解説記事

リスク評価

現代産業システムのリスクアセスメント論
講義シリーズ－第3回－
Lecture series of risk assessment methodologies for contemporary industrial systems No.3

丹羽 雄二 Yuji NIWA 横浜国立大学
吉川 榮和 Hidekazu YOSHIKAWA 京都大学

1．はじめに

第２回目の連載では、現代産業システムの特徴、それを構成する設備と人間の中に潜在するリスクの諸相、それらを低減するための方策について解説した。今回は連載のまとめとして、現代の産業システムのリスクアセスメント、即ち本連載で解説する確率論的リスク評価（PRA：Probabilistic Risk Assessment）が実際にどのように行なわれるかを解説する。

2．現代における大規模・複雑システムのリスクアセスメント

正確なリスクアセスメントでは、災害という形でリスクを顕在化させるトリガ事象から災害に至るまでのシナリオ（シーケンスと呼ばれることもある）を漏れなく洗い出すこと、トリガ事象が評価しようとする災害の原因となることを何らかの方法で確認すること、さらに洗い出すべき原因に網羅性が求められることを既に説明した。

さて、リスクアセスメントの実施にあたって、どのような災害を考えるべきか、つまり災害の状態をどのように規定するかが問題である。一般には、災害の状態を一意に規定することが多い。例えば、原子力発電所の災害の状態の場合、「原子炉（炉心）の損傷」と一意に規定してリスクアセスメントを行うことが通例となっている。

原子力発電所のように大規模・複雑システムの場合、前回解説したように、多様な災害への予防策が幾重にも講じられているので、個々の予防策がうまく働かないことを想定すると、非常に多くのシナリオを考える必要がある。

◆連絡先：
丹羽 雄二，e-mail: niwa@ynu.ac.jp
吉川 榮和，e-mail: yosikawa@energy.kyoto-u.ac.jp

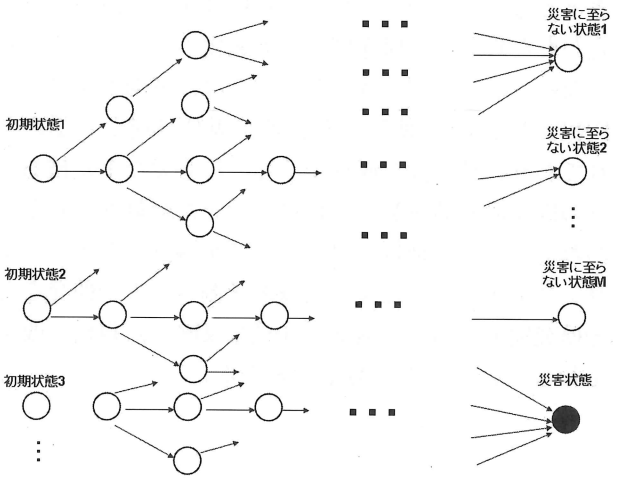
一方、原子力災害が万一起ったときに、結果としてどの程度の人命が失われるのか、その最も確からしい値は幾らかが、原子力発電所のリスクアセスメントへの世間の重大関心事である。これが本来社会に発信すべきリスクアセスメントである。

しかし、原子炉が溶融し、放射能が格納容器を貫通し、それらが、周辺及び、大都市等の人口密集地に到達するシナリオは想定できても、放射能を大都市まで運ぶ風の向きや風速など天候しだいでも災害規模は変わってくる。そこで原子力発電のリスクアセスメントでは、結果としての「人命損失」より、それを引き起こす「原子炉の損傷」の予想頻度を評価対象としている。

航空産業でも同様で、最終的な災害状態は「墜落」である。「人命損失」数は、墜落する場所によって大幅に変わるからである。

以上のような大規模・複雑系の災害リスクアセスメントパス（シナリオ）を図示すると図－１のようになる。図中、災害状態に行き着くパス（シナリオ）を選別し、その起こる予想頻度を求め、あらゆるパスの予想頻度の和をもってリスク値としている。

