SE Report

リスクが極めて高いシステムに対する安全設計思想について

― 原子力発電に対する一考察 ―

明治大学理工学部 情報科学科 教授

向殿 政男 *Masao Mukaidono*

1. はじめに

極めてまれにしか起きないが、いったん発生すると被害の規模がとてつもなく大きな災害や事故に対して、われわれはどのように対応すべきなのであろうか。今回の東日本大震災、大津波、そして福島第一原発という三重災害は、この問題を深く私たちに突きつけた。今回の大地震による津波によって、死者や行方不明者が二万人に及ぶという圧倒的な規模の被害からすると稀に見る大災害であった。一方、原発事故では、確かに直接の死者は一人も出ていないかもしれないが、その被害たるものは甚大であった。放射性物質は日

図1　福島第一原発事故
（3号機の水素爆発）

（インターネットより引用）

本はもとより世界中に拡散した（**図1**）。低濃度の放射線被害がどのようなものであるかという科学的な根拠が不明確な中で、日常の食品などに放射能被害が広がり、農産物に大きな影響が出て、ひいては風評被害をもたらしてわが国の産業を直撃し、民衆をパニック状態に陥れた。さらに深刻なのは、福島県を中心に数十万の人達が強制的に避難、移動をさせられ、故郷を離れざるを得ない人々が多く出たことである。ストレスが原因で、特に病院や施設などの移転に伴い高齢者や体の弱い人々において、多くの関連死が報告されている。このように原子力発電事故の被害は、津波による直接的な死者とは質的に違った意味で、甚大なものがあった。

ここでは、今回の原子力発電の事故のように確率は極めて低いが、いったん発生すると甚大な被害を及ぼすような人工的なシステムに対する安全設計思想はどうあるべきかについて考えてみることにする。

2. システムにおける一般的な安全の確保の考え方

まず、人工的なシステムにおける一般的な安全の確保のステップを振り返ってみよう。**図2**に示すように、最初に設計段階で未然防止方策を施す。予防安全である。次の実際の

図2　安全確保のステップ

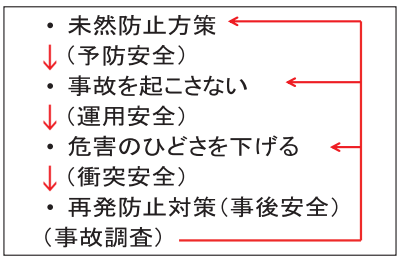
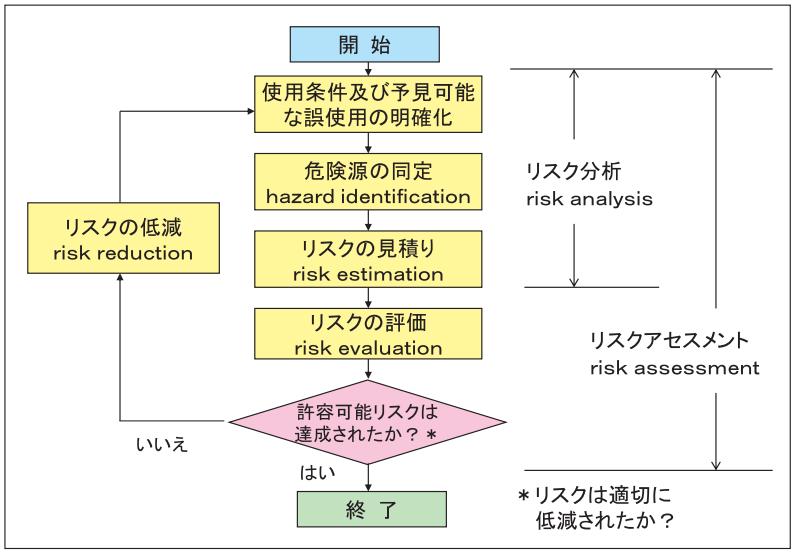


