＜特集＞

国際安全規格から見た最近の重大事故

ー事後から事前へー

清水久二

横浜国大名誉教授(〒241-0817 横浜市旭区今宿 1-10-9 Fax:045-362-5041)

概 要

化学プラントや設備類の安全管理の基礎となる最近の国際安全規格の動向について解説。更にこれをベースに国内での重大鉄道災害を分析し日本型安全管理の問題点を論じた。

キーワード:国際安全規格、IEC61508,IEC61511,鉄道災害、事前予防

1. 国際安全規格の動向

1.1 日本の安全管理方式の遅れ

安全機能(Safety function)を用いて安全性を高める、というこの国際安全規格の考え方は我が国では普及が非常に遅れており、むしろ中国やインドの方が導入が進んでいると言っても過言ではない。

その理由は日本の伝統的安全管理の方式が、人的過誤や失敗を抑えることに防止の主眼が置かれており、メディアもその様な路線で報道するために、安全管理の方式が一向に現代化しない、という事に起因している。

更に統計・確率論をベースにしたリスク分析の概念や手法も学校教育で教えられていない為に、知識レベルの高い技術者でも安全管理の為に何をなすべきか、について良く理解していない、という点も挙げられる。更に現在の学校のカリキュラムも伝統的な教科で満杯状態であり、統計・確率までは手が回らないということも災いしている。

1.2 先進諸国における安全管理の動向

欧米ではチェルノヴィルの事故(原発の爆発事故)以来、安全管理に関する法規類は劇的に変わった。特にドイツのライン川やドナウ川周辺の工業地帯では土壌汚染や大気汚染の拡大が明確になり、プラント側は住民の厳しい監視を受けており、安全法規も変わらざるを得なかった。1970年代の米国でも、例えばヒューストンの代表的な石油コンビナートにおいて、当時安全管理といえば騒音対策や衛生対策で、少人数の担当者がサイト内を巡回しているだけだった。管理の対象はあくまでも人であった。80 年代になると専門の安全技術の担当部門を設置し、管理の対象は人から技術へと移行した。

90 年代以降は全米において安全解析の専門家を増やし、全てのプラントにおいて技術的な安全対策を実施することになった。特に環境汚染と安全管理とは密接な関係があるとして、OSHA(労働安全衛生庁)と EPA(環境庁)双方の視点が融合した安全管理を行うような指導が行われている。加えて欧米では損害保険の活用が非常に活発であり、その面からも安全法規の現代化が急速に進行した。

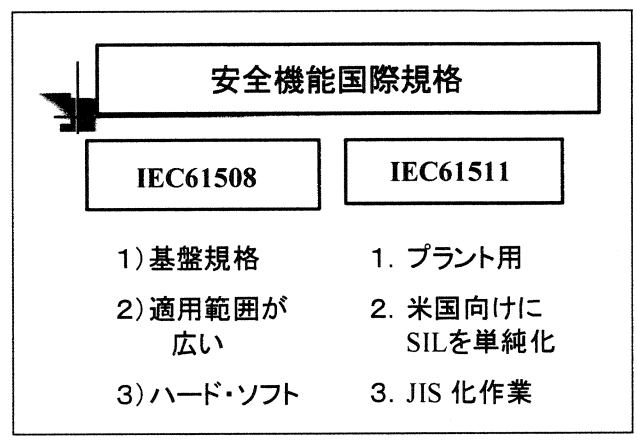

Fig. 1 国際安全規格の構成

1.3 「安全機能」規格の特徴

セベソ指令以降、EU の安全管理は規範遵守型からリスク低減型へ以降した。その後全てのプラント、機器類は安全の仕組み(safety task)が組み込まれていることになる。IEC61508 はその「安全の仕組み(安全機能)」の性能がどうあるべきかを規定している(Fig. 1) 。我が国の行政法には(一部を除いて)この様なコンセプトは目下のところ存在しない。

しかしこのコンセプトは非常に普遍的でその適用範囲は化学プラントは元より、宇宙・航空、海洋、陸上輸送、原発、炭鉱、医療技術へと全ての技術に対しても適用可能である。また技術のみならず人的組織の信頼性についても適用可能と思われる。

上記の安全機能の信頼性は防護しようとするプラント・機器の危険性に見合ったものでなければならない。その当該プラントの危険性として IEC61508 はグローバルリス

クを規範とすることを推奨している。安全系はこのリスク値を下げるのに十分な信頼性を備えることが設置の条件になるから、安全設計の目標は明確になり、技術開発が促進されることになる。

