

ソフトウェア技術者をめぐる 二つの倫理的アプローチ ——工学倫理とビジネス倫理——

竹島 尚仁

コンピュータシステムは、善かれ悪しかれ我々の個人的な生活に浸透している。パソコンを単体で使用することはもとより、ネットワークに接続することでさまざまな情報を手に入れたり交換したりするために使用されることが増え、商品を購入する機会も増えてきた。パソコンは情報機器としての座をより軽量で携帯可能なものに譲り、ユビキタス・コンピューティング——いたるところにコンピュータが偏在すること——が近い将来のコンピュータ像であると言われている。

またコンピュータシステム¹は、炊飯器などの家電製品や自動車、医療機器にも、制御のために組み込まれている。さらにそれは社会全体に幅広く浸透し社会システムそのものを支えている。交通（交通信号、列車運行システム、飛行機の管制システムなど）、通信（インターネットそのものや企業内情報ネットワークなど）、産業（原子力発電所、作業ロボット、電子商取引、コンビニエンスストアの販売時点情報管理システムなど）、金融（銀行のATM、銀行間取引、証券取引所など）、科学（人工衛星のなどさまざまな観測装置）、等々である。行政の領域でも、いわゆる住民基本台帳ネットワークや電子政府の構築、2005年には「世界最先端のIT国家」を目指すという触れ込みで、情報インフラが整備されようとしている²。

今後もコンピュータシステムが個人的生活や社会システムに浸透するという傾向は、コンピュータ技術が反復される（一連の）単純な作業の自動化という理由で使用されるとす

¹ コンピュータシステムとは、コンピュータハードウェアとソフトウェアで作られるシステムである。後に出てくる、情報システムとは、コンピュータシステムとそれを使用する人間からなる情報処理システムである。なお、たとえば工場や銀行など、情報システムによって機能を補完されるシステムは実体システムと呼ばれる。

² ITによって社会や国家が今後どうなるかという最も肝心な点の見通しにくさについては、たとえば、坂村健、『21世紀日本の情報戦略』、東京：岩波書店、2002年を参照。

るなら、IT 産業が不況であろうとなかろうと、今後も続くであろう³。そこで今現在求められているのは、コンピュータシステムの安全性⁴や信頼性である。以下ではとくにハードウェアではなくソフトウェア⁵に焦点を当てていきたい。それにはいくつか理由がある。

まずそれは、以上に見たようにソフトウェアが幅広く社会システムの基幹部分にまで使用されているという事実である。生命を直接脅かす危険性もある障害もあれば、経済的損失を生む障害もあるが、いずれにせよなんらかの危害が生じる潜在的リスクがあり、高まりこそすれ減ることはない⁶。また、ネットワーク上でのデータベース・プログラム・音楽などの知的財産の保護、個人情報の保護、さらにネットワーク上の有害情報の拡散など、さまざまな問題が露呈している。コンピュータウィルス、ネットワーク攻撃、などの問題も止む気配はない。

これらの問題を解消するには何が重要となるだろうか。これらに対するさまざまな経営判断や政策的判断はそれ自体重要であるが、それを実現するのはしかるべき情報制御技術である⁷。デジタル化された情報の流れはすべてソフトウェアとハードウェアの組み合わせによって制御される。もちろんハードウェアの品質も重要であるが、同時にハードウェアと一体となり機能するソフトウェアの品質もまた重要度において劣ることはない。

これと呼応するように、ソフトウェア品質をしっかりと管理し保証することに対する要求がさらに高まっている。政府による e-Japan 計画の一環として、政府調達・民間調達のソフトウェアが増えるであろうと予想されることもその一因である。これはまた、OECD によって提出された、「OECD 情報システムおよびネットワークのセキュリティのためのガイドライン」⁸の要請に応答することでもある。しかしながら日本にあった品質管理基

³ このようなコンピュータ技術が我々の生活に何をもたらし何を奪い取るのかを、包括的に検討しなおす作業が求められている。しかしここでは、コンピュータ技術とうまくつきあっていくことが当面不可避であるという前提のもとに話を進める。

⁴ 技術の安全性という概念は文化に依存する面をもつ一方で、経済のグローバル化に伴って安全性の基準には国際的な標準化が求められている。以下では基本的に「受容可能なリスク」という意味を核とする次の定義が、念頭におかれている。R・シンジンガー／M・W・マーティン、西原英晃監訳『工学倫理入門』、東京：丸善、2002年、159頁を参照。

⁵ ソフトウェアということで、コンピュータが実行可能なプログラムを念頭におくが、ソースコードもソフトウェアそのものだと見なせるし、広く取ればソフトウェアのマニュアルもソフトウェアの一部と見なしてもよい。

⁶ ソフトウェアが絡んだ事故については、たとえば T・フォレスター／P・モリソン『コンピュータの倫理学』、東京：オーム社、1992年、5章や、リスクダイジェスト <http://catless.ncl.ac.uk/Risks> などを参照。

⁷ このことは、情報技術だけで情報管理がうまくいくということを意味するわけではない。

⁸ OECD Guidelines for the Security of Information Systems and Networks: Toward a Culture of Security,

