# リスク評価について

三友　信夫*1

# Introduction to Risk Assessment

by

Nobuo MITOMO

## Abstract

In modern societies, we have very high awareness of the need to ensure safety for several matters. But, the method of realizing "safety" is not fully understood. In the engineering field, the concept of a "risk" is used as the method of reservation of "safety." However, the definition of the word "risk" is used in various meanings and in the dialectal way.

Originally, "risk" is a word used in the field of economics, where the meaning is "loss" to a profit, and is a "possibility" that "loss" will occur. In the field of engineering, a "risk" is defined as the product of probability or frequency that an accident will occur, and the result or damage of the accident. Further in the field of engineering, evaluating this "risk" aims at reservation of rational and economical "safety."

This report shows the concept and definition of “risk”, first. The method of “risk” assessment is shown with some technique for each purpose. And valuation method for the result of risk assessment is also shown. Then some problems of risk assessment are discussed in the final chapter of this report with researches in our institute.

*1 運航・システム部門

原稿受付　平成 21 年 1 月 19 日
審 査 済　平成 21 年 2 月 4 日

## 目　次



## 1. はじめに

現代社会では、「安全」に対する意識は高いものの、この「安全」を実現する方法については十分に理解されていないと思われ、さらには「安全」を犠牲にした経済性の追求をした結果と考えられる出来事も起こっているように思われる。

工学分野においては「安全」の確保の方法として、「リスク」という概念が用いられている。しかしながら、この「リスク」という言葉の定義は、分野により様々な意味で用いられ、いわば方言的な用いられ方をされている [1)]。

そもそも「リスク」とは経済学の分野から用いられた言葉であり、その意味は儲けに対する「損」であり、「損」の発生する「可能性」である [2)]。工学の分野では、「リスク」は、事故の発生する確率（頻度）とその結果（被害）の積として定義されるものである。さらに 工学の分野においては、この「リスク」を評価することにより合理的、経済的な「安全」の確保を目指している。

本報告では、このような「リスク」の評価方法について、その概念と手法等について説明する。なお、具体的な例としては、本報告書の他の報告を参考にされたい。

## 2. リスクについて

「はじめに」で述べたように、「リスク」という言葉は方言的な用い方をされている。しかしながら、本報告で扱う「リスク」は、当然のことながら工学的な「リスク」であり、事故の発生する確率（頻度）とその結果（被害）の積として定義されるものである。

この定義に基づき、公衆の「リスク」を初めて定量的に評価したのが、合衆国原子力規制委員会（Nuclear Regulatory Commission, NRC）によるレポートである WASH1400、いわゆるラスムッセン報告 [3,4)]である。図 1 は、このレポートの結果として得られたリスク曲線である。横軸は事故による死者数、縦軸は、ある死者数を上まわる事故が発生する頻度を表わしている。例えば、航空機事故についてみると、この報告書が公表された 1975 年当時、100 人以上の死者を出すような事故は、アメリカ国内で年に 1 度まではいかないが 10 年に 1 度以上の頻度で起きていたことが示されている。ひとつの航空事故で 1,000 人以上死ぬような事故は、経験がないので推定値になるが、乗客・乗員だけだとほとんど起きる可能性がなく、こうした事故は、航空機が郡市に落ちることによって起きる可能性があることを示している。また、1 番下の曲線は、米国内に 100 基の原子力発電所があることによってもたらされるリスクの評価結果である。リスクは決して 0 にはならないが、原子力発電所のリスクは他の技術のもたらすリスクに比べてはるかに小さいことがわかる [5)]。このラスムッセン報告以後、原子力分野においてリスクは重要な役割を果たしている。

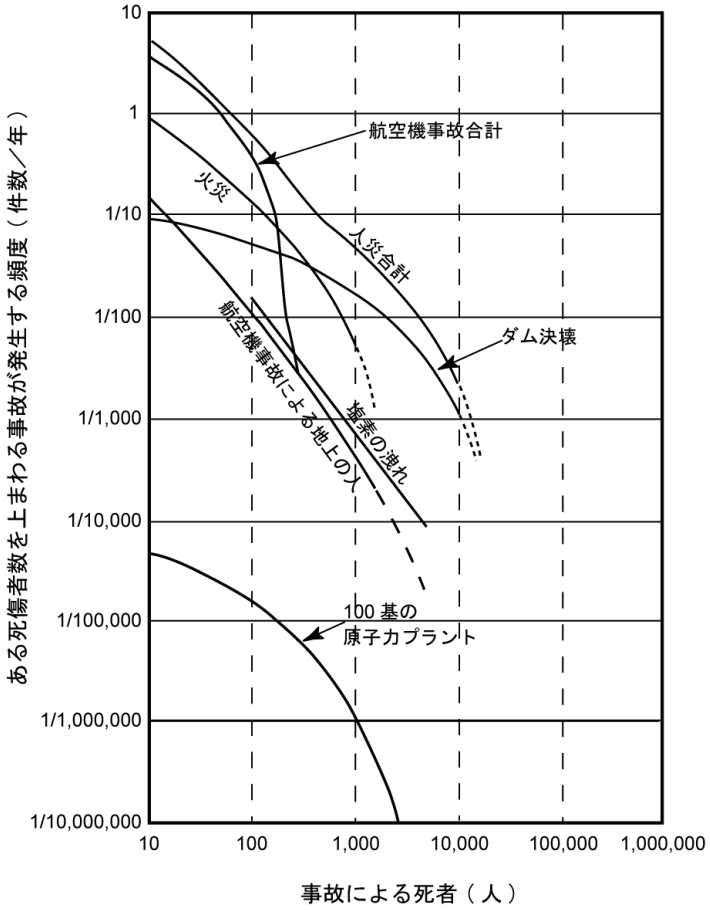



**図 1 様々な事象の社会的リスク** [5)]

また、主要な国際規格である ISO では、「リスク」を次のように定義している [6)]。

ISO12100：2003
・ 規格の名称 ：機械類の安全性－基本概念、設計のための一般原則
・ リスクの定義 ：危害の発生確率と危害のひどさの組合せ

本規格は、ISO/IEC GUIDE 51 の下に階層化された国際安全規格の最上位に位置する基本安全規格（A 規格）である。

## 3. リスク評価について

このように定義される「リスク」はどのような役目を果たすことが出来るのかについて考えてみる。「リスク」は、それが評価されることにより利用、導入されるものである。現在リスク評価が用いられている事柄としては、次に述べるようなもの等が考えられる。

・ 安全対策（安全上の課題の重要度）
・ 定められた目標値の妥当性の評価
・ 経済性の評価

ここでは、これらのような目的のために、実際にリスク評価を実施する際の手順について、述べる。

まず 評価対象において、事故に至る経緯の検討が必要の無い場合等、統計データ等により、発生する確率（頻度）と被害の積によりリスクを求めることが可能な場合がある。しかしながら、船舶航行時の事故や、船舶等大規模システムのトラブルに関するリスク評価を行う場合には、前述の様な方法では評価は出来ない。そこで、ここでは、この様な場合に用いられている標準的と考えられる評価手順を次に示す。

1. 危険因子の洗い出し

2. 解析シナリオ作成
3. 定量的評価

実際の解析を行う際には、それぞれのステップにおいて、そのステップにおける目的のために用いられる手法等もある。これらについて手順を追って説明、例示する。

### 3.1 手順 1 危険因子の洗い出し

このステップの目的は、解析の対象となる事象の危険因子を抜け落ちなく見つけ出すことである。したがって、リスク評価の対象となるプラント、機器、事象の調査、検討などといった作業が主であり、また多人数で行われるものが多い。

危険因子とは、「潜在的に危害となる何か」と考える。細かい定義は適用分野などにより様々に与えられているが、例えば、次のようなものが挙げられる。

· そこから事故につながる物理的な状況。多くはきっかけとなる何らかのイベントを伴う。
· 死亡、負傷、職業病、または装置、財産、環境の損害や損失から解放された状態でないこと。

