安全と危険の狭間(グレイゾーン)への対処と活用†

田中 健次*

最近の社会的な事故を調べてみると、グレイゾーンで発生する事故が多いことに気づく。本論では、このグレイゾーンを把握しリスク低下のための対応方法を提案することが、リスク工学の主たる課題であるという観点に立つ。初めにグレイゾーンを考慮した安全保証型と危険回避型のシステム設計の分類の重要性を説き、グレイゾーンを減少させリスクを低下させるための学習メカニズムを提案する。特に危険回避型では2つの学習によってグレイゾーンの縮小化が可能となることを示す。後半では、グレイゾーンに不可避部分があることから、むしろそれを積極的に利用してリスクを低下させる方法として、規則の記述方法への活用と、数理的なモデルに基づく高信頼性モニタリングの設計方法について述べる。

キーワード：グレイゾーン、安全設計、学習、インシデント、報告システム、安全監視システム

1. はじめに

リスク工学、リスク管理、リスク解析などリスクで始まる多くの概念がある一方で、安全工学、安全管理、安全解析など安全で始まる語もある。これらは、単にリスクを安全に置き換えただけの同じ対象を指す言葉であろうか。『「リスク管理」の語は危険な状況や事故の発生が前提にあるので、『安全管理』の方が望ましい』との発想であるならば、どちらの表現でも意味するものには変わりはない。この発想の根底には、危険と安全が二律背反であるという前提があるが、しかし2節で述べるように、実際には危険と安全は対称の言葉ではなく次元の異なる概念である。現実には存在するのは様々な危険性だけであり、許容できる範囲内を安全と称しているに過ぎない。注目すべきは、現実には発生しているアクシデントの多くが、危険性の高いところではなく、むしろ危険性のそれ程高くない箇所、危険性の不明な箇所が発生していることである。

本論は、リスク工学とはこの安全と危険の狭間、グレイゾーンを処理する工学であるとの立場に立つ。グレイゾーンを明確に把握し、それへの対応方法を提案することがリスク工学の主たる課題であるという観点から、前半でグレイゾーンへの対処方法を提案し、後半ではグレイゾーンを積極的に利用したシステム設計を考える。

初めに3節で、グレイゾーンで発生した4つの国内

事故例を示し、共通の原因を探る。筆者は既に、製品安全設計において安全保証設計と危険回避設計の区別を提案している [13] が、4節と5節でそれらがシステムマネジメントにも有効な概念であることを示す。そして、グレイゾーンを減少させリスクを低下させるためには運用における学習メカニズムが必要であり、特に危険回避型の設計やマネジメントでは、2つの学習構造が必要であることを示す。

一般にグレイゾーンは狭い領域であることが望まれるが、不可避な部分もある。しかし、それを積極的に利用することでリスクを減少させ、かつ使い勝手や性能を向上できる例がある。6節で規則の記述方法での活用例を考え、7節では、高信頼性のモニタリング設計への応用を考える。後者は Dempster-Shafer 理論に基づく解析を行う。

2. 安全と危険の非対称性

2.1 安全は証明不可能

安全追求と危険追求の関係は、科学論における帰納主義と反証主義との関係に似ている。

帰納主義とは、多くの事例(単称命題)を積み上げることで普遍命題を引き出す帰納法を科学の中心におく考え方である [4]。しかし、いくら事例を積み上げても常に反例が出てくる可能性はあり、普遍命題の正当性を論理的に根拠付けることはできない。このため、「科学は反証ができるだけで実証はできない」「しかも反証は一つの例で十分である」との反証可能性を中心とする反証主義に代わられた経緯がある。

安全も決して「証明する」ことはできない。様々な側面で、あるいは特定の条件下で危険性が小さいことを示す事実を積み上げることで、安全性への確度を高

† Dealing with and Utilizing Gray Zone between Safety and Danger
Kenji TANAKA

* 電気通信大学大学院情報システム学研究科
Graduate School of Information Systems
University of Electro-Communications

めているに過ぎない。確実に示せるのは危険性だけであり、安全性を崩すにはたった一つの事例で十分であるという点で、安全追求も科学における反証主義の立場に近い。我々は、決して安全性を導き出しているのではなく、その確信度を上げているだけである。

2.2 安全と危険の狭間

安全性は証明できなくとも、安全度の高い状況や危険な状況は、経験的、固有技術的に認識できることが少なくない。しかし多くの社会的な事故の原因は、この確信度の高い安全と明らかな危険の狭間、グレイゾーンに存在するケースが極めて多い。あるいは、危険領域の周縁(エッジ)で起こるといってもよい。そこは状況認識や状況予測が難しい領域であって、条件によって安全にも危険にもなり得る部分である。

一般に、故障モードや危険因子はFMEA等の信頼性手法で設計段階に抽出され、致命度の高いものには対策が施される。むしろ、対策対象の限界と判断する致命度ラインの前後の事象にこそ、着目すべき因子が含まれている。幾つかの例を次節で考えてみよう。

3. 事故の共通パターン

3.1 グレイゾーンで起きた事故

平成11年から12年にかけて、社会性の高いシステムでの事故が続発した。臨界事故、地下鉄の脱線事故、ダイオキシン流出事故、食中毒、患者取違え事故などである。それらの事故の原因は既に調査・追求され報告されているが、「事故の解析だけで終わっては、再発防止や未然防止には繋がらない」との指摘をよく耳にする。組織管理上の問題など根本的な要因まで踏み込んだ調査が少ないからである。表面上は異なる現象でも、多くの事故に共通した原因のパターンを追究し、背景まで踏み込んだ解析を行うことにより、システムに共通するトラブル原因の削除が可能となる。

そこで、グレイゾーンに着目して共通パターンを見出し、組織事故の発生を未然に防ぐための方法を探る[18]。4つの事故を取り上げよう。

(1) 臨界事故 [5]