準は、研究段階である。通常我々が手にするパッケージソフトウェアには必ずバグが含まれていると言ってもよい。

このような理由から、以下ではソフトウェア開発をめぐる倫理的問題を考えていきたい。その際議論の見通しはつぎのとおりである。専門技術者としてのソフトウェア開発者は、公衆の安全や雇用者への忠誠などの義務をもつ。こうした倫理は工学倫理の領域で考えられている。しかしながら、技術者は技術者であると同時にたいていは企業組織の一員でもあり、技術者の判断や行動はたえず経営者の判断と行動の影響下にある。したがって、技術者の倫理の実現を可能にするには、経営者の管理能力やその方法が問われざるを得ない。ソフトウェアの安全性や信頼性を保証する健全な組織がいかに形づくられるかは、企業倫理的アプローチ、したがってビジネス倫理的アプローチ⁹からでてくる。工学倫理とビジネス倫理のどちらのアプローチがよりすぐれているというのではなく、二つのアプローチは補完し合わなければならないと思われるのである。

そこで、まずソフトウェア技術者がつねに直面せざるを得ないソフトウェア開発の困難さに目をやり、最近の事例から、技術者と経営者とが技術上の要請と経営上の要請で対立する有様を取り出す(Ⅰ)。次に、組織事故のあり方から、安全管理における組織的な取り組みの重要性を考慮し、さまざまな組織内の制約のもとで働かなくてはならない技術者のあり方を考察する。その際技術者が倫理を実現する自由度に焦点を当てる(Ⅱ)。そしてソフトウェア開発の管理手法を取り上げ、安全管理を実現するために求められる組織の成熟と、内部告発を受け入れるために構築される、企業内外の制度の位置づけを考える(Ⅲ)。最後に、安全文化を社会全体で共有するために、企業活動における工学倫理的アプローチと企業倫理的アプローチの補完関係を強調する。

I ソフトウェアによる障害の特性とその事例

ソフトウェアは、通常の工業製品や建造物などと異なり、特殊な制作物であり、物質そ

2002.あるいは経済産業省の <http://www.meti.go.jp/policy/netsecurity/index.html> にある OECD 情報セキュリティガイドライン関係文書を参照。

⁹ これはある程度致し方ないところがあるが、どの程度のバグであれば許容できるのかどうか議論があってもよいだろう。たいてい使用許諾書にあるように、ソフトウェアを使用するには損害賠償請求権を一方的に放棄しなくてはならないが、それは経験的に言って問題があると思われる。

¹⁰ ここで企業倫理的、ないしビジネス倫理的アプローチというのは、さしあたり企業倫理全体を問題にしているのではなく、あくまで組織の一員としての技術者をとりまく諸制約を適正化し、技術者の倫理の実現を可能にすることを念頭においている。

のものではない「機能する情報」である。それ自体は目に見えず、複雑な論理的思考の積み重ねでできたものである。大規模な開発プロジェクトに関わる開発者は相互の進捗状況を確認しづらく、コミュニケーション上の問題が大きい。また、品質がシステムエンジニアやプログラマー個人の技能に依存する部分が多い、ソフトウェア開発技術のライフサイクルが短く次々と新たな技術が登場する、などさまざまな開発上の問題点が指摘されている¹¹。

このため、ソフトウェアが、他の商品と同じように（セキュリティを含む）安全性や信頼性を確保することは難しい。より本質的な理由を挙げるなら、それは、ソフトウェアを含むコンピュータシステムの複雑さ¹²にある。T・フォレスターとP・モリソンによれば、ある原子力発電所などの性能を判断するシステムを考え、システムの動きを許容誤差内に維持するのに、バルブや圧力ポンプなどの2進信号の信号源が100あるとする。このとき、システムがとりうる状態は、 2^{100} あるいは 1.27×10^{30} とおりになり、それぞれの状態に応じたプログラムの部分が実行されるとすれば、少なくとも 1.27×10^{34} とおりにのぼると概算している¹³。

そこで、毎秒100回の割合で検査プログラムを動かし間違った状態を訂正するプログラムを考えると、約 4×10^{24} であり、宇宙の寿命の何倍にもなると見積もられている。到底すべてのバグを取り除くことはできないし、また、バグを取り除くと新たなバグが生まれるとされ、当面のバグ症状だけを回避し根本的な手直しはせずに、システム改良のためにどんどんコードが継ぎ足されることになる。システムを動かしながら改良する場合にはなおさらである。さらに、一通りうまく書けていても、実際には想定外の負荷がかかることによりうまく動かないことが露呈することもある¹⁴。

さらに、障害時の影響の出方が、デジタル機器はアナログ機器と違っている。アナログ系は前の状態の正しさに依存せず、完全に動かなくなることは明白な障害を除けばめったにない。これに対してデジタル機器は前の状態の正しさに依存するので、決定的に簡単に

¹¹ たとえば、ソフトウェア開発・調達プロセス改善協議会、「ソフトウェアプロセスの改善に向けて～SPIへの今後の取組み～（案）」、2001年、21頁で簡潔にまとめられている。
<http://www.meti.go.jp/feedback/downloadfiles/i10626bj.pdf>

¹² 複雑性の意味については、塩沢由典、『複雑系経済学入門』、東京：生産性出版、1997年、さらに、齋藤了文、『<ものづくり>と複雑系 アポロ13号はなぜ帰還できたか』、東京：講談社、1998年を参照。

¹³ T・フォレスター／P・モリソン、前掲書、130頁以降。

¹⁴ 日経コンピュータ編、『システム障害はなぜ起きたか みずほの教訓』、東京：日経BP、2002年、59頁。

動かなくなることがある¹⁵。パソコンを使用していて突然動かなくなことはよく経験するところである。

このような特性をもつソフトウェアの安全性と信頼性を最大限得るには、プログラムの十分なテスト期間をとり、レビューをしっかりとこなうことが必要である¹⁶。さらにシステムを継続的に保守するが重要であることも、想像に難くない。