ここで、第１回目の連載に立ち戻り、評価すべき最終状態、即ち、災害状態が定義されたとすると、リスクは、



図－１　リスクアセスメントシナリオ概念図

$$R \overset{def}{=} \sum_{i=1}^{N} p_i C_i = C \sum_{j=1}^{k} p_j \qquad (1)$$

となる。ここで、Nは評価すべきシナリオ全ての数でCiはシナリオｉでの損失、kは予め災害状態が決められた場合の災害に至るシナリオ数である。原子力発電所の場合は炉心損傷に至るシナリオの数であり、Cは炉心損傷の結果生ずる損失である。もし損失を喪失する人命や損害コストとすれば、Cにはしかるべき定数値を与えれば良いが、(1)式で明らかなように既に定数であり、リスクアセスメントでは、Cは除外して炉心損傷が生じうる確率である次式をその評価対象とする。

$$R \overset{def}{=} \sum_{j=1}^{k} p_j \qquad (2)$$

すなわち原子力発電のリスクアセスメントでは、(2)式の定義に基づき、リスク量として特に各シナリオの災害状態に至る確率の総和を評価値とする。但し、その評価のための基礎データとして必要な機器故障率、ヒューンエラー率にはそれぞれの平均値を用いて計算し、その結果(2)式で得られた値をリスクの点推定と呼んでいる。一般に原子力のリスクアセスメントではリスク曲線を求めることは少ない。

3．PRAの長所－人間信頼性の考慮

3-1）最近の産業災害－「複合事故」の特質

産業災害について子細に原因を調査するとその殆どが、「複合事故」である。2005年４月、JR福知山線列車脱線事故では未曾有の死傷者が出て、これも「複合事故」とされている。前回も詳細に説明したように、鉄道では「深層防御」の設計を原子力発電所程明確には謳っていないが、それでも設計段階では反映されている。事実、脱線を防止する車輪形状、ATS（自動列車制御システム）等で、単一の故障、単一の人間のミスで生じる災害は防ぎ得る設計となっている。

「複合事故」とは、設備故障、人間のエラーが複雑に絡み合って災害に至るものである。人間のエラーを引き起こす原因には、意思決定までの余裕時間、設備のインタフェース（人間と機械の特に情報の接点を言い、列車では、運転席のCRT、指示計器等を言う）、物理的職場環境、教育、組織風土、組織からの要請、精神面も含めた健康状態等多岐にわたっている。実際、福知山線事故を俯瞰してみると、上層部から運転手に時間厳守の通達が行き渡っていたことが報告されている。ダイヤ通りの運行は、乗客にとって必須のサービスである。そこで運転手は、２つ前の駅でオーバーランを起こし、その遅れを取り戻そうとスピードオーバーを起こしたことが、災害の一因とされている。

この事故は一方的にJRに責任があるものの、「安全最優先」と「客の利便(convenience)」は運転手への相反する要求であることに十分留意しておきたい。「安全」を最優先すれば、少しの異常を人、機械が検知しただけでも、列車を止め、原因の徹底追及と再び起こることの無いように措置を講じなければ運転を再開してはならない。しかし、定刻どおりに運転しなければならないことが運転手の「安全無視」のスピード運転をもたらし、脱線事故につながった。

新幹線でも遅延を起こした場合、客が係員に食ってかかっているのを我々は目にする。人は列車の時間遅れに厳しいだけではない。人は列車にもアメニティを求める。その結果、外の景色が見やすいようにと窓はどんどん大きくなる。窓に鉄格子を安全のために取り付けようものなら、客から、我々は投獄されているのではないとクレームが出るであろう。又、中の人間を守ろうと、厚い鉄板で電車を作れば、その分、エネルギーを消費し、運賃の増大を招く。

利便性、アメニティを求めるなら、乗客はリスクを負い、安全を求めるならば、乗客は不便と運賃の上昇を受け入れなければならない。「安全神話」はマスコミが作り出した造語であり、虚構である。真に「技術の安全と社会の安心」を希求するリスクアセスメントにおいては、人間に起因する災害リスクと設備に起因する災害リスクを明確に区別した上で、事業者、或いはサービスを受ける者の意向の影響を受けることなく、双方のリスクを客観的なプロセスで評価する必要がある。

3-2）PRAにおける人間信頼性の考慮方法

鉄道産業では従来リスクアセスメントが設備まわりだけに集中していたようにも想像される。上記のJR事故の教訓として、経営上の力点が乗客サービスに傾いてそれが運転手の安全運転に及ぼす悪影響に思いが至らなかった点で人災対策が遅れていたことが指摘されている。