平成11年9月発生した臨界事故は、海岸沿いの原子力発電所内ではなく、街中にある民間のウラン加工工場内で起こった。原子力発電所内での危険な箇所やプロセスに対しては、2重3重の防護が施されており、事故対応もしっかりとマニュアル化されている。しかし、前処理工程の工場では安全体制が手薄になっていた。

また、この工場では通常時は軽水炉用の核分裂性ウランを加工しているが、事故時は通常時の6倍の濃縮度を有する常陽用ウランを加工していた。この燃料は

稀に扱うもので、3年ぶりの作業であった。

(2) 地下鉄の脱線事故 [20]

平成12年3月、中目黒駅近くのカーブで、地下鉄の車両が脱線し負傷者を出した。運輸省令では、曲率半径160m未満のカーブは原則として設置が禁止されているが、脱線事故は、曲率半径160.1mのカーブの地点で発生した。まさに、危険回避措置の境界のすぐ外で事故は発生した。

(3) ダイオキシン汚染

平成12年3月、藤沢の産業機械・プラントの大手メーカーが、基準を大きく超えるダイオキシンを川に排水していることがわかった。工場内の廃プラスチックなどを燃やす焼却炉で排煙をろ過するために使った汚水が、汚水処理施設ではなく、雨水路に流れ込んで川に注いでいたためである。通常のダイオキシン濃度基準1ピコグラム(1リットル中)のおよそ8000倍の濃度値が川で検出された。平成5年の工事で配管の接続を間違えたことが原因だが、当時、焼却炉本体の検査のみが行なわれ、配管までは検査されなかった。

(4) 食中毒事件

平成12年7月、5000名を超える食中毒患者を生んだ乳製品による食中毒では、黄色ブドウ球菌が、生産工程で余った低脂肪乳を予備タンクに戻すための仮設配管をつなぐバルブ部分で検出された。洗浄を怠ったことが原因といわれているが、問題となった箇所は貯蔵用のタンクではなく、通過するだけのバルブ部分で軽視されがちな部分であった。

これらの事故はすべて、危険度の高いところではなく、危険性が低く明確に把握できないところ、すなわち安全と危険との狭間のグレイゾーンで発生している(図1)。危険となる度合いの高いプロセスや明確な危険箇所に対しては、十分な対策が施され検査が行なわれていることが多いが、まれに危険になる個所、使い方によっては危険となりうる個所などで事故は発生し易くなっている。

図1 グレイゾーンと事故

3.2 偶然を必然に変えた要因

グレイゾーンで起こる事故に共通していることは、「これまではうまくいっていたのに事故が起きてしまった」という状況である。「偶然に」問題なく運営されてきたシステムで「必然的に」生じた事故であり、この偶然を必然に変えた要因もまた共通したものである。

(1) 標準・基準の緩和

臨界事故では、効率性、使用性の重視により作業マニュアルが書き換えられていた。事故を起こした会社では、昭和61年にクロスブレンディングと呼ばれる溶液均質化の手法が使われるようになり、平成6年にステンレス製バケツの使用へと社内手順が変更されている。平成11年9月には、臨界安全形状の貯塔の代わりに沈殿槽が使われることが提案され、事故に至った。地下鉄の脱線事故では、運営企業が独自に定める脱線防止ガイドの設置基準が当初の曲率半径200m以内から140m以内に変更されていた。多くの事故で、事故前にこのような標準の緩和が実施され、事故の要因となっている。

(2) 危険認識の喪失

前項の標準緩和が一度ではなく、繰り返し行われていることは、無事故からの学習活動と行うことができる。しかし一方でそれは、危険認識の喪失を生み出す危険性も秘めている。

臨界事故を起こしたウラン加工会社での連続的標準の緩和と同様、脱線事故を起こした会社の定めた脱線防止ガイド設置基準も、昭和26年の基準200mから4回の緩和措置を経て昭和43年には140mとなり、運輸省令の設計限界(原則160m 未満禁止)を下回る自主基準に至っている。

一定の期間、事故が発生しないと、人は、潜在的危険性の認識が薄れて安全性を過信する傾向にあることが予想される。グレイゾーンでは、小さな状況変化、条件変化が事故に繋がる可能性を有しているのである。

残念ながら人の過信のメカニズムは未だ解明されていない。過信が生まれた状況を、実験で計測、確認することが難しいからである。一方で、故障率や不信頼度が高いシステムで人は不信を抱く傾向にあることが知られているが、故障の発生程度だけではなく、故障発生のパターンも不信を引き起こす要因となり得ることが示されている [1]。例え同じ故障頻度のシステムでも、連続的に故障が発生する場合の方が、離散的に故障が発生する場合よりも不信に陥りやすいことが、実験により確認されたのである。このことは、オペレータの危険認識が、危険事象の連続発生によって過度に高まる可能性があることを示しており、正しく危険を認識することの難しさを示唆している。

(3) 管理システム導入の形骸化

食中毒事故を引き起こした乳製品会社は、食品業界で利用され始めている HACCP(Hazard Analysis and Critical Control Point)の認可を受けていた。しかし、実際の工程では規定通りの検査を実行せず、菌の発生を見逃していた。その後の厚生省の調査でも、全国の HACCP 承認施設の半数で、本来備えるべき洗浄記録が不備であることが明らかになっている。一方、ダイオキシン汚染を起こした会社は、ISO14000を取得しており、環境保全への意識の高い会社である。しかし、施設変更時の配管の誤りが見過ごされ、変更作業の届出も怠ったとされる。

これらの認可は、設計時あるいはある活動の時点で、プロセスが審査され承認されたものであり、フォローアップ制度はあるものの、運用は各組織に任されている部分が多い。管理システムを導入したことへの過信が生じた可能性が高い。