ここで日本の銀行の情報システムに目を向けてみよう。それは世界に類を見ないほど大規模かつ複雑なプログラムであると言われている。たとえば、勘定系システムは、ATMからの現金の引出しや預け入れの命令をうけるなどして口座残高を増減させるシステムであるが、全体で1億行にまで膨らんでいる。これは千人のエンジニアが10年かけて開発を続けるといけないうる量であると言われている¹⁷。これでは一個人がシステム全体を把握することさえ難しくなるであろう。

みずほファイナンシャルグループ（以下、みずほ）のATMの障害や口座振替の障害は、ソフトウェアの障害に関わった最近の大きな事件であった。銀行自体、障害発生後その要因を明らかにしている¹⁸し、また、日経コンピュータからまとまった報告も出版されている。後者は各銀行のシステム統合がどのように進んでいったかがより詳しく描かれているので、これを手がかりに、障害の原因はどこにあったのかを見てみることにしたい。

まず、銀行ごとにシステムが異なっており、どのシステムが統合後も使われるかはシステム開発や保守をこれまで行ってきた、各銀行のシステム部門、そして各銀行にハードウェアを専断的に納入してきた異なるメーカーにとって死活問題であった。これのみならず、統合される銀行同士の主導権争いもあって、統合方式の決定が遅れた。しかもシステムの統合の仕方が途中で変更されたりもした。

実際統合までに、プログラムは完成の域には達せず十分なテスト期間が取れていないことが明らかになっている。統合日直前にも口座振替処理に障害が発生していたにもかかわらず

¹⁵ T・フォレスター／P・モリソン、前掲書、136-137頁。

¹⁶ オープンソースの成功の一端は公開されたピアレビューにあり、この方法がソフトウェア工学的な優位性をもつことが指摘されている。川崎和哉編著、『オープンソースワールド』、東京：翔泳社、1999年、とくに262頁。また、ポール・ヴィクシー、「オープンソース開発におけるソフトウェアの工学的側面」、Ch・ディボナ他編著、倉骨彰訳、『オープンソースソフトウェア 彼らはいかにしてビジネススタンダードになったのか』、東京：オライリー・ジャパン、1999年（Web公開版）、所収。
http://www.oreilly.co.jp/BOOK/osp/OpenSource_Web_Version/chapter07/chapter07.html

¹⁷ 日経コンピュータ編、前掲書、18頁。

¹⁸ <http://www.mizuho-fg.co.jp/pdf/disclosure/data0203d/senryaku04.pdf>

らず、なんとか解消できるだろうという見通しの甘さがあった¹⁹。さらに、対外接続システムという重要なシステムの障害にそなえてフェールセーフ機構も構築されていなかった。それは、経営的な判断で構築されなかった可能性も指摘されている²⁰。

結局経営上の大きな目的が忘れられ、統合方式に関する意思決定が非常に遅れてしまい²¹、システム制作の不完全さが生じたわけである。意思決定が遅れたのは、そもそも経営陣が情報システム自体の重要性にそれほど敏感ではなく、システム統合の困難さとそれに伴うリスクの認識も甘かったからであると、指摘されている²²。これはみずほ自身がみとめる反省点でもある。つまり、システム障害の最大の原因は経営判断のまずさにあったということになる。経営者の側が、Ⅲで見る、プロジェクトマネジメントを疎かにしてしまった、と言えるだろう。

これに対して、情報システムの統合が成功した銀行では、経営者が技術者の見解に耳を傾けそれを聞き入れたことが決定的であった²³。また別の銀行では、重要な経営上の変更点が発生してどうしてもシステム変更を迫る必要が出てきたときにも、システム開発をする技術者の側がその経営上の要請を押しとどめるということでシステム統合に成功した。経営陣や技術者の活動が協調的に進んでいったということが成功の大きな要因ひとつであると言えよう。

このような事例と比較すると、みずほの事件の背後には、技術者の倫理と経営者の管理能力・倫理との複雑な組織的関係を見出せると思う。まず、経営者側と技術者側をそれぞれ切り離して考えてみたあとで、両者の複雑な組織的関係を考えたい。

経営者側は、情報システムの重要性を十二分に知り、障害が発生した場合のリスクを考慮できていれば、延期ということを考慮できたかもしれない。結果論であるとはいえ、1ヶ月もの間自宅に帰ることもままならずシステムの復旧に尽力した、現場の技術者や担当者のエネルギーをもっと効率的に配分できたのではないだろうか。もちろん、新組織の発足は、すでに一度延期していたこともあり、何としても予定通りやり遂げなければならないという経営上の切迫感が上回ったであろうことは想像に難くないが、この状況下では、技術者の倫理よりはむしろ経営者の管理能力と倫理が問われるであろう。

¹⁹ 口座振替障害の復旧過程で、焦りと疲労から人為的ミスによって、二重引き落としや二重送金が出たことは本稿の考察から省いている。

²⁰ 詳しくは、日経コンピュータ編、前掲書、60-61頁。

²¹ 2001年秋にやっと決まる。2002.4は一度延期したあとの日程。

²² 日経コンピュータ編、前掲書、54頁。

²³ 日経コンピュータ編、前掲書、82頁。

他方、技術者側はどうであったか。なるほど、日経コンピュータの報告では、技術者が重要な局面でどのような考えをもっていたのかがほとんど見えてこない。しかし執筆者は、推測によって技術者の考えをつぎのように補完している。4月1日のシステム稼働を「見切り発車」あるいは「不具合を承知で稼働」と決めつけるのは、いささか微妙なところである。……現場の担当者はこの段階でも、「何とかできる」、「何とかしたい」と思っていたと考えたい」²⁴。