このような危険因子を対象となるプラント、機器、事象の中で発見、評価するのがこのステップの目的である。

危険因子の同定は、リスク評価の最初の段階に位置づけられるものであり、リスク評価の対象において論理的に存在しうる危険因子を系統的に洗い出し、定量的、準定量的、あるいは定性的な解析によってそれらの重要性を大まかに見積もることで、リスク評価の方向付けを行うものである。

このステップで用いられる手法としては、以下のようなものが挙げられる。

- FMEA (Failure Modes and Effects Analysis), FMECA (Failure Mode, Effects, and Criticality Analysis)
- HAZOP (Hazard And Operability Study)
- SWIFT (Structured What IF Technique)
- Delphi 法

また、このステップの前にスクリーニングとして対象物の調査を行うとする場合もある。以下、上記の各手法にについて概要を述べる。

#### 3.1.1 FMEA 及び FMECA について

##### 3.1.1.1 FMEA の概要

FMEA は、比較的規模の大きい施設などを対象にした場合に比較的良く用いられる分析手法のひとつであり、「故障モード及び影響解析」と呼ばれることもある。評価対象について、品質改善の観点から専門家チームによる評価を行うことで、故障を予防、減少させようとする手法である。米軍での使用のために開発され、その後 NASA で宇宙開発のために長く使用されてきた。その後、様々な分野で適用されている。IMO では、高速船の建造時に行うべき安全性の評価手法として FMEA を規定している。

FMEA では、システムの構成機器のひとつに故障が発生した場合に、システムに及ぶ影響について表を使って解析する。各機器の本来の機能、発生しうる故障モードと原因、影響、故障検出方法、是正処置などの項目について検討する必要がある。また、見落としを避けるため、システムを系統的に調べる手順が定められている。その手順の概要を以下に示す。

1. 必要な情報の収集 (設計情報、関連データ)

2. 専門家チームによる作業
- 構成要素の選択
- 構成要素の機能の特定
- 構成要素で生じうる不具合の種類の特定 (故障モード)
- 故障により生じる局所的な影響 (局部的影響)
- 故障によりシステム全体に及ぶ影響 (最終的影響)
- 故障からシステムを防御するための方法 (故障検出の方法、是正処置)

検討は、各構成要素毎に順番に選択して行われる。そのため、一度に複数の機器が異なる原因で故障した場合は検討から除外される。一方、単一機器の故障が他の機器の故障を引き起こす場合や、単一原因による複数の機器が故障する場合は検討する。

3. 報告書の作成

報告書は主として以下の要素で構成される。
- 専門家チーム名簿
- 対象システムの記述 (システム名、構成、機能)
- 解析対象部分、除外部分の一覧
- 解析結果の集計と要点
- 各部ワークシート
- 各部ワークシート作成時の議論

表 1 機能レベル FMEA 手法による解析例 [8)]

| System | Sub-system | Component | Failure Mode (FM) | Cause | Effects to System | Detective Measures | AE Type | Other Conditions |
|---|---|---|---|---|---|---|---|---|
| sintering | sintering furnace | electric heater | failure to heat | failure of heater | incomplete sintering | thermometer | - | |
| | | temperature control unit | overheating | failure of control or power supply | air intrusion to furnace | thermometer | fire and/or explosion | |
| | | | | | | | loss of confinement | *1 |
| | | | failure to heat | | incomplete sintering | thermometer | - | |
| | | thermal insulation | failure to function | degradation, defectiveness | air intrusion to furnace | periodic inspection | fire and/or explosion | |
| | | | | | | thermometer | loss of confinement | *1 |
| | | pressure regulator | failure to open | failure | internal leakage | pressure gauge | loss of confinement | |
| | | shell | leakage | falling heavy object, degradation, overheating | air intrusion to furnace | pressure gauge | loss of confinement | *1 |
| | | | | | | | fire and/or explosion | |
| | | gasket | transformation | degradation, defectiveness, overheating | air intrusion to furnace | pressure gauge | loss of confinement | *1 |
| | | | | | | | fire and/or explosion | |

*1: When internal pressure equals outer one,　AE: Abnormal event

・　結論 (推奨事項等)

しかしながら、この FMEA 手法では、部品の点数分の分析を必要とするため施設全体を分析対象とする場合、多くの分析時間を要するなどの問題がある。そこで、玉置らは、作業の効率化を図るために，設備・機器の機能に着目し、その機能が喪失した場合の影響がどのような異常事象に進展する可能性があるかを分析するという「機能レベル FMEA(Functional FMEA : FFMEA)」を考案した [7)]。機能レベル FMEA の解析結果の例を、表 1 に示す。

### 3.1.1.2 FMECA の概要

FMEA に加えて、故障モードのシステムへの影響を故障等級として定量的に評価する CA (Criticality Analysis) を加味した分析手法のことである。構成要素の故障モードについて、システムおよび人の安全に及ぼす影響を評価し、定量化する。致命度 (Criticality) は、故障の影響度、故障の発生頻度などの関数で与えられ、得られた値を用いてリスクを推定する。

### 3.1.1.3 致命度の分析方法

2 種類の致命度分析: 量的分析と質的分析の手法がある。

量的致命度分析を行うために、解析チームは次のことを行う、

1. 所与の操作条件の下での、各部品の信頼性・非信頼性について定義する
2. 部品の非信頼性の部分と関連する潜在的故障モードを特定する
3. 各故障モードの発生による損失や深刻さの割合を求める
4. 3 つの要素の積によって致命度を計算する
   モードの致命度= 非信頼性 × 非信頼性の割合 × 損失の可能性
5. 各部品の致命度を関連付けられた各故障モードの和によって計算する
   部品の致命度= モードの致命度の計

質的致命度分析は、リスクを評価し、回避措置に優先度を付けるために行う。この目的のために、解析チームは次のことを行う、

1. 故障の潜在的な影響の深刻さを見積もる
2. 各潜在的故障モードの起こりやすさを見積もる
3. 故障モードを Criticality Matrix と比較する。これは横軸に深刻さを、縦軸に頻度を描いたものである。

### 3.1.2 HAZOP について

#### 3.1.2.1 HAZOP の概要

HAZOP は､FMEA 同様比較的規模の大きい施設などを対象にした場合に比較的良く用いられる分析手法のひとつであり､「運転性解析」逸脱と呼ばれることもある。不具合から開始して、両側へ解析を進めることで、ありうる原因と生じうる影響を求める。化学プロセスにおける複数の独立した事象が複雑に絡む故障を扱うために開発された。

そのため、主として、

1. プロセスプラントに潜在的に存在する危険
2. プラントの操作性、特に設計仕様を逸脱した運転を行なった場合の問題

を、確認するのに用いられることが多い。また、この方法は、危険シナリオ分析手法のひとつとして分類される。米国では連邦法やいくつかの州法でプロセスの危険因子分析に用いるべき手法として HAZOP を採用することが規定されている。

#### 3.1.2.2 HAZOP の特徴

HAZOP では､ガイドワード(Guide Words)と呼ばれるキーワードによって質問を設定し、回答を求めていく。そのため、系統的に危険なシナリオが把握しやすい。質問対象とするのは、設計仕様 (例えばケミカルプラント等では、温度、圧力、pH、攪拌、反応等) から逸脱した運転を行なった際に発生する危険因子とその原因である。

例えば、

- どこでどのような逸脱があるか
- 逸脱による危険因子は何か
- 逸脱の原因、操作上の問題点は何か
- それぞれの原因から危険事象への進展を阻止するための防護機能は何か
- 改善すべき対策は何か