図3　リスクアセスメント（ISO/IESガイド51）



運用段階では、人間が注意をしながら、また保守点検や保全をしながら事故を起こさないように安全を確保する。運用安全と呼ぶことができよう。現実には、絶対安全はあり得ないので事故の可能性は常にある。実際に事故が発生した時には、危害のひどさを下げる、拡大を防ぐ、再稼働を早めるなどの対策を施す。自動車や交通機関などで言えば衝突安全である。その後、事故調査が行われ、原因を科学的、客観的な事実を背景や組織まで含めて明らかにして、再発防止策を提案して、各ステージにフィードバックをする。例えば、新しい安全設計基準などを設けて再度設計段階の予防安全から繰り返すことになる。

予防安全のステップにおける設計段階では、安全設計のバイブルと言われているISO/IECガイド51に示されているリスクアセスメントの考え方が基本となる（**図3**）。ここでは、使用条件を明確化すること、人間がやるだろう予見可能な誤使用も明確にすること、危険源（ハザード）を洗い出すこと、危害の頻度とひどさからリスクの大きさを見積もり・評価すること、リスクが許容可能か否かを判定すること、および許容可能でない場合にはリスクを低減することなどが重要なステップとなっている。リスクの低減策に関しては、重要な概念として、同じくISO/IECガイド51にスリーステップメソッドが示されている（**図4**）。まず本質的安全設計、すなわち、最初から危険源がないように事故が起きてもそのひどさは小さくなるように、人間が関与する機会をなるべく少なくするように、本質的に安全を確保する設計とする。しかし、現実にはそれだけでリスクをなくすことはできないので、残るリスクに対して付加的に安全装置などを含めた安全防護対策行う。これでも決してリスクはゼロにはならない。最後の手段として、残った残留リスクを使用上の情報として提示して、作業者に安全の確保を委ねる、というステップである。ここまでは、設計者側の役割で、残ったリスクに対しては注意、訓練、管理などを通して安全を確保する作業者の役割となる。

図4　スリーステップメソッド

（1）本質的安全設計によるリスクの低減
（2）安全防護対策（安全装置等）による
リスクの低減
（3）使用上の情報の提供による
リスクの低減
↑設計製造側の役割　↓利用者・作業者の役割
＊訓練、個人防具、組織・体制・
管理によるリスクの低減

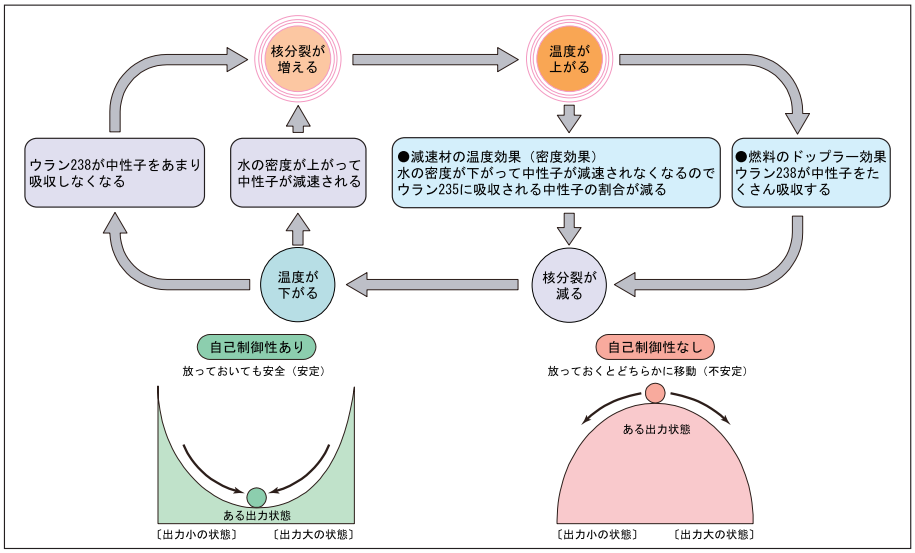
3. リスクが極めて高いシステムに対する安全設計思想について

図2のステップでは、未然防止からスタートしているが、現実には事故を経験して再発防止のステップから始まる事例が多い。事故から学ぶ考え方である。しかし、今回の原発事故のように被害が甚大であるような場合に、事故から学ぶにしては、あまりに悲劇的すぎる。再発防止よりは未然防止を徹底すべきであることは間違いない。