実際欧州のオランダ、ドイツ、英国を中心に安全装置の専門メーカが育っており、その技術を認定する第3者機関も活躍している。この様な制度が不慮の事故のみならず、環境汚染をも全体的に減らしていくように機能することは明らかである。日本の過失責任主義では全て後追いで対処することになるから、国民の不安は一向に減らない。

またこの規格ではコンピュータのソフトウエアを検査する方式も規定しているから、次の世紀の批判にも十分耐えうる国際安全規格を目指していることになる。

2. 事後から事前へ

株式市場等の世界は事実に対する思惑により支配される。普通、思惑で買って事実で売るのが常道であり得策である。何故なら、事実からは何も生まれない。これは賭博的な市場のみの特徴であろうか？

我が国では公害や環境問題が起こる度に、その原因である事実が重視され、それが判るまでは誰も動けない。従来の公害体験（水俣、アスベスト事件）では累々と死体が横たわる段階になって、漸く「あの災害の原因はこの事実であった」と学会（医学界）も裁判所もやっと重い腰を上げるのである。それは全て後日談である。狡猾な政治家はこのトリックを良く知っており、官僚的な学会や裁判所決定を待つと言いながら、何もしないで時を稼いでいる。今後、安全・環境・公害の分野で再発を防止するには仮説の段階で何らかの強制処置を発動できる法制を確立しなければならない。さもなければ同じことが再び延々と続くことになる。

ところで EUの**セベソ指令**はこの危険性（一種の仮説）を管理し制御する方策を法制化するように加盟各国に求めた憲法である。以後全ての安全・環境法規はこれをベースにしている。

我が国がこの仕組みを直感的に理解できないのは、国民の民度というよりは専門知識への過度な評価という時代の風潮であるまいか。それにしても私達の子孫が理由もなく癌で夭折するのはご免蒙りたい。

ところで原理的に確率で表現される思惑（仮説）と、同じく確率で表される結果との間には**ベイズ確率**と呼ばれる関係定理がある。ここで思惑とはリスク頻度の事である。この学説は**古典確率論**とは世界観が異なり、両者との間には永年の論争があった。しかしフランスではベイズ確率論の産業的応用は非常に成果を挙げており、今やその原理を疑う人はいない。英国でもベイズ確率は工業規格に採用されている。一方日本では古典確率論が優勢で、ベイズ理論とその応用は大学においても殆ど教授されていない。

ベイズ確率論の優れている点は災害事例が少なくても、実時間的（遅れなし）に仮説を更新し、必要な処置がとれる点である。更に最小自乗推定法や繰り返し演算法と組み合わせば「**事実よりも早く正確に**」真実に肉薄することが出来る。宇宙の慣性誘導技術にはこの手法が採用されており、また国内でも鉄鋼各社が設備診断に応用し多大の成果を挙げている。

3. 最近の重大事故

3.1 事故は人の業か神の業か？

鉄道事故であれ、航空機事故であれ、それらは何れも最先端技術を駆使して建設し、運行されているのだから、それらが安全でないのは人間の能力不足が原因である、という通説は相当根深くこの国に行き渡っている。さらにその技術欠陥は事故によって初めて顕わになるのだから、徹底的な調査によって究明し、それを修復すれば再び安全が確保されるであろう、という主張も尤もである。

とりわけ、通常は存在しない欠陥が生じるのは、多くの場合不確かな人間が介在するためであり、その意味で災害は「人間の業」以外の何物でもない、という学説は今日極めて支配的である。

しかし、筆者がこれまで3回視察団を組織し、欧米の化学プラント関連企業（損保や第 3 者検査機関等々）の安全・環境問題に対する姿勢を調査した限りでは、その「人の業」説は徐々に「災害は自然の理」という説に傾いている様に見受けられる。つまり災害は必然であるという仮定のもとに技術システムの危険源を洗い出し、常にそれを補完して行こうとする姿勢へ移行している。

この「自然の理（神の業）」のコンセプトは第 2 次大戦中のドイツの V2 等ロケットの開発経験に遡ることが出来る。筆者自身は専門外であるが、ある筋から提供された資料によれば V2 ロケットは試射と実射と含め通算数千回（一説では 4000 回近く）打ち上げられたが、その成功率は概ね 60%を超えることは無かったという。

普通、開発とは「実験と事故研究、修正」の繰り返しであって、失敗の後には不具合は徹底的に調査され修復される。ドイツ人の性格は思えばこれは徹底的に行われたに違いない。しかしそれでも成功率が 0.6（≒0.63）を超えられなかったというのは興味深い。何故ならこの数値は黄金分割比（フィボナッチ数等）に関わる自然界固有の数である。それは人間が作りだした数ではない。市場経済に携わっている方には釈迦に説法だが、例えば外国為替の市場において相場が崩れた場合の自立反発の限界は最高値の 0.63 を超える事はない。これは世界的にも公知の事実だが数理的には説明がつかない。この数は自然科学の分野にも多く現われるが（付録参照）、例えば何故光

