦割組織にあまりなじまないところがある。

例えば、「常務取締役営業本部長」というのは存在するし、また、「取締役 サービス部長」というのもあり得る。それは、組織としては縦型で事業分野と対応している(ライン組織)。機能の方を徹底し、どちらかという「横割」で一元管理をする(スタッフ組織)のは、「人事部」や「経理部」といった、昔の総務人事系、経理系、購買系にはあるが、それ以外のところでは「縦割」の方が主だというのが日本的組織である(これは中根 [1963] 以来の、「タテ社会」の一面と言えそうだ)³⁸。

そこに例えば CIO というのを置くと、あらゆる部門のシステムを横串にして責任を負うということになるから、これは大変だ。それぞれの業務に違いがあると、アプリケーション・スペシフィックなことが分からないといけないことになる。そうすると、全部を知らなければならぬということになってしまう。

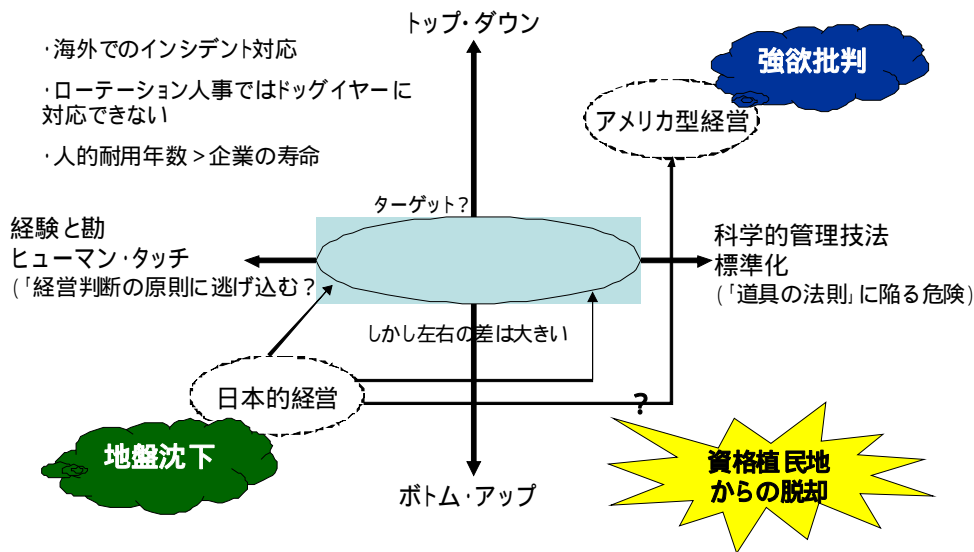
³⁸ このような説明ではなく、図表 5.にある「取締役と執行役の機能分化」の問題と捉えるべきかもしれない。今後の課題としたい。

セキュリティも然りで、これはもっと難しいことになる。情報システム全体であれば、そのシステムを他の事業部から委託され作成したり直したりすることがあるので、その限りにおいて話はつきやすい。ところがセキュリティというのは、システムよりもさらに狭い部門となり、しかも関連部門の要請を受けてやる訳ではない。その狭い部門の長となる人が、号令をかけて関連部門が全部従わなければならない、というやり方ができるのか。よほど日本的経営の考え方を変えないと、フィットしない恐れがある。

6.4 ベスト・ミックス: 日本的経営と情報セキュリティ

以上の関係を図示すると、以下の図表9. のようになる。ここで縦軸はトップ・ダウンかボトム・アップかを、横軸は ISO などの科学的な管理技法を重視するか、人間関係(ヒューマン・タッチ)を重視するかを示している。典型的なアメリカ型経営は図の右上、すなわちトップ・ダウンで科学的な管理法重視の位置にある。一方、典型的な日本型経営は、ボトム・アップでヒューマン・タッチを重視するものである。

図表9. ベスト・ミックスを求めて



しかし残念ながら、両方式とも行き詰っている。アメリカ型は、サブプライム・ローン事件以来、あまりに「資本」の意向を重視すれば、「利益のためなら手段を選ばない」ことになって、「強欲資本主義」に墮すのではないかと非難されている。一方の日本型も、1980年代の栄光は失われ、90年代以降デフレとゼロ成長で「地盤沈下」に悩まされている。