リスクとは、その定義にあるように[1)]、危害の頻度(確率)と危害のひどさの組み合わせであるが、組み合わせを乗算や加算などの計算で定める場合には、被害が甚大である場合であっても頻度が極めて小さい場合には、被害は小さいがよく発生する事故と同じリスクになる可能性があり、許容可能と判断されることがあり得る。ここに頻度とひどさかのどちらを優先させるべきかという価値観の話は入ってくる。危害のひどさを優先して、余りに被害が大きすぎる場合には、頻度がいくら低くても認めないという立場があり得る。頻度は確率で評価され、確率は不確定さを含み、いくら小さくても明日起きるかもしれないからである。一方、リスクの高いものに挑戦することで科学技術は発展して来たし、どんなシステムでもリスクはゼロにはならない。利便性を受けているシステムにリスクが存在するのは当然である。われわれは事故に学びながら進歩を続けて現在の便利で豊かな社会を築いてきた。便益を受けるためにはある程度のリスクは覚悟すべきである。歴史的に考えれば、医学がそうであり、列車がそうであり、飛行機がそうであり、有人宇宙飛行がそうである等等という事実がある。現在、われわれが有している人工のシステムで、いったん事故が起きると最も大きな被害を出すものの典型が現在の形の原子力発電であろう。多重防護の考え方で悲劇的な被害が発生する確率が極めて小さくなっているから安全であるという理由で許容され、各国で稼働し、わが国でもエネルギー問題の解決策、従って産業活動の維持の基本として、原子力発電の稼働が認められて来た(しかし、現実には、原子力発電が稼働して約60年、その間にわれわれは3回のシビアアクシデントを経験しているので、稼働台数を考慮しても過去のデータからは決して確率が極めて小さいとは言えない)。

確率は極めて小さいが、いったん発生すると甚大な被害を及ぼすような人工的なシステムに対してどう考えるべきだろうか。そのためには、まず、信頼性と安全性の違いを明確にしておく必要がある。信頼性は、果たすべき機能をいかに保ち続けるかを問い、安全性は機能が果たせなくなった時にも人命などに危害を及ぼさないようにすることを問う。一般に信頼性が上がれば安全性は上がると考えてよいが、安全性を高めるために信頼性を下げる(安全が確保されなければ稼働させない)ことがあり得るので、両者は実は異なった概念である。安全を確保するためには二つのアプローチがある。一つは、本来の機能を果たせなくなったら安全側に固定する構造を組み込んでおくものであり、ほかの一つは信頼性を高めることで安全性を確保するものである。前者は確定論的、または構造的アプローチ、後者は確率論的なアプローチと呼ばれている。例えば、列車は故障などが生じて本来の機能を果たせなくなった場合には止めることにより安全を確保することができる。前者の確定論的に安全を確保している。一方、飛んでいる飛行機は、飛ぶという本来の機能を果たせなくなったら落ちるしかない、すなわち安全側に固定することはできない。従って、飛んでいる飛行機の安全性は、いかに飛行を続行するかという本来の機能を維持し続ける

