

リスクに基づき安全を考える

氏田 博士*

Risk Informed Safety Concept

Hiroshi Ujita*

「システム安全」「リスクに基づく意思決定、RIDM」「ヒューマンパフォーマンス向上」の関係性について述べる。

Keywords: システム安全、リスク情報に基づく意思決定 (RIDM)、PRA、HRA、COVID-19

1. はじめに

社会－技術システムや大規模複雑システムでは、トラブルや事故は単に故障だけで起こるものではなく、実際には安全設計や運用で想定した以外の事象も起こる。そのため、網羅的に起こるトラブルや事故を想定することは容易ではなく、どうしても確率論的アプローチになる。つまり、想定漏れとならないように、事象の組み合わせの連鎖(事象シーケンス)を可能な限り体系的に想定して、それら個々の事象シーケンスについても安全解析を行い、もし現行の設計案に重大な事象が発生する可能性が発見されれば、設計にフィードバックして事前にシステムに安全策を組み込むようにする。安全に関する問題意識の原点には「部分最適は全体最悪を生む」があり、システムのバランスを見て総合的に安全性を向上させる「システム安全」の考え方がある[1]。要は、システムを過不足なくバランス良く設計し運用して安全を作り上げることが肝要である。そのために、社会－技術システムあるいは大規模複雑システムの安全解析には、確率論的リスク評価(PRA: Probabilistic Risk Analysis)が重要である[2]。もちろん、安全対策にはコストがかかるので、リスクの重要度の優先順位とその対策コストのバランスでどこまで対策するのかを合理的に判断し

意思決定する必要がある。この必要性が、日本におけるリスク情報に基づく意思決定 (RIDM: Risk Informed Decision Making) 導入のインセンティブとなっている。

特に PRA は、現在の安全の水準を総合的に評価し数値化した安全目標:「どこまで安全であれば安全といえるか?」を議論でき、安全評価と対策立案に有効活用することができる。

システム運用時のシステム安全性はもちろんのこと、システムや機械が故障した際の人間によるバックアップにおいても、あるいはまた人間の関与があるシステム安全関連系においても、システムの安全には人間の信頼性が直接関わる。このため、システムの安全解析や安全設計において、人間の信頼性を解析する(HRA: Human Reliability Analysis)ことが不可欠である[2]。

2. リスク論からコロナ（新型コロナウイルス、COVID-19）禍を考察する

この「アドバンスシミュレーション」発行の時期においてもその後も、2次あるいは3次のコロナ禍が猖獗を極めている可能性が考えられる。このコロナ禍をリスク論の観点から検討してみる。ここでは、2つの点について考えてみたい。1つは、皆さんがよくご存知のPCR法の在り方はどうなのか?もう1つは他のリスクと比較して考えないで良いのか?である。いずれにしても、何が本当のリスクかを見極めることであり、人々を取り巻くリスクのバランスを考えることであり、その

*アドバンスソフト株式会社 リスク研究開発センター

Risk Research and Development center, AdvanceSoft Corporation

ためには合理的なシステム思考が大切である。

2.1. PCR 法の功罪

PCR 法とは、ウイルスの遺伝子を見つけ出す検査だが、見落としが多すぎる(なんと 100 人中 30 人以上も見落とす確率があるそうである)。しかも費用も時間もかかりましてや検査できる技師が少ないにもかかわらず。しかし、この検査しか感染を見つける方法がない現状ではこれに頼るしかない[3]。

ここで見つけなければならない対象は、“無症状の濃厚接触者”であり、すなわち患者の周りにいた人で、無症状だからコロナだけ疑えばよく、周囲に感染を撒き散らしていないか、すなわちクラスター化していないかを調べるために行う。こういう検査法を積極的疫学調査と言うそうである。日本もこれを実施していて実効的な方法と判断できる。しかし、最近はとにかく検査のみを行う施設を作ろうという方向性にある。確かに、早く見つけることで意味がある病気なら頑張って検査するべきであろうが、現状治療法がないから検査をしても何もできない。インフルエンザのような簡便なものができれば良いが。

人口 1000 人の小さな街で全数 PCR 検査を実施することを想定して、PCR 法の課題を摘出してみる。

- 特異度 (誤判断率) : 1%
- 感度 (判断ミス率) : 30%
- 真のコロナ患者 : 10% (これが総ての確率にきいてくる)、もし[1%]だと

100[11]人の真のコロナ患者のうち陰性として見過ごされる偽陰性は 30[3]人、この人は大丈夫というお墨付きをもらってスーパースプレッダーになる可能性があり非常に危険である。

しかし本当の問題は、900[990]人のコロナでない人が検査を受けると 9[11]人も陽性と判断される偽陽性が出ることである。この人たちは謂れもなく自由を束縛されてしまうことになる。それ以上に、1000 人の小さな街で 9[11]人の陽性患者が出れば確実に医療崩壊に繋がってしまう。

闇雲に検査するのではなく、PCR 検査の前に確実

性を高めておくことが重要である。長期対策として、PCR 検査の実施の頻度の拡充と医療受け入れ態勢の整備は同時並行でバランス良く実施しなければならない。個人としての対策は、かも知れないと思ったら、自分から自宅隔離することに尽きる。普段の三密対策とうがい手洗いは当然として。

このことから、現状において実施されている、専門家の判断で本当に怪しい人に絞って PCR 検査を実施する方法が合理的で有効な対策であることは確率統計の知識と計算から明らかである。

2.2. 人々を取り巻くさまざまなリスク

このように多くの人がコロナしか心配していない方向に向かうことに不安を覚える。世の中には何百何千もの病気があり、コロナなどはその 100 位にも入っていないのに、そのことばかり医者も患者も心配している。さらに、人類を取り巻くリスクは医療リスク以外にも多数あり、しかもそのリスクの方が圧倒的に大きい。

下の表は、人間のリスク認知の矛盾を示している。多くの死亡者が出ている交通事故や自殺をごく普通のこととして受け入れるにもかかわらず、ほぼリスクがないといえる 0157 や狂牛病には過敏に反応して大騒ぎとなったことは多くの人が経験している。今回のコロナ禍の騒ぎもこの構図に則っている。