日本の一部では、このような惨状を脱するには、一足飛びにアメリカ型に移行するしかない、という見方もある。しかし、アメリカが理想郷ではないことをさて置いても、長い伝統を持つシステムを180度転換させるのは冒険でもあり、短期には不可能でもあろう。とすれば当面の施策は、純粋の日本型でも純粋のアメリカ型でもない、中庸を得たシステムを工夫することではないか、と思われる。

しかし、以下の理由によって、それが「ややアメリカ寄り」にならざるを得ないことは、認識

しておくべきかと思われる。理由の第 1 は、企業活動がグローバル化している以上、世界共通の管理システムを用意するしかないことである。英語が国際公用語になることと同様、好き嫌いにかかわらずアングロ・サクソン系のシステムを、デフォルトとしては受け入れざるを得ないだろう。

第 2 の理由は、情報セキュリティなど専門性の高い職務が増えてくると、CIO や CISO といったプロフェッショナルが活躍する場が増えてくるが、日本型のローテーション人事では対応できないからである。わが国の現状では、専門家のレベルに達する前に転勤しないと昇進面で不利になるため、世界と伍していけるセキュリティの専門家が育たないことになってしまう。

第 3 の理由は、終身雇用を前提にすると、ドッグ・イヤーで環境が変わり会社の寿命が短くなる中で、人的資源の耐用年数が突出してしまい、立ち行かなくなる恐れが強いことである。この面からは、「人本主義」そのものが変質を迫られるであろう。わが国は国全体として「高齢化」に向かっているが、「企業の高齢化」はそれ以上に深刻である。アメリカ経済が 90 年代以降、インターネットの流れに乗って成長したのに対して、わが国のベンチャーの勢いは相当劣っている。

以上の 3 点から見て、デフォルトとしてはアメリカ型に近づく中で、日本的経営の特色をどの程度生かすことができるのか、という問題設定をすべきであろう。その際の最大の課題は、技術標準をアングロ・サクソンに握られたことの副作用として、情報セキュリティに関連する資格が、ほとんど英米に押さえられてしまった状況(図表 9. では「資格植民地」と表現した)から、いかに失地回復できるかであろう。

6.5 2つの分断: その 1 = 経営学対技術経営論

このような事があるからなのか、経営学の本の中で「情報セキュリティ」がどれくらい取り上げられているのかというと、驚くほど少ない。それより前に、経営学の本で「経営情報システム」や「経営情報論」に触れているものでさえ、さほど多くはない。それに関しては、「他の本をあたってくれ」となっている。試しに、遠山・村田・岸 [2008] を見たら、情報セキュリティの部分は約 10 ページしかなかった。

そうすると、全体の「経営学」があって、その中で「経営情報」というのが入っている場合もあるけれども、入っていても少なく、外にはみ出していることもある。さらに「情報セキュリティ」となると、ごく一部入っているけれども、それ以外にはみ出していることの方が多いことになる³⁹。

例えば、「技術経営論」(MOT = Management of Technology) が必要であるということになって、MOT のコースが色々な大学で開設されることになり、それだけの専門職大学院もある。しかし、そこで、セキュリティをどれだけやってくれるのかというと、甚だ心許ない。本稿の文脈からすれば、情報セキュリティは経営問題そのものであるから、技術系とか事務系を問わず、誰もが関心を持ってもらいたいところである。

しかし、このことは学問の問題として、我々にも責任があるところだろう。特に、当大学院において「非技術系」の分野を統括してきた私は、その責任の大部分を帰せられても仕方

³⁹ 経営学の大家の伊丹敬之氏に会った際「あなたのような経営学の大家が、標準化の問題と情報システムの問題もふまえて、情報セキュリティがいかに大切かということを書いてもらわなければ困る」と訴えたら、「林さん、お互いこんな歳になって今から始めても駄目じゃないですか」と言われた。このような状態が、正直なところではないかと思われる。

