特集●リスク管理

リスク管理概論

井上紘一*　　幸田武久**

システムに生じるリスクを低減する視点からリスク管理について概説する。リスクは事故の発生確率とその損失の大きさの関数として表わされ、基本的なリスク低減策は事故発生防止と事故時の損失抑制である。リスク管理は、リスク同定、リスク評価、リスク対策検討とリスク制御からなり、対象とするシステムの設計・計画、製作、運用の各段階に応じて行われる。リスク発生の主要因であるヒューマン・エラー対策についても言及する。

Introduction to Risk Management

Koichi INOUE*　　Takehisa KOHDA**

This paper gives an introduction to the risk management from the viewpoint of preventing risks caused in a subject system. Since the risk is quantitatively defined as a function of the accident probability and its loss, the basic strategies to reduce the risk are to prevent the accident occurence and to reduce the loss caused by the accident. The risk management, which is composed of risk identification, risk assessment, consideration of risk prevention, and risk control, should be performed depending on the system stage, which is either its design and planning, construction or operation. The prevention of human errors a major cause of the system accident, is also briefly reviewed.

1．はじめに

最近でも、新幹線車両事故、タイ航空機事故や中国でのヘリコプター事故など、システムの異常や故障により多くの人命が失われたり社会的影響が生じている。原子力プラント、航空機、新幹線をはじめとするシステムが高機能化、複雑化するにつれて、その事故や故障による影響は以前にも増して大きく、また予測しがたい。システムの信頼性や安全性の確保がますます重要になってきている。システムの事故や故障の発生をなくせばよいわけだが、完全にゼロにすることは困難で現実的にも不可能であり、かつ経済的にも効果的でない。一方、事故や故障が発生したときに損失拡大を抑制することが考えられるが、あらゆる状況に前もって対処することは不可能である。したがって、システムの信頼性や安全性を維持するための有効な対策をいかに作成するかが重要な問題となる。さらに、現在では環境問題などのように、単に対象とする人工的システムのみでなく、環境条件である自然システムも考慮したより大規模なシステムを対象とする必要がある。このようなシステムの安全性や信頼性を検討・維持管理していくためのシステマティックな枠組みとして、リスク管理（Risk Management）がある。

リスク管理といっても、対象とするリスクや立場によりその管理方法が異なる。リスクにも企業の事業展開、海外進出、設備投資など経済活動に関連する投機リスクから、火事、地震、風水害、労働災害などの純粋リスク等さまざまなものがある。前者に対しては経営管理論的リスク管理があり、後者に対して保険管理論的リスク管理がある。ただ、これらのリスク管理に共通している点は、リスクの低減を目的としていることである。本稿では、プラントや機械などの工学的システムに生じる事故や災害によ

＊　京都大学工学部航空工学教室教授
Professor, Dept.of Aeronautical Engineering, Faculty of Engineering, Kyoto University
＊＊京都大学工学部航空工学教室助教授
Associate Professor, Dept.of Aeronautical Engineering, Faculty of Engineering, Kyoto University
原稿受理　1992年8月27日

るリスクの低減を目的としたリスク管理について概説する。リスク管理は、リスクの同定、解析・評価、対処策検討とリスクを防止するリスク制御からなると考えられる。対象とするシステムの設計・計画、製作、運用というライフサイクルを通してそれぞれに対応したリスク管理が行われる。まず、リスクの定義について述べ、その後で対象とするシステムの設計・計画、製作、運用の各段階でのリスク管理について考察する。また、安全性や信頼性向上で問題になっている人間に関連して、ヒューマン・エラー対策について述べる。

2．リスクとは

リスクは、辞書によれば「システムに生じる人的あるいは物的損失の可能性(chance,possibility)」とある。これでは少し抽象的すぎるので、システム改善案等を比較評価するためには定量的な尺度として、損失の大きさと損失の発生する頻度(確率)との関数で表わされる。リスクの最も単純な定義として、

リスク｛損失レベル／単位時間｝＝
頻度｛事象／単位時間｝
×大きさ｛損失レベル／事象｝

がよく用いられる。例えば、1000年に1度生じる大事故のため1,000人が死亡する場合のリスクは、

1／1000｛事故／年｝×1000｛死亡／事故｝
＝1｛死亡／年｝

となる。

個人的リスク（個人が死者となる年当たりの確率）にもさまざまな場合がある。例えば、1000年に1度生じる大事故のために1,000人中すべてが死亡する場合と、1年に1度生じる小事故のため1,000人中に1人が死亡する場合ではリスクの値は等しい。しかし、日常茶飯事としての小さな事故はニュース性に乏しいが、まれに起こる惨事には人々は重大な関心を示すという社会特性に注意する必要がある。すなわち、リスクを考える場合には、リスクの値だけでなく、リスクの定義にあるように、事故の頻度と損失の大きさという2大要素を必ず考慮しなければならない。