以下の図は、日本における年毎の自殺者数の推移を示しているが、2 万人を超えていることが分かる。現状において、コロナの死者数は千人前後である。本当に議論すべきリスクは、より大きなリスクであり、たとえコロナ禍の中においてであっても、コロナの議論や対策より自殺者対策が優先されるべきであろう。さらにこの図のポイントはもう 1 つあり、自殺者がリーマンショックで 3 万人を超えたことでありかつそれが 10 年以上も継続したこと、すなわちリーマンショックの影響だけで 10 万人に近く自殺者が増えたことである。

次の図は自殺者数と失業率との関係を示すが、失業率と自殺者数は線形の関係にあり、自殺者を減らすには失業率を下げることに尽きる。経済に及ぼすコロナショックの大きさはリーマンショッ

表 1 原因別死亡者数（「反原発」の不都合な真実：藤沢数希著 2012）

対象	死亡者数/年	報道価値	一般の反応
放射能、 O157 、狂牛病	0-100人	高	パニック
HIV 、殺人、熱中症	100人-5,000人	中	社会的問題
交通事故、大気汚染、自殺、喫煙	5,000人-20万人	低	日常茶飯事

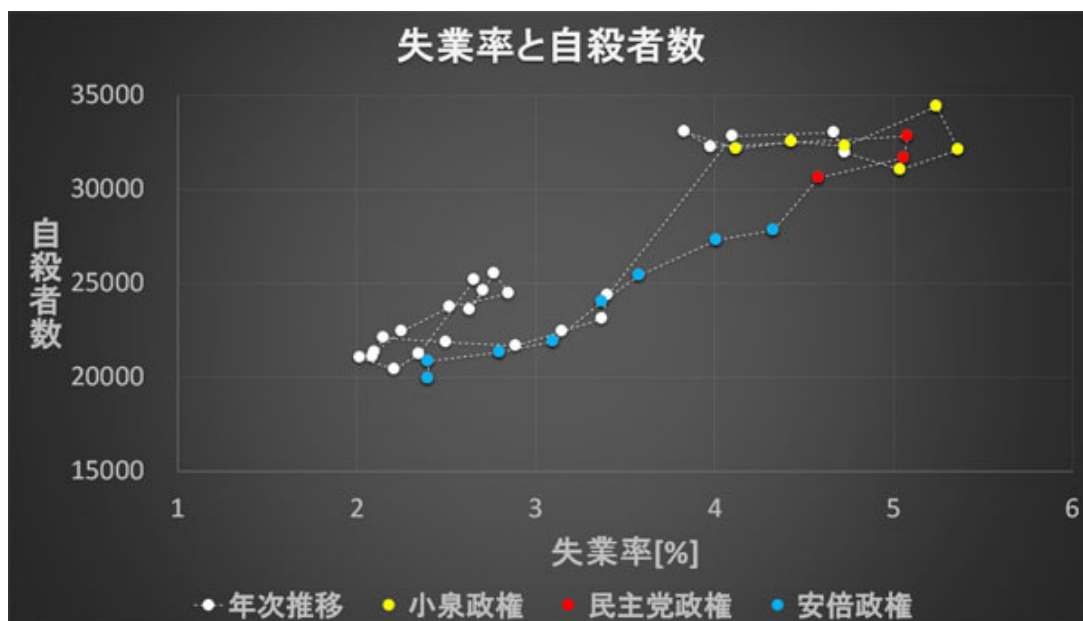
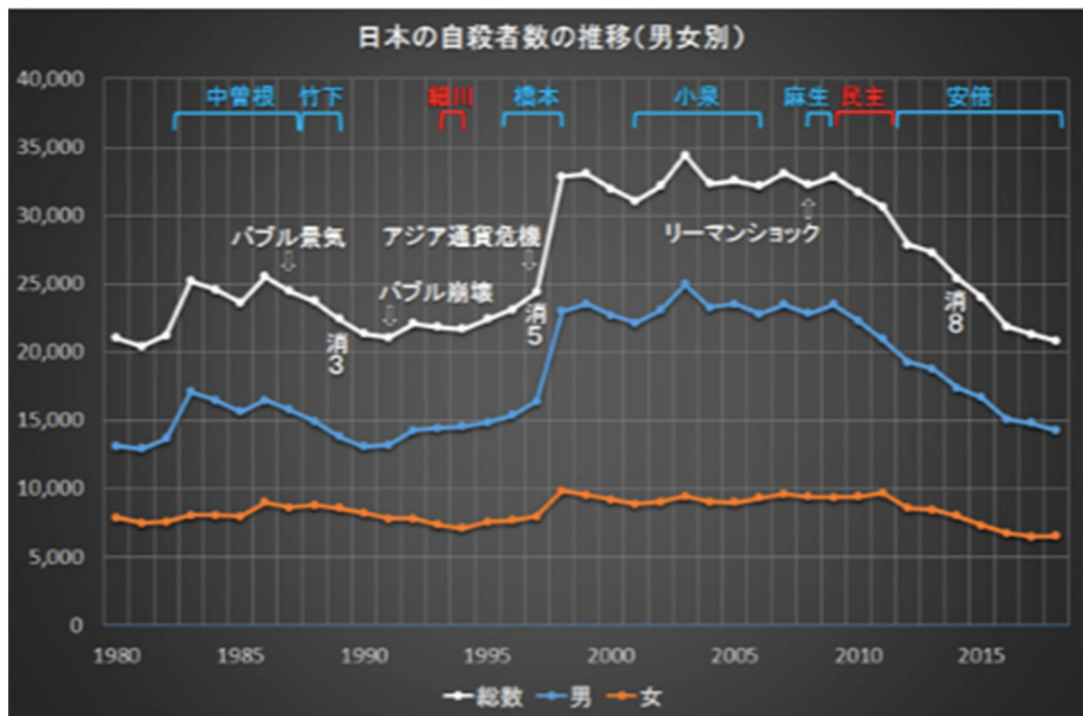


図 1 自殺者数と失業率（厚生労働省）（上）日本の自殺者数の推移 （下）失業率と自殺者数の関係

クの倍であろうといわれているようだ。だとすれば、コロナへの対策はもちろん必要だが、コロナの自粛による景気を維持回復し失業率を低下させる施策が強く望まれる。それが日本の政策における RIDM であろう。