図5　原子炉の固有安全

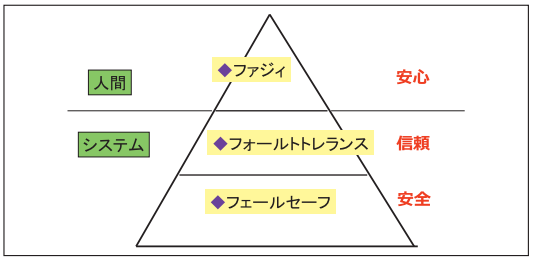


（出典：原子力・エネルギー図面表2011）

後者の信頼性のアプローチとなる。前者の典型的な安全設計思想がフェールセーフ（故障しても安全）であり、後者のそれはフォールトトレランス（多重系、冗長系による高信頼化）である。

原子力発電はどのような安全設計思想に基づいているのであろうか。電源が喪失したら制御棒が重力で落下して核分裂が止まる構造（沸騰型ではこの構造は採用されていない）、核分裂が暴走してもある安定した状態になり決して原子力爆弾にはならないという固有安全の構造など（**図5**）、多くの場面で構造安全の機構は組み込まれている。しかし、今回の事故の真の原因となった長期の全電源喪失からは必然的にメルトダウンに至る。従って、現在の形の原子力発電は、フェールセーフになっていない。いかに長期的な全電源喪失をさせないかという信頼性に頼った安全なのである。確定論的な安全性に基づいたフェールセーフな原子力発電はあり得ないのだろうか。このことを考える前に、リスクが極めて大きなシステムに対する安全設計思想の一つを紹介しよう。**図6**は、筆者が提案しているトリプルF（F^3）システムの考え方である。まず基本は、フェールセーフの構造を組み込んでおき、どうしようもなくなったら安全側に

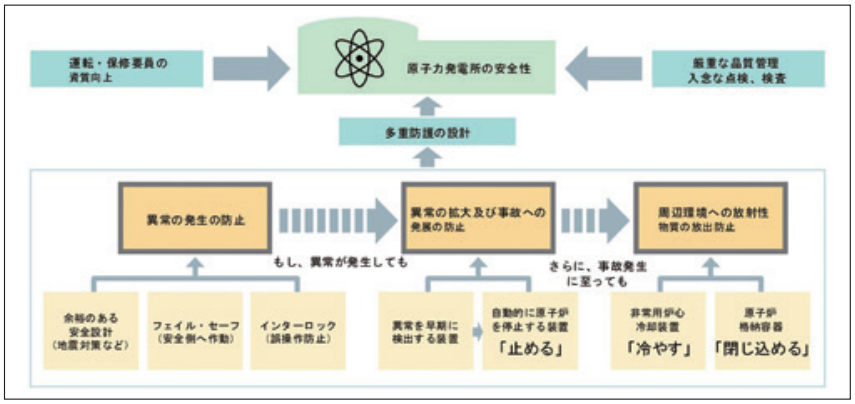
図6　トリプルF（F^3）システム



止まって固定する構造とする。その上で、頻繁に故障などで安全側に止まってしまっては不便なので、本来の機能を果たすべく信頼性高く稼働し続けるようにする。これはフォールトトレランスの概念に基づく信頼性で確保である。ここまでが利用者や作業者には見えなくてもよいインフラの部分である。人間に接する部分は、ファジィの精神で持って設計する。すなわち、ある程度のあいまいさを許し、人間にとって分かりやすく柔軟で、少しぐらいの誤りを許し、たとえ人間が間違えても大丈夫なようにフールプルーフな構造とするものである。ここは人間の安心につながる部分である。

F^3システムの考え方に近いのは鉄道であろう。列車は安全が確認できない場合には止まることによって安全を確保する。信号機や踏切などの故障はフェールセーフの考え方に従い安全側に固定される。この構造が構築さ

図7　原子炉における安全確保のしくみ



（出典：原子力・エネルギー図面表2011）

れている条件の上で、高信頼部品や多重系の使用、および保全活動などで信頼性高く稼働し、スケジュール通りに運用される。人間との接点では、例えば、ドアがすべて閉じないのに誤って運転手が発車命令を出しても列車は動かないし、乗客が挟まれないようにホームドアが設置されている。現実には人身事故が起きているのは、これらのシステムが完全でないためである。