後章で詳細を説明するフォールトツリー（fault tree：FTと書く）は多くの産業で、災害の原因の把握、事故の未然防止のために活用されている。しかし、状況に応じた人間の振る舞いの信頼性について考慮されて

いる評価のフレームワークはPRAを除いて寡少である。人間と機械が複雑に干渉する現代の大規模・複雑系、或いはインフラシステムにおいては、設備信頼性と共に、同じ努力を傾注して、人間の信頼性を評価する必要がある。

原子力分野では米国スリーマイル島第2号機事故が、「人災」といってもよいものであったので、人間信頼性解析に関する研究が盛んに行われた。その中でTHERPと俗称される人間信頼性解析手法[1]は、世界中で実際の原子力発電所のリスクアセスメントに最もよく適用されている。

3-3）PRAの持つ意味と留意事項

THERPを用いることにより、システムにおけるヒューマンエラー発生に影響を及ぼす種々の要素を入れて評価できるPRAのフレームワークは有用である。但しTHERPが予測するヒューマンエラー発生率の基礎データの根拠や、その手法の適用の是非を巡って、現在でも議論が行われている。しかし著者らはこの議論は本質的ではないと考えている。人間の信頼性評価そのものに、真の値は求めようがないと考えるからである。

PRAから出てきた数字だけが一人歩きし、数字が出るまでの過程はブラックボックスでは折角のリスクアセスメントも意味がない。まして根拠不明なリスク値で一般社会に「安全度」の説得に用いるというのは言語同断である。

よりリスクを低減させようとする不断のリスクマネジメント活動のための一つの指標として、PRAで推定したリスク値を活用するためには、そのリスク解析の過程、仮定を第三者が理解してチェックできるようにすることに意味がある。つまりリスクアセスメントを組織的なリスクマネージメント活動に有効に活用するには、データの根拠、仮定、解析の過程が第三者に追試可能になるよう、トレーサビリティ（Traceability）とそのための透明性（transparency）を具備させることが、リスクアセスメントの絶えざる改善にとって肝要である。

PRAでは、設備、人間信頼性のデータベースをどのように整備するか、これが真っ先に真剣に取り組まれねばならない。従って、様々な分野においてPRAをもとにリスクアセスメントを試みようとするならば、先ず、適用可能な信頼すべきデータベースが存在するかどうかを、まず十分に調査する必要がある。例えば電子部品であれば、MIL-HDBK-217というアメリカの軍事データベースで膨大で適用可能なデータベースがある。

4．PRAの流れと定量化の道筋

4-1）フォールトツリー解析

現代の産業システムのPRAを行う場合、大まかに言えばフォールトツリー（FT：fault tree）とイベントツリー（ET：event tree）の2つの大きなシステマティックな解析とその統合によって行われる。さらに、他のアセスメントでは見られない独特の評価も実施しなければならない。前節でも述べたようにアセスメントにあたっては、当然使用する機器故障やヒューマンエラーのデータベースが既に決定されている必要がある。

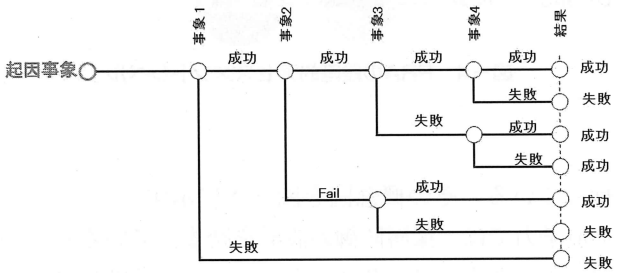
FTの概略を述べる。一般的には、何か故障原因を分析する場合、その原因を突き止めるために、考えられる故障原因を論理条件と共に詳細に書き下していく方法として採用されている。不具合事象をトップとして、詳細に原因を書き下していくので、トップダウンアプローチの一種である。一般にFTだけを用いて故障分析するなら、解析の打ち切りは解析者の判断に委ねられるが、PRAの中でFTを用いる場合は、故障率やヒューマンエラー率のデータベースが存在するところまで解析を行う。この解析打ち切り事象を基本事象や基事象と呼んでいる。FTの事象が論理関係で結合されていることを考えると、基事象の生起頻度－一般的には故障率で与えられる－が既知であれば、今度は基本事象を、ボトムからトップ事象に遡って行けば、トップ事象の生起頻度が計算できるはずである。基本的にANDは故障率の乗算、ORは和となる。このように、故障率データベースがあれば、FTで解析したトップ事象の生起頻度が定量化できることになる。