リスクを事故の頻度と損失の大きさで表現する方法に、Fig.1に示すようなFarmer曲線[1]がある。

Fig.1は原子炉における放射能放出のリスクを表わしたもので、横軸は放出規模、すなわち損失の大きさを間接的に示し、縦軸は1年当たりの頻度を示している。このような2次元平面でのリスク分布を求めることがリスク評価の目的であり、またリスク管理における対処策検討や意思決定の基礎となる。リスク管理におけるFarmer曲線を求める重要性は、それを求める過程において対象とするシステムをより深く理解でき、リスク低減のための対処策が明らかとなる点にある。

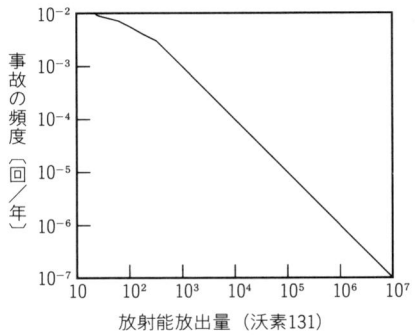

Fig.1　放射能放出量のＦａｒｍｅｒ曲線

3．リスク管理

3－1　システム設計・計画でのリスク管理

リスクの実現過程を考えると、何もないところから生じるわけではない。まず、リスクを生じる事故や災害の原因がシステムに発生し、それが事故や災害へと発展して損失が生じ、いわゆるリスクが実現すると考えられる。したがって、リスクの低減を図る場合には、まず対象とするシステムにおいて、どのような種類の事故・災害が起こりうるのか、その損失はどの程度のものか、どのように発生し、どれぐらいの確率（頻度）で起こりうるのか等について十分分析して、システム改善策や事故対策を検討することが重要であり、これがリスク管理の第一ステップに相当し、システムの設計・計画段階で事前にやるべきことである。このようなリスク解析・評価をシステマティックに行う枠組みとして確率論的リスク評価(PRA:Probabilistic Risk Assessment)[2]がある。Fig.2は、その評価法の流れを簡単に示したものである。

1）リスク源の同定

PRAにおける最初の仕事は、対象とするシステムに固有なハザードを同定することである。ここにいうハザード(hazard)とは、もともと「人的あるいは物的損失を引き起こす事故の潜在力（potentials for an accident）」と定義される。しかし、潜在

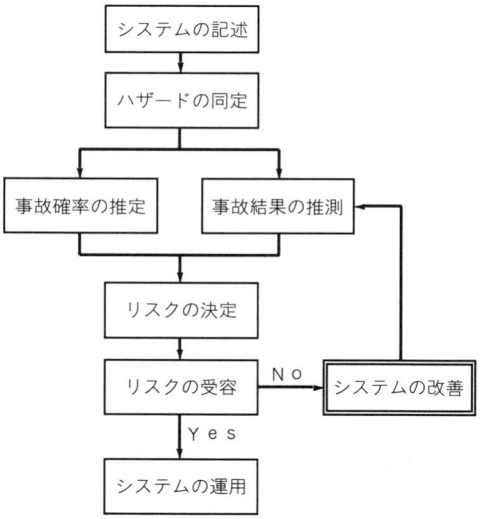

Fig.2 確率論的リスク評価の概要

力という概念では抽象的すぎる。一つの潜在力には種々の損失発生形態が対応し、この方がより具体的である。ここではハザードを現象面から見て、「潜在的発生状態」と同一と考える。たとえば、化学プラントで可燃性物質、爆発性物質、毒物の予期せぬ流出が典型的なハザードである。

ハザードを同定するためには、システムを部分に分割し、ハザードの種類と関連場所を列挙すればよい。このときには、何を考慮し何を無視するかを明らかにするシステムの境界条件の設定が必要となる。ハザードを同定するための手法としては、Dow & Mondのハザード指標、PHA (Preliminary Hazard Analysis) 、What if法、HazOps (Hazard and Operability Studies)、FMECA (Failure Modes, Effects and Criticality Analysis) などがある[2,3]。