以上の3点は、他の事故でも共通して見られる組織レベルの問題である。特に、効率化を向上させるための標準変更が原因の一つになっていることが多く、効率化を狙ったことやそれを促した組織がたびたび批判される。しかし、効率化のための改善は品質管理活動の一環であり、真の問題は、効率化を考慮する際に、

①標準の変更に伴うリスク増加はないか？

②新しいリスクの発生は考えられないか？

の事前検討を怠った点にある[11]。特に、人員削減が目的の標準変更では、削減された担当者によって実現されてきた危険回避が同時に削減されることになるから、削減分を補うための新しい対策が必要になる。しかし、その点を忘れていたケースが多い。

また、社会的に問題となるのは、事故の発生自体だけではなく、発生した事故への組織の対応が遅い点にあることを注意すべきである。医療事故でも、病院側の迅速な対応、再発防止策立案などの活動に、訴訟を取下げたケースが起きている。すべての事前予測が要求されているわけではなく、素早い事故対応が社会的な大事故への拡大を回避する可能性があることは、システム設計でも考慮すべき点である。

4. 安全保証設計と危険回避設計

4.1 グレイゾーンの原因

3節で述べたように、グレイゾーンの存在が事故の原因になるが、残念ながらグレイゾーンを設計で完全に回避することは不可能である。それは、グレイゾーンの発生原因として、

(原因1) 設計者の予測の限界

(原因2) 設計者には防げないユーザの使用エラー

(原因3) 情報不足

があり、(原因1、2)は設計者には不可避な要因だからである。したがって、設計段階ではなく運用の段階で事故を回避する方法を導入する必要がある。本論では、学習によるグレイゾーンの縮小化、あるいは明確化による回避を提案する。

4.2 グレイゾーンでの二つの学習

Swainは「人の方を変更するには限度があり、安全は設計の問題である」と述べた。日本でも1995年製造物責任法が施行されて以来、本質的安全設計の重要性が唱えられ、製品やシステムに安全の仕組みが作り込まれてきた[9]。

筆者は、製品の安全設計のためには、設計を安全保証設計と危険回避設計とに分けて考えるべきであると主張してきた[13]。安全保証設計とは、グレイゾーンをも回避する設計方法であり、高い安全性のもとで使用できる設計である。例えば、fool proof 構造は安全保証設計の典型例であり、決められた方法、手順でのみ使用が可能となるため、(原因2)を回避できる。一方の危険回避設計とは、グレイゾーンには対応せず、明らかな危険に対してのみ対応するものである(図2)。

これらは、機械設計分野での安全確認型設計と危険検出型設計の分類[10]と類似の概念である。そこでは安全確認型設計が安全確保には必須とされているが、一般のシステム設計では必ずしも安全保証型が要求されるというわけではない。実際、安全保証設計の方が安全性は高いが、構造的、経済的観点から、あるいは使用上の自由度を確保する理由から、危険回避設計で十分と判断されることも少なくない。例えば、予測されても頻度が小さな事象は通常、対策対象外となる。したがって、危険回避設計ではグレイゾーンで発生するアクシデントに対する別の対応が必要になる。

ここでは、グレイゾーンに対する二つの学習活動による対応方法を提案する。

一つは、レポートシステムなどによる問題指

図2 安全保証設計と危険回避設計

摘を活用する方法である。製品の使用上の問題点をレポート収集し、製品設計にフィードバックする方法である。クレーム情報や事故情報が有効だが、未然防止には、積極的なインシデント情報(事故に至る前の段階の情報、ヒヤリハット情報)の活用が重要になる。

今一つはユーザに委ねる方法である。使用者が危険性と安全性を認識し、使用者自ずから危険を回避できる仕組みを組み込む設計方法である。最近の機器はブラックボックス化の傾向にあり、内部のメカニズムがわかりにくい。安全性は危険認識によって獲得できるという2.1節の立場からは、ユーザ自身が危険を認識しやすい設計、透明化によるユーザ自らの安全性確保が重要と思われる。例えば、電源延長コード等で過電流を自動遮断する前に過電流を示す警告ランプを点灯させるなどである。ここでは安全学習指向設計と呼ぶことにする。

前者の報告システムは設計側の学習により設計段階の予測限界(原因1)を補完し、後者はユーザ側の学習により誤使用(原因2)の回避を狙うものであるから、後者は特に危険回避設計で効果的な方法になる。双方とも運用上の学習を狙うものだが、そのための仕組みは設計段階で作られていないことが必要である(図3)。

5. 安全保証型と危険回避型のマネジメント

5.1 マネジメントへの応用

システムマネジメントに関連するアクシデントは「システムの失敗」と呼ばれており、組織事故はその典型例である。「システムの失敗」とは、実際の結果が期待された結果とミスマッチのとき、あるいは目標に達しない状況を指す概念である[3]。

3節でみたシステムの失敗は、グレイゾーンを明確に意識しないために生じた事故であり、マネジメントにおける安全保証型と危険回避型を区別しないために発生した事故と考えることができる。例えば、地下鉄の脱線事故では、危険回避の限界として定めた政府の曲率半径の限界を、会社は安全保証の境界と誤って解釈したものと考えられる(図4)。危険回避の限界付近はグレイゾーンであり、危険となる可能性を考慮して、脱線防止ガイドを設置するなどの安全策が必要であっ