3. リスク概念

リスクを安全性の尺度として用いることによって、対象システムの安全性を確率として定量的に、そしてより具体的に検討できる。そればかりでなく、リスクは、対象システムの安全性の改善目標の決定や技術システムの選択においても重要な役割を果たす。例えば、技術システムの安全性をどこまで改善する必要があるかは、リスク解析の結果と安全目標の比較により定まる。また、さらなる安全性の向上を必要とするかどうかは、コストベネフィット解析によって判断され、さまざまな代替案の中から最適改善案の選択はリスクの改善度合いとそれに要するコストとのトレードオフに基づき決定できる。さらに、ある技術システムが社会に受け入れられるか否かは、その技術システムがもつリスクとベネフィットとのトレードオフに係る。

「リスク(risk)」の語源は、「絶壁の間を船で行く」という意味だといわれている。たとえ兩岸が絶壁であっても、あえてそこを越えないことにはチャンスに巡り合う可能性もない、しかしそれは将来という不確定なものである。米国の経済学者フランク・ナイトは、不確定なことについて確率によって計測できるものをリスクと呼んでいる。

一般に、リスクには、健康に対するリスクのみならず、環境リスク、投資リスク、企業経営リスク、政治リスク等さまざまなリスクがある。また、個人のリスクと社会のリスクの分類もあり、さまざまな指標が使われている。

ISO/IEC Guide 51 (JIS Z 8051:2004) (4)では、リスクとは「危害の発生確率及びその被害の程度の組み合わせ」、危害(harm)とは「人の受ける身体的傷害もしくは健康被害、または財産もしくは環境の受ける害」とされ、人に加えて、財産、環境も対象になっている。

また、リスクマネジメント用語規格(ISO/IEC Guide 73: 2009)では、リスクの再定義によって、リスクは「事象の発生確率と事象の結果の組み合わせ」、結果は「事象から生じること」と定義された。事象の結果には、好ましくない影響と好ましい影響の両方が含まれ、また期待値から乖離しているものとなっている。このように結果が、好ましくない結果だけに限定されなくなったが、安全においてリスクを考える場合は、結果は常に好ましくないものであるもので、従来通り好ましくない影響だけを考えることとされている。

4. システム安全解析

システム安全のためには、システム全体のリスクのバランスを見ながらリスク低減対策を実施することが望まれる。リスク低減の手法としては、過去に起こったエラーを分析することによりシステムの脆弱性を見つけ、それをフィードバックして再発防止や未然防止対策を図る原因分析と、システム全体の将来のリスクを予測しリスクの重要度（および対策コスト）に応じて対策立案に結びつける確率論的リスク評価、PRA が車の両輪として存在する。最近発生する事故は、深層防護の設計思想が確立されたこともあり、多様なシステムのエラーの重畳が原因となっている。このため、エラー分析も重要であるが、効果的な対策立案のために確率論的安全評価手法、PRA が広く使われている。本項では PRA について記述する。

複雑な社会－技術システムあるいは大規模システムの安全解析には、PRA が不可欠であり、それにはイベントツリー解析(ETA : Event Tree Analysis)とフォールトツリー解析(FTA : Fault Tree Analysis) が使われる。また安全解析手法の中でも、特に多くの技術システム分野で故障モード・影響度解析(FMEA: Failure Modes and Effect Analysis)と FTA が要求される。以下、ETA と FTA について述べる。

4.1. 確率論的リスク評価(PRA)

国際原子力機関(IAEA)は、確率論的リスク評価(PRA: Probabilistic Risk Assessment)を安全に関わ

る決定に用いることを PRA と定義している。つまり、PRA(Assessment)の過程の中に、PRA(Analysis)が位置することになる。原子力では、確率論的リスク評価(Assessment)の名の下、1975 年の Reactor Safety Study, WASH-1400 によって本格的な取り組みが始まった。

システムは、何らかの想定に基づいて設計されるので、その範囲で安全性を確認するのが安全評価の基本である。しかし、実態を見ると設計想定外の事象も起きる。したがって、設計想定に沿った評価に加え、想定外についても安全評価を行い、重大な事象が発生する可能性が発見されれば事前に手を打つ必要が生じる。原子力プラントも例外ではない。

しかし、すでに高いレベルで安全設計がなされているシステムで想定外の重大事象が起きることは稀である。想定外の事象を網羅的に捉えようとすると多くを検討しなければならない。全てに対策を講じようとすれば多大な経済的負担を生じてシステムの存在意義そのものが失われかねない。ここにリスクに基づく安全評価を行う必要性と価値が生じる。すなわち、PRA では、結果の重大さ、不安全事故が起りえる頻度、そして対策に要する資源を考慮して、多数の可能性の中から手を打つべき重要な想定外事象（事故シナリオ）を合理的に割り出す。システムの安全には人間の信頼性が直接関わるので、PRA における適切な人間信頼性解析(HRA: Human Reliability Analysis)なしには適切な PRA はありえないといっても過言ではない。

4.1.1. 確率論的リスク解析(PRA)による事故シーケンスと影響の定量化

PRA を用いて、事故シーケンスを定量化して、シーケンスそれぞれの重要度をランク付けする。また、これによって事故のロジックモデルを求められる。これも PRA の主たる目的の 1 つである。事故シーケンスの定量化のプロセスは、次のタスクの実行である。

- (1) 事故シーケンスのブール等価式の導出
- (2) 事故シーケンスの一括

- (3) 基本評価
- (4) システムの詳細評価
- (5) 重要度および感度解析

これらのタスクを実行した結果として、次のようなことが明らかになる。

- 卓越した事故シーケンス、およびそれら事故シーケンスを発生させる故障の組み合わせであるカットセット
- それらの事故シーケンスに含まれるシステムに対する事故シーケンスを発生させる故障の最小の組み合わせであるミニマルカットセット
- 事故シーケンス、システム、カットセット、要素に対する重要な対応策
- 従属およびヒューマンエラーの影響
- リスクに最も影響するシステム、要素、手順への洞察