2) リスクの解析・評価

ある一つのハザードが同定された後に行う仕事は、そのハザードが従業員、近隣の大衆、その企業などに与えるリスクを評価することである。リスクを評価するためには、まず事故をその源となる引き金事象 (initiating event) から結果 (consequence) に至る一連の事象の連なりとしてとらえ、この事故連鎖 (accident event sequence) の引き金事象および中間事象 (intermediate event) を同定するとともに、事故結果の性質について分析しなければならない。このための手法として、前述のWhat if法、HazOps、FMECA、ヒューマン・エラー解析が役立つ。また中間事象を同定するためには、FTA (Fault Tree Analysis)、ETA (Event Tree Analysis)、CCA (Cause-Consequence Analysis) などが用いられる。

各事故の事故連鎖すなわち損失を生じる事故シナリオが同定されたならば、その事故によるリスクを推定することができる。リスクの2大要素の一つである結果の大きさ (損失の程度) は工学的分析により推測され、もう一つの要素である発生確率はFTA、ETA、CCAなど論理図を用いる手法により推定される。

3) リスク対策の検討

推定された全体のリスクが受け入れがたい水準のものであれば、リスクを低減するための修正がシステムに加えられることになる。すでに述べたように、リスクは事故の発生確率とその損失の大きさの関数であるから、そのどちらかあるいは両方を小さくする方策を検討することになる。

ある場合には、より良い要素部品を用いる、保守・保全を綿密に行う、冗長要素を導入する、訓練を強化する、計測表示装置を改善するなどにより、ハードウェアの故障あるいはヒューマン・エラー (以下HE) の発生確率を低減し、結果としてリスクを低減することができる。またある場合には、安全システムを用いることにより、事故の拡大を防止する方向が検討されるであろう。代替案の比較・検討は、各代替案に対してPRAで得られるリスクの定量的評価と、代替案実施のための経済的要因を考慮して行われる。

PRAが進むにつれて、安全システムを導入するか、あるいはシステムに必要な改修を加えることにより、望ましいリスク水準が達成できることが明らかになれば、その時点でPRAが完了することになる。

PRAに基づいて、リスクに対する一連の検討や意志決定を行う過程が、リスク管理の主要な部分である。

3－2 リスク対策

PRAをFig.3に示すような一連のステップとみれば、リスクを低減させるための方策がより細かく明瞭になる。Fig. 3はPRAの各ステップとそれに応じてとりうるリスク低減のための方策を示したものであり、それらは以下の通りである。

(1)システムに固有なハザードを同定する。

(2)(1)で同定されたハザードから生じる結果を推測する。

(3)(2)で得られた結果を減少させる方策を同定する。

(4)(2)で推測された結果に連なる事故の引き金事象を同定する。
(5)引き金事象の発生確率を推定する。
(6)引き金事象の発生確率を減少させる方法を同定する。
(7)(2)で推測された結果に連なる事故の事故連鎖（システムの応答）を同定する。
(8)(7)で同定された事故連鎖の確率と結果を推定する。
(9)(7)で同定された事故連鎖の確率または結果、あるいは両者を減少させる方策を同定する。
(10)必要ならば、さらに確率および結果の推定に含まれる不確定さを減少させるための定量的ＰＲＡを続行する。

明らかなように、ステップ(3)、(6)、(9)からリスク低減のためのシステム設計に有用な情報が得られる。PRAから得られるリスク低減のための方策はつぎの５種類に分けられる。
(1)物理的な設計または制御システムの変更
(2)操作法の変更
(3)プロセスの変更（圧力、温度など）
(4)プロセス材料の変更
(5)重要な安全項目のテストおよび検査の変更

さらに、可能な数多くの方策のなかから選択する場合には、それぞれつぎの３つのカテゴリに分けて考えることが役立つ。
(1)ハザードを消滅させる方策
(2)結果を消滅あるいは減少させる方策
(3)確率を望ましいレベルに減少させる方策

一般に、ハザードを消滅させる方策が望ましく、かつより有効である。ハザードそのものを消滅させる適当な方策がなければ、事故の起こる確率を減少させるような方策あるいは事故が起こったとき人間とシステム自体を護る方策を考えることが必要となる。

また、リスクへの対処法は、一般的につぎの４つに分類される[4]。
(1)リスク回避（Risk Avoidance）
リスクの原因の除去や潜在的に存在するリスクから物理的な意味で逃避する。
(2)リスク軽減（Risk Prevention）
事故発生頻度や損失と影響の深刻度を軽減する。
(3)リスクの他者転嫁（Risk Transfer）
一般に保険料を支払って、被害時の損害を保険会社に負わせる。
(4)リスクの保有（Risk Retention）