図3 本質的安全設計

図4 運輸省令と管理会社の設計限界の解釈相違

た。

このように、二つの設計タイプをマネジメントに適用すると、他のシステムの失敗原因も把握しやすい。以後、話を単純にするために、システムマネジメントとは規則・標準の制定と維持が主な内容と考え、安全保証型のシステムマネジメントとは、安全保証を目的とする規則を採用・維持すること、危険回避型のシステムマネジメントとは、危険を回避するための規則を採用することと考える。そして、前節同様、危険回避型のマネジメントでは、使用者が学習指向になれるシステム作りが必要であり、両マネジメントで、レポートシステムの採用が望ましいことを以下で示す。ここで使用者とは、システムの利用者や組織で働くオペレータ、作業員等に相当する。

5.2 安全提供型から安全獲得型へ

学習指向のシステム作りは、事前に「安全を設計する」という発想ではなく、運用段階に「皆で安全を獲得する設計」という発想に基づく。

例えば、医療の現場で、病院側が医師对患者という観点から「質の良いサービス(治療)の提供」を重要と考えるのではなく、患者親族も含めたチーム医療という観点から「皆で協力し患者を最高の治療で治す活動」ととらえる方法である。既に船橋市立医療センターなどで試みられているが、例えば、点滴の薬はいつもと同じか、飲む薬は何のための薬かを家族(親族)がチェックし、手術室の台に載るまで家族が付き添うなど、患者親族が医療に参加することで、医療におけるグレイゾーンでの事故を防止できる可能性が高まる。それは医療機関側の学習につながると同時に、医療機関と患者のコミュニケーション不足を解消する効果も期待できる。一般システムであれば、システム管理者とユーザ(作業員、利用者等)間の協同活動による危険防止活動である。

前述のように、安全学習指向設計は、危険を認識さ

せることで、使用者エラーを自ずから防止する効果を期待するものである。グレイゾーンでのユーザの学習を期待するためには、危険情報の「共有化」またはメカニズムの「透明化」が必要である。グレイゾーンで危険が存在するのは、設計者の責任ではなく設計者の限界と考えるべきであり、むしろ、危険性を判断するための情報提供の仕組みが具備されていないとき、設計者は責められるべきである。

地下鉄の脱線防止ガイドの基準緩和でも、度重なる緩和において、閾値のシフトが潜在的な危険性をどの程度増加させているかを、自ずから学習することが必要であった(図5)。

グレイゾーンでの発生事象は、発生確率が小さいため無視されやすいが、一度発生すると、大事故や大損害を引き起こすものもある。発生確率が小さいのは、自由度が大きく条件の組合せが複雑であるためで、ある条件が同時に発生すれば事故は発生する。2002年7月ドイツで発生した航空機衝突事故では、保守点検のために管制塔の異常接近自動警報装置が切っており、ニアミスが発生、管制官の指示遅れ、指示誤りに繋がるなど幾つもの要素が同時に発生した。様々な条件が従属的に連鎖発生する可能性を考えると、一つの状況変化(保守点検でoffなど)がどのような潜在的な危険性を新たに発生させているかを、常に理解することが必要である。

5.3 インシデント・レポート・システム

もう一つの学習システムである、インシデント・レポート・システム(IRS)は、未然防止に最も効果が期待される方法として、近年注目を集めている。IRSは、インシデント情報を用いてアクシデントを事前に回避する方法であり、いわゆるハインリッヒの法則を根拠に、フィードバックの機会が多いと期待されている。航空業界で早くから導入され、最近では医療分野、海運業界でも導入され始めているが、その目的が組織全体に浸透せず、有効に稼働できない状況である。

図5 基準緩和による危険領域の拡大

筆者は、ある病院で IRS が円滑に稼動しない理由を調査し、3つの要因を導出した [18]。

第一に、専属の解析者がいないことである。リスクマネージャの役割を担う医師が解析しているため、解析の時間が少ない。さらに事前の安全対策が十分でないため、余りに多くのレポートが集まり過ぎて解析できない状況に陥っている。本来、事前に FMEA などを取り除いておくべき危険要因まで報告に含まれているからである。IRS は、グレイゾーン領域での情報収集を中心として導入するからこそ、少数だが貴重な情報がクローズアップされるものである。

第二に、インシデント情報を活用する組織体制が構築されていないことである。インシデント情報は、オペレータ層からマネジメント層（意思決定層）へ流れ、対応がとられる（図 6）。従来の規則を変更するだけでなく、規則の定め方の変更など評価基準、価値観の再考まで含める場合、この役目はメタ層と呼ばれる「意思決定の意思決定」という上位機能の役目となる。ダブルループ学習 [2] ととも呼ばれるこの機能に依れば、単に規則変更に限ることなく規則変更の理由まで遡ることで、同じ原因で発生することが予想されるトラブルの未然防止が可能になる。多くの医療機関ではインシデントレポートの収集システムだけを導入し、このメタレベルの機能を組織に導入することを忘れている。

第三に、モチベーションが十分でない点が問題である。レポートを出す動機を大切にすることが必要である。確実に迅速なフィードバック、容易な報告、匿名性など幾つかの要点が既に指摘されている [11]。アクシデントの情報収集の場合は、欧米のように免責が前提になるが、日本では学会でその必要性が議論され始めたものの実現性は全く見えない。したがって、インシデントレベルの情報を重視すべきであろう。

図 6 メタ層を含むマネジメントシステム

6. グレイゾーンを利用した規則の記述法

ここまでは、グレイゾーンで学習することによりグレイゾーンを如何に明確にするかを、言い換えれば、グレイ部分を如何に減少させるかを考えてきた。しかしここからは、設計段階には回避不可能なグレイゾーンを積極的に活用してリスクを下げる工夫について考える。本節では規則の記述方法での活用を、次節では高信頼度のモニタリング設計方法への利用を考える。

規則やマニュアルの記述方法には、「positive 記述（P 記述）」と「negative 記述（N 記述）」の2通りが存在している。P 記述のマニュアルとは、「何をすればうまく行くか」が明示してあるマニュアルであり、標準、手順書である。一方の、N 記述のマニュアルとは、「何をしてはいけない」かが記されている注意書、警告書などである。