4-2）イベントツリー解析

イベントツリー（ET）の構築では、先ず事故に至るまでの事象の推移を、状態の遷移として離散化することから始まる。この離散化された状態のことをヘディングあるいはノードと呼ぶ。以下ではノードを使う。ノードは通常、時間の推移順に書いていく。各々のノードで、成功する場合と失敗する場合に分岐させてさらに後続事象の発展を書いていく。このようにすれば原因から最終状態まで、同じ作業を繰り返して事象発展のシナリオを漏れなく表現することができる。

FTが、結果から原因を推定するというトップダウン的なアプローチであったのに対して、ETは原因から結果を推定していく意味でボトムアップ的アプローチであると言うことができる。FTが盛んに様々な分野で適用されるのに対して、ETは若干、解析を進めることも困難とあって、現在適用されている分野はFTよりも限られるようである。簡単なETの例を図－2に概念的に示す。

ETを導入することの大きなメリットは途中の事象記述で、人間の運転操作等を、比較的分かりやすい形で入れ込めることである。従って、人間－機械系のリスク要因を記述することができるのである。無論、FTに入れ込むことは可能であるが、この場合は単一の人間のエラーを入れ込むことが多い。大規模・複雑系のリスクアセスメントは膨大な情報を必要とし、その対策として、ETとFTに情報を分散させて解析させていると考えても良いであろう。



図－2　ETの例

4-3）リスクの定量化

基本的なPRAのプロセスは、先ずETを構築することから始まる。図－2のようにノードがN＝4個存在する。各ノードでの分岐はPRAでは成功、失敗のみを扱う。従って、シナリオの数は、$2^N=2^4=16$個存在する。この程度のETであれば、各シナリオの意味を認識しやすいが、ノードの数が例えば10を超える場合、シナリオの数は、1024となり、各々を精査することが困難となる。従って、ETのノードの数を余り増やすことは、解析の透明性や、現在よく問題にされるトレーサビリティの観点から十分慎重であるべきである。

実際には設備間の依存性等を考慮に入れて、シナリオの数はもっと低減するテクニックがあるが、これはノードの入れ替えが生ずる。一般的に、ETは時間の推移の順序に沿ってノードが並べられているので、これらの推移が分からなくなり、ETの評価に支障を来すと言う欠点がある。

ETにおいて、失敗のシナリオの生起頻度を加算した値は、ある一つの起因事象に対して、それが災害に至る予想頻度を与える。

さて、ここで成功、失敗の分岐確率をどのようにして見積もるかというと、ETのノードは実際には、事象か状態となっているので、これをトップ事象として、FTで展開し、故障率データベースが存在する基本事象まで分解し、各々の故障率を後に述べる演算によって、ボトムアップで、トップ事象生起頻度（即ちノードの失敗確率）を見積もる。人間の操作が入っている場合は、これも基本的に同じ方法で操作に失敗する予想確率を求める。成功の場合は、1から得られた失敗確率を減じる。

最終的に災害状態に至るシナリオの予想頻度は、各ノードでの分岐確率を乗ずればよい。あるノードで成功しても、あるノードで失敗すれば災害に至るシナリオは多数存在するので、各シナリオがどのような結果を招くのかを精査しておくことは非常に重要になる。

以上のプロセスを考え得る全起因事象について定量化し、それを加算したものがリスク値である。読者は気づくであろうが、PRAというものは、評価しようというシステムは複雑になればなるほど大型化して、サブシステムや部品の数が多くなればなる程、莫大なマンパワーが必要となる。リスクアセスメントを行おうとするものは先ずこの事実に気づいておく必要がある。一般的には、運用サイド（運転員、保守作業員）、設計サイド（機械設計、電気・制御システム設計）、アセスメント専門家等のスタッフがチームを作り、包括的で現場の実情を反映したアセスメントを行う必要がある。これら一連のアセスメントの流れを図－3に示した。

4-4）PRA独自の解析

先ず、ETの中で「サクセスクライテリアの決定」というものがある。これは前述のように各ノードでの失敗が最終状態（災害状態）にどのような影響を及ぼすかを評価することである。換言すれば、各ノードで災害状態に至らないのは、どのような状態なのかを決定することである。例えば「ノードiでは、多重化されたポンプN台の内、少なくともM台が動いていけば、災害状態には至らない」というような、ノードが成功の分岐状態となるために必要な条件の規準（クラ