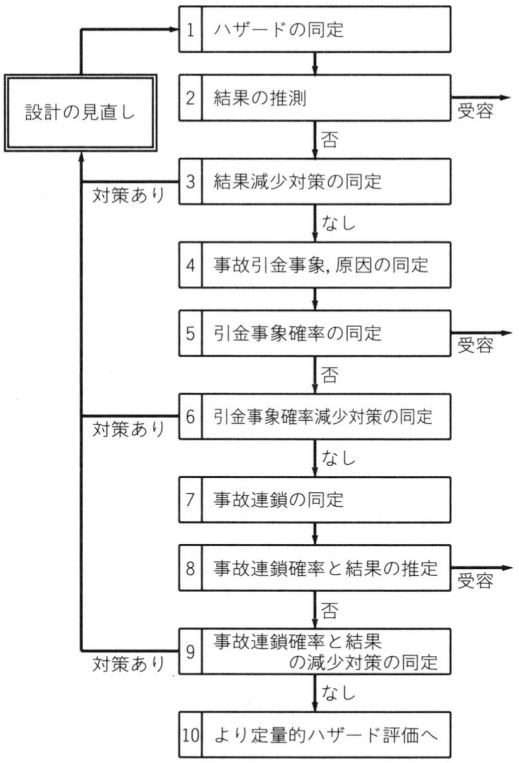

Fig.3　ＰＲＡのステップとリスク低減対策

リスクを個人あるいは企業自体で保有する。

ここで考えているリスクを低減するという意味からの対策は(2)リスク軽減に対応し、(1)、(3)と(4)はリスク自体の低減ではなく、リスクによる損失への対処策であるといえる。

３－３　システム製作でのリスク管理

システムの製作段階においては、設計・計画段階で検討された設計基準や設計仕様が満足されていることを保証することがリスク管理の主要な目的である。

化学プラントの配管でステンレスを用いるように指示されていたのに通常の鉄が使用されていれば大事故の引き金となるのは当然である。システム製作時には、使用する部品や材質の品質管理が重要になる。単に部品や材料の仕様選定にとどまらず、納入者の品質管理も十分に考慮しなければならない。また、石油タンクでは溶接技術の不備が応力集中を引き起こし、破損や破壊の原因になる。製作技術を向上させることもリスクのない安全なシステムを製作するときには必須である。とくに、人手に頼っているところでは作業行程ミス等の製作エラーのＨＥがでないように、明確な作業マニュアルや監視・監督

体制を確立することが重要である。

新規設計のシステムでは、技術的にも未経験の部分が多く、またシステムや部品の異常や故障に関するデータが乏しいので、できる限り開発試験を行い性能・機能確認を行うとともに、異常や故障に関する情報収集を行うことが重要である。設計・計画段階の検討不足や予想とのずれなどによる設計・計画見直しが必要になるかもしれないので、テスト結果を十分に解析して設計や計画にフィードバックしなければいけない。

3－4　システム運用でのリスク管理

リスク管理はリスク発生が起こらなくて当たり前であり、一方うまくいかずにリスクが発生すると大損害が生じるという見返りのない仕事である。システム運用におけるリスク管理は、システム設計や計画段階で検討された対策を実際に行われるように現実化することである。システム運用中のリスク管理がうまくいかないと、ホテル火災における警報装置のスイッチがオフになっていて作動せずに大事故に至るようなことになる。また、システムも時間の経過につれて性能劣化がおこり設計段階とは違った仕様になり、当初のリスク対策を変更する必要も生じる。運用段階でのリスク管理は、大きく、

(1)異常・事故発生の防止あるいは早期発見

(2)異常・事故の波及拡大防止

に分類される。

まず、運用段階でのリスク管理で最も基本的な仕事は、設計段階で同定されたハザードを監視して異常や事故が発生しないように努めることである。また、誤って設計仕様通りにシステムが運転されずに事故に至ることがないかをチェックすることも必要である。もし、状況設定ミスが生じるととんでもない予想外の事態を引き起こす。特に、最近旅客機を始めとしてコンピュータ制御の導入により入力ミスによる事故が起きている。オペレータ等の誤操作には注意する必要がある。ＨＥをなくすためにできるかぎり作業を自動化することも考えられるが、自動化といっても人間の作業をすべて機械で置き換えることはできないし、人間に頼らざるをえない部分がある。特にシステムに異常が生じたときには高度の判断が必要となり、人間に依存しなければならないところに自動化の問題点がある。他方、最初から人間が誤りを行っても大丈夫なように、インター・ロックやフール・プルーフを採用することも考えられる。