等がある。

#### 3.1.2.3 HAZOP の手順

HAZOP の標準的な手順としては次のようなものである。

1. 分析対象となるプロセスの範囲設定と分析の目的の策定
2. メンバーの選定(数名)
   - 経験豊富なプロセスに詳しいリーダー
   - 設計や運転に携わる化工、化学、機械、計装などの各エンジニア
   - 安全担当者など
3. 基礎資料の収集 (PI ダイアグラムなどの情報とデータ)
4. ガイドワードの選定
5. 質問の作成（ガイドワードを用いた設計仕様の逸脱の仮定)
6. ワークシートのフォームの作成
   - 各設計仕様の項目､ズレ､原因､危険因子、防護機能、対策などのマトリックス表
7. 逸脱による潜在的な危険因子、操作上の問題点、対策の検討
   - リーダーによる質問､各メンバーによる回答、グループ討議を経た結論付け
8. 分析結果のワークシートへの記述

#### 3.1.2.4 HAZOP に必要な基礎資料

1. 分析作業の基本資料
   - プラントの構成要素である機器、装置類、配管および計装が示されているプロセス系統図等
2. その他の資料
   - プロセス・フロー・ダイヤグラム (PF ダイアグラム)
   - プロットプラン (機器配置図)
   - 運転保守マニュアル
   - 温度、圧力、流体のレベルなどの設定値に関するデータ
   - 過去の事故、トラブル情報

等である。

#### 3.1.2.5 HAZOP の質問の作成

プロセスの設計仕様から逸脱した状態に起因する潜在的な危険を特定し、操作上の問題を分析するために質問を作成する。この質問は、ガイドワードを手がかりに作成する。

### 3.1.3 SWIFT について

#### 3.1.3.1 SWIFT の概要

SWIFT は、専門家チームで行う危険因子特定の

ためのシステマティックなアプローチ技術である。化学プロセスプラントの危険因子特定を目的とする技術のひとつであるが、他の分野へも適用される。SWIFT はシステムと手順を高レベルで特定する。

SWIFT は通常の操作からの逸脱をブレインストーミングによってとりあげる。

「もし○○だったら?」

「どのようにして○○が起こりうるか」

ブレインストーミングにおいて危険因子の見落としを避けるため、チェックリストを使用する。

#### 3.1.3.2 SWIFT の特徴

主として、以下のように使用される。

- その後の定量的評価を目的とし、単に危険因子の特定だけを行うために使用する。
- 危険因子の定量的な評価を行う手段がない場合等に、推奨される防御策を論じるために使用する。

SWIFT の場合、標準手法が決まっていない。柔軟性のある点が長所でもあり、個々の応用に対して改変できるが、一定の方針が必要な場合もある。

#### 3.1.3.3 SWIFT 専門家議論の進め方

SWIFT の標準的な手順としては次のようなものである。

1. 解析対象となるシステムやプロセスを定義する。
2. リーダーの司会の基に、個々について順番に考えていく (リーダーは議論を構造化する)。
3. 論理的に存在しうる危険因子をブレインストーミングする。それらを抽出するが、議論はまだ行わない。
4. 議論が行えるよう、挙げられた危険因子を論理的な順番に並べ替える。主要なものから始め、順序付けをする
5. 各危険因子について順番に考えていく
   - イベントのありうる原因
   - イベントが発生した場合に起こりうる結果
   - そのイベントの発生を防御するよう、すでにシステムに組み込まれている安全策、安全策の妥当性
   - これらの議論を SWIFT 記録シートに書き込む (記録係)
6. もう一度、取りこぼした危険因子がないかどうか確認する。チェックリストを用いて、以前の事故記録等があれば参照し、万全を期す

#### 3.1.3.4 SWIFT の質問

SWIFT で出される質問は、次のようなものとなる。

- 機器を構成する、ある要素が壊れたら? 「ポンプが故障で停まったら」 「バルブが閉まったら」
- 操作者が適切な手順を実行しなかったら? 「不純物が混入したら」
- レベル調整機能が操作できなくなったら?
- プラントのある場所で火災が発生したら?
- 自然災害 (地震、洪水) が発生したら?

SWIFT 手法により抽出される危険因子は、ワークシートにまとめられる。

### 3.1.4 Delphi 法について

#### 3.1.4.1 Delphi 法の概要

Delphi 法は、専門家の合意形成のための手法である。潜在的リスクを抽出するための質問票を専門家の間で回覧して行き、順にそこにコメントを書き加える。参加している専門家が誰かは知らされるが、発言は匿名扱いとする。コメントが数周回覧されることで、プロジェクト全体のリスク、起こりやすさ、結果について、要素間の順位付けなどの合意が形成される。Delphi 法により、先入観や、特定の専門家による過度の影響を排除しやすいという点で、リスク評価において効果を発揮する手法。

#### 3.1.4.2 Delphi 法の応用先

応用例としては、専門医の意見を集約して治療スケジュールを構築する場合 (なるべく複数の専門医の意見により偏りのない計画が必要な場合など) などが挙げられる。その場合、以下のようなステップで合意形成が行われる。

1. まず複数の専門家に対して調査 (通常どの回答が誰のものかは明らかにしない)
2. 回答が集まったら、集計結果を提示しながら再度同じ調査
3. 各回答者は他者の回答結果の分布と自分の意見を比較した上で再度回答
4. こうしたプロセスを通常 3 回繰り返し、集約された回答を調査結果として用いる

この手法のポイントとしては、調査に参加する専門家に対し、調査の方法をよく周知させることが重要である。特に、繰り返し調査であること、および他の回答者の意見を参考に自分の回答の修正する手法であることを理解してもらうことが肝要である。

実際にこの作業を行った報告書等もあるが、例えば後述するデータベースの一つでもある IEEE

Std 500 RELIABILITY DATA においても、この手法による専門家の意見を収集してあり、その際に用いた質問票等も掲載されている[9]。

### 3.1.5 その他の手法

詳細は省くが、他にもマスターロジックダイアグラム(MLD)と呼ばれる手法もある[10]。これは、FMEA等が一つ一つの機器の故障を想定し、その影響を調べるボトムアップの探求方法であるのに対して、MLD はトップダウンの系統的分類方法であり、ボトムアップ式である FMEA 手法と組み合わせることにより、起因事象をさらに抜け落ちなく確認することが可能である。

以上、様々な手法について述べたが、この段階の目的は、「危険因子の抜け落ちの無い洗い出し」であり、手法は目的に応じたものを選ぶべきである。

### 3.2 手順 2 解析シナリオの作成

このステップにおいては、手順 1 で得られた危険因子から起こりうる解析シナリオを作成する。このシナリオの作成により解析の成否が決まるといっても過言ではない。つまり、シナリオの正しさはもちろんのこと、解析時の合理性等にも影響を与える作業である。

### 3.3 手順 3 定量的評価

手順 2 で得られた事故シナリオを基に、リスクの定量的評価を行う。この段階で用いられる手法としては目的等に応じて様々なものがあり、さらに書く手法については詳細な論文や専門書がある。そのため、ここでは代表的な手法について、それらを適当にまとめている参考文献[11]から紹介することとする。さらに詳細な説明については、それぞれの手法に応じた専門書等を参考にされたい。

### 3.3.1 イベントツリー手法について

イベントツリー手法は複雑な事故シーケンスの展開に適した解析方法で、図 2 に示すようなツリー構造を持っている。左端に起因事象が置かれ、順次各種安全機能/安全系統を表す見出し（ヘディグ）が上部に書かれている。各ヘディングにおける機能の成否に対応して事故のシーケンスが上下に分岐していく。このようにして、論理的に起こり得るすべての事故シーケンスを同定することができる。

イベントツリーの作成においては、ヘディングの選択、並べる順序が重要となる.論理的に不要なヘディング、まとめられるヘディングを検討し、簡略なイベントツリーを作成する必要がある。また、ヘディングの順序としては、