P 記述の利点は、既知の事象には確実に対応できることである。明確な操作指定だから確実に安全を保証できる。しかし、深い思考を必要としないため学習効果は乏しく、柔軟な利用や応用には適さない。強い強制は規則違反の原因になることもある。一方の N 記述は、禁止事項の明示に留まるため、操作の選択の自由度が多く、未知の事象にも柔軟に対応できる可能性を有している。ただし、その注意書きさえクリアすれば 100% 安全という保証はない。

P 記述は、きわめて安全性を高く要求される場合や初心者への操作指示などに効果的である。一方、設計外の事象に対しては、N 記述が重要な役割を果たす。マニュアルが用意されていない状況でも、運転員は状況を判断し、その結果に基づいて何らかの操作することが要求されるが、試行錯誤や慎重な予測は、危険な操作が明確になって初めて有効に働くものであろう。ベテランによる経験や勘に基づく試行錯誤は、ランダムな試行錯誤ではなく、N 記述に相当する危険操作の排除を経験的に無意識に行いつつ、P 記述と N 記述を効率的に併用しているものと予想される。

以上のように、P 記述と N 記述を目的に応じて使い分け、グレイゾーンを生かした対応を如何に取り入れるかが要点である。そこでも、ユーザ側の正しい認識が要求される。脱線事故における政府の規制のように危険回避としての規制が安全保証の規制と誤解されることのないよう、正しい伝達が重要になる。

7. グレイゾーンを利用した高信頼度モニタリング

7 節では、グレイゾーンを利用して高信頼度に対象を監視するセンサシステムの設計方法を考える。

7.1 誤作動と不作動

高信頼度のモニタリングは、ITS(高度輸送システム)やプラント制御の自動化を成り立たせる大前提として重要である。特に安全監視システムでは、敏感に反応するセンサの場合には誤作動が、鈍感に反応するセンサでは不作動がそれぞれ問題となる。そこで、センサで判断の難しい領域にグレイゾーンを設け、グレイゾーンでは新たな情報を加えた2段階のモニタリング方法を考えると、効率的で精度のよい安全監視が期待される。どのような状況でこの種の2段階監視の効果が得られるのか、どの程度のグレイゾーンの設定が望ましいかなどは、数理モデルで定量的に解析することができる。

ここでは、誤作動と不作動をまとめて「誤動作」と呼ぶことにする。誤動作の原因として、従来からノイズの影響が考察されてきた。最近では携帯電話からの電磁波が医療機器に影響を与えるなど、周囲環境からの影響による誤動作も増加している。これら一過性の誤動作に対しては同質の複数センサによるモニタリングが効果的であり、k-out-of-n型の判定が最も有効である[7]ことが知られているが、監視特性と監視対象の状態とのずれに起因する誤動作は、グレイゾーンの設定で初めて回避することができる。(図7)。「センサは正しく反応」しても監視特性の性質から判定を誤る場合であり、例えばタバコの多量の煙に反応する火災報知機の誤報は正にこのタイプの誤動作である。明らかに同質センサの複数化では、この種の誤動作に対して効果がない。このタイプの誤動作は、いわば監視特性依存型誤動作と呼ぶべきものである。

7.2 2段階判定法

監視特性依存型の誤動作を回避するシステムとして2つのタイプが考えられる。異種の特性を組み合わせ

図7 監視特性依存型の誤動作

て状態を推定する Heterogeneous monitoring system (図8(a)) [17] と、同一特性を2つの異なる閾値のセンサで監視し、グレイゾーンを含む3値で判定する Non-homogeneous safety monitoring system (NHSMS, 図8(b)) [14] [16] とである。前者では、どのような特性値の組を選ぶことが必要か、得られた結果をどのように統合するかが問題となる。ここでは、単独の特性値で簡単に作れる後者の NHSMS を一つの3出力センサ(安全、危険、グレイゾーン)と考えて、それを利用したモニタリングを考える。

グレイゾーン出力に対する状態判定の方法として、次の2通りを考える。

Strategy I 確定的判定法

・予めグレイゾーンに対する判定を1通りに決めておく方法。それを常に危険と解釈するとき敏感システム (Sensitive system: S-Sys) と呼び、常に安全と解釈するとき鈍感システム (Blunt system: B-sys) と呼ぶ。

Strategy II 2段階判定システム (図9)

・グレイゾーンでは更なる情報を加えて判断する方法。

グレイゾーンを固定し、2段階判定システムが望ましい条件を求める。さらに、2段階目の情報を、精度の高いセンサなどで自動的に得る場合と、人が判断する場合とでどちらが望ましいかも比較する。

7.3 Dempster-Shafer 理論モデルによる解析

評価規準として総期待損失の最小化を採用する。総期待損失 E は、不作動に因る損失 $Z_{No\ alarm}$ と誤作動に因る損失 Z_{alarm} の期待値の和として表される。ここで、真に危険を D 、真に安全を S で表す。

$$E = E[Z_{No\ alarm}, D] + E[Z_{alarm}, S] \quad (1)$$

本論では、証拠理論として知られる Dempster-Shafer 理論 (DS 理論) に基づき、不定状況を取り入れたモデル化を試みる。少し準備が必要である [8]。

Ω を監視対象の全体状態集合とし、安全領域 S と危

図8 監視特性依存型の誤動作を防ぐ2つの方法

図9 3値センサによる2段階判定法

領域 D に二分されるものとする。すなわち、 $\Omega = S \cup D$ かつ $S \cap D = \emptyset$ である。真に安全な場合に状態判定された結果“S”(安全)、“D”(危険)、“X”(不明)への基本確率 (basic probability assignment (BPA))、 $m_s(S) : \{“S”, “D”, “X”\} \rightarrow [0, 1]$ を、

$$\begin{cases} m_s(“S”) = \text{真に安全のとき安全と判定される確率} \\ m_s(“D”) = \text{真に安全のとき危険と判定される確率} \\ m_s(“X”) = \text{真に安全のとき判定不可能となる確率} \end{cases}$$

