原子力発電：ヒューマンエラー対処への新しい視点

北村　正晴

1. はじめに

「人間は機械でないから常に同じ機能や性能を発揮することは期待できず，時にエラーもおかすことがある」という事実は，少なくともヒューマンファクター研究者レベルでは分野を問わず共通の認識となりつつあろう．しかしその対応策に関しては，いくつかの異なった主張が並立している．まず直接的には，エラーをしがちな人間はなるべく現場から排除して自動化を進めるべきと言う発想は広い範囲に見られるが，そこでは機械による人間の代替，全自動システムの構築が解決策として志向されるわけである．

また別の立場からは，「機械で出来るような定型的作業については，その作業は機械装置に任せて人間側の負担を軽減し，その代わりに状況判断や意思決定などの高度な作業を重点的に担当させるべきである」という主張もしばしばなされる．この方式では人間は，管理者としての役割を期待されるので監視制御（supervisory control）方式[1]とも呼ばれ，人間中心の自動化（human-centered-automation）の実現を通じて人間と機械の役割分担の適正化とエラーの低減[2]が志向される．いずれの方式もそれなりの正当性，有効性がありそうに思われるが，人間と機械の相互作用の実態はそれほど単純明快に割り切れるものではないことが明らかになってきた．原子力発電所や大型航空機に代表されるような，万一の事故の被害が非常に大きくなるため，極めて高い安全性が要求される領域においてはいずれの主張も固有の難問を抱えている．本解説ではまず具体例として参照する原子力発電所の仕組みについて簡単に紹介した後，そのようなエラー低減策の抱える問題点について実態を概説する．そしてそのような困難な課題の解決を目指して現在進展中の，エラーの検知とリカバリーの効率的という観点からのアプローチを紹介する．最後にORの観点から貢献が期待される課題に関しての私見を述べて結びとしたい．

きたむら　まさはる
東北大学　工学研究科
〒980-8579 仙台市青葉区荒巻字青葉

2. 原子力発電所におけるヒューマンエラーの概要

2.1 原子力発電の仕組みと安全技術

代表的な原子力発電所（加圧水型プラント）の大まかな系統図は図1に示すとおりである．簡単にいえば原子炉で発生した熱が高圧水によって蒸気発生器に移送され，ここで蒸気に変換される．この蒸気がタービンを回すことにより発電がなされることは火力発電と同じである．ただし図1は発電のための主要系統図であるが，実際にはこの他に，原子炉の緊急停止装置，冷却が不足になった場合に備えての冷却水注入系などがあり，しかも高信頼化の目的でこれらの系統は複数種類，また同一種類の系統も複数併設されているために，実際の配管系や計装系ははるかに複雑な構造を持つことになる．これらの工夫により高いレベルの安全性が確保されていることは事実であるが，一般には気づかれていない問題も無しとしない．直観的に考えてもシステムを構成する配管系統や機器要素の数が多くなれば，注意深い監視や補修を行うにしてもどこかに故障が起こる可能性は相対的に大きくなる．また対象の状態すべてを一目で認識することが状況によっては困難になることも避けられない．今後何か危惧される問題が認識される都度，その対策のための装置を，十分な事前検討無しで逐次導入するような方式では高いレベルの安全を実演することは困難であることにも注意する必要はあろう．

2.2 安全性の実態

JCOの事故は死者2名を含む大きな影響をもたらしたが，原子力発電がトータルとして高い信頼性，安全性を実現している実態は正しく評価されるべきである．航空，化学工業，建設業などのいずれに比べても，労働災害による死傷者，利用者または公衆の死傷者と