がない。それは、どのような局面で現れるのか、例を挙げてみよう。私は「セキュア法制と情報倫理」という科目を共同で担当しているが、私たちの授業に対して理系出身の院生が、次のようなことを期待していることが判明した⁴⁰。他の社会科学系の授業に対しても、多かれ少なかれ同じような「期待」を持っているとみて、間違いはなさそうである。

- ・ 「情報セキュリティ法」とか、「情報セキュリティ基本法」といった法律は無いのでしょうか？
- ・ 沢山の法律が関連しているとしても、「情報セキュリティ六法」という「まとめり」も無いのでしょうか？
- ・ 個別の法レベルで「まとめり」を付けるのは難しいとしても、学問体系として「情報セキュリティ法」という領域が未確定だとは、信じられません。
- ・ 法学の専門家は、いつも「その先は専門家でないと分からない」と言って、インシデントに法的に向き合うことを、避けているのではないのでしょうか？
- ・ ISMS など、手続き的なセキュリティ施策が普及している中で、それが法的な保障とどう関連しているのか、あるいは関連していないのかが、知りたいところです。
- ・ 仮に、これまでは専門家任せで良かったとしても、インシデントが誰の身にも降りかかる現在では、素人にも分かる法理論が、求められているのではないのでしょうか？
- ・ 裁判員制度が定着しつつある中で、法的な問題を素人に分かりやすく説明することは、マストではないのでしょうか？

しかし、有体物の法は明治以来それなりに機能してきたが、「情報」という無体財に関する法は未だ発展途上にあり、直ちに要望に応えることはできない。どう対応したら良いのか、数年にわたって試行錯誤を繰り返してきたが、現在では「情報窃盗」を例にして、「一緒に考える」ことがベストだという、(暫定的かもしれないが)結論に至っている。具体的には、図表 10. の問いを発して、院生自身に考えてもらうのである。

図表 10. 情報窃盗のブレイン・ストーミング

あなたが「情報窃盗」を刑法に追加したい場合、以下の態様のどれを、罪の対象に含めますか？

- ・ 電車で座っているときに、隣の人が読んでいる新聞を、盗み見する。
- ・ 観光ツアーの一回の後部に密かに加わり、ガイドの案内を盗み聞きする。
- ・ 試験において、隣の人答案を書き写す。
- ・ 社員として勤務中に、発注先から預かった個人情報、友人に漏らす。
- ・ 社員として勤務中に、「営業秘密」(社外秘)として管理されている情報を、ライバルの会社に漏らす。
- ・ 書店に行って、他人の著作からレポートに役立つ部分を書き写す。あるいは、カメラ付き携帯で写し取る。
- ・ カリスマ美容師に弟子入りして、ノウハウを盗む。あるいは、ビデオに収録する。
- ・ USBメモリーを盗んだが、肝心の情報には暗号がかかっている、読めなかった。

このようにして、いわば「参加型」で対話をする、「教師から教えてもらえる」と考えていた院生が、「自分で考えるしかない」ことを自覚するようになり、理解が一段と進む。これは教育一般に通じることで、情報セキュリティに固有のことではないかもしれない。しかし、専

⁴⁰ ここでは簡素化のため、法と倫理の関係や、倫理プロパーの疑問は除いている。細部を知りたい方は、矢野・林 [2009] を参照されたい。

門性が高くとっつきにくい法律という分野で、このようなことが可能であることは、意外な発見であった⁴¹。

もともと、わが国における学会の雰囲気は、狭い分野の先端的研究を追いかけ、隣の分野を覗くこともしないし、研究と同程度に教育に労力をかけることもしない、という偏狭なものであった。時代の変化に伴って、狭い分野を深堀することも大切だが、学問分野をまたがることも疎かにできないことが、次第に認識されつつある。しかし、学際研究にはさらなる努力と、相互理解が必要だろう⁴²。

特に、文系と理系の対話は、その必要が言われてから久しいにもかかわらず、期待通りの成果が上がっているとは言えない。私のように、勤めた会社に理系と文系が半々程度におり、私自身が一般的には理系と目される部門に通算で 9 年もいた者からすると、これは怠慢以外の何者でもない。学問も国際競争にさらされているのだから、もっと自覚を持ってもらいたいところである。