確かに執筆者がそのように断定するのを躊躇することにもうなずける。結果論として現場の担当者の見込みが甘いということは簡単であるが、ソフトウェア開発自体やってみなければどれくらいで終了できるか分からないとも言われる。予定していたより長くなったり、短くなったりすることはよくあることだと言われる。また、統合プロジェクトの重要度からすると、一技術者がそう簡単に流れを変えられるようなものではない。

それでも技術者側が技術者としてできることはなかったのであろうか。経営者側に対してシステムに現在もなお残っている問題点、その解消のための作業内容とそれに必要な人員と時間を告げるというプロセスがあったのかどうか。そして起こりうる問題が生じたときどのようなリスクを負わねばならないかをはっきりと分かりやすく示していたのであろうか。技術者個人としては難しくても情報システム部全体の見解としてそのリスクを経営者側に明確にしていれば、経営者側が判断を変えた可能性もある。

企業組織としては、経営者が最終的な判断を下しその責任をとるべきであることは明らかである。しかしあのような状況では、何よりも技術者の判断が経営判断の前提になる。ソフトウェアの障害の除去がいつできるかには不可測性が伴うとはいえ、リスクの大きさをより認識しそれを経営者に認識させることができたのは、技術者だけだからである。

しかしここで主眼点としたいのは、このように経営者側と技術者側に対して倫理的反省を突きつけることよりもむしろ、両者の間の複雑な組織的關係である。つまり、経営者は情報システムとその重要度に無知な状態でありながら、あるいはそれゆえに、無理なシステム統合計画を技術者に押し付け、他方で技術者は、後に見るように組織内で置かれた従業員としての弱い立場から、経営者の要求を無理であると考えたにせよ、それを受け入れるしか選択肢がなかったのではなかろうか。こうした複雑な組織的關係のなかに、手ひどい失敗にいたる悪循環が潜んでいたのではないだろうか。

この悪循環を認めたうえで、なおかつ技術者に対してあえて経営者に統合の延期を執拗に助言すべきであるという倫理的要請を掲げるとすれば、それは、技術者が単に良心から

²⁴ 日経コンピュータ編、前掲書、56頁。

義務を果たそうとすることではなく、同時にこれまでの自らの職業的態度を変えることをも意味する。経営者もまた、情報システムの重要性を認識し、技術者が説明する技術上の問題を真剣に考慮に入れるとすれば、それは自らの経営責任を果たすことを意味する。経営者と技術者との複雑な組織的關係が陥った悪循環の解消こそが事柄の中心にある²⁵。

次章ではこの点を踏まえ、技術者が倫理を実現するうえで、組織的制約が彼にどのような影響を及ぼすかを考える。そのために、組織的な原因が危害とする事故、すなわち組織事故の場合に焦点を当てることにする。

II 企業組織のなかでの技術者

J・リーズンによれば、主要な事故の80から90%がヒューマンエラーによって起こるという考え方が主流であるとされる。ヒューマンエラーによる事故の安全管理には3つのアプローチがあり、それぞれのアプローチは対立しあうものではなく調和させ共存させることが可能である²⁶。

①人間モデル。これは伝統的な事故に対するアプローチであり、労働者は「安全行動から不安全行動に至る行為を自由に実施できる個人」とであると見なされている。これに対応して、ヒューマンエラーの原因は個人の心的属性に求められ、「不注意、忘れっぽさ、やる気のなさ、いい加減さ、技能や経験の不足、怠慢、……無謀さ」であり、防御策は「恐怖に訴えるポスターキャンペーン、報酬と処罰、不安全行為の取り締まり、手順書の増補、および訓練と選別」となる。

②工学モデル。人間は制御器のひとつであるとみなされ、ヒューマンエラーは、人間と機械の不適合、あるいは貧弱なヒューマンエンジニアリングにより生じるものだと思なされる。したがって解決策は、人間の認知的特性の長所や短所をより適切に考慮することにある。

③組織モデル。ヒューマンエラーを原因としてよりも結果として見ている。エラーは組

²⁵ 爆発事故を起こしたスペースシャトルチャレンジャー号の打ち上げ決定に関しても、経営陣と技術者との倫理的対立の構図が鮮明にでている。Ch・E・ハリス、M・S・プリチャード、M・J・ラビンス、日本技術士会訳編、『第2版科学技術者の倫理 その考え方と事例』、東京：丸善、2002年、215頁以降。J・リーズンは、経営者側の決定を非難する一般的な見方とは異なる見方をしている。打ち上げの決定という最終局面だけを取り出すとそうなるが、潜在的に NASA の「日常化された逸脱」があり、打ち上げの決定もこの脈絡に収まるという見方をも示している。外部からは無謀なリスクを犯しているように見える行為も、内部的にはそれが仕事上当然のものだと意識されてしまっているのである。J・リーズン、『組織事故』、東京：日科技連出版社、1999年、222頁以降。

²⁶ J・リーズン、前掲書、319頁以降による。

組織のどこかに潜在的原因があることを示す徴候に他ならない。したがって、「安全健全性維持のための事前対策、及びシステムの基本プロセスの継続的な再編が必要であること」が強調される。②のモデルも、このモデルによって補完されなくてはならない場合も多い。なぜなら、誤った経営判断などによって不適切なヒューマンエンジニアリングが採用されている場合があるからある。

事故の影響が個人レベルに収まる事故（個人事故）と、その影響が組織全体および組織外に及ぶ事故（組織事故）では、その影響は組織事故のほうがはるかに大きい。昨今の JOC 臨界事故、雪印乳業、東京電力などの事件は組織事故の典型であり、上で見たみずほの事件もそうある。