設計・計画段階で設定されたシステム性能や機能はいつまでも維持されるわけではない。機械部品等であれば当然摩耗や疲労が生じて故障しやすくなる。時間の経過とともにシステムは徐々に性能劣化していく。したがって、性能維持のために定期点検や保全を行わなければならない。性能劣化を調べるために目視検査では簡単に判明しないので、Ｘ線回折[5]や超音波探傷などの非破壊検査技術が必要となる。損傷の兆候を確実に検出するためにはその診断精度の向上が望まれる。故障や異常発生のメカニズムを解明して、異常兆候を早期発見することが重要である。さらに、システムを構成するクリティカルな単一要素に対しては、定期的に点検するだけでなく、できれば常時モニタリングを行って異常検出することが必須である。

保全時においても、ＨＥに注意する必要がある。バルブの締め忘れなどにより事故が拡大することがある。制御操作時と同様に誤判断や作業忘れが生じないように、確認動作の徹底を図らなければならない。設計・計画段階では、ＨＥが生じないように人間工学的見地等から制御盤や制御装置の形状等は決定される。運用段階では、どのように人員を配置し、どのような作業手順で行えば、作業ミスを防止し、または復旧できるかを検討しなければならない。

いくら防止に努めていても、異常や故障は発生する。その場合は速やかに適切な処置をとり、その影響拡大をおさえることが必須となる。このためには、異常や故障を早期に検出して、その原因を同定し、その影響等を推測して適切な処置をうつ、故障あるいは異常診断技術の確立が重要である。

まず、異常や故障を早期に検出するには、異常や故障によりシステムにどのような状態変化が生じるかを明確にしなければならない。回転機械であれば、振動音を観測しその周波数成分を分析すれば異常が検出できる。このように、異常によって生じる状態変化に基づいてその現象を確実に捉えられるかどうかを検討しなければならない。着目する状態変化をセンサで検出する場合には、センサの信頼性にも注意しなければならない。センサの信頼性が対象とするシステムの信頼性より高くなければいけないことはいうまでもないが、センサが異常や故障を確実に警報し、かつ異常や故障がないときには警報を発生しないことが必須条件である。あまりに誤報が頻繁に発生すると、システム自体の稼働率を減少させかつ不必要な防御措置を招き経済的損失が大きくなり、

さらにセンサが遮断されて肝心の必要時に作動せずに大事故に至ることになる。

また、種々のセンサにはそれぞれ検出方式による特徴があるので、それらの特徴をうまく組み合わせて利用することが重要である。煙感知器にはイオン式と光電式の二種類があり、前者は発炎燃焼に、後者は非常に低温の薫焼に適している。誤報を低減するためには、いくつかのセンサの多数決論理で状態を推定することも一つの改善策である[6]。

異常・故障が検出されれば、その原因を同定し適切な対処策を施さなければならない(狭義の異常診断)。原因の同定方法は、基本的には原因と兆候あるいは症状の相関関係を基にして、センサで検出された状態から推定を行えばよい。しかし、センサからあらゆる情報が得られるわけではないので、未知状態をチェックして確認を行いながら同定しなければならない。元来、急を要する場面であるから、オペレータには過度の緊張やストレスがかかり、誤判断や誤操作を犯しやすい状況である。また、異常診断には、経験豊富な熟練した専門家の知識が必要であるが、そのような専門家を異常に備えて常時配置しておくことは困難であり、その育成にも時間を要する。異常診断に用いられているエキスパート・システムは、このような専門家に代わりオペレータの異常同定過程を支援して適切な処置をとるように誘導するものである[7]。エキスパート・システムでは、過去の故障や異常に関する情報やシステムに関する情報が知識ベースに格納されていて、現在の状況と比較されて一致した規則が抽出される。一致する規則がなければ、適切な対処のしようがない。このように、エキスパート・システムがあらゆる状況に対処できるわけではないので、最悪の場合の次善策すなわちエキスパート・システムの枠外に対する対策を考慮しておく必要がある。これは、設計・計画段階で設計ベースとして考慮されなかった苛酷事故に相当するものであり、システム停止などの最終手段を用意しておかなければならない。

4．ヒューマン・エラー（HE）対策

PRAなどにより対策が検討されても、実際に事故が発生するのはシステム稼働時であり、それに対処するのは人間である。PRA等を用いて計画立案されたリスク低減策がうまく実行されるかどうかはオペレータあるいは監視者である人間に依存する。システム稼働時のリスク管理がうまくいかない場合に、いわゆるHEにより重大な事故につながることが多い。Table 1は、いろいろな分野で発生した事故災害のうち、HEが主原因であったものの比率を文献により調査した結果（日本学術会議安全工学研連WG）である。全般的に、HEに起因する事故災害の比率は予想外に高い。今後科学技術の発展によりハードウェアの信頼性はますます向上してゆくであろうが、人間自身の信頼性向上は期待できない。したがって、リスク管理でもHEに起因する事故災害を未然に防ぐ必要がある。以下では、HEの分類、対処策と評価方法について述べる。