4.1.2. 確率論的リスク解析(PRA)のプロセス

PRA は、通常時は異常もなく安定して運転継続されているプラントにおいて、何らかの事象の発生により事故につながる可能性を評価するものである。そのプロセスを図 2 に示す。まず点推定としてのリスク評価では、イベントツリーやフォールトツリーを用いて事故のシナリオを同定し、記述する。次いで、起因事象の発生頻度、機器故障率、人的過誤率、シビアアクシデント時の物理現象の解析、放射性物質の移行や健康影響の解析などを用いて、これらのツリーの定量化を行って事故シナリオごとの発生頻度と各事故シナリオの影響を評価する。この影響とはその事故シナリオが発生した場合の個人の条件付き死亡確率で表現される。そして個人の死亡リスクは、すべての事故シナリオの発生頻度と条件付き死亡確率の積和で表される。

このためまず、起こりえる起因事象を想定しそこから安全機能の有効性を見てイベントツリーを作成し、そして個々の安全機能の有効性についてはフォールトツリーで評価する。

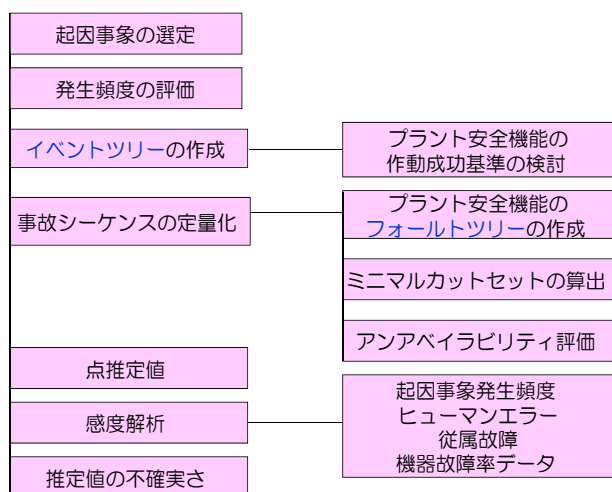


図2 ETA/FTAを用いた安全解析のプロセス[1]

(1) 深層防護の分岐を評価するイベントツリー解析(ETA)

ETAの典型例として、図3に原子力プラントにおける大破断冷却材喪失事故(LOCA: Loss Of Coolant Accident)を初期事象として、必要とされる安全系の作動/不作動によりシナリオが分岐している様子を示す。

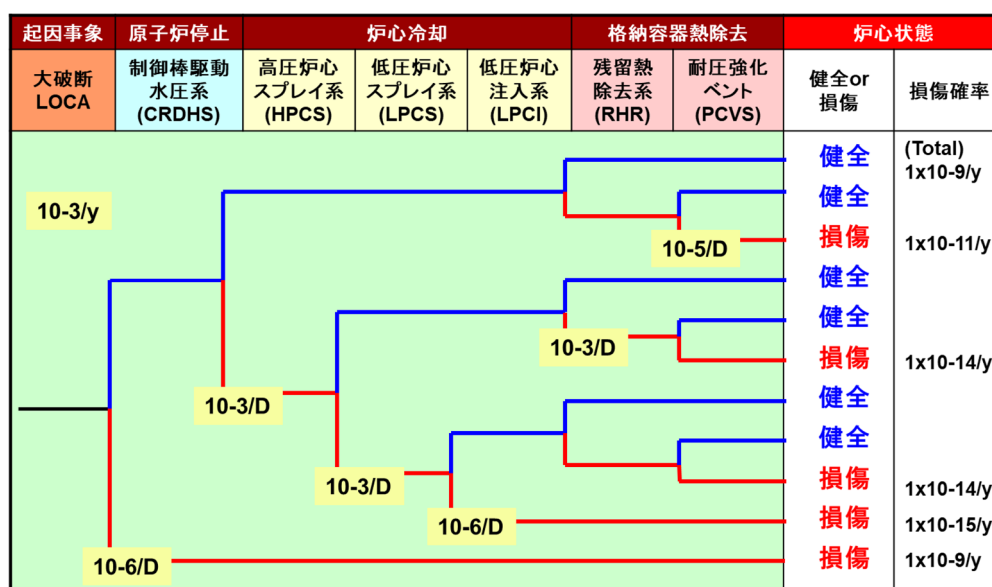


図3 深層防護のレベルごとに分岐するイベントツリーの作成と評価[1]

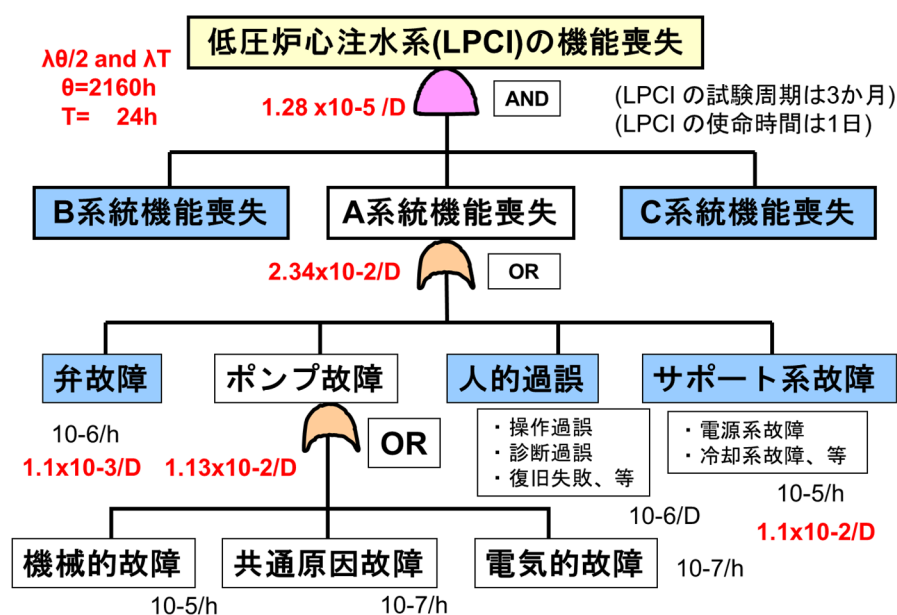


図4 深層防護における個々の安全機能毎のフォールトツリーの作成と評価[1]