③のアプローチが必要とされるのは、しばしば指摘されるように、刑事責任の追及は、誰が責任を取るかを確定することに動機づけられているし、それゆえどこかで因果関係の連鎖を収束させようとしてしまうからでもある。そして事故を結果から見てその因果関係が見通されたとき、個人の行動はたやすく変えることができるもののように見えてしまう。もしあのときあの人がああしていなかったとしたら、その事故は防げたであろう、その人は別の行動を取るべきであった、と。たしかに因果連鎖のなかに立つ個人が別様に行動すれば、事故を防げたかもしれない。しかし組織事故の原因の真の追求にはならない。これは、結果から考える思考法であり、そうではなくて、そもそもなぜ別様に行動できなかったのかに焦点を当てなくてはならない。組織事故は、組織体制に潜在する欠陥が引き起こしたものであるがゆえに、ただ責任者を同定し処罰を与えることで一応の満足を見ることはできず、さらになぜさまざまな防御機構がありながらも事故に至ったのかを考えなくてはならない。

もちろん個人の技術知識の欠如や注意力散漫といったことが原因となって引き起こされる事故は非常に多い。しかし個人が十分な技術知識をもち注意力・集中力もあり仕事に対して前向きで真剣な場合でも、事故が生じる場合がある。それが②や③のモデルに合致する事故の怖さである。

①のアプローチが通用する領域では、技術者は、公衆の安全などを最優先にし、公的な発言において客観的であり、雇用者や依頼人のために誠実であり、行為において欺瞞的でないことが求められる。これは、たとえば NSPE の倫理規程²⁷などの基調となっている人間像である。その実現に良心的に努力することが極めて重要であることに疑いはない。

²⁷ 「全米プロフェッショナル・エンジニア協会 (NSPE)、技術者のための倫理規程」
<http://www.nspe.org/ethics/eh1-code.asp>

②や③のレベルでは、そのような自由が制約されている。この制約は、③に限って言えば、技術者を取り巻く組織的状况に他ならない。組織の問題というとき、それは大きく分けると三つの側面をもつと思われる。ひとつは、組織内部の問題であり、経営者と技術者（あるいは他の従業員）に関わる。もうひとつは、ひとつの組織内部での各部門の関係、競争しあう企業同士、親会社と子会社等の関係に関わる。最後にそれは、監督官庁などの機関や議会、そして非政府組織、広くは世論などに関わり、組織を外部から何らかのかたちで規制しようとするものに関わる。

ここでは組織内部の問題にかぎって考えてみる²⁸。そこには技術者にとってどのような制約があるだろうか。経営者はつねに有限の資源のなかで、企業の存続と利潤の追求のためにプロジェクトを進めざるを得ない。資源には、時間（納期）、資金、人員などが含まれる。技術者は、意思決定の遅れや変更による混乱、納期短縮、人員不足、人員の配置ミスなどにさらされる。これらは製品の品質や安全性・信頼性に関わる制約であり、技術者はそれに打ち勝って倫理を実現しなくてはならない。技術者は、正当な労働条件の範囲外であっても、組織上の制約に耐えながら働かざるを得ないことも多い。このような制約が市場圧力などにより急激に悪化したり、悪い状態が常態化したりすると、組織事故の可能性が高まる²⁹。

このような技術者をとりまく組織上の制約のほかに、従業員としての存在自体を脅かす潜在的な制約もある。それは、解雇、減俸、昇給や昇進の見送り、畑違いの仕事、重要なプロジェクトからの締め出しなどである。これは常態として顕在化するような制約ではない。上司や経営者に倫理的に対立する場合、あるいは会社への忠誠を疑われるような場合に、技術者はこのような制約を意識しはじめ、それによって仕事上のリスクに無関心になり倫理を実現することを放棄する場合も出てくる。そのような状態が放置されれば、組織事故の可能性は高まる。

これらの制約を念頭におくとき、技術者が倫理を実現する自由度は制約の強さによって変化すると考えられる。組織事故の場合、あらゆる場合に技術者個人に原因を求めるという極端をとることと同様に、すべてを組織的制約の劣悪さに還元するという極端をとることが適切でないことは、言うまでもない。組織事故においては、技術者が特定の制約のも

²⁸ ここでは、組織の問題を技術者と経営者との関係を軸に取り出しているのので、組織における他の従業員の問題には立ち入れない。

²⁹ これは資源の欠如の問題であり、ドライデン市営空港近郊でのオンタリオ航空機墜落事故などにおける事故原因として特徴的であったものである。J・リーズン、前掲書、231頁。

とで自由に判断し行動を選択できたのか、より正確に言えば、判断や行動の自由度³⁰は十分であったのかが、技術者の倫理を測るために重要なポイントになる。

なるほど、技術者がいかなる状況下であろうと、NSPE や CSDP が公表するように、プロジェクトにおいて技術的に達成できないことがあれば雇用者にその旨助言するのが、義務である³¹。しかし現実問題としては、その義務の実現が重要になる。このような義務の実現の実在的条件³²が整っていなければ、義務は絵に描いた餅になってしまう。極めて有徳で勇気のある技術者であれば、いかなる状況下であろうと果たされるべき義務を果たすことができるかもしれない。しかし社会にとって重要なのは、平均的に有徳で勇気がある技術者が義務を実現できることである。そのためには、義務が実現しやすい条件を整えることが重要になる。これは企業にとっては、企業活動の適正化であり、企業体制の改善を意味する。

次章では、技術者と経営者の成熟した組織的関係を考えるために、ソフトウェア開発の管理手法に目を向ける。それによって、両者の組織的関係の改善が目指されていることを確認したうえで、内部告発の必要性和それを避けうる組織を考える。