イテリア）を言い、一般的にはシステムの仕様や設計情報から得ることができる。設計情報から決定が困難な場合は実際にシミュレーションコードを動かして、当該の条件で事態が推移した場合のプラントの状況を予測し、シナリオが成功となる条件を決定しなければならない。

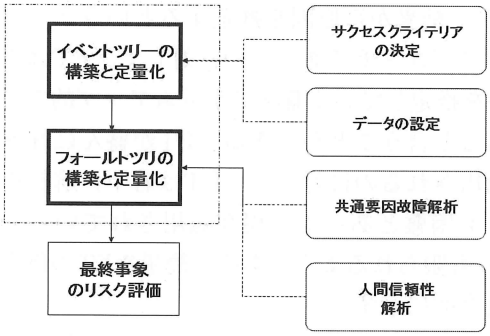
次にPRAで使用するデータベースの決定を行う必要がある。例えば、起因事象、機器故障率、人間の過誤率にどの統計データを採用するかを決定することである。

一般の化学プロセス産業と比べて、航空宇宙産業関係や原子力発電所ではシステムの多重化が実施されており、信頼性のさらなる向上が図られている場合が多い。ところが、そのシステムの多重化（と独立化）が無効化されてしまうような事態がしばしば起こる。例えば、同じメーカーで同じ工程で製作された機器が多重系を構成している場合に、同時に同じような故障が起こってシステム全体の機能が失われるというような状況が起こりえる。PRAでは、アセスメントの精度を上げるために考え得る要因をできるだけ積極的にアセスメントの対象にしていこうという考えがある。このような同じ原因による同時故障を「共通原因故障」（CCF：common cause failure）と言う。[2]「共通原因故障」には様々なモデルが提唱されている。PRAの分析者は、アセスメントを行おうとする対象に最もよく適合したモデルを選定しなければならない。人間信頼性を考慮できることがPRAの大きなメリットであることは既に述べた。図－３でもそれが示されている。図－３では人間信頼性評価はFTの評価の際に実施することになっているが、重要で複雑な操作は、ETのノードとして評価する場合が多い。

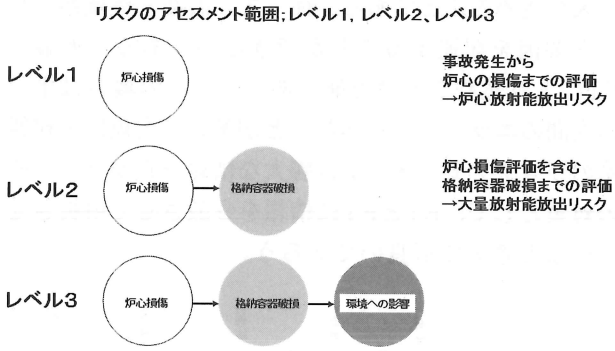
５．内的事象と外的事象（地震、津波他）

PRAには、どの被害までのリスクをアセスメントするかという段階の設定と、起因事象の範囲の設定もある。内的事象とは、評価しようとするシステム（社会、交通、プロセスプラント等）内部の不具合が原因となって災害に至る事象であり、外的事象とは、地震、火災、浸水（台風等による）、津波等の原因により評価対象が災害に至る事象を言う。

災害に至らないようにするための深層防御については既に説明したが、原子力発電所のリスクアセスメントでは、これに対応する形で、３段階に分けて評価を



図－３　アセスメントの流れの概要



図－４　PRAの段階的アセスメントレベル

行っている。その概念図を図－４に示す。

原子力では、深層防御の設計を踏まえているので、図－４のようにアセスメントのレベルを多段階に分けることができる。レベル１は閉じたシステムが深刻な炉心損傷という事態に至る予想頻度を計算するフレームワークであり、既に説明したように、ET、FTが結合する形で評価される。レベル２は閉じた系が破壊される予想頻度を評価するものであり、自ずと用いる手法も若干異なってくる。レベル１の起因事象に該当するレベル２のアセスメントで初期のトリガとして与えられる情報は、原子炉容器がどのような損傷の仕方をするかである。例えば、完全に水がない状態で、原子炉の炉心が溶融してしまうのか、或いはある程度の水が持ち込まれた状態で溶融するのかといった数種類のモードが予め設定されている。