各分岐の確率計算とそれぞれの分岐の現象解析の結果を総合してリスクを評価している。この場合は、5つのシナリオの損傷確率の和を求めることにより、炉心損傷確率を計算できる。

(2) 深層防護の各機能の評価するフォールトツリー解析 (FTA)

図4に深層防護の個々の安全機能毎に展開したフォールトツリーの例を示す。この場合、図3のイベントツリーの左から3つ目の分岐である低圧炉心注水系 (LPCI) の機能喪失確率は、待機系である LPCI の試験周期が決まれば計算できる。LPCI の試験周期を3か月とすると、ポンプ故障確率は、3つの故障モードの故障率と試験周期の半分との積から計算でき、 1.1×10^{-2} となる。同様に、A 系統機能喪失の確率は 2.3×10^{-2} となる。3 系統が独立してあるのでその 3 乗となり LPCI の機能喪失確率は 1.2×10^{-5} である。

4.2. 人間信頼性解析(HRA)

システム運用時のシステムの安全性はもちろんのこと、システムや機械が故障した際の人間によるバックアップにおいても、あるいはまた人間の関与があるシステム安全関連系においても、システムの安全には人間の信頼性が直接関わる。よって、システムの安全設計において、人間の信頼性を解析(HRA)し評価し、それを設計に考慮することが不可欠なのである。システム設計にかかわる原則：「システムの安全評価においては人間信頼性を考慮せよ」は、またシステムにおける人間の役割を、大局的観点に立って解析・評価することを指している。よって、システムの安全評価における HRA には、システムのライフサイクル全体を見渡すことを必ず念頭においておく必要がある。

HRA は、信頼性工学のアナロジーとして生まれた。人間はシステムを構成する部品とされ、手順書のとおり「人間部品」が機能するか否かが関心事であった。この時代の HRA の典型は、後述する THERP 手法[5]、TRC 手法および SLIM 手法である。これらは、米国スリーマイル島原発事故以

降、原子力の分野でも広く使われている。

最近は、人間を単なる部品としてではなく、「主体性をもって自ら判断する生身の存在」として扱う、「第二世代 HRA」と呼ばれる手法が開発されている[6]。第二世代 HRA の特徴は、下記の認識に基づいて、「認知」、「物事の前後関係（文脈性といわれる）」、「組織」を積極的に評価に取り込もうとする点にある。

- 従来の HRA では、「ランプで機器状態を確認する」といった、手順書に定められたタスクを単位に評価を行う。しかし、失敗の原因を探るためには、行動の背後にある認知過程に立ち入る必要がある。
- 人間は、手順書に書かれていなくても、行うべきことを自ら判断して行動する。経験・知識をベースに、前後関係や予測に基づいて行動を決める。このような文脈性を扱える手法が必要である。
- 組織における仕事のやり方、すなわち組織文化は個々人の判断行動を大きく左右する。従来の HRA に、組織因子の扱いを取り込むべきである。

(1) THERP 手法

THERP (THERP: Technique for Human Error Rate Prediction) [5]はもっともよく知られ、広く利用されている手法である。米国スリーマイル島原発事故を契機にハンドブックにまとめられ、原子力の HRA を席卷することになる。批判も多いが、代わる手法がないとして、今日でも広く利用されている。手順書にしたがってステップバイステップに行うタスクの評価に使われる。

THERP ハンドブックには、ふんだんにノウハウが盛り込まれているが、基本は単純である。THERP 手法は、一連のタスクを構成するタスクステップを枝にしたイベントツリーを定義して、各枝に成功失敗確率を割り付けることによってタスク全体の成功失敗確率を求める手法である。

THERP 手法には、HRA 手法ならではの特徴がある。例えば、1つの仕事を複数の人間で行うことによって人間系の信頼性を高めようとする「人間多重系」の評価方法が挙げられる。機械系であれば、多重系を構成する要素が故障する機会は独

立と考えるのが普通であるが、人間は「他人を過度に信頼する」する傾向があるので、完全独立な多重系とは思えない。このような人間の特性を評価に盛り込むため、THERP 手法は「依存性モデル」と呼ばれる評価モデルを導入した。具体的には、人間多重系を独立系だと考えて標準データを2回かけるのではなく、標準データより大きな値を標準データにかけて保守的な評価を行うしくみである。

(2) TRC 手法

多くの場合、人間の時間応答は対数正規分布で近似できることが知られている。早くタスクを終わる人も、時間がかかる人もいるが、横軸に時間、縦軸に時間内にタスクを終了した人の割合をプロットしてみると、概ね対数正規分布に従うことが多い(図5参照)。そこで、制限時間内にタスクを終了した人の割合を1から引けば、制限時間内にタスクを終了できない人の割合が得られるので、時間制限のあるタスクの人間信頼性の評価に利用できる。これを異常診断タスクに用いたのが TRC (Time Reliability Correlation) 手法である。実験データに基づいて、タスクを開始してからの時間と、それまでにタスクを終了した人(チーム)の割合を、それぞれ対数でプロットしたものである。直線近似すると、任意の時間においてタスクを終了している人(チーム)の割合(成功確率)を推定できる[7]。

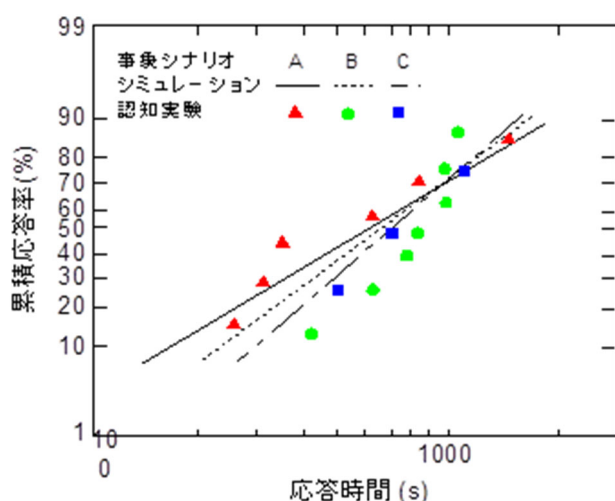


図5 TRC のイメージ[7]