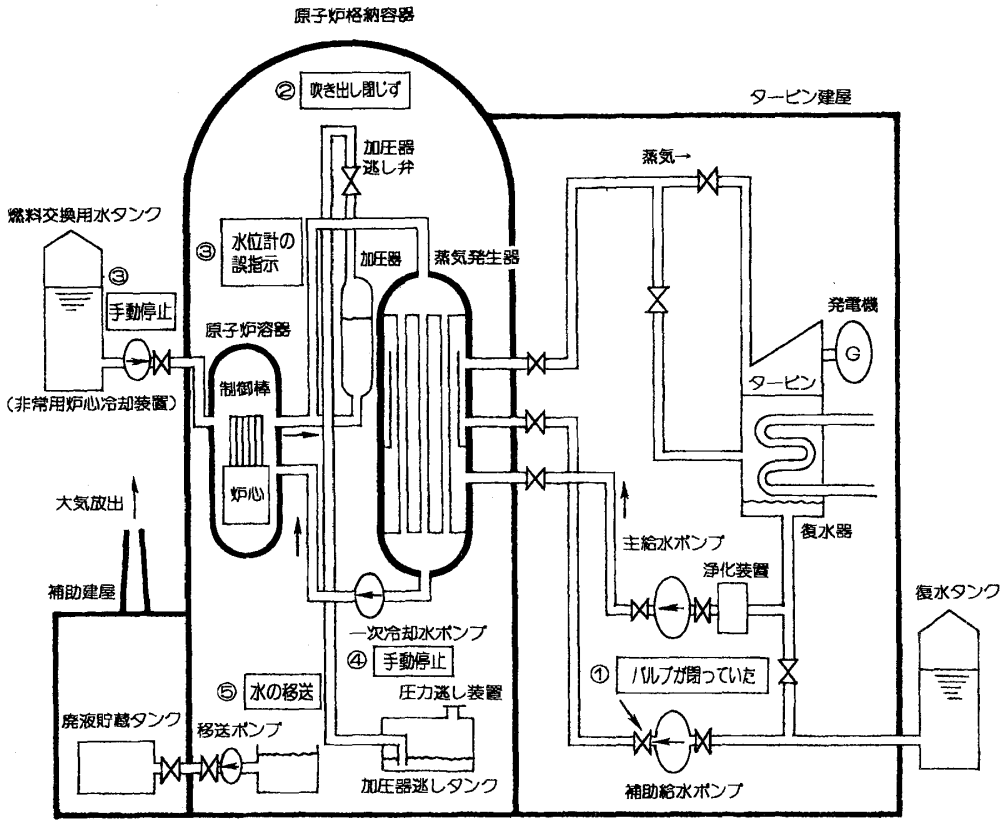

図1　原子力発電所（加圧水型）の構成概念図
図中に番号を付した説明文は事故シナリオに影響した故障，エラーなどを生起順に表している．ただし本文中の説明とは番号が一致していない．

も格段に低い実績があることは事実である．航空機産業を例にとれば，本邦の航空会社では500人を越える死者を出した1985年日航123便の大惨事以降は大きな事故は経験されていないものの，国外各社では毎年のように多数の死者を伴う事故が何度となく発生しており，最近ではコンコルド事故が記憶に新しい．化学工業分野の事故も，1984年の2,500人を越える死者を出したボパール事故ほどの事態はその後起こっていないものの，本邦でも毎年のように爆発や火災事故は発生している．建設業の分野では，本邦だけで毎年1,000件近い死亡災害が報告されている．作業の内容や労働条件が異なることから単純な比較はできないが，実績として放射性物質の環境への放出量や，労働災害の件数は低いレベルに抑えられている．また配管からの微少量の冷却水漏洩や部品の故障などに起因する一部機器の誤動作など軽微な異常事象に対する原因の究明と対策の導入，さらに他発電所への水平展開などの活動は，綿密かつ積極的に行われている．これらを総合的に見たとき，原子力発電の現場で実現されている安全性のレベル自体は一般産業と比べて相当に高いといえよう．しかし潜在的危険の大きさを考えれば，さらに高い安全レベルを目指すことは当然と考える．ただしその目的に向けた安全工学的技術，特にヒューマンエラー対応技術の開発と導入には，システム的視野に立った体系化，洗練化が必要であることに注意したい．

2.3　ヒューマンエラーの位置づけ

事故原因の分析に際してしばしば，機械的故障なのかヒューマンエラーなのか，また事故の責任はどの組織または個人にあるのかという問いかけがなされる．刑事罰の対象を絞り込んだり賠償の請求を行う場合には，このような問いかけは避けられないかも知れない．しかし，人工物を対象とした場合，機械故障かヒューマンエラーかという2分法的な区別は困難であり，往々にして無意味でもある．国際的にも広く知られたTMI事故（Three Mile Island；米国ペンシルバニア州ハリスバーグ近郊の原子力発電所で1979年3月に主給水ポンプの停止をきっかけとして炉心の一部が溶融するに至る事故が発生し世界中に大きな衝撃を与えた）を例に取り上げて，図1を参照しつつこの事情を説明する．この事故シナリオのおおまかな進展は以下の通りであった[3]．

(1) 主給水ポンプの停止．(機器故障)