① システムが機能/動作する時間の順に並べる
② システムAが機能するためにシステムBの動作が必要な場合はシステム B、A の順に並べる。
③ ある故障が必然的に他の故障を引き起こすような従属関係にある場合は従属している系統を後ろにおく。

| 初期事象 | 原子炉停止系作動 | ポンプAによる非常用冷却水の注入 | ポンプBによる非常用冷却水の注入 | 事故後の崩壊熱除去 | 結果 |
|---|---|---|---|---|---|
| A | B | C | D | E | |

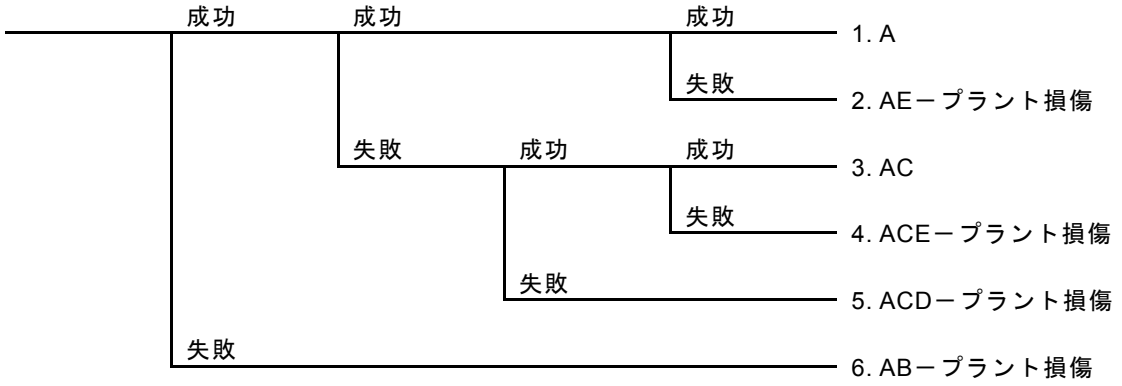
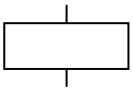
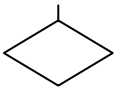
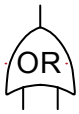



図 2 イベントツリーの例

表 2 フォールトツリーの要素例

| | | |
|---|---|---|
|  | **中間事象** | 複数事象の結合から成り立ち、さらに分割可能な事象 |
|  | **基事象** | これ以上展開不可能な基本的事象 |
|  | **未分解事象** | 情報不足あるいは不必要のためこれ以上分解しない事象 |
|  | OR ゲート | 入力事象が一つでもある場合出力を発生する |
|  | AND ゲート | 全ての入力事象が存在するとき一つでもある場合出力を発生する |

このイベントツリーにより得られる各事故シーケンスを定量的に評価するためには、起因事象の発生頻度とあわせて各ヘディングの機能の成否に対応したシステムの成功／失敗確率を求める必要がある。

### 3.3.2 フォールトツリー解析手法について

フォールトツリー(FT)解析手法は、航空機産業界における 30 年以上の経験およびラスムッセン報告に採用されて以来の原子力産業界における使用経験がある。FT は複数の機器から構成されたシステムに起こる望ましくない事象を、それぞれの機器の故障、誤動作などを表 2 に示すような AND、OR のような単純な論理関係で結合して表現したものである。

FT 作成にあたっては、まずシステムの機能を十分理解し、システムが複雑な場合はフロー図を作成する。次に機能の論理的なつながり、などを把握しておく。最後にそれぞれの機器の故障がおよぼす影響を FMEA により解析しておく。

準備段階が終了した後、頂上事象を定義する。頂上事象はシステムに起こる望ましくない事象

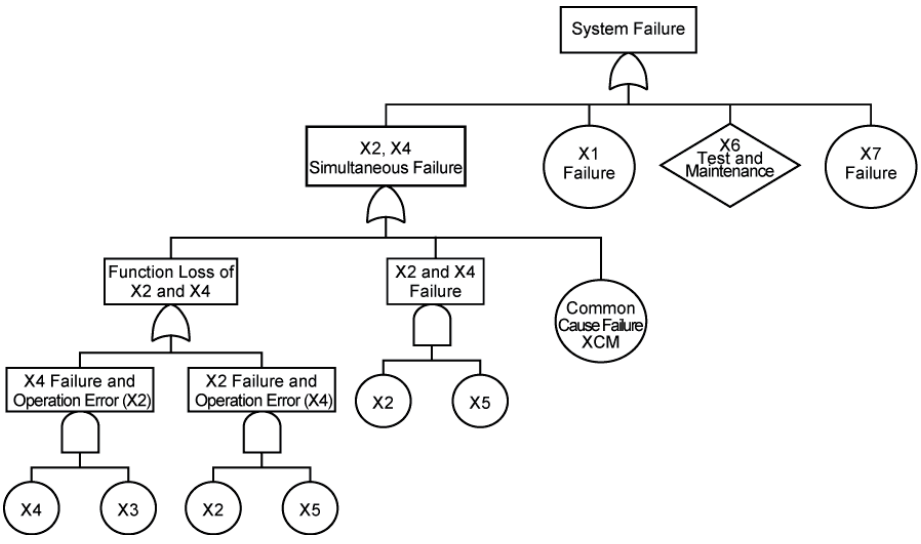



図 3 フォールトツリーの例

であり、解析の目標といえる。図 3 に示す FT の例では単純にシステム故障となっているが、実際の解析では厳密な定義、混同の起こりにくい記述にしておく必要がある。そうでないと、FT 作成の途中で頂上事象の理解が揺らいでしまい、FT 中の各分岐間に一貫性がなくなってしまう。

### 3.3.3 GO 手法について

GO 手法はフォールトツリー解析とは異なり、成功経路を追う解析方法である。この手法はもともと 1960 年代から電気回路の解析のために開発・利用され、その後原子力の分野でも使用されるようになってきた。

GO 手法においては、系の構成や機能をモデル化するために GO チャートを作成する。GO チャートは、標準オペレータと呼ばれる 16 種類の要素および必要に応じて解析者の定義したオペレータと、それらを結ぶ信号線より成り立っている。標準オペレータは、AND、OR の論理ゲート、機器の故障・動作などを表している。最終信号線の Likelihood の値により系の動作成功確率などの解析の目標とする結果が得られる。これらのオペレータの概要については、次に示す GO-FLOW 手法と類似なものである為ここで詳細は示さないこととする。

GO 手法の特徴は、GO チャートと対象とする系の構成との対応が明確な点にある。そのため、GO チャートの作成が容易であり、再チェック、正当性の評価、修正も容易に実施できる。また、1 つの GO チャートによりシステムの複数の状態も解析できる。さらに、フォールトツリーの最小切断集合（MCS:ミニマル・カット・セット）と呼ばれる評価方法に対応したフォールト・セットも得られる。しかし GO チャートには、故障モードが記述されない、フェーズド・ミッションと呼ばれる時間依存性の問題を取り扱うのが容易ではないなどの弱点もある。

### 3.3.4 GO-FLOW 手法について

GO-FLOW 手法は成功確率を追うシステム信頼性解析手法であり、システム信頼度・アベイラビリティ（規定時間内に機器が故障状態にある確率）の評価を行うことが可能な特徴を持つ。解析対象とするシステムの構成、機能をモデル化するため、図 4 に示すオペレータと信号線を用いて構成される GO-FLOW チャートと呼ばれる図を作成する。オペレータの動作モード・故障に対して発生確率をデータとして与え、・オペレータの定義にもとづき信号を処理していくことにより、最終的に系の動作／不動作確率を求めることができる。

GO-FLOW 手法による解析例として、図 5 にサンプル問題を示す。この図は、図中左上に示した簡単な電球を用いた回路図を GO-FLOW チャートで表したものである。GO-FLOW チャート上、回路図がそのイメージを反映して表現されてい