わが国でも、ヒューマンクレジットに関する検討の一部として TRC 手法を用いた例がある。図5に示すように、プラントシミュレータを用いて設計想定事象の判別に要する時間を計測し、カーブフィッティングによってパラメータを推定して人間信頼性を定めている[7]。

(3) 第二世代 HRA 手法

第二世代 HRA の代表選手としては、米国 NRC が開発した ATHEANA (ATHEANA: A Technique for Human Event Analysis) 手法がある[6]。ATHEANA は「正しいと判断して、実は不適切な行動」を行ってしまう可能性を評価するために用いる。ATHEANA 以外にも文脈性を考慮した手法として MERMOS 手法や CREAM 手法が知られている。MERMOS 手法は、フランス電力会社(EdF)が開発した手法で、同国の N4 型軽水炉プラントを皮切りに、フランスの原子力プラントの PRA に広く使われている。E. Hollnagel が開発した CREAM 手法は、適用分野を特定せずに開発された一般性を持った手法であるが、事故対応に用いられるガイドラインの評価に適用された例がある。

(4) HRA の手法の結果と実験結果の比較

図6に NRC と Halden による Comparison Study の結果を示すが、HRA は、手法の計算結果だけでも実験結果だけでもさらにモデルと実験の結果の傾向比較でも、評価結果が大幅に異なること示されている[8]。6つの事故シナリオの計算結果の比較を示しているが、手法による計算結果のばらつきが3桁近くある。そのうち3つのシナリオでは実験との比較も示されているが、実験結果にも3桁ほどのばらつきがある。この結果の中でも特に最初の2つのシナリオの計算と実験の結果の差異が問題であると考えられる。

- ・1B：フィードアンドブリード失敗では実験に比べモデルは過小評価ではないかと判断される。
- ・2B：1B+復旧の遅延では、逆にモデルは過大評価ではないかと判断され正反対の結果となっている。

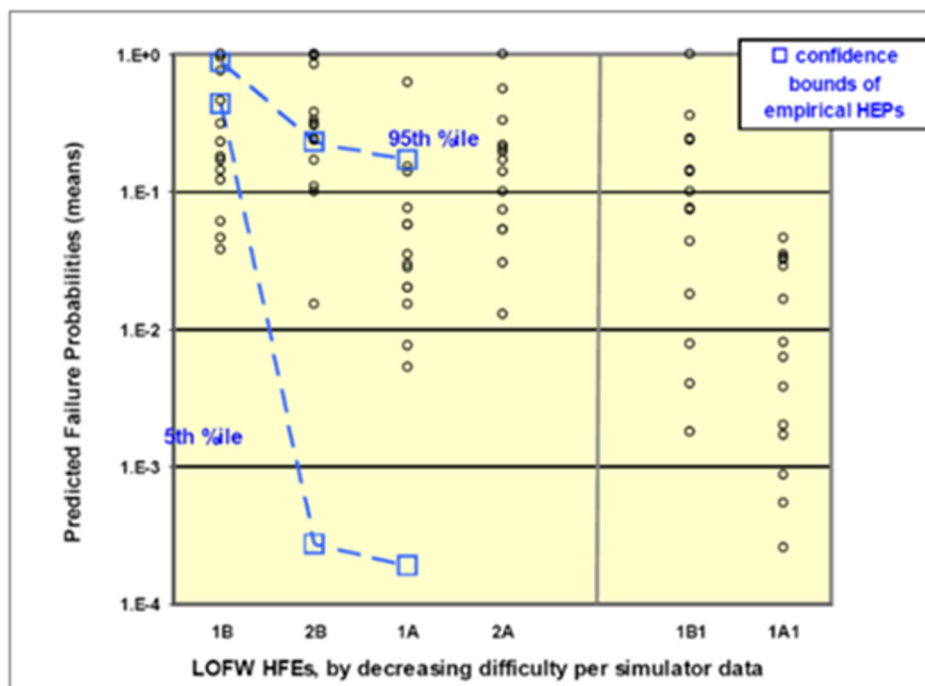


図 6 HRA モデル整備と HE データ整備の必要性[8]

Dotted blue lines are the 5th and 95th percentile Bayesian bounds for the empirical HEPs (HAMMLAB data); the small circle dots are the predicted HEPs from various HRA methods in the study.[9]

この結果は人間の対応特性におけるコンテキスト依存性の大きさを適切に捉えられていないことが原因と考えられ、実験では認知過程とコンテキストのより深い理解が、モデルでは認知のメカニズムとコンテキストへの依存性を考慮した評価手法の開発の必要性が指摘できる。

(5) HRA の課題

工学システムにおける機器故障の発生とは本質的に異なる「人間のエラー」を確率論的リスク解析 (Probabilistic Risk Analysis: PRA) という 1 つの体系の中で扱うことの難しさは初期の PRA 研究者の間では共有されていたが、現状では PRA の中での HRA の重要性の認識は低いと言わざるを得ない[8]。PRA の結果として得られるリスク情報に含まれる不確実性の大部分が人間信頼性解析 (Human Reliability Analysis: HRA) の結果の不確実性に起因するものである。不確実性があることを前提にしてリスク情報を活用することがリスク情報に基づく意思決定 (Risk Informed Decision Making: RIDM) の考え方の基本であるが、

そのためには HRA における分析手法に関する十分な理解が必要である。

5. 合理的な安全の考え方による社会との対話

巨大複雑システムは社会性が高い以上、システムを合理的に捉える RIDM の視点で安全を評価し社会と対話を図ることが必要とされる。RIDM は、リスクを定量化するリスク評価 (PRA)、それが安全目標を満足するか対策が必要かを判断するリスクアセスメント、評価結果に基づき社会と対話するリスクコミュニケーションからなる。リスク評価とリスクアセスメントの現状とあるべき姿を検討し、そしてそれを社会に発信し議論することは、リスクコミュニケーションの一環である。

5.1. 安全目標

安全目標の設定は社会的課題である。安全目標とは、科学技術利用における国および事業者の安全確保の使命に対し、科学技術利用に伴うリスクの抑制の程度を表すものである。リスクと安全目標の関係を、英国の例で図 7 に示す[10]。安全は