レベル２では原子炉の炉心が溶融して、格納容器圧力の耐圧以上になるまでの事故進展を評価する。従ってETによる評価が中心となる。レベル３となると、どのような核種（ソースターム）がどれくらいの量、どれくらいの予想頻度で出るかを入力とし、地形、風向き、保健物理の知見を利用して、災害即ちガンに至

るであろう予想頻度を評価する。レベル３になると地形の表現（モデル化）、風向きの大きさ、風向の評価について余りに不確定性が大きく、現在この不確定性をどのように解決していくかについての検討が行われている。

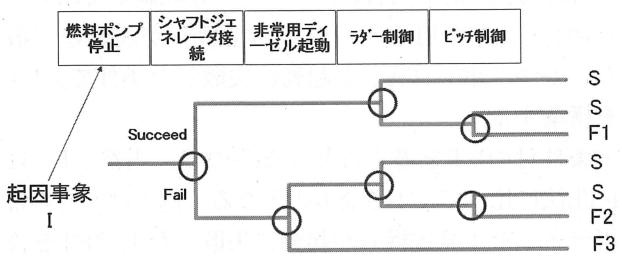
外的事象の評価は、例えば、プラント内で火災が起こったとして、どの範囲に影響が及ぶかを決定論的に評価する。その状態を起因事象として、従来のPRAのフレームワークで評価するのである。地震に関しても過去の立地地域で起こった歴史地震動から、将来起こるであろう大地震のマグニチュード、震源を評価し、実際にどの機器がどの程度の影響を受けるかを評価する。殆どがレベル１の起因事象として地震の影響が反映されるが、原子炉そのものが地震で影響を受ける場合や、格納容器そのものが影響を受ける場合も評価対象となる。このように外的事象PRAでは、地震、火災、津波他、個々で評価方法をカスタマイズしていく必要がある。

6. FTとETの合成

6-1) PRAにおける基本的なリスク定量化

前章、レベル１、２、３、内外事象の中で方法論として、もっとも確立しており、適用分野の広いものは内部事象のレベル１のPRAである。本解説では専らこれについて述べる。

一般の産業災害のETを実際に書き下すとノードが莫大な数になることは既に述べた。このような場合は、ETの評価が困難になる場合が多いので、評価結果をより分かりやすくするためには、できるだけETを簡便に書くことが得策である。そのほうが、解析結果を第三者が理解しやすくなる。FTは歴史的にも古く、ETよりも多くの人が解析を実施することができるので、FT中心にアセスメントを行うほうが解析者にとっても好ましい。



図－５　ETの例

図－５はある船の座礁のETである。まず図－５の上部の矩形の並びが（起因事象も含めている）ノードである。時間の推移とともに起こると予想される状態が記述されている。「ラダー、ピッチ制御」とあるのは、制御システムが作動する状態を示す。起因事象は人間が誤って燃料ポンプを停止させたことであるが、このようなエラーを起こす統計値が得られていたとして、この起因事象が起こって災害に至る予想頻度p_Iは次のようになる。

$$p_I = I \cdot (F1 + F2 + F3) \qquad (3)$$

F1, F2, F3 のパスが生ずる予想頻度は、分岐点での失敗、成功の確率をパスに沿って乗じていけばよい。例えば、一番簡単な例は、*F3* については、「シャフトジェネレータ接続」ノードの失敗確率、「非常用ディーゼル起動」ノードの失敗確率を乗ずればよい。各々のノードをトップ事象として先ずFTを構築し、これを機器故障率データベースが引用できるまで展開し、トップ事象の非信頼度を計算する。これを分岐確率として採用するのである。このようにET、FTを結合させて、災害に至る予想頻度を計算するのがPRAの基本原理である。

6-2) FTとETの統合化の方法

前にもFTに情報をシフトさせた方が、見通しを得やすいと少し触れたが、ETとFTの結合のさせ方には２通りある。一つは、FTに情報をシフトさせる方法、即ち、「大きなFT、小さなET」で、シナリオの予想頻度を評価する方法である。