6.6 2つの分断: その2 = 係長セキュリティ対社長セキュリティ

さて、現在日本企業で行なわれている情報セキュリティは、せいぜい「係長セキュリティ」で、よく言っても「課長セキュリティ」止まりだろう。これを「社長セキュリティ」にするためには、何らかの発想の転換が必要と思われる。そのために、なぜ両者が分断されているのかを考える必要がある。そこには、係長側の問題、社長側の問題、の両者が含まれているようである⁴³。

まず、係長側の問題としては、情報セキュリティを技術問題と理解し、またそのように上司に説明することが挙げられる。これでは、直属の上司は説得できても、社長にまでは届かない。社長の時間や頭の中には、多くの案件が詰まっている訳だから、優先度が高いものでないと真剣になって考えてもらえない。これでは、社長の関与を婉曲に拒否しているようなものである。

そして実際、係長にとっては現在の「係長セキュリティ」の状態が心地よいのではないかと、といった疑いが持たれてさえいる。社長が関心を持ってあれこれ言われるよりも、黙って聞いてくれさえすれば良い。それもまた、1 つの生き方ではあろう。しかし、そのように「口を出さないで任せて欲しい」という対応では、必要な投資資金を予算化したり、優秀な社内人材を確保することは期待できない。それでは情報セキュリティが、いつまでもマイナーな存在に終わってしまう。何よりも、係長本人がいつまでも係長の発想から飛躍できない。

他方、社長の側にも問題がある。特に文系の社長の場合、技術的な説明をされるとなかなか理解できない。そこで勢い「その件は任せたまよ。しっかりやってくれ」という態度に出がちである。さらにコスト削減に熱心な社長の場合は、業務そのものをアウトソースすることまで考えるかもしれない。しかし、業務が情報システムに大きく依存している現状では、アウトソースしても全体を把握できる社員を確保しておかないと、いざという非常時にとんでもないことになりかねない⁴⁴。

⁴¹ 現在「ハーバード白熱教室」として評判を呼んでいる Sandel 教授の科目(サンデル [2010])は、公共哲学ないし社会倫理といった地味なものである。従来なら人気の無かった、こうした科目が多数の学生を惹きつけることができるなら、理系の学生に対する人文・社会科学の授業にも、工夫の余地がありそうである。

⁴² 学際研究そのものに伴う困難については、林 [2009b] を参照。

⁴³ さらに根本的な問題として、わが国ではリスクを認識するチャンスが少ないこと、ナショナル・セキュリティが表立って論ぜられないこと、といった全体的な視点がある。しかし、紙幅の関係から、ここでは省略する。

⁴⁴ この点では、2005年に東京証券取引所で連続して発生したシステム事故が、格好の教訓になろう(矢野・林 [2009])

そこで、ここでも両者の対話が必要になるが、その際のキーワードは「セキュリティ」よりも、「リスク」という言葉を使って対話することではなかろうか。最初に「企業はリスク・テカーである」と言ったが、経営者であれば、この点については細かく説明をしなくとも分かるだろう。

「リスクにどう対応するのがセキュリティです。そのリスクの中には、もちろん商品が売れるのか売れないのかという、経営者がまず考えなければならないこともあります。しかし、今の仕事の流れというのは、ほとんどが情報システムに依存しています。情報システムに情報リスクが伴っているのであれば、その中には情報セキュリティのリスクがあります。」といった説明をすれば、比較的理解しやすいのではないと思われる。

「係長セキュリティから社長セキュリティ」への転換、あるいは弁証法の用語によれば「止揚」は、「言うは易く行なうは難い」ことかもしれない。「社長になって見なければ、社長の難しさが分からない」という言葉があることは、「社長の気持ちになる」ことにも限界があることを示しているようである。