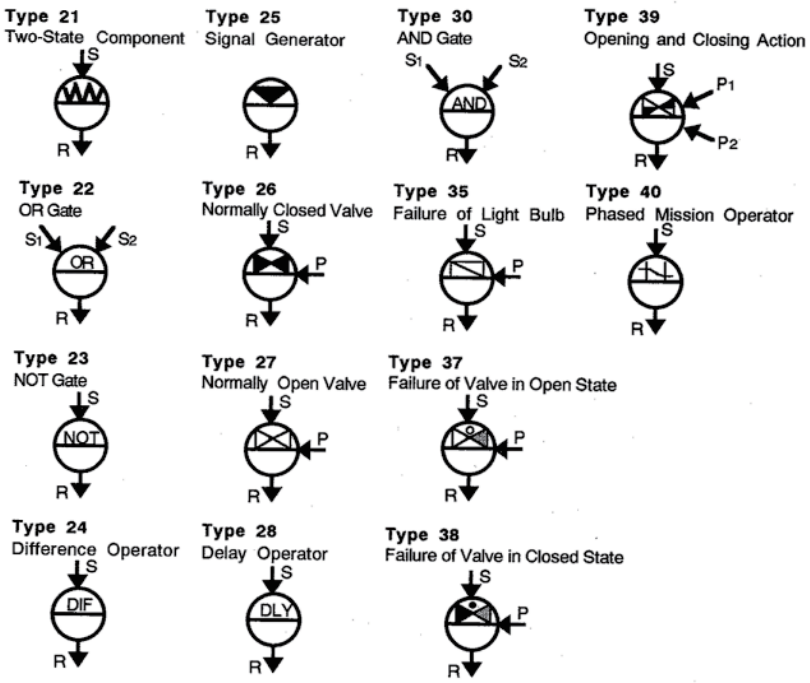



図 4 GO-FLOW 手法における標準的オペレータ

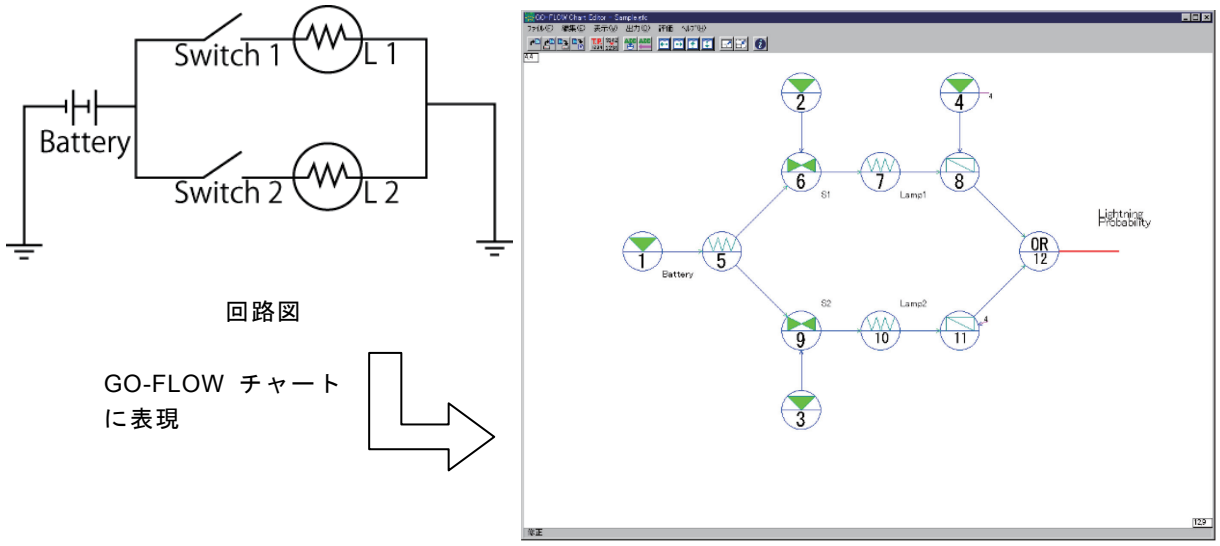



図 5 GO-FLOW チャート例

ることが分かる。この様な点も、この手法の特徴である。なお、この GO-FLOW 手法は、原子力試験研究費により当所で開発したものである。

また、最近ではベイズの定理を応用したベイジアンネットワークによる解析も注目を集めている [12]。当所でも、この手法の導入を検討し、航海支援機器の導入の評価を行っている [13]。

### 3.3.5 評価に用いるデータベースについて

以上のような手法を用いて解析作業を行う際には、解析対象に関する故障率等のデータが必要になる。このような際に用いられるデータベースの例を以下に示す。解析に用いらるデータは、当然のことながら解析対象により選択されるべきものである。

- リスク解析に関する各種報告書
- Offshore Reliability Data（海洋構造物）[14]
- IEEE Std 500 RELIABILITY DATA（原子力）[9]
- 合衆国原子力規制委員会報告書（原子力）

等がある。これらデータベースにおいては、対象機器、システム等について運転時間と故障回数等が示されている。したがって事故の頻度としては、時間単位のものが主である。しかしながら、リスク解析を行う際には、普段は停止状態であり、必要に応じて作動すべき機器も解析の対象となる。例えば、船舶や原子力発電所に設置されている非常用発電機がこれらにあたる。つまり、何らかの異常事態により、常用発電機が停止した場合等に運転されるものであり、通常は停止している。このシナリオの発生頻度は、以下のように考えられる。

常用発電機の停止(P1)→非常用発電機の起動(P2)
P1：常用発電機の停止確率
P2：非常用発電機の起動失敗確率

このシナリオにおいては、P1 は時間単位で考えるが、P2 は運転を要求された回数で考えなければならない。このような故障率は「デマンド故障率」と呼ばれるものであり、前述のデータベース等にも掲載されている。

また、データベースという観点からは、リスク解析においては、後述するように人間の関る部分についても解析対象となるため、この人間の操作の失敗確率等に関するデータベースというものも必要となる。しかしながら、実際のリスク解析に耐えるデータベースは、現在 殆ど無い状態である。そこで実際の解析においては、後述の人間信頼性解析において必要とされている基本的なデータの一部が用いられることが多い。

以上、リスクの定量的評価に関する幾つかの手法について述べたが、解析に用いる手法としては、解析結果の信頼性という観点から実績のある手法が望ましい。実際のリスク解析例においては、イベントツリー、もしくはイベントツリーとフォールトツリーの組み合わせによるものが多く報告されている。

## 4 評価結果の検討

### 4.1 リスク評価の結果の検討

3 章で得られたリスク評価の結果については、その結果を得ただけでは意味を成さず、検討を加えることにより リスク評価を行った意義が生じる。リスク評価を行う目的により検討すべき対象、方法は異なるが、例えば IMO 提案の Formal Safety Assessment (FSA)[15]では、Step3 と呼ばれる評価プロセスにおいて、得られた定量的リスク評価の結果について、リスクを低減させる安全対策を検討する。この考えられた安全対策について、それらを導入した場合にどの程度のリスクの減少が得られるかを再度評価し、安全対策としての効果を評価する。FSA の場合には、さらに Step4 と呼ばれるプロセスにおいて、この安全対策に関してさらに経済的な評価、費用対効果の評価を行う。前述の安全対策の導入にかかる費用と導入の結果得られるリスクの低減値とにより決められるものである。

また原子力分野で行われる確率論的安全評価手法(Probabilistic Safety Assessment, PSA)では、レベル 1PSA と呼ばれる段階で、次のような評価が行われる [16]。

重要度解析…各機器や操作の失敗がどれほど重要かを分析する。レベル 1PSA と呼ばれる評価においては、対象となる炉心損傷頻度への寄与の観点から行われる。機器等の失敗確率を個別に変化させることにより、炉心損傷頻度への影響を系統的に調査する。代表的な指標として Fussel Vesely 指標やリスク達成価値（Risk Achievement Worth: RAW）指標等が用いられる。