(2) 補助給水ポンプは，自動起動．しかしポンプ出口の弁が閉鎖されたままであり，蒸気発生器への給水喪失．(作業後の修復エラー)

(3) 原子炉圧力上昇にともない加圧器逃し弁が開く．(正常動作)

(4) 給水が不足しているため原子炉の圧力は上昇継続し原子炉は緊急停止．(正常動作)

(5) 発生熱量が減少したこと，かつ逃し弁が開放状態のため，原子炉の圧力は低下．これに伴い，逃し弁は自動的に閉動作すべきなのに，開放状態に固着したまま事態が推移．(動作異常)．

(6) 運転員はこの異常に気づかず，弁の誤った開放状態が継続．(監視エラー)

……

この後もシナリオは進展するのだが，ヒューマンエラー問題の実態を考えるにはここまでで十分である．まず(1)はこのポンプに関する限り機器故障である．しかしその原因には別の保守作業の影響がからんでおり，その面からはヒューマンエラーともいえる．(2)については一見して明らかな保守作業者個人のヒューマンエラーである．しかしこのエラーが事前に保守グループによって発見されなかったことは，作業後の確認怠慢またはチェック体制の不備という保守担当組織上のエラーも示唆している．またこんな重要な弁の誤閉鎖を検知できないことは，弁が閉状態のままであることを示す指示計は動作していたとされている以上，運転員のエラーでもある．(5)は明らかな機器故障であるが，この故障が長時間にわたり検知されないままであったことは，現象としては運転員のヒューマンエラーである．しかし実はこの弁の開閉状態表示は，開閉状態を直接に示してはおらず弁を動作させる電磁駆動系の電流オン・オフ状態を表示していることが知られた．この条件下では運転員側から見れば，表示器が正しい情報を提供してくれていないのであるから計器異常であり，そのような計装系（インタフェース）設計は不適切であるから設計者のエラーともみなしうることになる．

ここまででも，機械故障かヒューマンエラーか，根本原因は何かという問いかけが現実的でないことは理解されよう．やはり基本的には機械側も人間側も区別することなく，トータルシステムとしての健全性を維持，向上させることが，安全性の向上にも再発防止にも実効ある方策なのであり，犯人探しと個別原因だけに着目した部分的改変は非効率的対応と言わざるを得ない．

2.4 エラー低減策の試みと困難

すでに述べたように，従来型のヒューマンエラー低減策には，自動化と supervisory control という2通りの方向が試みられてきており，ある程度の安全性向上効果が得られていることは間違いない事実である．しかし一段と高いレベルを目指した場合には，これらの方策の導入に際して予見されなかった問題点についても十分に検討し対処する必要がある．

前者の自動化方式が成功したのは，主としてシーケンス制御やフィードバック制御などの領域であった．たとえば原子炉の起動時などは複雑な手順を逐次的に実行する必要があるが，これを自動化することで運転員の作業負担が大幅に軽減できている．しかし異常や故障への対応まで含めた自動化を進めようとすると，複雑なシステムにおいて起こりうるあらゆる事象を想定して対策を作り込んでおかねばならず，実際にはそれは不可能に近い．さらに自動化によって機器操作習熟の機会が少なくなること，にもかかわらず機器が故障した場合にはそのトラブル収拾という難しい問題は人間に委ねられること，しかもそのような状況は突然起こることが多く，安心していた人間がいきなり重大な局面に直面させられるという退屈から動転状態への突然移行（boredom to panic）問題が起こるなど様々なジレンマが指摘されている[4]．

後者のアプローチに関連しては，human-centered automation という表現は耳に快いもののその具現化には多くの問題があることが指摘されている[5]．たとえばそのガイドラインでは「人間と機械にそれぞれ得意とするタスクを割り当てよ」という主張がなされているが[2]，実際には機械が出来ることは限られているのでいわゆる難問題の解決は人間に要求されてしまう．また「人間を機械の上位の意思決定者とせよ」という主張についても，時にパニックにもなる人間をそのような立場に置くことが常に適切とはいえず，状況によっては機械の自動判断を重視した方が安全性が向上しうる[6]．以上により，これらの方策はヒューマンエラー回避策として効果的に機能することは期待できない．