速とフィボナッチ数と関係があるのか、という問いは神様に聞いて見なければ判らない。結論的にいえば、巨大輸送システムであれ、原発であれ、ある技術システムが自然崩壊してゆくプロセスは必然であり、人は偶々そこに居合わせただけであると考える事も出来る。従って特別の冗長系(並列系)が組み込まれていない限り、個別の修復作業ではその回復率は高々当初設計目標の 63%に止まり、危険性の自然増大を止める事はできない、という推測が成り立つ。ところで英国は蒸気機関による産業革命を生み出した国である。従って工業の何たるかを熟知している。その国が提唱する国際安全規格の精神は工業の後発国日本の思いを遥かに超えている。そこで国際規格から今回の脱線事故を解釈するとどうなるかを敢えて挑戦した。

3.2 失敗の教訓が新たな失敗を生む

さて、福知山線脱線事故を機に、当事者である JR 西日本の首脳陣が、信楽高原鉄道事故(1991 年 5 月)にも関わっていた事を知り、早速当時の記録を調べてみた。事故の状況[1]や 裁判の記録[2]は既にサイトで公開されている。筆者はそれらを丹念に読んでみた。そして思わず溜息と共に表記の感想が出た。何故経験から学べないのか、それは危険の本質に対する理解が一向に進歩していない、つまりは安全研究が全く行われていないからである。

事故原因の概略を説明する前に「事故の真の原因は何か」という問いかけに対する典型的な二つの学説を紹介しておこう。それは上に述べた通り人的過誤学説と危険源学説[3](何れも仮称)である(かなり粗雑な分類であるが)。何れの学説においても事実は一つの筈だ、という疑問が湧くが、しかし事実は常に絶対事実一つではない。地上における事実の発見(帰納法)はモデルとしての学説(演繹法)の支配下にあり、無色透明な事実は学説に因って色付けされる[4]。

(a) 人的過誤学説:

鉄道であれ、航空であれ、定常的な運行からの逸脱、つまり異常事態の発生は別に珍しいことではない。全体の異常はその部分(要素)の逸脱から始まるが、ここで運行という一つのミッション(業務の目標)は各要素機能(ハードとソフトの要素)が直列構造によって模式化されると考える。各要素が正常状態から逸脱し、機能を喪失するのはハードであれば故障・誤動作であり、ソフトの代表は人的過誤である。さらにこの方法論では「技術を過信するな」という定説が流布しており、安全対策も人間の認識と判断能力に依存する。

(b) 危険源学説

これに対して本学説では全体の損害統計から(演繹的に)当該技術の危険性を推定する。つまり何処でも何時でも一度あることは又起こるのである。その危険性に対して並列的に安全対策を設置する(鉄道では ATS のような装置)。

3.3 安全対策のレベル(階層)

安全対策は損害を低減するための人の営為であるが、その性質から見て大きく 2 種類のレベルに分類される。これを仮に第 1 種、第 2 種の安全対策と呼ぶことにする。正式の呼び名がないのは、安全とは民族興亡の歴史と深く関係し、近代科学の安易なアプローチを排除してきたためであろう。

ところで「第 1 種」とはいわば安全を「有用性(アベイラビリティ)」と呼び替えた対策である。例えば飛行機のエンジンが不調を来たした時、操縦士は何とか機器を騙して近くの飛行場に着陸させようとする。その動機は勿論社会的価値(特に経済性)である。また船が浸水を始めたとき、船体と貨物、乗客を救うための努力もこれに相当する。その危険か安全か、のきわどい判断基準は同じ価値にある。これは化学プラントや原発においても同様である。

これに対して「第 2 種の安全対策」とは、上の全ての有用性を排除し、自分を含めた人命を救うため、プラント(テクノロジー)を直ちに停止或いはその危険場所から急いで離れる行為である。飛行機でいえば操縦士は落下傘で機外へ脱出する、或いは船舶では救命ボートに移乗する。ここでの判断基準は「天(神)対自分」であって、社会は入ってこない。絶体絶命の窮余の処置が人には許される。これは人間の特権であって、本稿では一時的に「安全ストップ(安全特権[5])」と呼称する。つまり危険性を有する先進技術に従事する人間には、常に自分で自分を救う権利が認められており、航空機で言えば機外脱出に地上の許可は必要ない。具体的にはこれは緊急停止・脱出等の総称である。

第 2 種は最後の手段であるだけに、その信頼性は地上で実現しうる最高の水準でなければならない。欧米の宇宙訓練設備を見学するとこの安全ストップに対する配慮が実に行き届いており、逆に日本ではそのレベルは非常に低い。