で定義する。これらの基本確率は、フィールドデータや実験データを基に、安全または危険な状態のときにそれが安全や危険と判断される確率を求めて、1からそれらの値を引いたものを判定不可能な場合の確率とすればよい。以後、真の安全 S と、判定された結果の安全“S”とを同じ S で表現するが、混乱はないであろう。真に危険なときの基本確率 $m_D(*)$ も同様に定める(図10)。さらに以下の記号を用いる。

$$\begin{cases} \pi : \text{対象システムが危険である確率} \\ \bar{\pi} = 1 - \pi : \text{安全である確率} \\ C_s : \text{誤作動1回当たりの損失} \\ C_D : \text{不作為1回当たりの損失} \end{cases}$$

敏感システムと鈍感システムの総期待損失は、DS理論で使われる Belief 関数 Bel と plausibility 関数 Pl を用いて、

$$E_{S-\text{sys}} = \pi C_D Bel_D(S) + \bar{\pi} C_s Pl_S(D) \quad (2)$$

$$E_{B-\text{sys}} = \pi C_D Pl_D(S) + \bar{\pi} C_s Bel_S(D) \quad (3)$$

でそれぞれ表される。ここで、 $Bel(A)$ は事象 A が成り立つと確信する確率の値であり、 $Pl(A)$ は A が成り立つ可能性があるとする場合の確率の和を表す。したがって、常に $Bel(A) \leq Pl(A)$ であり、センサモデルでは、 $Bel_D(S) = m_D(S)$ 、 $Pl_D(S) = m_D(S) + m_D(X)$ 等で得られる。

2段階判定法の損失期待値を算出するために、2段階目に誤判定するエラー率として、真の危険に気づかず安全と誤判断する確率 R 及び真の安全を危険と誤る確率 $\bar{R}$ を導入する。ここで R は、判定が遅れて判定結果が出る前に致命的な状況に陥る場合等も含む確率とする。また、2段階目の判定で使用するセンサの使用コストを C_l とする。このとき、2段階判定方法の総期待損失は、

$$\begin{aligned} E_{2-\text{step}} = & \pi C_D Bel_D(S) + \pi (C_l + R C_D) m_D(X) \\ & + \bar{\pi} C_s Bel_S(D) + \bar{\pi} (C_l + \bar{R} C_s) m_s(X) \end{aligned} \quad (4)$$

と表される。第2項は、真に危険な場合にグレイゾーンと判断され、2段階目の判定が行われたがその判定を誤り損害を発生させた場合である。第4項は真に危険な場合の2段階判定で誤判定を下した場合である。ここで以下の仮定をおく。

$$[A1] \quad R \bar{R} \leq (1 - R)(1 - \bar{R})$$

通常は R 、 $\bar{R}$ もに小さな値であり、常に成り立つ仮定である。初めに簡単のために $C_l = 0$ とし、損失関数(2)-(4)を比較することにより、最適判定システムの選定条件を求めることができる。ここで

$$K = \pi C_D, \quad L = \bar{\pi} C_s \quad (5)$$

と表す。 K と L は環境で決まる定数であり、制御できない定数である。

【命題1】

最適判定システムは、

$$\begin{aligned} 1. \quad & \left(\frac{1 - \bar{R}}{R} \right) \frac{m_s(X)}{m_D(X)} \leq \frac{K}{L} \Rightarrow \text{敏感システム} \\ 2. \quad & \left(\frac{\bar{R}}{1 - R} \right) \frac{m_s(X)}{m_D(X)} \leq \frac{K}{L} \leq \left(\frac{1 - \bar{R}}{R} \right) \frac{m_s(X)}{m_D(X)} \\ & \Rightarrow \text{2段階判定システム} \end{aligned}$$

$$3. \quad \frac{K}{L} \leq \left(\frac{\bar{R}}{1 - R} \right) \frac{m_s(X)}{m_D(X)} \Rightarrow \text{鈍感システム}$$

図10 3値センサと基本確率

(a) 真に危険のときの観測分布、(b) 真の状態と3値センサ、(c) 真に安全のときの観測分布

図11は特に $R = \tilde{R}$ の場合を表したものである。命題1は固定された R に対する判断方法の選択基準であり、図の縦方向の変化に相当する。一方、一定の環境(すなわち K/L) 下で、グレイゾーンでの2回目の判定誤り率がどの程度の値のとき、確定的判定に移行すべきかは横方向で分かる。

7.4 2段階目の判定

グレイゾーンでの判定に2段階判定を利用する場合、自動的に別センサの情報を利用し判定する方法と、オペレータ等がその都度、適当な情報を基に判定を下す人的方法とがある。

自動判定の場合、グレイゾーンで用いる新たな情報源として、(1) 精度の高いセンサの利用 (2) 異なる特性のモニタ情報、が考えられる。いずれの場合でも、誤判定の確率 $R, \tilde{R}$ は一定値と考えてよい。本論では、どのような情報を併用して統合判定することが効果的であるかは、システムに依存するため議論しない。

一方、グレイゾーンでオペレータや専門家など人間が判定する場合は、他の複数の監視情報を用いて総合的に判断できるなど、高信頼度の判定が期待できるが、この場合、判定時間の問題が浮上する。判定に長く時