しかし、この言葉は半分は正しいが、半分は間違っているかと思われる。正しいという意味は、社長と副社長とでは責任の重さに雲泥の差があり、「社長の気持ちになる」ことには限界があるからである。副社長から社長に昇格した人が、「責任の重さを痛感する」という言葉を発したり、社長就任後に顔つきが変わってくるのは、このことを暗示している。社長と副社長との間でさえそうなのだから、社長と執行役員との間では、「社長の立場になって考える」ことは、ほぼ不可能に近い。

しかし、社長を経験しなければ社長の器がどうか分からない、というのでは堂々巡りしかないことになって、新しい社長は生まれない。現実には、毎年多数の新社長が誕生し、彼ら・彼女らは通例期待に応えている。その意味では、上記の命題は半分は間違っている。現に、社長を経験していないコンサルタントの助言が有効なことがあるし、高名な経営学者の大半は社長未経験者である。

6.7 「Awareness 提言」を超えて

本稿の結びにあたり、「1. はじめに」で紹介した「Awareness 提言」を、再び思い出していただきたい。この提言は、これまで縷々説明してきたことを圧縮して、社長にも理解してもらえよう、簡素化したものである。冒頭にも述べたとおり、新規性のある提言でも、進歩性のあるものでもない。いわば「基本動作」として当たり前のことで、しかも優秀な社長なら既に実施済みのことをまとめたに過ぎない。

しかし最後まで読み通された読者が、冒頭で感じたものとは若干は違った印象を持っていただけるなら、本稿の目的はほとんど達成されたと言って良い。そして、こうした「基本動作」は平時においては忘れられがちなので、繰り返し「思い出す」(aware)必要があること、さらにはこうした「基本動作」に関する限り、社長も係長も差がないことを感じ取っていただければ、幸いである。

参考文献

- [1] 浅井達雄 [2007] 『情報セキュリティと企業活動 実践と理論』 亀田ブックサービス
- [2] アベグレン, ジェームス, 占部都美(訳) [1958] 『日本の経営』 ダイヤモンド社
- [3] 飯塚悦功 [2005] 『ISOを超える』 日本規格協会
- [4] 池尾和人・池田信夫 [2009] 『なぜ世界は不況に陥ったのか』 日経 BP
- [5] 伊丹敬之 [1987] 『人本主義企業:変わる経営, 変わらぬ原理』 筑摩書房
- [6] 伊丹敬之 [2000] 『日本型コーポレート・ガバナンス』 日本経済新聞出版社
- [7] 稲盛和夫 [1998] 『稲盛和夫の実学:経営と会計』 日本経済新聞社
- [8] 岡本浩一 [2001] 『無責任の構造』 PHP 新書
- [9] 岡本浩一・今野裕之 [2006] 『組織の社会技術1. 組織健全化のための社会心理学』 新曜社
- [10] 岡崎哲二・奥野正寛 [1993] 『現代日本の経済システムとその歴史的源流』 岡崎・奥野(編) 『現代日本経済システムの源流』 日本経済新聞社
- [11] 奥村 宏 [1975] 『法人資本主義の構造 日本の株式所有』 日本評論社
- [12] 奥村 宏 [1991] 『新版 法人資本主義の構造』 社会思想社
- [13] 奥村 宏 [2006] 『株式会社に社会的責任はあるか』 岩波書店
- [14] 奥村俊宏・村山浩・横山蔵利 [2008] 『ルポ内部告発』 朝日新書
- [15] 菊澤研宗 [2007] 『命令違反が組織を伸ばす』 光文社新書
- [16] 小池和男 [2009] 『日本産業社会の神話』 日本経済新聞出版社
- [17] 郷原信郎 [2007] 『コンプライアンスが日本を滅ぼす』 新潮新書
- [18] 篠塚英子・石原恵美子 [1977] 『オイル・ショック以降の雇用調整:4カ国比較と日本の規模別比較』 『日本経済研究』 No.6, 日本経済研究センター
- [19] 渋沢和樹 [2010] 『挑戦者』 日本経済新聞出版社
- [20] 城繁幸 [2004] 『内側から見た富士通成果主義の崩壊』 光文社ペーパーバック
- [21] ダートウズ, M.L. 依田直也(訳) [1990] 『メイド・イン・アメリカ:アメリカ再生のための米日欧産業比較』 TBS ブリタニカ
- [22] デッカー, シドニー, 芳賀繁(監訳) [2009] 『ヒューマンエラーは裁けるか』 東大出版会, Decker, Sidney [2007] "Just Culture: Balancing Safety and Accountability," Ashgate Publishing Co.
- [23] 遠山暁, 村田潔, 岸真理子 [2008] 『新版経営情報論』 有斐閣
- [24] 中根千枝 [1963] 『タテ社会の人間関係』
- [25] 野口悠紀雄 [1995] 『1940年体制:さらば戦時経済』 東洋経済新報社
- [26] バーンスタイン, ピーター, 青山護(訳) [2001] 『リスク:神々への反逆』 日経ビジネス人文庫 (原著「Against the Gods」は1996年)
- [27] 畑村洋太郎 [2000] 『失敗学のすすめ』 講談社
- [28] 浜口友一 [2010] 『ニッポンのIT:その未来』 日本経済新聞出版社
- [29] 林紘一郎 [1994] 『情報ハイウェイと生産性:ホワイトカラーに照準』 『朝日新聞』 5月14日 「ゼミナール」欄
- [30] 林紘一郎 [1995] 『ITS 資本主義における米国の優位』 『アスティオン』 春号 TBSブリタニカ
- [31] 林紘一郎 [1998] 『情報エコノミーに適応した新しい米国方式』 『世界』 7月号特集「アメリカは本当に強いのか」 岩波書店
- [32] 林紘一郎 [2009a] 『セキュリティタイゼーションとセキュリティ』 『金融情報システム』 (2009年夏号) 巻頭言, 金融情報システムセンター
- [33] 林紘一郎 [2009b] 『実学とは何か:創刊の辞に代えて』 『情報セキュリティ総合科学』 Vol.1
- [34] 林紘一郎 [2010] 『著作権(著作物)と property, property rule, そして property theory』 『アメリカ法』 2010年 号(近刊)