不確実さ解析…解析の結果が、故障率データの不確実さや解析モデル（例えばイベントツリーやフォールトツリー）作成時の仮定にどれほど依存しているかを調べる。イベントツリーを用いた場合には、作成の時の項目選定の任意性、分岐確率のデータに存在する統計的なばらつき、分岐確率の値を専門家判断に依存する場合等種々の不確定な要因が考えられる。そこで、イベントツリー中の分岐において不確実さが存在すると見られる項目について事象の発生確率値を上限値、下限値間での一様分布から乱数により各々 1 つ選定しイベントツリー解析を実施する。これを一定数繰り返すいわゆるモンテカルロ法を実施し最終結果の不確実さ幅を求める方法がある。

これらの検討は、いずれもリスク評価の結果の正当性、また得られたリスクの合理的な低減のために行われるものである。

### 4.2 許容されるリスクの合意

リスク評価で得られる結果については、許容されるリスクの大きさについて利害関係者の間で合意されていることが重要である。我々は実際の日常生活において、我々は様々なリスクに曝されていると考えることが出来る。しかしながら、この日常生活におけるリスクについては、そのリスクを低減する行為を行うことにより、共存していると考えることが出来る。例えば、自動車について考える。自動車は、移動手段、輸送手段等とした場合には便利なものであり利益性の高いものである。しかしながら、自動車に関わる様々な事故と事故による被害を考えた場合には、それらは無視できないものである。この自動車の「便利さ」と事故等の「危険」を比べた場合には、現実の社会では「便利さ」が勝り、普及、利用されている状況、つまり共存していると考えられる。（図 6）


**図 6 自動車の価値観の天秤**

また、このような状況は、危険（リスク）を低減させるべく努力が行われてきたことにより得られたものでもある。全てのことがこの考えに基づくとは, 限らないが、現在用いられている、また新たに導入される技術やシステムについては、それらによる日常生活の便利さと生じるリスクとのバランスが重要であるという考え方が出来る。「便利さ」とまで言わなくとも、リスクが必要以上に増大することはあってはならない、このような場合には、それらの技術・システムは許容されないことになる。このような考え方に基づき、具体的に、そのリスクがある値以下であればそれを受容し、リスクがこの水準になるようにするべき考え方を示したのが英国で提案、採用され多方面で引用されているリスクの受忍可能性（Tolerability of Risk）の枠組みである。これは、図 7 に示すように、

1) いかに利益のある活動でもリスクがあまりに高ければ、社会はその活動を受け入れない、
2) それ以下のリスク水準の活動については、合理的に実行可能なリスク低減努力が行なわれた結果であるならば受け入れられる（as low as reasonably practicable, ALARP）、
3) リスクがある水準以下であれば、リスク低減のために更に費用を投じることが求められない、

とするものである。なお、この受忍限度としては、特定原因による公衆個人の死については $10^{-3}$（作業者）/年, $10^{-4}$（一般）/年が、ALARP 領域と広く受容される領域の境界については $10^{-6}$/年を超えないこととされている [17]。

この ALARP の考え方は、リスク評価が導入されている様々な分野で用いられており、例えば前述の IMO 提案の FSA、また原子力における PSA でも用いられているものである。

## 5. リスク評価における課題

ここまで、リスク評価を行う為の手順・手法等について紹介してきた。しかしながら、リスク評価を行う場合に、検討すべき点として幾つかの点がある。例えば、

a) 現状のリスク評価の方法論は、静的なものであり、現実的な動的な現象（時間的な因果関係）を十分なレベルではモデル化出来ていない。
b) 評価手法に関しても、現在の ET, FT 等といった標準的に用いられる手法でさえ、評価作業は膨大な作業である。
c) 評価作業には、リスク評価の専門家、評価対象に関する専門家そして利用者の共同作業が必要。
d) 安全評価で不可欠な人間の信頼性の評価が不十分である。完全な自動化システムは存在せず、想定外事象におけるシステムの安全性は人間の信頼性に依存するものである。

等が挙げられる [18]。これらについて検討する。

まず b)については、様々な評価支援システムが開発されていること、また計算機の高速化等の進歩により、今後の開発等により緩和されることが期待できる。

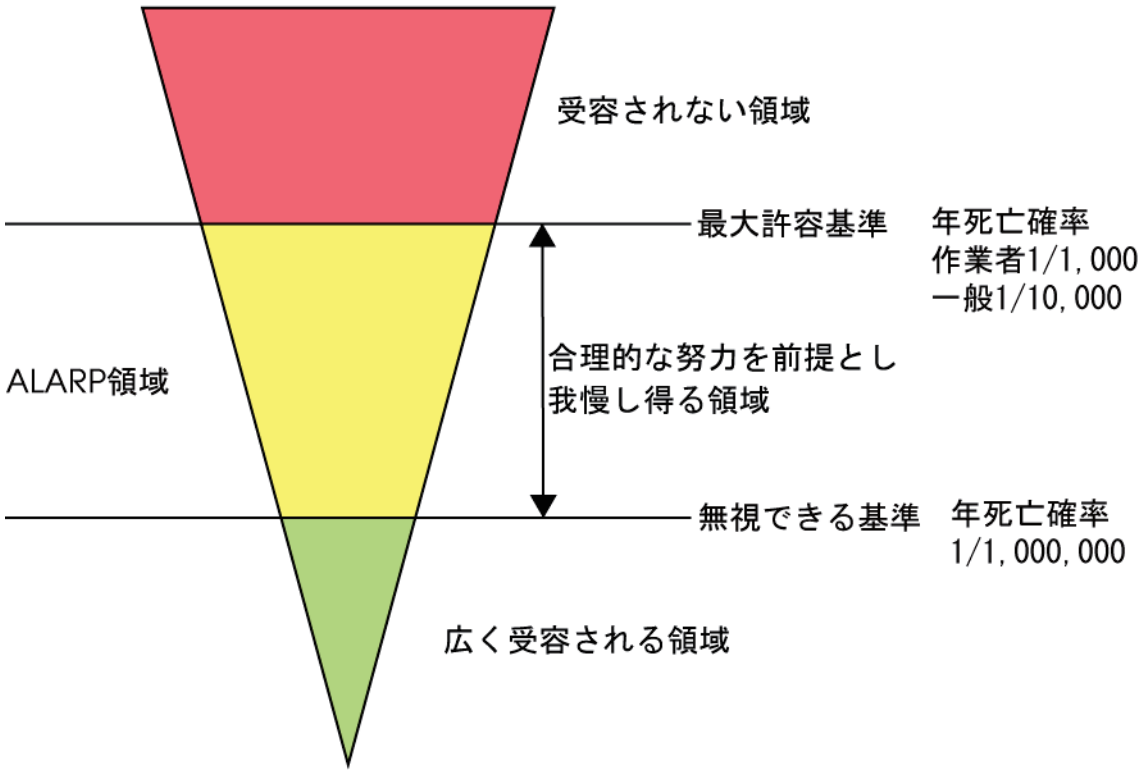



図 7 受忍可能なリスクの枠組み

c)についても設計的なものは、技術仕様から評価しやすく、統計データが存在するものはかつ精度が高く信頼できるものであることから、全てに対応しているわけではないが、課題としては残りの 2 つに比べ小さいと思われる。

以上のことから、ここでは a)及び d)の 2 つの点について考えることとする。

### 5.1 動的な現象のモデル化について

まず、a)について述べる。リスク評価を行う場合に、解析対象に必要な故障率データを用いることは述べた。これらの故障率は一定値であり、現状のリスク評価では経年劣化による故障率の変化等に対応した評価は、ほとんど行われていない。このような経年劣化つまり故障率の変化は、必ずプラント、システム、機器等には発生するものであり、リスク評価ではこれを無視できないものである。しかしながら、この故障率の時間変化に対応した、リスク評価に用いられる手法は殆ど無いのが現状である。