III 組織の成熟と企業倫理の確立

技術者の行動を左右する組織的要因を見直し、企業活動全体を見直す動きは実際に強まっており、みずほの例に対する反省からも、プロジェクトマネジメントの遂行は経営上死活問題であるという認識が広まっている。プロジェクトマネジメントは、あるプロジェクトの達成にいたる、企業内の様々なプロセスを調整し管理し、そのなかで適正な組織関係を目指しているが、同時に安全管理の実現にも寄与すると考えられている³³。

ソフトウェア業界では、成果物としての製品だけではなく、ソフトウェアの開発プロセスに注目してそれを評価しようとする手法、ソフトウェアプロセスアセスメント(SPA)を

³⁰ 自由が存在するかどうかという存在論として重要な問題はここでは棚上げされている。ともかくもある行為の非難可能性がどの程度成立するかどうかを念頭においている。

³¹ NSPE の倫理規程、III 1.b., <http://www.nspe.org/ethics/eh1-code.asp>、およびアメリカ電気学会(IEEE) コンピュータ学会による、ソフトウェア開発専門技術者保証(CSDP)プログラムが公表する「ソフトウェア工学における倫理規程と専門的実務」、2.06, <http://computer.org/certification/ethics.htm>。

³² 単なる形式的な条件と区別して、実際に何かが起こりうる条件を、ヘーゲルは「実在的可能性」として明らかにしている。G. W. F. Hegel, *Gesammelte Werke*, Bd.11. 385ff.

³³ J・リーズン、前掲書、324頁。

取り入れようとする動きが高まっている³⁴。こうした手法によってソフトウェア開発プロセスを管理することにより、内部評価および外部評価の指標を与え、内部的にはソフトウェア品質の改善に、外部的には受注側の信用度をあげようとするわけである³⁵。

プロジェクトマネジメントは、SPA にも組み込まれている。旧来のプロジェクトマネジメントの対象となるのは、品質、コスト、納期の3つであった。製品を管理対象とする QC(Quality Control)や生産プロセスを管理対象とする TQC(Total Quality Control)という手法が確立してきた。さらに経営の質を管理対象としてその向上を図り、企業全体の質の向上を目指す TQM(Total Quality Management)³⁶が考え出された。この TQM の影響を強く受けた、新しいプロジェクトマネジメントは、「各プロジェクトはもちろんのこと、経営までも巻き込んだ、組織全体のマネジメントとの整合性も持たせた」ものであり、モダンプロジェクトマネジメントと呼ばれる³⁷。

これらの手法の特徴は、(1)管理対象が製品・サービスからむしろプロセスへ移り、(2)納期、コスト、品質のみならず組織、リスク、コミュニケーションなどを含めた統合的な質を評価し、(3)各プロセスを継続的に改善し、(4)製品と技術者の国際的な往来に対応すべく、手法を国際的に通用するものにすること、にあると言われる³⁸。結果からプロセスへの重点が移り、さらにプロセス全体を管理すること、言い換えれば企業活動全体の質の管理が重視されてきたわけである。

SPA は、そのプロセスの一部にプロジェクトマネジメントを取り込むことによって、しっかりした品質管理・継続的改善を目指そうとする³⁹。とりわけソフトウェアは、I 節で

³⁴ 開発プロセスに注目する評価手法は、SPA(Software Process Assessment)と呼ばれる。CMM (Capability Maturity Model)や、ISO/IEC TR 15504およびそれを元にした SPICE (Software Process Improvement and Capability dEtermination)が代表的手法である。それぞれ、

<http://www.sei.cmu.edu/cmmi/>、<http://www.sqi.gu.edu.au/spice/>を参照。

³⁵ たとえばこれによってソフトウェアの政府調達にも役立てようというわけである。情報政策に関わるパブリックコメント募集に付された資料を参照。

<http://www.meti.go.jp/feedback/downloadfiles/i10626bj.pdf>;

<http://www.meti.go.jp/feedback/downloadfiles/i10626cj.pdf>;

<http://www.meti.go.jp/feedback/downloadfiles/i11226bj.pdf>

³⁶ たとえば、<http://www.juse.or.jp/>にある、日科技連の定義も参照。

³⁷ その集大成とも言うべきものが、PMI (The Project Management Institute) が発行している PMBOK(Project Management Body of Knowledge)である。

³⁸ 足立芳寛編著、『ソフトウェア品質管理のためのプロジェクトマネジメント』、東京：オーム社、2002年、23頁以降。

³⁹ プロセスの重点をはっきりさせ各プロセスの定義を行うなどして、プロジェクトのプロセスを改善する、プロセスマネジメントもまたソフトウェアアセスメントの重要な要素であり、SPA に含ま

見たように、目に見えず、各プログラマーの進捗状況を把握し他の作業とコーディネートすることが基本的に易しくなく、品質が各人の技能に大きく依存するため、開発プロセス（たとえば、要件を決定する、計画を立てる、設計する、プログラムを書く、など）に注目して管理し評価することが重要になる⁴⁰。

プロセスを継続的に管理してゆくという、手法上の特徴は、事故や事件の発生を継続的に減らすという企業全体の目的にも合致する。結果のみに注目しても組織的な改善策は出てこない。完全に事故をなくすという、達成が極めて困難な目標を設定するのではなく、むしろ組織活動の様々なプロセスの健全性を定期的にチェックすることが最善である⁴¹。