図11 $R = \tilde{R}$ の場合の最適判定タイプ

間をかけるとその間に状況が悪化する可能性があるから、制約時間 T を予め設定することが必要である。しかし、その時間が短ければ判定誤り確率は高まる可能性がある。そこで、判定の誤り確率を制約時間 T の関数 $R(T)$ と考えるとき、一般に $R(T)$ は制限時間 T の減少関数となることが予想される。実際、ある種の作業を行う認知実験によりその減少傾向が示されているが[15]、判定作業一般に成り立つ性質か否かは定かでない。さらに、制限時間 T が判定時間の分布やモード(分布のピーク)に影響を与えることも上記の実験で確かめられている。 $R(T)$ をさらに詳細にモデル化し解析することが必要であろう。

人による判定の場合、一般に危険と誤判定する確率と、安全と誤判定する確率とを、それぞれ精度よく同定することは難しい。そこでそれらを同じ値 $R(T)$ であると仮定して、人による判定と自動判定のどちらが有効かであるかの判断目安を求めてみる。人の誤判定による期待損失は、式(4)の $R, \tilde{R}$ を $R(T)$ で置き換えればよく、それを自動化による判定の場合の式(4)と比較することで次の命題を得る

【命題 2】

グレイゾーンでの2段階目の判定で、人による判定が自動判定よりも効果的であるのは、

$$\left[\frac{\frac{K}{L}}{\frac{K}{L} + \frac{m_S(X)}{m_D(X)}} \right] R + \left[\frac{\frac{m_S(X)}{m_D(X)}}{\frac{K}{L} + \frac{m_S(X)}{m_D(X)}} \right] \tilde{R} \geq R(T)$$

のときである。

命題2は、自動判定での2段階目の不作動確率 R と誤作動確率 $\tilde{R}$ の値を $m_S(X)/m_D(X) : K/L$ の比に分け

る点と $R(T)$ との大小関係で最適な判定法が決まることを示している。 $R(T)$ が制限時間 T の減少関数であるならば、制限時間がある閾値以上確保できる場合には、人による判定が自動判定より優位になるということになる。

また、グレイゾーンでのセンサコスト(あるいは人の配置費用)を考慮する場合($C_l \neq 0$ のとき)、命題 1-2. の 2 段階判定法の最適条件は下記に修正される。命題 1 と同じく式 (2) と (4) の比較から右の不等号が、式 (3) と (4) より左の不等号が導出される。

$$\frac{\frac{C_l}{C_s} + \tilde{R}}{(1 - \frac{C_l}{C_d}) - R} \frac{m_s(X)}{m_d(X)} \leq \frac{K}{L} \leq \frac{(1 - \frac{C_l}{C_s}) - \tilde{R}}{(\frac{C_l}{C_d}) + R} \frac{m_s(X)}{m_d(X)} \quad (6)$$

7.5 DS 理論のメリット

DS 理論モデルの利点は、(2) ~ (4) 式がシンプルに表現される点にある。グレイゾーンを含まない *Bel* 関数とグレイゾーンを含む *Pl* 関数で期待損失がわかりやすく表現できる。しかし DS 理論が効果を発揮するのは、グレイゾーンと判定する確率 $m_s(X)$ (以下では $m(X|S)$ と表す) を算出するプロセスにある。本論は、NHSMS 型センサが、同一監視特性上の 2 つの閾値で判断するため確率 $m(X|S)$ を直接求めることができるとの前提で説明した。しかし、異なる監視特性の 2 つのセンサ、安全確認型センサ(Safety Preservation type: *SP*)と危険検出型センサ(Fault Warning type: *FW*)と組み合わせ判定する場合には、2 つのセンサの基本確率、 $m_{SP}(*|S)$ 、 $m_{FW}(*|S)$ から、

$$m(C|S) = kq(C|S) \quad \text{for } C \neq X \quad (7)$$

$$q(C|S) = \sum_{C=A \cap B} m_{SP}(A|S) m_{FW}(B|S)$$

で求めることになる[16]。ここで係数 k は、矛盾するセンサ出力の組み合わせに対する基本確率

$$q(\phi|S) = m_{SP}(S|S) m_{FW}(D|S) \quad (8)$$

を 0 とするための正規化パラメータである。特にグレイゾーンは、両方のセンサが反応しないときに判断されるから、一般式は

$$m(X|S) = k m_{SP}(X|S) m_{FW}(X|S) - (1 - k(1 - q(\phi))) \quad (9)$$

となる[6]。いわゆる Yager's rule は $k=1$ のときであり、 $m(X|S) = q(X|S) + q(\phi|S)$ 、すなわち矛盾す

る出力はグレイゾーンと考えることになる。これがもっとも標準的な処理であろう。

このような矛盾結果を設計問題として処理する場合、あるいは、情報の増加によりグレイゾーンを縮小する過程を記述するなど、グレイゾーンのダイナミクスを解析するには、DS 理論モデルは便利な表現であると予想される。それらは今後の課題である。

8. さいごに

本論は、グレイゾーンを考慮した枠組みを導入し、その枠組みの中では社会的な問題を考察することができただけでなく、安全監視システムの設計等の工学的な問題も議論できることを示してきた。これらの結果は、リスク工学をグレイゾーンを処理しリスクを減少させるための工学として統一的に体系化できる可能性を示唆するものである。アクシデントを防止するためには、グレイゾーンを考慮してマネジメントを安全保証型と危険回避型に区別することが重要であることを示し、グレイゾーンを減少させるための 2 種類の学習メカニズムを提案した。組織学習などの知識を背景に、より具体的な学習方法、学習内容を体系化することが今後の課題である。設計の限界を運用上の活動で補うために、運用上の活動のし易さを設計で作りこむことが重要である。また、グレイゾーンを積極的に利用することでリスクを減らすことのできる例を示したが、どの程度のゾーンを設定することが最も効果的かは、未解決の問題である。