3. 新しい展開

では今後どのような方向を目指すべきであろうか．筆者は多くの事例の分析と機械システム知能化技術の

限界，さらに最近の航空分野における熟練者技能の捉え方を参照して，ヒューマンエラーの完全排除ではなく，その検知と対処（リカバリー）に重点をおくことを提案したい．さらに検知とリカバリーの手法としては，「視点の多様化」もしくは「他者の視点の統合」という方式を追求しつつある．以下にその内容を紹介する．

3.1 エラーゼロ追求から検知とリカバリー機能の充実へ

ヒューマンエラーは作業者の能力や注意力の不足，怠慢などに起因するという見方がなされたことも過去にはあった．しかし最近になって，人間の優れた能力，たとえば必要ない事柄を無視して重要度の高い事柄に意識を集中できる能力とか，一連の作業を個別に意識することなく自動的に想起したり遂行できるチャンキング能力などとエラー生起メカニズムとは表裏一体をなすものであることが次第に明らかになってきている[7]．この立場からは，教育や訓練の強化などでエラーの回避を目指すことは必要であっても，ゼロを目指すことには無理があることになる．しかし一方でエラーのもたらす悪影響は原子力発電所を含む多くの産業分野では無視できないことも事実である．このジレンマの解決策としてヒューマンエラーの捉え方に関する新しい提案[8]は注目すべき指摘を含んでいる．この研究では戦闘機パイロットに代表される時間的制約が厳しい条件下で業務を遂行している専門家の行動観察を通じて，エラーが少なければ少ないほど人間・機械システムのパフォーマンスが高いという単純な想定は成り立っておらず，熟練者の高い能力は，エラーを限りなくゼロに近づけるという形で実現されているのではなく，エラーを犯した場合に的確に検出し回復操作を実施するという形で実現されていることを見出している．この知見は人間の資源制約下における問題解決モデルの基本的な枠組みに大きな変更を及ぼすものであり，インタフェース設計や人間機械協調の方式に対しても，教育訓練のあり方についても新しい視点を提供している．エラーゼロを要求するのではなくエラーはしてもリカバーすれば良しとする着想は直観的にはより人間的であり，問題解決の枠組みとしてより自然なものに思われる．そのための技術的な枠組みについて次節に考察する．

3.2 新しい視点からのエラー対処技術

エラーを検知する可能性としては，(A)自分自身のモニタリング，(B)環境の変化が与えてくれるヒント，(C)他者による検知の3つが指摘され，具体的な方策例も若干提示されている[7]．ここで環境とは発電所の場合には対象機械システムも含む意味を持つ．この提言は一般論として妥当と思われるが，ここでは最近の情報処理・提示技術や人間の認知活動モデルの進歩をベースとしたより強力な技法の可能性について述べることとする．

エラー検知の本質は，同一の対象を複数の視点から観察した結果に不整合を発見することと言える．言い換えれば観測の冗長化と整合性評価とを通じてエラーは検知されることになる．もっとも単純な例として，自分の行為前の意図と，行為の後の対象に観察される結果が不整合である場合を想定してみよう．この場合には明らかに，自分の行為にエラーがあったことが検知されるが，この情報処理過程の本質は，同一の対象挙動の予測と実際を比較していることになる．すなわち時間的前後関係はあるにせよ冗長情報が比較され整合性が吟味されているわけであり，前掲の分類では(B)のカテゴリーに属する検知になっている．

原子力発電所や航空機においては，重要情報の多くは複数の手段で観測することが可能である．特定の変数の計測系統が多重化されている場合も多いが，それらの出力信号の相互比較を通じて最も妥当性の高い計測値を提示する方式が典型的なハードウエア多重冗長化方式（hardware redundancy）である．この方式を採用すれば妥当性の高い計測値が得られるに加えて異常値を示した計測系の判別も出来るため，異常診断技術としての機能も含まれることになる．

計測系統は多重されていない場合でも，変数相互の間には対象のシステムとしての挙動を反映して定まった動的関係が成立している場合も多い．このような冗長情報提示方式は機能的冗長化方式（functional redundancy）[9]とも呼ばれ，ハードウエア冗長化方式とほぼ同様に計測器異常の検出に活用できる．ただし動的関係のモデル化が適切になされていることが前提である．

これらの冗長関係は計測系の監視に加えて人間による誤認識検出にも全く同様に活用可能である．運転員がなんらかの異常な信号を観測した場合には，それを盲信することなく上述の冗長関係を駆使して多面的に確認することで観測にヒューマンエラーが持ち込まれても検知修正できる確率は格段に増大しよう．機能的冗長性の活用を支援するためには，これらの関係をモデル化して計算機による自動推定を内部実行させ，要