SPA は、工学的信頼性と安全性を達成する優れた手法であろう。これによって、みずほの場合でも、経営上の意思決定の重要性がつねに意識され、それにともなう合理的な資源配分がなされれば、技術者が開発に専念できる条件が整い、彼らの倫理の実現の制約は低減されたであろう。大きな障害を除去できる可能性も高まり、先に見た銀行の統合プロジェクトは成功の確率はずっと高くなっていたであろう。

したがってこのような手法は、公衆の安全やその他の利害を守ることにつながり、企業倫理を実現する実質的な方法論であると見なすことができる⁴²。企業倫理を基礎づけるビジネス倫理学は、80年代中頃ようやくひとつの学問としての体裁をとったと言われる。利益の最大化こそが企業の唯一の目標であり、株主（ストックホルダー）に対する義務であるとする、通念とも言える見解に対して、ビジネス倫理学は、企業の利益追求を否定しはしないが、その追求のあり方を考えるのである。つまり企業は、株主のみならず、技術者を含む従業員、顧客、メディア、地域共同体、一般大衆などをステークホルダー（利害関係者）と見なし、各ステークホルダーの権利あるいは利害を調整する役割を果たさなくてはならないのである⁴³。

れている。

⁴⁰ 足立芳寛編著、前掲書。

⁴¹ J・リーズン、前掲書、162頁。

⁴² ここでさらに立ち入ることはしないが、技術者の労働者としての権利や人間としての基本的権利を守るとは、企業が果たすべき何よりも重要な倫理である。それが守られていなければ、技術者がみずからの倫理を実現することは著しく困難になるであろう。

⁴³ 宮坂純一、『ビジネス倫理学の展開』、京都：晃洋書房、1999年がとても参考になった。現在のビジネス倫理学においては、代表的な論者の間でも、株主に対する企業の受託義務の扱いに違いが見られ、企業が果たすべき倫理的要請内容も一致を見ていない。また企業を道徳的主体と見なせるかどうか、見なすとすればどのような意味でかという点も決着を見ていない。さらに90年代になって、ビジネス倫理はもう十分だという批判も現れ、規範的アプローチと実証的アプローチの対立や統合も重要な争点になっている。ビジネス倫理に関する有益な情報は、<http://www2.justnet.ne.jp/~juka/>か

このようにビジネス倫理から見た企業目的の中心には、法律や倫理的慣習に従うことと利潤を追求することとのバランスをどう考えるかという問題がある。もちろん SPA のような管理手法を導入したからといって、それが既成化し形骸化する恐れはつねにある。企業組織は活動体なのであり、ある管理規格に合格したからといってその規格に見合った活動がつねに行われるとは限らず、重大な帰結を招く可能性もある。またプロセスを定量化し評価することで満足してしまう可能性もある。

したがって、内部告発にいたる可能性を完全に排除することはできない。組織内部の悪循環を断ち組織を倫理的に健全化するためには、ひとつには制度構築が求められることになる。組織上のフェールセーフとして倫理委員会や企業倫理ホットラインやなどの制度を設けることにより、組織内部での議論を尽くした解決が促進されると期待される。そしてその担当者には大きな独立の権限が与えられていなくてはならない⁴⁴。また倫理的な訓練プログラムを継続的に実施することも期待される。これらによって体外的に企業の倫理的健全性を示すことができるであろう。

しかしここにも企業倫理の形骸化の危険性はある。たとえば、「企業倫理に関する社内の教育研修体制が重要である。何か問題がおきたときに、きちんと社内研修をやっていたことで会社の責任が軽減されるといった判例も出てきている」⁴⁵と言われる。このように倫理を手段化すること自体、反倫理的であると思われる。

さらに、企業組織全体の意識改革も重要である。まずトップが倫理に対して真剣であることを示すことである。単に訓示を垂れるだけでは効果がない⁴⁶。経営者が倫理に真剣であり、倫理的な言葉に敏感でなければ、技術者もそうではなくなりがちだからである。倫理を推進するにあたって、違反に際して罰則を課すということを前面に押し出すと、それは失敗に終わると指摘されている⁴⁷。これは直観的にも非常に納得のいくものである。倫理の教育が倫理の強制のように見えることも多い。逆に技術者も、どうせ何を言っても無駄であるという、いわば学習された無力感をなくしていかななくてはならない。

安全性や信頼性を確保するための技術上の要請と経営上の要請との対立は、組織内部で

らも得られる。さらに、高巖、T・ドナルドソン、『ビジネスエシックス 企業の市場競争力と倫理法例遵守マネジメント・システム』、東京：文真堂、1999年が、日本企業の具体的な分析を取り入れた議論を展開している。

⁴⁴ 高・ドナルドソン、前掲書、350頁。

⁴⁵ 「国民生活審議会消費者政策部会自主行動基準検討委員会(第15回)議事要旨(2002. 10. 25)」、<http://www.consumer.go.jp/>

⁴⁶ 高・ドナルドソン、前掲書、344以降。

⁴⁷ R・シンジンガー／M・W・マーティン、前掲書、37頁以降。

解決することが望ましいが、それでも外部への内部告発の必要性も出てこざるを得ない。組織内の倫理ホットラインなどが機能していない場合には、第三者機関（弁護士、支援団体など）に届けられることが必要であろう。このように本当に信頼がおけるかどうかという疑念が残らざるを得ないとすれば、あるいはそのような制度を設けるほど組織が大きくない場合にも、よく言われるように第三者機関による支援が必要となるであろう⁴⁸。さらに内部告発者の法的保護も早急に進められなくてはならない。告発者が抱えるリスクあるいは不利益を減らすようにしないと、正直者がばかを見ることになってしまう。