この場合、若干なりとも考慮すべきことがある。多くの機器は同じ電源や制御系統を共有している場合が多い。一般に、機能（または目標達成といっても良いであろう）の維持・達成に直接関わる機器をフロントライン系の機器と呼んでいる。フロントライン機器を設計通り動かす機器をサポート系の機器と呼び、具体的には、交流電源、直流電源、制御空気用コンプレッサ、軸受冷却機器、潤滑用機器等である。実際は、これらは複雑に干渉している。例えば、緊急時の重要な電源であるディーゼル発電機について考えよう。これは、正常な交流電源が使用できない場合、機器の電源を供給する極めて重要な機器である。ところが、当然

回転機器なので、冷却が必要である。即ち、冷却系がなければ、電源の供給という目標を達成できない。ところがよく考えてみると、緊急時、冷却系のポンプ電源は、ディーゼル発電機から供給を受けている。従ってモデル化に当たって、サポート系間での依存関係の無限のループに入り込んでしまう恐れがある。現実的な解決として、PRAの多くの場合、サポート系間の依存関係は、１次の関係、即ち一つのフロントライン系に関連するサポート系は独立として解析するが、著者らが試みた例では、考慮（モデル化）する次数によって、これらサポート系を有するフロントライン機器からなるサブシステムで点推定値に、影響があることを確認している。[3]この問題は今まで見過ごされてきた問題であるが、十分に検討、考察されて良い問題である。このようにPRAでも未だ解決すべき問題が残されている。

サポート系の扱いについては、基本的にブール代数を適用する。例えば、FTで得られた値が

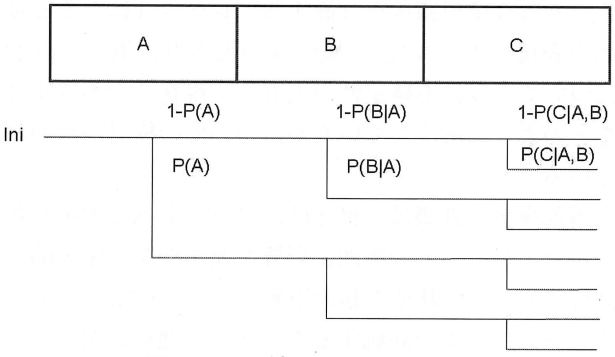
$$ABC + AB + AC \qquad (4)$$

となったとしよう。これは明らかにブール代数で

$$A(BC + B + C) = AB + AC \qquad (5)$$

となる。このようにブール代数を適用し、これ以上は簡単化できないところまで簡単化して得られた項（例ではABとAC）をミニマルカットセットと言い、大FT、小ETでPRAを行うには、非常に重要な概念である。最終的な災害状態に至るリスクはミニマルカットセットの和となる。(4)、(5)式を見れば明らかなように、値として異なってくる。特にブール代数適用前の値が、適用後の値より小さくなる場合は、リスクを過小評価することになる。これは避けなければならない。従ってブール代数の計算（簡単化）も最大限の注意を払っておこなう必要がある。

上記の方法は、 PRA実施者の間で、フォールトツリー・リンキング法（FTL：fault tree linking）と呼ばれている。本解説では、１つのFTについてのミニマルカットセットについて解説したが、この作業を複数のFTで行わなければならない。ミニマルカットセットを求めることに非常にマンパワーを割かなければならないことを意味している。しかしながら、実はミニマルカットセットを求める論理演算は計算機の得意とするところで、計算機による評価を念頭に置くと、実は非常に魅力的な方法である。FTは、人間の思考構造に沿った階層的なアプローチであり、ETに比べて、特別な情報、訓練なしで、大規模・複雑系の解析も可能である。一旦FTを構築してしまえば、ミニマルカットセットの計算そのものを計算機に任せればよい。



図－６　ETL法におけるETの解釈

これとは別に「大きなET、小さなFT」で同様の評価を行う方法である。この方法は前者FTLに対して、イベントツリー・リンキング法（ETL：event tree linking）若しくはバウンダリ・コンディション法と呼ばれる。前者はサポート系の状態について、ETに入れないのに対して、ETLでは、サポート系の状態をETのノードに全て入れ込む。当然、ETは多くのノードから構成されるものとなる。従ってミニマルカットセット計算の労苦からは解放される。しかしながら、ETの構築とその各ノードの分岐確率の計算について、労苦を強いられる。ETの分岐確率は正確には図－６の各分起点で記載した確率で表される。