社会的な価値の問題であるため、そのシステムが許容できるか否かはリスク（ここでは事故の発生頻度）の大きさで決定される。例えば一般大衆の個人の死亡リスクが1万年に1回くらいのシステムは無条件に受け入れられないであろう。この値を安全限度（Safety Limit）と呼ぶ。一方で百万年に1回くらいに頻度が少なければ、社会から広く受け入れ可能であると考えられる。これを安全目標（Safety Goal）と呼び、多くの国が技術システムの受け入れ目標として定めている。この目標の設定にあたっては、システムの効用（ベネフィット）がリスクを上回るから多くの人々に受け入れられるので、当然のことながらリスクベネフィット解析を前提としている。同様の目的をもつシステムとの採否やバランスは、システム間のリスクとベネフィットの相対的な比較に基づき決定することになる。その間のレベルは、ALARP（合理的に達成可能な限り努力する）領域と呼ばれ、リスク低減効果（ベネフィット）とそれにかかるコストとのトレードオフを分析するコストベネフィット解析により、対策の有無を検討することが大切である。さらに積極的に安全性向上を図るのであれば、システムにおける安全対策が不十分な所と余剰な所のバランスを取ることで、システムの安全とコストを総合的に合理化することである。この精神がRIDMの基礎になる。

安全目標を設定する目的は、安全に関わる国の判断の基礎を与え、事業者の達成すべき安全のレベルを公衆の認識できる尺度で示すことである。安全目標の設定により、次の利益が期待される。

- ・ 国の行うリスク管理に、透明性・予見性・整合性を与え、合理的で整合のとれた安全確保措置の体系の構築に資する。
- ・ これにより、産業界・事業者のリスク管理の効果的な実施、技術開発を促進する。
- ・ 共通の尺度を用いて公衆と対話することにより、目指すべき安全のレベルに関する認識の共有に資する。

国は、国民のために確保する安全水準を適切な水準にするべく規制活動を行うことになる。したがって安全目標は、国が規制活動において選択す

る、安全水準を示すものである。一方、事業者においては、これを上回る水準の達成するあるいは最適化する方法として、リスク削減に関するコストベネフィット解析等の考え方を活用することが考えられる。リスクマネジメントを実現するうえで、安全目標とリスク解析は必須の要件である。

5.2. コストベネフィット解析とリスクベネフィット解析

コストベネフィット解析とは、「リスクマネジメントの段階でいくつかのリスクの削減策が提案された場合、必要に応じ選ばれた削減策の評価を行うための手法であり、企業や、場合によっては行政当局も、リスク削減策を実施するための必要な経費と、実施に伴い得られるベネフィット（削減されたリスクに伴うすべての便益）とを評価し比較する手法」であり、RIDMには必須の手法である。

一方で、リスクベネフィット解析とは、「ある活動から得られる経済的便益と環境や安全へのリスクとを計量比較する手法」である。実際のリスクベネフィット解析では、さまざまな代替案を議論することになるので、コストベネフィット解析も適用されることが多い。図7の安全限度や安全目標の設定においてはシステムのもつベネフィットを考慮して定まることになるので、リスクベネフィット解析に基づいて検討される。

中西は、環境問題を考える時の手がかりとして、リスクベネフィット解析の観点から図8に示すように環境影響と経済性（環境保全に要する費用）の2軸で考えることを提案している[11]。環境問題も安全問題も対策をすればコストがかかると思われているが、実は経済性と安全性・環境特性とが両立する世界（第1象限）が存在する。例えば、安全問題では高信頼性設計が、環境問題では高効率化や省エネが、それに相当する。もちろん、両方とも成立しない世界はありえない（第3象限）。第2象限と第4象限はコストベネフィット領域で、例えば地球温暖化問題でいえば、京都プロトコルは第4象限に相当し、先進国はその過去におけるCO₂排出の責任からも経済能力や技術能力からし

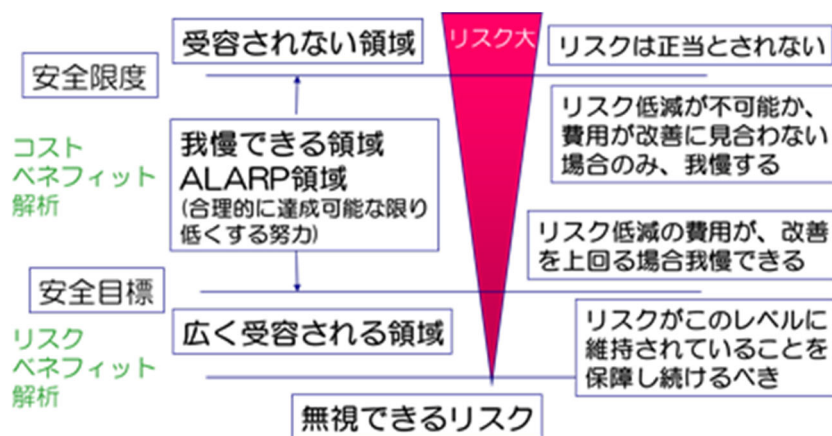


図7 英国の安全目標の基本的考え方[10]

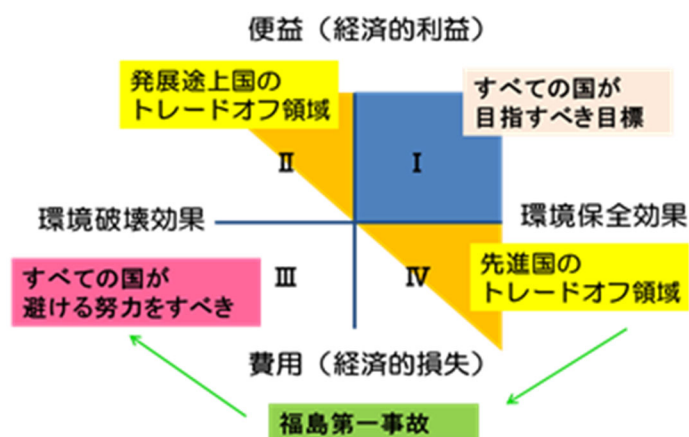


図8 リスクベネフィット解析に基づく環境保全と経済性の関係(中西,1994 改変) [11]