4－1　HEの分類

HEは、人間に要求される機能と実際に人間が果たす機能との間のずれによって生じ、その結果が何らかの形でシステムに悪い影響を与える可能性のある人間の過誤であると定義される。

HEによる事故を防止するためには、まず過去の事故データからHEがどのように発生するかを、整理・分類することが重要である。通常、人間が関与する状況によりつぎのように分類される。

(1)設計エラー

Table 1　HEに起因する事故の比率

分　野	HEに起因する事故の比率	発表者	年
構造物事故	90%以上	Allen	1975
	78%（800件中）	Hauser	1979
	66%（287件中）	前田	1983
製造業事故	40%以上	労働省安全年鑑	1984
ロボット事故	45%（18件中）	杉本	1979
電子装置（故障）	50～70%	Christensenら	1981
化学プラント事故	60%以上	林	1979
		大島	1980
石油化学コンビナート火災爆発	45～65%（483件中）	高圧ガス保安協会保安情報センター	1978～1982
海上石油掘削事故	70%	Jensen	1982
危険物工場火災	50%（1,270件中）	上原	1985
船舶事故	63.6%	Meister	1971
船舶機関損傷事故	84%（600件中）	池西	1985
航空機事故	70～80%	笠松	1979
		黒田	1979
航空機・船舶	70～90%	Rubinstein	1979
発電所事故		Danaber	1980
		Billings	1981
医療事故	80%以上（16件中）	古橋	1980
自動車事故	90%以上	橋本	1979

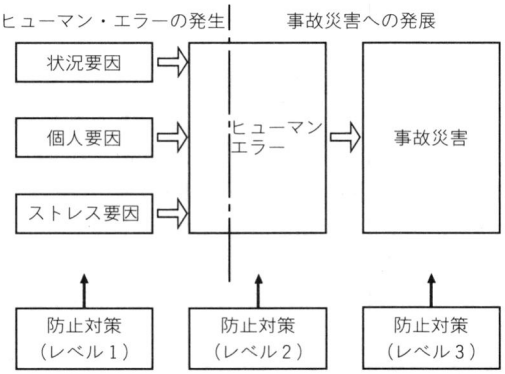

Fig.4 ＨＥに起因する事故災害の過程とその防止対策

計算間違いや思い違い等による設計誤りや不十分な設計により生じるエラー。

⑵製造エラー

技量不足、間違った材料の使用や図面の要求通りでない製造などによるエラー。

⑶操作エラー

通常のＨＥが意味するもので、作業員が正しい操作に失敗するエラー。

⑷保守エラー

機器や装置の取り付け誤りや修理ミス。

⑸点検エラー

不良品の見逃しや、良品を不良品と誤判定するエラー。

⑹取扱いエラー

製造者の推奨方法に合致しない物品の保存や輸送等により生じるエラー。

ソ連チェルノブイリ原子力発電所事故は運転員の多数の規則違反（操作エラー）が事故の引き金になったが、原子炉の危険状態を示す表示や警報の不備等の⑴が事故の背景にある。また、関西電力美浜原発２号機の蒸気発生器細管破断事故の直接原因は細管振動防止金具の取り付けミスで⑵に相当する。“運転者のミス”が原因とされる米国スリーマイル島原子力発電所事故は⑶に、日航ジャンボ機123便墜落事故は「しりもち事故」後の隔壁修理不十分とその後の定期検査で疲労き裂を発見できなかった検査不十分、すなわち⑷と⑸に起因する。

また、ＨＥは行動上の性質から、①やり忘れ、②やり損ない、③筋違いの行為（やってはならない不必要な行為）、④順序違いと⑤時間過誤（早過ぎや遅過ぎ）の５つに分類される。③～⑤も②のやり損ないと考えられるが、その原因が異なるので別個に分類される。

４－２ ＨＥの防止対策

ＨＥが発生し、それが原因となって事故災害が引き起こされるまでの過程と各過程での防止対策を簡単に表わしたものがFig.4である。

ＨＥの発生要因は大きくつぎの３種類に分けられる。

⑴状況要因

作業環境の悪さ、あるいは操作勝手の悪さなど、システム設計に依存する要因。

⑵個人要因

人間の個人的特性に関するもので、動機や志気の欠如、技術・慣れ不足、体調の悪さといったもの。

⑶ストレス要因

心理的、生理的ストレス。

これらの要因により、ＨＥの発生ポテンシャルが高められ、不確定な確率現象としてＨＥが引き起こされる。しかし一方、ＨＥが発生してもそれが直ちに大事故災害に結びつくとは限らない。多くのＨＥは無害であるか、各種の防止対策によって無害化あるいは局限化され、大きな事故災害の発生が防止される。Fig.4に示すように、ＨＥおよびそれに起因する事故災害の防止対策として３つのレベルの対策を用意することができる。