- [35] 林紘一郎・鈴木正朝 [2008] 「情報漏洩リスクと責任 個人情報为例として」 『法社会学』 第 69 号
- [36] ベック,ウルリッヒ,東廉・伊藤美登里(訳) [1998] 『危険社会』 法政大学出版局 (原著は 1986 年)
- [37] 深尾光洋・森田泰子 [1997] 『企業ガバナンス構造の国際比較』 日本経済新聞社
- [38] ボーグル,ジョン C.,瑞穂のりこ(訳) [2008] 『米国はどこで道を誤ったのか』 東洋経済新報社, Bogle, John C.[2005] “The Battle for the Soul of Capitalism,” Yale Univ. Press
- [39] 本間道子 [2007] 『組織性逸脱行為過程—社会心理学的視点から』 多賀出版
- [40] 村上陽一郎 [1998] 『安全学』 青土社
- [41] 矢野直明・林紘一郎 [2009] 『倫理と法 情報社会のリテラシー』 産業図書
- [42] 山田肇 [1997] 『技術標準』 NTT 出版
- [43] リーズン,ジェームズ,塩見弘(監訳)高野研一・佐相邦英(訳) [1999] 『組織事故』 日科技連(原書は 1997 年)
- [44] 渡辺幸一 [2009] 『イギリス流融通無碍のススメ』 講談社 新書
- [45] Baumol, William J. and J. Gregory Sidak [1993] “Toward Competition in Local Telephony” AEI Press
- [46] Brynjolhsson, Erik and Lorin Hitt [1998] ‘Beyond the Productivity Paradox: Computers are the Catalyst for Bigger Changes’, CACM, August
- [47] Hirschman, Albert O. [1970] “Exit, Voice, and Royalty,” Harvard Univ. Press, なお邦訳は, 矢野修一(訳) [2005] 『離脱・発言・忠誠 企業・組織・国家における衰退への反応』 ミネルヴァ書房
- [48] La Porta, Rafael, et al. [2008], “The Economic Consequences of Legal Origin,” Journal of Economic Literature
- [49] Solow, Lester [1987] ‘We’d better watch out.’ The New York Times Book Review, July 12, 1987