例えば、ノードBの分岐確率を計算する場合には、Aが起こったという条件での分岐確率を計算しなければならない。より具体的には、例えば、ノードAが、「非常用ディーゼル発電機起動」であった場合に、ノードBの分岐確率を計算するに当たって、「非常用ディーゼル発電機」が起動に失敗した条件で、ノードBに失敗するFTを書く必要がある。ノードBが「ポンプA起動」である場合、ノードCの分岐確率を求めるために、「非常用ディーゼル発電機」が起動に失敗し、かつ「ポンプA」が起動に失敗した条件で、FTを構築する。

条件付のFTを書くことになるので、当然、FTはFTL法に比べて、小さなものとなる。例えば、「非常用ディーゼル発電機」が起動に失敗した上でFTを書くことを考えると殆どの機器は起動不能に陥っている

であろうから、これらの機器の考察はノードBの分岐確率を評価するFTでは考慮する必要がない。これで、FTで考慮しなければならない機器が減少し、FTを書くマンパワーが軽減される。又、例えば上図の例で、ノードA、B、Cに全て成功した場合のみ、災害を免れるとすると、災害を免れる確率は、

$$\{1-p(A)\}\{1-p(A|B)\}\{1-p(A|B,C)\} \quad (6)$$

となり、災害に至る確率は、

$$1-\{1-p(A)\}\{1-p(A|B)\}\{1-p(A|B,C)\} \quad (7)$$

となる。ミニマルカットセットの計算もする必要がなく、ノードの分岐確率をそのまま乗ずればよい。

このように例を使って説明すると、後者のETLの方が、マンパワーが少なく、比較的楽に、起因事象が起こって災害に至る予想頻度を求めることが可能ではないかと印象を持たれる読者もいるかも知れない。ノードの数が高々、2～3個の場合は、両者は余り変わらない。どちらかかと言うとETLの方が評価しやすいと思われるだろう。ところが実際は、ノードの数はETLでは、2～3個で済むはずもなく、膨大な数になる。その結果、意味のないシナリオを除外したとしても、シナリオの数は最早、紙に書くことすら困難になってくる。このETL法を適用して、アメリカのセコイヤという原子力発電所のPRAが実施されたが、各起因事象毎のETは、シナリオの数が、数万となってしまい、個々のシナリオは省略されている。結局、この方法でETとFTの統合化を図ると、余りのシナリオの数の多さに、解析者以外はそのETを評価することができなくなる。或いは、解析者自身も追えないかも知れない。これが、本解説でETL法を推奨しない理由である。トレーサビリティに問題があるからである。

これに対して、FTL法では、最も困難なミニマルカットセットの計算を計算機に任せることができる。その意味で、この部分のトレーサビリティは無くなってしまうが、コードの正当性が保証されておれば単純計算なので、かえって計算機が行う方が結果に信頼がおける。解析に用いられたETとFTを参照することができ、ETもノードの数が少なくなっていることから十分に評価することが可能である。FTは少々大きくても十分意味がわかるし、評価することができる。このような背景を踏まえ、世界中のPRAでは、殆どがFTL法によってFTとETを統合し、リスクの評価が実施されている。

7. まとめ

本連載では、連載の最終として、人間－機械で構成される現代産業システムのリスクアセスメントのためにPRAが適していること、また、そのために如何にPRAを進めるかの概略について解説した。実際のPRAは非常にマンパワーを要する作業で、この解説を読んでただちにPRAを実施できるとは思っていない。本連載の解説が、読者諸氏にリスクアセスメントの一つの方法として、PRAの原理を理解し、評価結果の意味を正しく認識いただければ幸いである。最後に本連載を行うに当たって貴重な示唆、意見を賜った東京電力原子力運営管理部横村忠幸氏に深い謝意を表します。

参考文献

[1] 例えばTHERPハンドブック、Swain and Guttman NUREG/CR-1278 (1983).

[2] NUREG/CR-4780, Procedures for Treating Common Cause Failures in Safety and Reliability Studies, Volumes 1 and 2(1988).

[3] Y. Niwa and N. Sugiyama: Study of Modeling Intersystem Dependencies in NPP, The 3rd International Conference on Probabilistic Safety Assessment and Management(PSAM-III), pp.1524-1529, Springer, Crete, Greece(1996).

(平成18年5月6日)