このような状況の中で、当所でもこの問題を解決するための研究を行い、3.3.4 節で述べた当所で開発した GO-FLOW 手法の特徴を利用した、故障率の時間変化に対応したリスク評価に利用しうる評価手法である TSAR (Time-dependent System Availabilities Research tool)を開発した [19]。この手法では、前述の問題点に対応するために 2 種類の時間の取り扱いと保守点検の反映という観点から ALDEMIR ら [20] の更新理論を GO-FLOW 手法に導入した。

機器の故障率を表現する式については、合衆国原子力規制委員会の報告書の一つである NUREG/CR-5587[21]より、経年故障率の推定方法として、

ii) 線形モデル
iii) Weibull 分布モデル
iv) 指数型モデル

の 3 種類の評価モデルが紹介されていることから、これらの式の導入を行った。その結果の一例として、図 8 に参考文献 [22]から得られたデータを用いた解析結果を示す。この解析例は、T-A タイプ機器（参考文献でも詳細は不明）について運転開始後 15 年で点検周期を 12 ヶ月から 9 ヶ月に変更した場合のアンアベイラビリティ（規定時間内に機器が故障状態にある確率）への影響ついて解析を行ったものである。この結果から、アンアベイラビリティは点検周期の変更により小さくなっていることが明らかであり、その影響がわかる。

また、GO-FLOW の問題点の一つであったユーザビリティについても、図 9 に示すように、オペレータをサブウインドウからドラッグアンドドロップすることを可能とする等、インターフェースにも変更が行われている。

TSAR については、PSA の分野で世界的規模で行われる唯一の会議である PSAM8 (the Eighth International Conference on Probabilistic Safety Assessment and Management)での講演、また経年劣化の影響を PSA に導入するための同様の研究を行っている EU の JRC(Joint Research Center：共同研究センター)にある IE(Institution for Energy：エネルギー研究センター)主催で開催されていた "The use of Probabilistic Safety Assessment (PSA)

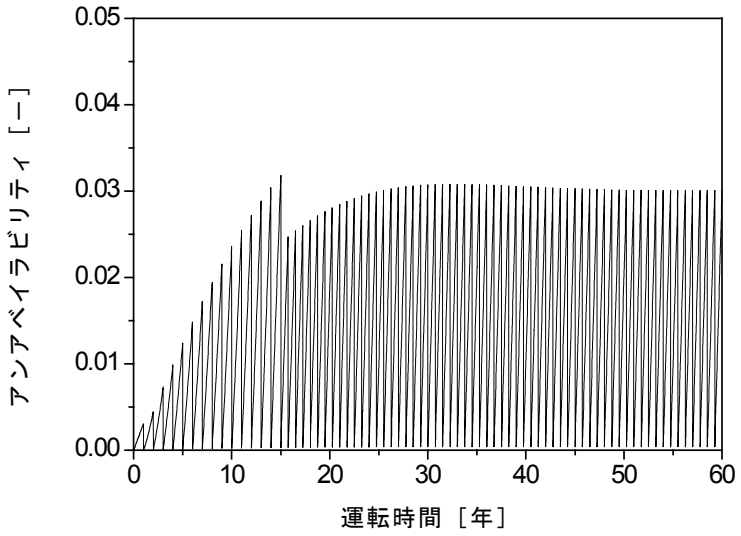



図 8 TSAR による解析結果例（T-A タイプ機器）

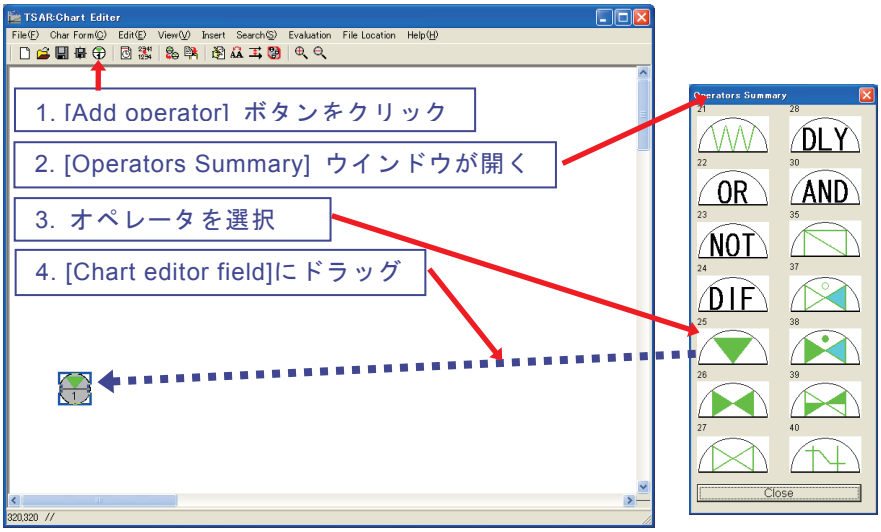



図 9 TSAR チャートの使用例

for Evaluation of Impact of Ageing Effects on the Safety of Nuclear Power Plants"（原子力発電所の安全に対する経年劣化を導入した確率論的安全評価手法に関するワークショップ）での講演等においても高い評価を得ている。現在 TSAR は、完成度を高めるために、さらに検討を加えているところである。

### 5.2 人間信頼性の評価について

次に d)について述べる。現実的な対象物についてリスク評価、信頼性解析を行う場合、どのような解析対象においても、様々な形で必ず人間が関与するものである。例えば、3.3.5 節で述べたようなシナリオでも「常用発電機の停止(P1)」については、機械的な故障によるものもあれば、それを操作する操作員の操作ミスに依存するもの等が考えられる。つまりこの場合には操作員の操作、判断等は、当然のことながら安全に関わるものとして考えなければならない。したがって、解析対象によっては操作員の操作等の失敗・成功等の評価が行われるべきであり、このような人間の行動に関する解析は、人間信頼性解析（Human Reliability Analysis, HRA）と呼ばれる。人間が関るシステムにおいては、適切な HRA なしには適切なリスク評価はありえない、と言っても過言ではない。さらに HRA は、プラント全体の挙動を人間との関係を見ながら評価するため、プラントの総合的なシステム設計にも有効な手法である。

この HRA の代表的な手法としては、

- THERP (Technique for Human Error Rate Prediction)
- ATHENA (A Technique for Human Event Analysis)
- CREAM (Cognitive Reliability & Error Analysis Method)

等が知られている。

HRA においては、その手法を第一世代、第二世代と分類している。第一世代 HRA としては、上記 THERP 等があり、第二世代 HRA としては、ATHENA, CREAM 等がある。第一世代 HRA とは、システム信頼性解析の応用といったものが多く、作業の結果としての人間の信頼性（成功・失敗）の定量化に重点を置いている。HRA に関しては、その概念・手法に関する説明等だけでも膨大なものとなる為、詳細は各専門書等を参考にされたい。

第一世代とされる THERP 手法は、原子力発電所の PSA への適用を目的として開発された手法である。作業を分析し、発生しうる人的過誤を同定し、人的過誤の発生確率のモデル化及び定量化を行うものである。

THERP 手法においては、人間の行為の失敗確率を、対象となる行為をサブタスクに分解して分析し、余裕時間、熟練度、前の操作との依存関係、ストレスレベルなどを考慮して評価するものである。

図 10 は、THERP 手法のハンドブック [23]から抜粋したものである。この図からもわかるように THERP 手法は、前述のイベントツリー手法と同様、人間の行為をツリー図を用いて表現、評価を行うものであり、成功、失敗により分岐が行われる。失敗確率は各行為の失敗に至る発生確率の和