レベル１の防止対策はＨＥそのものの発生ポテンシャルを減少させるための対策である。具体的には、個人要因に対して職能教育・訓練、動機付け、志気の高揚等がある。また状況要因に対しては、システムの見直し、環境の改善、マン・マシン・インタフェースの改良等がある。ストレス要因に対しては、ストレス・レベルを最適な水準に保つために、単調な繰り返し作業を避けること、あるいは常に必要かつ十分な情報を与えるようにすること等があげられる。最近のＢ767やＡ310のコックピットでは、従来の多数のアナログ計器類に代えて計算機と数台のＣＲＴ（Cathod-Ray Tube）を採用し、必要な情報を必要な時に表示したり、緊急時には警報で注意を喚起したりして、パイロットの作業負荷を軽減するように考慮されている。

レベル２の防止対策は発生したＨＥを直ちに無害化あるいは修正するためのものである。フール・プルーフ、フェール・セーフ、インター・ロックなどの各種の安全設計がこのグループに属する。また、ＨＥの発生を直ちに音や光により、作業者にフィード・バックし、ＨＥの修正を求める警報装置の設置

も効果が大きい。例えば、鉄道におけるＡＴＳ（列車自動停止装置）は、乗務員が停止（赤）信号にも拘らず停止操作を怠った場合に強制的にブレーキが作用するようになっているバックアップ装置である。停止信号に近づくと乗務員の注意を喚起するためにブザーを鳴らし、乗務員のブザー確認後もブレーキ操作完了までチャイムにより要注意の意識を持続させるように工夫されている。

レベル３の防止対策は、ＨＥによって発生した事故を局限化し、それ以上発展させないための種々の工学的安全装置および安全対策からなり、場合に応じて多重化される。

いずれのレベルにおいても、今後はコンピュータによる人間支援システム、特に人工知能化された人間支援システムによって、ＨＥおよびＨＥに起因する事故災害を防止することになろう。また、コンピュータの発達により人間に要求される作業が従来の手順的作業から認知判断へと変わりつつあり、今後は人間の認知判断支援がますます重要になる。

４－３　ＨＥの評価

各種の防止対策によりＨＥの発生とそれに起因する事故災害は未然に防止されるが、ある特定の条件の重なりが生じた場合には各種安全装置・安全対策の隙間をぬって大きな災害が発生する。この事故災害に至る条件の重なり合いを追求し、有効な対策を確立するためにPRA等のシステム工学的方法が用いられる。PRAでは、どんなＨＥが、事故の引き金、事故を進展させる要因、あるいは事故要因の発生頻度に影響する因子になるかが解析される。評価結果は、マン・マシン・インタフェース設計やバックアップ・システムの性能改善に反映される。

PRAで定量的評価を行うために、ＨＥの発生確率も定量的に評価する必要がある。代表的な評価方法に、米国サンディア研究所のSwainらにより考案されたTHERP (Technique for Human Error Rate Prediction)[8]がある。人間の一連の仕事を解釈、操作、読みとり等の基本的な単位仕事のつながりで表わし、各単位仕事を成功する場合と失敗する場合に分岐しながら、どのような結果に至るかを評価する。個人的要因、状況的要因やストレス要因の影響ならびに仕事間や作業員間の従属性を考慮して各単位仕事の失敗確率を評価して、仕事全体の失敗確率を得る。

システムを人間－機械系としてとらえると、人間の行動は関連する装置の状態などに依存してその対応が変化する。ＨＥと機器故障を同時に考慮して解析を行う方法として、マン・マシン・システム信頼性解析手法[9]や人間や機械をペトリネット（互いに関連しあう同時進行的な要素からなるシステムのモデル化に適したグラフ表現）によりモデル化する方法[10]がある。

コンピュータの発達で人間に要求される仕事が手順的作業から総合的な認知判断に変化してきた状況では、仕事遂行に対する許容時間の考慮が重要となる。人間が外界からの刺激に対して反応・判断・対処する時間とその対応行動に失敗する確率との関係は、慣れているか、熟知しているか、あるいは未経験かで対応関係が異なる。このような認知判断でのエラー確率と許容時間の関係を定量的に評価する方法にHCR (Human Cognitive Reliability)[11]がある。また、判断誤りの原因やその影響をシステム工学的に解析・評価する方法にＣＭ(Confusion Matrix)[12]がある。