でも、たとえコストがかかっても温暖化対策をすべきであると考えられている。ただしむやみに実施するのではなく、コストとリスクのトレードオフで、安いコストで有効な効果がある対策のみを実施することになる。これに対し、第2象限の途上国ではこれからの成長を阻害しないように、少しの排出量で大きなエネルギーを得られるのであればそれを許容しようという領域である。第2象限は、発展途上国が考慮すべき領域であり右上ほど望ましく、第4象限は先進国が考慮すべき領域でありこれもまた右上ほど望ましい。

安全の問題では、この図の横軸を安全性向上にかけると費用に読み替えれば同様な議論が成り立つ[1]。常識的には安全対策はコストの増大要因になると信じられており、安全性と経済性（生産性）はトレードオフの関係にある。すなわち、安全性を優先して安全方策にコストをかければ、事故による損害を減らせるかもしれないが、生産性が落

ちてトータルコストは上昇してしまう。逆に、生産性を優先して安全方策のコストを抑えれば、事故による損害が増すことになる。したがって、両者のトレードオフ点を探すことになる。それには、可能な限りのリスク算定を行い、リスクの大小による優先順位に基づいて安全方策を施すことになる。さらにいえば、状況は環境問題とまったく同一であり、第四象限の安全方策はトレードオフに基づき実施すべきであるが、究極的には第一象限の経済性と安全性の両立を目指す努力が最も望まれる。

6. 技術システムの社会的受容

技術立国の日本にとり、技術システムの社会的受容は一企業の利益の議論ではなく国家百年の計の問題である。安全は確かに技術システムの社会的受容を支配する要素であるが、それは安全が第一義であることを意味するものではない。安全

は技術システムの社会的受容に対する制約条件として働くが、技術システムの社会的受容は他の価値項目とのバランスで判断しなければならない。これは、システム安全の一般原則の 1 つの、「システム設計におけるトレードオフの重要性および対立を認める」という観点に合致する。

しかし、技術システムの社会的受容の議論の実態は、安全か危険かそしてその判断に基づき推進か廃止かの二分論が多い。本来は、合理的なリスクベネフィットの議論に基づき技術システムの社会的受容を判断すべきである。対象とする技術システムの社会的受容に係るリスクとベネフィットのトレードオフの線引きには、例えば、以下の事項を考慮することが望まれる。

- ✓ 事故リスクや環境リスクなどを、他産業のリスクや自然災害のリスクと比較
- ✓ 地球温暖化・環境問題などに対する貢献、エネルギー、食料などのセキュリティ問題に対する効果
- ✓ そのシステムの経済性などのベネフィットを他産業のそれと比較
- ✓ 国家における当該産業技術の位置づけ（推進・規制、賠償責任、地域共生の在り方）
- ✓ 自主技術開発のリスクとベネフィット

人々が、リスクとベネフィットの判断ができるには、当該技術システムの意義と技術システムに関する最小限の知識が必要になる。それを知ることの人々に求め、あるいは期待するのではなく、関係者の責任として、少なくともその技術システムで「できること」と「できないこと」、それによって生じる「メリット」と「デメリット」、「守れること」と「守れないこと」、などを人々に明示することが不可欠である。

7. 終わりに

終わりにあたり、総括として「システム安全」「リスクに基づく意思決定、RIDM」「ヒューマンパフォーマンス向上」の関係性について述べておきたい。巨大複雑システムにおける「システム安全」とは、「部分最適が全体最悪をもたらす」こ

とがないように、過不足のないバランスの取れたシステムの設計（ハード/ソフト）と運用（人間）により安全性向上を実現しようとする活動といえる（ここに PRA の価値がある）。言い換えれば、それは、リスクの優先順位に基づき、コストも考慮して合理的な範囲で脆弱性をつぶしていく「RIDM」活動である。ところで、今ある巨大複雑システムは、深層防護や設計基準事故などの安全の論理に基づくハード設計や品質保証活動を通じてハードに起因するあるいは関するリスクは低減しているので、残ったリスクは人間が絡んだ事象といえる。このため、リスク低減活動は、リスクに係る人間行動を良い方向に誘導する「ヒューマンパフォーマンス向上」活動という言い方もできる（ここに HRA の重要性がある）。さらには、組織の業務プロセスにおける脆弱性を見つけつぶしていく RIDM 活動を継続することによって、初めて「安全文化の維持向上」にも繋がっていくと期待できる。

参考文献

- [1] 氏田博士、柚原直弘：『システム安全学-文理融合の新たな専門知』2015.9、海文堂出版。
- [2] 日本医療安全学会 特別寄稿、システム安全 - 確率論的リスク解析と人間信頼性解析、第 2 回日本医療安全学会学術総会、医療安全文化と医療安全ガバナンスの向上-医療事故死亡ゼロ社会を目指して。質向上とリスク科学の立場から-、2016 年、東京大学
- [3] PPT 資料「新型コロナウイルスの NOW!」、2020 年 4 月 26 日、公立陶生病院 感染症内科 武藤義和
- [4] ISO/IEC, Safety aspects-Guidelines for their inclusion in standards, Gude51, 2014 : (JIS B 8051、安全面—規格への導入指針)。
- [5] NUREG/CR-1278:Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, USNRC, 1983.
- [6] NUREG-1628: Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA)), USNRC,

2000.

- [7] 氏田、久保田、河野：プラント運転員の緊急
時における認知過程の実験的分析、人間工学
Vol.29, No.4 pp.239-248, 1993.
- [8] 高橋信, 氏田 博士：原子力学会誌 連載講座、
良く分かる PRA～うまくリスクを使えるた
めに～第5回 人間信頼性解析の現状
- [9] U.S. Nuclear Regulatory Commission, The
International HRA Empirical Study, Lessons
Learned from Comparing HRA Methods
Predictions to HAMMLAB Simulator Data,
NUREG-2127, August 2014.
- [10] 英国の安全目標の基本的考え方 UKHSE:
Health and Safety Executive, 1992.
- [11] 中西, 水の環境戦略 (岩波新書)1994.

※ 技術情報誌アドバンスシミュレーションは、
アドバンスソフト株式会社ホームページのシ
ミュレーション図書館から、PDF ファイルが
ダウンロードできます。(ダウンロードしてい
ただくには、アドバンス/シミュレーション
フォーラム会員登録が必要です。)