として計算される。図 10 は原子力発電所において、非常用炉心冷却のための注水系と呼ばれるものについて、注入開始後、水源の水位が低下したとの警報に対応して行うべき水源切換え操作の実施成功確率を THERP 手法により評価した例である。前述のように、この場合の失敗確率は、

失敗確率=$F_1+F_2+F_3$

として与えられる。

THERP 手法は、現在 原子力における PSA への適用のみならず様々な分野で用いられている手法でもある。

この様な HRA における現状の問題点としては、

- 異なる手法間で結果の一致が良くない
- 人間行動のモデル化が不十分
- データベースが不十分

等が考えられる。これらは、いずれも今後解決されるべき課題と考える。

これに対して第二世代 HRA では、第一世代 HRA の欠点の克服が行われ、確信的失敗への対応、失敗を起こすまでの状況（環境、心理、組織等）をも考慮している。

この様な HRA における研究においても、現在のところ公開されている参考文献としては無いが、当所では、第 2 世代である CREAM を用いた海難事故分析を行っている。また HRA に関連した研究として、人間の緊張度の指標の観点から、当所所有の操船リスクシミュレータを用いた研究も行っている [24]。操船リスクシミュレータを用いた研究は、前述の今後の課題である、人間行動のモデル化やデータベースの構築にも有効であろうと考えられる。

## 6. 結　言

リスク評価に関して、凡その流れと必要な手法について述べてきた。孫子の言葉に「敵を知り己を知らば百戦危うからず」というものがあるが、「安全」の確保のためにリスク評価を行うことは、まさに「敵」を知ることと考えられる。今後、「安全」を犠牲にすることの無い合理的な経済性の追求のためにも、リスク評価が適切に用いられることを期待したい。

## 参考文献


1) 木下冨雄 :「リスク認知の構造」、日本機械学会誌、第 106 巻、第 1020 号 (2003)、pp.849-852

2) 小林英男 :「リスクベースの工学／技術」、材料科学、第 37 巻、第 4 号 (2000)、pp.171-177

3) USNRC: “Reactor Safety Study: An Assessment of Accident Risks in U. S. Commercial Nuclear Power Plants,” WASH-1400 (1975)

4) 村松健 :「リスク情報を参考とする規制 (RIR) に係わる研究の現状と今後の研

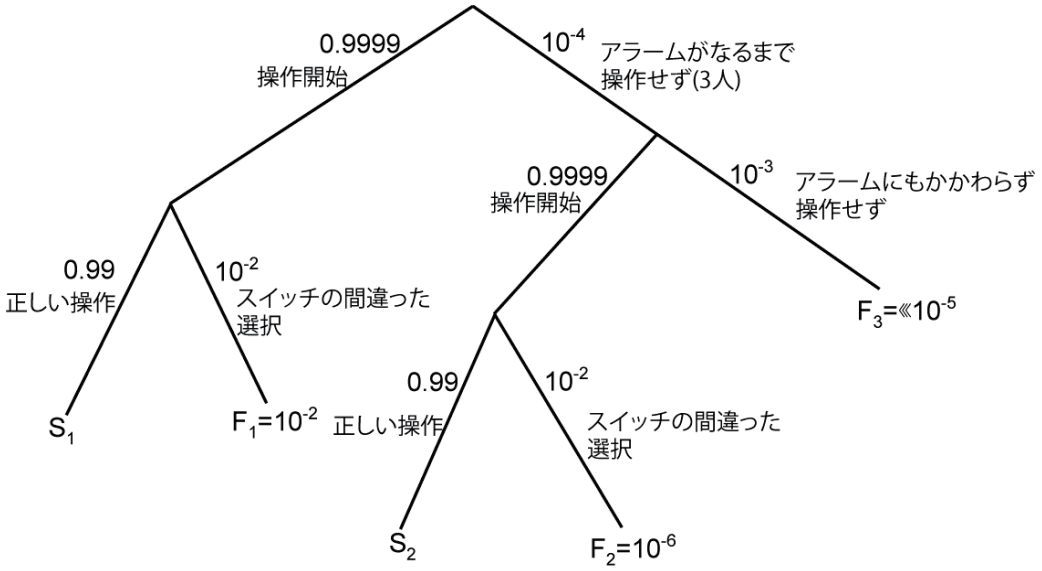




図 10 THERP 手法の例

究課題」、平成 14 年原子力安全委員会安全研究成果報告会資料
5) 阿部清治：「原子力発電所のシビアアクシデントーそのリスク評価と事故時退所策ー」、JAERI-Review-95-006、(1995)、p .49
6) 原子力安全基盤機構：「国際規格等における「リスク」の定義について」、平成 17 年 7 月
7) H. TAMAKI, K. YOSHIDA, N. WATANABE, et al: “Hazard analysis approach with functional FMEA in PSA procedure for MOX fuel fabrication facility," Proc. Int. Topical Meeting on Probabilistic Safety Analysis, PSA'05 (2005), p. 474～484
8) 玉置等史、吉田一雄、渡邉憲夫、村松健：「MOX 燃料加工施設に対する確率論的安全評価手法の開発」、日本原子力学会和文論文誌、第 5 巻、第 2 号 (2006)、 p.125-135
9) IEEE: IEEE Std 500-1984 RELIABILITY DATA (1983), p.27-30
10) USNRC: “PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants,” NUREG/CR-2300 (1983)
11) 松岡猛：「確率論的安全評価のためのシステム信頼性解析手法 GO-FLOWー基本概念から実際の使用までー」、株式会社 CRC 総合研究所、 (1996)
12) 本村陽一：「ベイジアンネットワーク：入門からヒューマンモデリングへの応用まで」、http://staff.aist.go.jp/y.motomura/paper/BSJ0403.pdf
13) 財団法人 日本船舶技術研究協会：船舶の安全評価手法に関する調査研究(SPF)（2005 年度報告書）、(2006)
14) Offshore Reliability Data (OREDA), SINTEF, 4th Edition (2002)
15) IMO: “MSC 83/INF.2: FORMAL SAFETY ASSESSMENT,” (2007)
16) 村松健： 「軽水炉の確率論的安全評価（PSA）入門、第 3 回内的事象レベル 1 PSA」、日本原子力学会誌、第 48 巻、第 6 号 (2006)、pp.409-416
17) 近藤駿介：「安全を確保するための工学的アプローチ」、第 8 回東京大学工学部イブニングセミナー（2003）、p. 14-15
18) 氏田博士：「リスク解析におけるヒューマンエラーや組織事故の取り扱い方について」、第 3 回「原子力の安全管理と社会環境」ワークショップ資料集(2008)
19) T. OKAZAKI, N. MITOMO et al: “The Use of GO-FLOW Methodology to Investigate the Aging Effect in Nuclear Power Plants,” Proc. the Eighth Int. Conf. on Probabilistic Safety Assessment and Management PSAM8 (2006) PSAM-0113
20) Tunc ALDERMIT et al: “Aging Effects on Time- Dependent Nuclear Component Unavailability: An Investigation of Variations from Static Calculations,” NUCLEAR TECHNOLOGY, VOL.112 (1995) p.21-41
21) USNRC: “Approaches for Age-Dependent Probabilistic Safety Assessment with Emphasis on Prioritization and Sensitivity Studies,” NUREG/CR-5587 (1992)
22) APSA: “APSA in risk informed applications Appendix B3.1,” http://www.energyrisks.jrc.nl/APSA/PDF/Results_Case_Studies/Demonstration%20Examination.pdf
23) USNRC: “Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications,” NUREG/CR-1278 (1983)
24) N. MITOMO et al: “A Few Comments on Visual System of Ship Handling Simulator Based on Arriving Port,” Proceedings of The 2008 IEEE Int. Conf. on Systems, Man, and Cybernetics (2008) T.P1.310(S).2