参 考 文 献

- [1] 安部原也、伊藤誠、田中健次：「自動化システムにおける信頼感の推移：誤動作発生パターンへの依存性」計測自動制御学会論文集, Vol.36, No.12, pp. 1138-1144 (2000).
- [2] Argyris, C., Schon D. A.: "Organizational learning II," Addison-wesley (1996).
- [3] Bignell V., Fortune J.: "Understanding Systems Failures," Manchester University Press (1984).
- [4] Chalmers A. F.: "What is this thing called Science?", 3rd ed., Open University Press, Buckingham (1999).
- [5] 原子力安全委員会：「ウラン加工工場臨界事故調査委員会報告」(1999).
- [6] Inagaki, T.: "Interdependence between Safety Control Strategy and Multiple-Sensor Schemes via Dempster-Shafer Theory", IEEE Trans. Reliability, R40-2, pp. 182-188 (1991).
- [7] Inoue K., Kohda T., Kumamoto H. and Takami I.: "Optimal Structure of Sensor Systems with Two Failure Modes", IEEE Trans. Reliability, R31-1, pp. 119-120 (1982).
- [8] Klir, G. J., Folger T. A.: "Fuzzy sets, Uncertainty,

- and Information," Prentice-Hall, New Jersey, (1988).
- [9] 宮村鑑夫:「PL制度と製品安全技術」, 朝倉出版 (1995).
- [10] 向殿政男:「国際化時代の機械システム安全技術」日刊工業新聞社 (2000).
- [11] Reason, J.: "Managing the Risks of Organizational Accidents", Ashgates(1997) (「組織事故」, 塩見監訳, 日科技連).
- [12] 鈴木和幸, 田中健次, 伊藤誠:「品質危機とヒューマンファクター -未然防止への基本的考え方-」, 品質管理誌, Vol. 52, No. 9, pp. 812-824 (2001).
- [13] 田中健次:「ユーザーインターフェイスによる安全な製品の原理・原則」, 日本品質管理学会誌, Vol.28, No.3, pp.237-245 (1998).
- [14] Tanaka K.: "Dempster-Shafer Theoretical Modeling for Reliable Monitoring Design under Uncertainty," Proc. of 4th International Conference on Probabilistic Safety Assessment and Management (PSAM-IV) pp.187-192 (1998).
- [15] 田中健次, 伊藤誠, 後藤慎也:「状態判定の誤りへの時間制約による影響 -スキルベースとルールベースの場合-」, 第29回信頼性・安全性シンポジウム, 日本科学技術連盟/日本信頼性学会 pp.263-268 (1999).
- [16] Tanaka K, Klir G. J.: "A Design Condition for Incorporating Human Judgement Into Monitoring Systems," Reliability Engineering and System Safety, Vol.65, pp.251-258 (1999).
- [17] Tanaka K., Itoh M., Iguchi W.: "Heterogeneous Sensors System Design for Prevention of Model-Induced Failures", Proc. of 5th Int. Conference on Probabilistic Safety Assessment and Management (PSAM-V), pp.175-180 (2000).
- [18] Tanaka K.: "Management Learning for Prevention of Organizational Accidents", Proc. of 4th Int. Quality Management and Organisational Development Conference (QMOD), Linkopings, pp.159-168 (2001).
- [19] Tanaka K., Itoh M.: "Judgement of Gray Zone in Safety Monitoring System -Automatic mode vs. Humanly Mode-", Proc. of 8th IFAC/IFIP/IFORS/IEA Symposium on Analysis, Design, and Evaluation of Human-Machine Systems, Kassel, pp.257-262 (2001).
- [20] 事故調査検討会:「帝都高速度交通営団日比谷線中目黒駅構内列車脱線衝突事故に関する-調査報告書」(2000).
- (2002年7月29日 受付)
(2002年11月26日 採録)
- [問い合わせ先]
〒182-8585 調布市調布ヶ丘1-5-1
電気通信大学大学院情報システム学研究科
田中 健次
TEL: 0424-43-5661
FAX: 0424-43-5682
E-mail: tanaka@is.uec.ac.jp

著者紹介

田中 健次 [非会員]

1982年京都大学理学部数理学系卒業, 東京工業大学大学院システム科学専攻博士課程修了後, 茨城大学工学部助手を経て, 現在電気通信大学大学院情報システム学研究科助教授, 筑波大学先端学際領域研究センター客員研究員を兼任。システム安全学、ヒューマンマシンシステムの信頼性・保全性、不確実性下の意思決定、事故情報システムなどの研究に従事。PM優秀論文賞、日本設備管理学会論文賞受賞。IEEE-SMC, SICE, JSQCなどの会員、理学博士。

Dealing with and Utilizing Gray Zone between Safety and Danger

by

Kenji TANAKA

Abstract :

Organizational accidents have occurred repeatedly in Japan over the past several years. Most of these accidents seem to have been occurred within a gray zone between the safety zone and the danger zone rather than within the danger zone. The present paper considers "risk engineering" as engineering for preventing such accidents that occur within the gray zone, and proposes a framework for analyzing design methods of reducing the gray zone. Firstly, it asserts that safety management design should be classified into a safety-assurance design, and a danger-avoidance

design and, that the danger-avoidance design method should incorporate two types of learning mechanism. Next, our paper shows two positive examples utilizing a gray zone for reducing risk; one is a description method for operation manual or rules, and the other is a reliable safety monitoring design method.

Keywords: gray zone, safety design organizational learning, incident, reporting system, safety monitoring system

Contact Address : **Kenji TANAKA**

Graduate School of Information Systems

University of Electro-Communications

1-5-1 Chofugaoka, Chofu-shi, Tokyo, 182-8585 JAPAN

TEL : 0424-43-5661

FAX : 0424-43-5682

E-mail : tanaka@is.uec.ac.jp