ＨＥに関する定量的データが少ない現状では、その評価はどうしても専門家の判断に頼らざるをえない。専門家の判断から人間のエラー確率を合理的に導出する、コンピュータを用いた方法にＳＬＩＭ－MAUD (Success Likelihood Index Methodology - Multi Attribute Utility Decomposition)[13]がある。

スペースシャトル事故に見られるように、人間組織の意思決定機関での情報伝達や指示経路等での問題が重大事故を引き起こすこともある。人間組織上の不備であり、広い意味での設計エラーのＨＥに相当する。このような管理体制の欠陥を検出する方法にMORT(Management Oversight Risk Tree)[14]がある。管理体制の現状と一般的に作成された管理欠陥の論理樹とを参照比較して問題点を発見しようとするものである。

５．おわりに

システム設計・計画段階から、製作、運用段階を通して、システムに生じる事故や災害に生じるリスクを低減するためのリスク管理について考察してきた。しかし、実際にこれら考えられる低減策がシステムに適用されるかどうかは、最終的にはリスク管理を行う最終的な意思決定者に依存する。企業であれば最高責任者の考え方で、リスク管理に取り組む作業者の姿勢も決定される。意思決定者が、システムに生じるリスクを低減することは社会的義務であ

ると考え、リスク管理に取り組まなければならない。システム設計・計画段階から十分に、システムから生じる利益とともに事故、損失の影響を検討しなければならない。システム製作、運用段階では、考慮漏れのリスクに対しては単に善後策がうてるのみである。リスクに対する多角的視野からの検討・評価が必要であり、このために設計・計画段階でのPRAのようなシステマティックに評価・検討する枠組みの果たす役割は大きい。

従来、災害や損失などのリスクはシステムが正常状態から逸脱して異常や故障を起こしたときに発生すると考えられがちであった。しかし、公害汚染や環境破壊のようにシステムが正常に稼働していても問題が生じることがある。ＰＣＢ問題のように化学工業で生産された製品が使用、消費、廃棄にいたるプロセスを通して環境へ放出されて広域にわたる環境汚染から人間に害を及ぼすことがある。したがって、システムのリスク管理を検討するときは、多角的視野からシステムに関連する事項について評価、検討することが重要である。

参考文献

1) F．R．Farmer：Sitting Criteria－New Approach, Containment Sitting of Nuclear Power Plants, Proc. Symp. Vienna, Pap. SM-89／37, 1967
2) AIChE ed：Guidelines for Hazard Evaluation Procedures, AIChE, 1985
3) 井上紘一、熊本博光「リスクアナリシスの方法論」『安全工学』23、pp.323～329、1984年
4) 井上威恭監修『ハィンリッヒの災害防止論』海文堂、pp.281～282、1982年
5) 山崎弘郎編著『異状の検出と予防－センサと設備診断技術－』工業調査会、1988年
6) 井上紘一、幸田武久、熊本博光、高見勲「安全監視システムの最適論理構成」『計測と制御』24－2、pp.142～154、1985年
7) 幸田武久、井上紘一「診断エキスパートシステム」『電気学会論文誌D』108D－10、pp.872～875、1988年
8) A.D.Swain and H.E.Guttmann：Handbook of Human Reliability Analysis with Emphasis on Nuclear Plant Applications,NUREG／ＣＲ－1278, USNRC, 1983
9) 夏目明典、高見勲、寺西進、井上紘一「マンマシンシステム信頼性評価システム」『第４回ヒューマン・インタフェース・シンポジウム論文集』pp.251～256、1988年
10) T．Kohda，T．Hagino and K．Inoue：Human Error Analysis Using Petri Nets,Proc. International Symposium on Reliability and Maintainability 1990－Tokyo,pp.72～77,1990
11) G.W.Hannamann,et al:A Model for Assessing Human Cognitive Reliability in PRA Studies, Presented at the Third IEEE Conference on Human Reliability, Monterey, C A,1983
12) D.J.Wakefield:Application of the Human Cognitive Reliability Model and Confusion Matrix Approach in a Probabilistic Risk Assessment, Reliability Engineering and Systems Safety,22, pp.295～312, 1988
13) D.E.Embrey,et al:SLIM－MAUD:An Approach to Assessing Human Error Probabilities Using Expert Judgment,NUREG/CR－3518,USNRC,1984
14) W.G. Johnson: MORT Safety Assurance Systems,Marcel Dekker Inc.,1980