内部告発⁴⁹はあくまで最終手段であり、企業の常態においては正規ルートでのコミュニケーションをうまくとることを目指すべきであることは言うまでもない。経営者と技術者との関係を軸として組織の健全性をみれば、よい協働の大きな要因の一つは、経営上の要請と技術上の要請とをうまくバランスを取るところにある。

制度には形骸化の危険性がつねに伴うから、社会制度上のフェールセーフ機構を無際限につくらないためには、最終的には、経営者や技術者が、たえず注意を怠らず状況認識を行い、倫理的判断および倫理的反省能力を働かせつづけることが求められる。制度を生かすのは、各人の倫理への真摯さ以外にはないであろうからである。

さて、ここで気づかれるのは、技術者の内部告発の倫理的正当性や、第三者機関による内部告発者の支援・保護は、工学倫理的アプローチからでてくるが、これに対して、倫理委員会や倫理ホットラインといった制度を企業内に設置することは、企業倫理的アプローチ、したがってビジネス倫理的アプローチから出ている、という点である。さらに、そもそも企業内プロジェクトマネジメントを推進するのは経営者の側から出てくるものであり、ビジネス倫理的アプローチから出てくるものである。

IV 結論——工学倫理とビジネス倫理の相互補完

工学倫理は、個々の技術者が会社への忠誠や公衆の安全を心がけ、製品の信頼性と安全性の保証に努めることを求めるものであった。しかし組織における技術者は、さまざまな制約のもとで働かなくてはならないがゆえに、安全性や信頼性をみだせない選択を習慣的

⁴⁸ 実際に弁護士らの活動が始まり、その成果が期待されている。たとえば公益通報支援センター。
<http://www006.upp.so-net.ne.jp/pisa/index.html>

⁴⁹ 内部告発そのものは、技術者の倫理にのみ関わる問題ではなく、経理や人事担当者など、他の組織成員の倫理にも関わるが、ここでは考察されない。内部告発が許容される基準やそのために考慮すべき事柄についても立ち入らないが、Ch・E・ハリス、M・S・プリチャード、M・J・ラビンス、前掲書、223頁以降などを参照。内部告発が義務であるかどうかという論点についても同様。

にしましめていたり、またやむなくとらざるをえなくなったり、逆に内部告発せざるを得なくなる場合もある。そこに組織のなかにおかれた技術者が陥った悪循環や倫理的葛藤を見た。他方、製品品質のみならず経営組織の質が重視されてきた昨近では、経営者が技術者の労働上の制約を改善し、技術者に対する甘えという組織的悪循環をいかに乗り越えていくかが、企業組織の健全化にとって重要な要素となっている。

そのためには、経営者側と技術者側が有効なコミュニケーションを行い相互の信頼関係を築くことである。健全で機能する組織では、各人が他者の役割を理解しているのと同時に自分が何を求められているかをよく理解していると言われる。それは以心伝心ではなく、言葉を用いた学習と訓練によって獲得されるものである。

技術者にとって、技術知識や技能のみならず、コミュニケーション能力を高めることが重要になる⁵⁰。とりわけ技術的な事柄を経営者に分かることばで説明する能力が求められる。技術者が経営者をうまく説得する技術も求められる。とくに上級の技術者は経営上の問題を知っておくことが重要となる。技術者が技術的な事柄にのみ携わっていることはできず、企業の活動プロセスでは経営的な事柄に無関心でいることはできない。特にソフトウェア開発の領域では、技術上の提案が経営改善に有効であることが多い⁵¹。

経営者の側でも、技術的な事柄が経営上の決定に大きな比重をもつ場合には、技術者の意見を率直に反映させるべきである。その際、意見をただ形式的に求めているのではなく、率直な意見を求めているのだということを、技術者に理解してもらえるような態度でつねに接するべきであろう。コミュニケーションに対する信頼性は継続的なやり取りのなかで培われるものであり、一朝一夕に獲得されるものではない⁵²。

もしこのような健全な組織性が維持されているなら、そこでは工学倫理と企業倫理とが相互に補完しあうことが実現されていると言えよう。人間は倫理的に完全ではありえないけれども、そうだからこそ工学倫理と企業倫理とが相互に補完しあうかたちで、技術者の役割と経営者の役割をともに果たせる企業組織を維持していかななくてはならない。

そのためにはさらに、企業組織内部にとどまらず、社会全体で安全文化に対する意識を高め基本的な考え方を共有することもまた大切である。なぜなら、技術者にせよ企業にせ

⁵⁰ コミュニケーション能力は、文化や習慣に大きく影響されるものでもあるから、例えば小中高という教育のなかでもうまく動機づけされ、その能力が磨かれるようにしていかなければならない。そのためには一学級の人数を減らすことが死活的な条件であると言えよう。現状では物理的な制約が大きすぎ、各生徒が発言できる自由度はそもそも高くない。

⁵¹ ソフトウェア開発では技術者相互の間のコミュニケーションも非常に重要視されている。

⁵² 安全文化にとって組織内での情報システムの構築が重要であることを強調するのは、J・リーズンである。前掲書、276頁以降。

よ、安全性や信頼性に対するインセンティブを保ちうるのは、社会がそれをどう見なすかにも大きく依存するからである。OECD のセキュリティガイドライン(2002)には、安全文化(Culture of Security)の概念⁵³が導入され、すべての情報システムへの参与者（個人ユーザーから企業や他の組織そして政府にいたるまで）が果たす役割が強調されている。つまり企業倫理的に言えば、こうしたすべてのステークホルダーが安全文化への参与者でなくてはならないのである。

⁵³ 1988年、国際原子力機関(IAEA)が安全文化の考えを詳細に述べた報告書を出版したことにより正式に認知されたとされる。