請に応じて提供できるインタフェース機能の実現が望まれる．

信号観測エラーよりマクロな問題として状況認識エラーの重要性にも注意が必要である．計測系故障の有無に関わらず，状況を誤って認識してしまうエラーは重大な事故に直結することから，検知とリカバリーについては的確な手段が望まれる．このための技法として筆者らは，計測の冗長化を拡張した概念である認知的多様性（cognitive diversity）ベースの状況認識方策を提案している[10]．人間は単一の視点方向からの観察では，単純な物体の形状ですら正しく認識できない．まして複雑な状況の認識を単一の視点から行うのは困難であり時に危険でさえある．このcognitive diversity実現の方策としては様々なものが考えられるが，例としては，(a)局所的視点と大局的視点，(b)現在の観測と過去の観測，(c)トップダウン視点とボトムアップの視点などの整合性吟味が挙げられる．ここで(a)はプラント全体のマクロ挙動分析と個別機器挙動観察との統合，(b)は過去の計測結果のデータベース化が前提であるが，現在と直前の観測データ比較に加えて前日のデータ，前年のデータなどとの比較，(c)は仮説生成・検証型の視点または事例想定型の視点と，観測結果積み上げ型，診断ルール組み合わせ型の視点の統合を意味している．このようなcognitive diversityは機械側（主としてインタフェース）への知的機能導入によって実現されるので，そのような機能実現のための基盤技術開発が現在も進行中である[9]．ただし，同様な機能は運転員それぞれがあえて異種類の見方を分担することでも実現できるので，教育訓練の中でもその実現が図られることが強く望まれる．

3.3 教育訓練の見直し，高度化

従来の原子力発電所運転訓練においては，対象の特性と作業の内容を確実に理解して，状況に対応した的確な操作を実行できる能力の涵養に力点が置かれてきたと思われる．この訓練が十分な成果を挙げていることは運転トラブルの発生頻度の低さから見ても疑いのない事実であるが，この訓練を分類すればいわゆるknow-how中心の訓練とみなすことが出来よう．しかし最近ではknow-howだけでなくknow-why，すなわちそのような操作や操作実施上の制約の背後にある意味を理解することが，確信と理解に支えられた操作の実現のために望ましいという見方が広まっている．JCOの事故は，十分なknow-whyの裏付けのないままに与えられたknow-how知識を，なし崩しに改悪してしまった結果と見ることもできる[11]．

これとならんで，上に述べたようなインタフェース技術革新，たとえばfunctional redundancy情報提供などがあればそれを的確に反映する事，前掲のcognitive diversityについても積極的に配慮することなどは当然ながら期待したい．このような教育訓練への努力傾注，資本投下などを怠ることは，長期的には必ず経営的にもマイナスに作用することは多くの事例によって明白に示されている[3]．

3.4 組織論，社会論的な見直し

またJCO事故における組織ぐるみ違反問題や英国核燃料会社（BNFL）におけるデータ改竄事件など，組織のモラルハザードともいえる，従来はあまり見られなかったヒューマンエラーが近年顕在化している．ここで，モラルハザードの実例は，原子力分野のみならず官庁，警察，金融，食品，医療，土木，教育など，高い信頼性とモラル規範の維持が期待されるありとあらゆる領域で，並行的に起こっていることに注意が必要である．それぞれの組織がその存在理由の原点に立ち戻って真剣に反省し再生に努力すべき事はいうまでもないが，ここではそれを前提とした上で，現在までの批判やモラル再建策には抜けている問題点を指摘したい．

公衆社会側が検討してみるべき重要課題として，逆説的に聞こえるかも知れないが，過誤の許容という視点がありえよう．これはいうまでもなく無責任にエラーを連発しても良いという意味ではない．しかし3.1節で述べたように人間のエラーを完全に排除することは原理的に困難である以上，「このような安全を担う組織ではエラーなどは絶対にあってはならない」とする厳格な批判姿勢は，組織側の自己防衛意識の過剰を生み出し，社会的圧力が組織内状況を一層悪化させて誤判断や不適切行為を生み出す要因にもなりうる．「エラーはあってはならないから，あったならそんな組織は解体だ」などと批判されたとしても，一方でエラーゼロなど実現できない．許されないから隠そうとすることはモラルハザードである一方，組織としては自衛でもある．あらゆる技術には利便性だけでなくリスクがつきまとうこと[12]を共通の認識として，悪意のない軽微なエラーなら，外部への悪影響がなく組織としても直ちに対応に取り組んでいる場合，過剰な弾劾や犯人追及は行わないことが結果として社会全体のリスクレベル低下に効果的である可能性について真剣に考えてみるべき時代ではないだろうか．