3.4 信楽高原鉄道の事故分析

42 人が死んだこの事件では幾つかの不幸な偶然が重なった。しかし第 2 種の安全対策(安全ストップ)がある限り、列車というものはそう簡単に衝突するものではない。当時の信号系統において第 2 種の安全対策は下りの列車をストップさせる「誤出発検出装置」であったが、この辺りの JR 側と私鉄側の認識や理解にはかなりの温度差があった。

そもそも、異常な事態が発生すれば、その技術設備の操作担当者はかなり迷うものである。それは日常性から逸脱した状態で、判断の基準を失うからである。間違いなく安全側にとればよいが、下手に輸送を停止させればここでは「上司の叱責と罵声」とが待っていたという。二兎と追うものは一兎をも得ず、で信楽駅の担当者は赤信号でも列車を発車させてしまう。

現在の国際規格によれば、「誤出発検出装置」という安全装置の SIL は最高レベルでの 4 である。これを実現するには担当者の資質や、安全解析の義務付け、第三者の認証が義務付けられている。ところが当時上記装置の変更工事が信号設備会社の部長も知らない内に行われてしまった、という。当然鉄道会社にも知らされていなかった。それが信号の主システムへ予想外の影響を及ぼし、大きな誤動作を誘発した。国際規格[6]では「安全装置は主制御系から完全に独立すべし」と規定しているので、国際規格に従っていればこんな惨劇は起こる筈もない。

3.5 教訓の分析

これだけの死傷者を出したとあれば、裁判において人の過失を明らかにしなければ遺族が納得しない。そこで捜査においても人的過誤説をベースに調べが行われ、逆に安全管理の体制、特に安全ストップを含む信号系の改善と認証については殆ど反省が行われずに今日にいたった。変更工事は近畿運輸局に届け出をすることになっていたが、果たしてリスク解析等の実質的な審査が行われていたが否かは疑問である。得られた教訓は兎に角「ヒューマンエラーだ」という確信であり、これは一種の信仰となって、運転士の過酷な訓練プログラムを生み出した。その反面危険源を洗い出すという本質的な手順は等閑にされた。

20 年前の日航機の事故で 500 人、今回の事故で 100 人という現実を噛み締めれば、次の 10 年で約 300 人程度が不慮の大事故で犠牲になるであろう、というのは合理的な予見である。事故災害の原因の全てが人の業と考えれば「打つ手」は限られてくるであろう。今後は失敗を教訓とせず、国際規格に従って多面的な安全対策を研究して頂きたいと思う。

[参考資料]

(1)http://www.kyoto-np.co.jp/kp/special/shigaraki/shigaraki1.html
(2)http://www.tasksafety.org/shigaraki/
(4)失敗学を批判する:
(http://www.h6.dion.ne.jp/shim-his/sippai.pdf)
(5)運手士は死刑か:
(http://www.h6.dion.ne.jp/shim-his/noda.htm)
(6)IEC61508(JIS C0508),and 61511(2006年9月 JIS化),
福田・清水:機械安全工学、養賢堂,2000

[付録]

1). フィボナッチ数は伊のピサ生まれの数学者フィボナッチが発見した数字で、自然現象の成長、衰退を特徴付ける箇所には必ず出てくるマジック数である。
この数値は自然対数の底 e とも密接な関係があり、

$1-e^{-1} \fallingdotseq 0.6$

である。e も数学史上マジック数と呼ばれ、その由来に筆者の知る限りにおいて定かではない。ある物の本によればフィボナッチの生きた時代に既に使われていたのではないか、という説があるが、そうであれば古代エジプトに遡る。因みに和算の歴史にこの数字が現われることはない。

2). 自動制御系での時定数
周知の如く一次系のステップ入力に対する応答は

$y(s)= 1/(Ts+1) * 1/s$

であるが、値1の入力に対して出力がその 63%に達する時間を時定数 T と称する。入力値に到達するには理論上無限大の時間を要する。

3). 放射能物質の自然崩壊
自然崩壊の方程式は $dm/dt = -\gamma * m$ であり、指数関数に従って崩壊してゆく。この場合の時定数ガンマ$^{-1}$ に対応する量も e が関係してくる。

4). 信頼性理論における指数分布
信頼度が指数関数で表される場合の部材（物質）の故障特性は非常に特徴的であり、空間量が時間量と結び付けられる。つまり部材の消耗、崩壊は波動として捉えることが出来る。

以上述べた様に、何故ここに指数やフォボナッチに関係する数字が出てくるかは数学的には説明する事ができない。その理由を人間は答えられない。