4. ORへの期待

OR学会の主要な対象分野である数理計画法や最適化技術，待ち行列やスケジューリング技法などは直接にはヒューマンエラー問題への適用は困難である．しかしヒューマンエラー対策として様々な手法や技術の現場導入を図っていく場合には当然ながら，経営上の意思決定がなされねばならず，そのための手法として異種の評価基準を統一的に扱えるAHP（Analytic Hierarchy Process：階層化意思決定法）[13]などには大きな期待を寄せている．またリスクの評価と組織的，社会的受容の問題は，ヒューマンエラーとの関連が高いことは3節に論じたとおりである．リスク認識と受容に関しては，人間の感覚（主観的評価）に関わる尺度構成論の見直し[14]も重要な課題であろう．

企業の社会的責任，利益とリスクの配分の公正さなどが従来にもまして要求される今日，経営のための意思決定技法を対象とするORが有する重要性は，上記のような文脈においてますます大きいと言えよう．

5. おわりに

「人間は機械装置ではないから時にエラーをすることは避けられない．」と本論のはじめに記したが，この記述は本邦においてどの程度に受け入れられているのか改めて問い直してみたい．ヒューマンファクター研究者のレベルでは，この記述の正当性は理解されていても日常的なレベルでは，このようなエラー許容的な視点は社会的にほとんど受け入れられていないように思われる．しかしヒューマンエラーの低減だけでなく，本稿で述べたように検知やリカバリーまでを含めた対応策を適切な形で策定し現場に導入するためには，その実際の姿を反映するデータを集積し分析することがどうしても必要であり，もう少し許容的な姿勢が社会の各所に広がることが望ましい．そのような姿勢を背景として，真の意味で実効性の高いエラー対応策の構築に向けて努力を続けることが今後とも重要かつ唯一の現実的方策であろう．様々な先端的技術を基盤としている現代社会においてこのような見方をベースとしつつ合理的な意思決定が各局面でなされることを期待する次第である．

参考文献

[1] Sheridan, T. B.; Telerobotics, Automation and Human Supervisory Control, MIT Press (1992)

[2] Billings, C. E.; Human-Centered Aircraft Automation: A concept and guidelines. NASA Technical Memorandum 103885, (1991)

[3] Leveson, N.; SAFEWARE. Addison-Wesley (1995)

[4] Bainbridge, L.; Ironies of Automation. Automatica, 19(6), 775-779 (1983)

[5] Sheridan, T. B.; Human-centered automation,: oxymoron or common senmse?, Proc. IEEE International Conference on Systems, Man and Cybernetics, Vancouver (1996).

[6] 稲垣：誰のための自動化？ 計測と制御, 32(3), 181-186(1993)

[7] Reason, J.; HUMAN ERROR, Cambridge University Press (1990)

[8] Wioland, L. & Amalberti, R.: When errors serve safety: towards a model of ecological safety, Proc. CSEPC 96, Cognitive Systems Engineering in Process Control, Kyoto Japan, 1996, pp. 184-191 (1996)

[9] Patton, R. J., R. N. Clark, P. M. Frank (ed.): Fault Diagnosis in Dynamic Systems, Prentice Hall (1988).

[10] Takahashi, M., Diantono, C. and Kitamura, M.: Life Cycle Integrity Monitoring of Nuclear Plant with Human Machine Cooperation, Proc. 7th IFAC/IFIP/IFORS/IEA SYMPOSIUM on ANALYSIS, DESIGN AND EVALUATION OF MAN-MACHINE SYSTEMS, Kyoto, 1998, pp. 431-435 (1998).

[11] Furuta, K., K. Sasou, R. Kubota, H. Ujita, Y. Shuto, E. Yagi; Human Factor Analysis of JCO Criticality Accident, paper to appear in a special issue of International Journal of Cognition, Technology, and Work

[12] 村上：安全学, 青土社, 1998

[13] 刀根：ゲーム感覚意思決定法—AHP入門, 日科技連, 1986.

[14] 鷲尾, 元田：属性変量の尺度認知に基づく構成的法則発見手法, 認知科学, 5, pp. 1-14 (1998)