さて、原子力発電の安全ではどうであろうか。前述したように、現在の原子力発電では、長期の全電源喪失が起こると必然的にメルトダウンが生ずる。実際には長期の全電源喪失が起こらないように多重系で、すなわちフォールトトレランスの考え方、信頼性に基づいて安全が確保されている。この場合のリスクは、危害が起る確率（長期の全電源喪失が起こる確率）とその危害のひどさ（メルトダウンから引き起こされる被害、現実には今回の悲惨な原発事故の被害）との組み合わせであり、われわれはこのリスクを許容するか否かで原発の存在を認めるか否かが判断されることになる。従って、原発が安全であると判断されるためには、このリスクをいかに下げるかにかかっている。原発の設計者にとって最も重要な点は、長期の全電源喪失の発生する確率をいかに下げるかである。今回の事故は津波がきっかけであったが、いくら防潮堤を高くしてもそれを超える津波が来ないという保証はない。コスト、利便性、管理費、景観などを考えると、防潮堤をいたずらに高くするのは考えものである。津波は来ると仮定して長期の全電源喪失の可能性を下げる方に努力を傾注すべきである。長期の全電源喪失を引き起こすきっかけは何も津波だけではない。隕石の落下もあるだろうし、旅客機の墜落もあるだろうし、テロも考えられるだろう。現在の原子力発電の設計ではここに最も注意を払うべきなのであるが、国の原子力安全委員会の指針では、原発の設計に際して、「長期間にわたる全電源喪失を考慮する必要はない」と規定されているとのことである。安全設計の基本を忘れているとしか言いようがない。また、このリスクを下げるもう一つの方法は、被害のひどさを軽減することである。そのためには原発の運用者にとって最も重要な点は、事故が起きた後の対策を十分に準備しておくことである。事故は起きないとしてその対策をおろそかにしていたことは、安全運用の基本を無視しているとしか言いようがない。

現在の原子炉で事故が起きた時には、止める、冷やす、閉じ込めることを基本としており、このために電源が必須なのである（**図7**）。これは能動安全（能動的に働き掛けることで安全を確保する）と呼ばれ、信頼性に基づく安全の確保である。これに対して、もう一つの方法である構造に基づく安全によって原子力発電を設計するにはどうしたらよいだろう

か。それは、フェールセーフな原子力発電を考えることである。F^3システムの考え方に従い、どうしようもなくなった時には、止まる、冷える、閉じ込まることを基本とする受動安全(何もしなくても自動的に安全になる)と呼ばれる考え方を採用する。フェールセーフな原子力発電は可能であろうか。現在の原子力発電は、効率を重視するために極めて大型となり、かつ密集して設置されている。リスクが高まるのは必然である。長期の全電源喪失でメルトダウンが起きるのは余熱による燃料棒の溶解が原因である。例えば、簡単に言ってしまえば、燃料棒の余熱を賄うだけの水を用意し、その中で原子炉を稼働させ、事故が生じてどうしようもなくなった時にはそのままにしておけば、燃料棒の余熱は除去されるという構造が考えられる。これ以外にも、フェールセーフな原子炉の形態は考えられるであろう。これらの形態では、大きな原子炉はできないかもしれないが、効率よりも安全性を優先し、小型のものを作って分散して設置すべきである。なお、原子力発電に存在する大きなリスクには、この他にも原子炉からの高濃度放射性物質の拡散、高レベル放射性廃棄物の処理などもあるが、ここでは触れない。

4. あとがき

人工的なシステムの安全性は、一般的には安全基準に従い設計され、残されたリスクの大きさを開示し、それが許容可能か否かで判断されることを基本とする。今回の原子力発電の事故で、今まで対応していなかった危険源やリスクが明確になり(地震の大きさや津波の大きさ)、新しい安全基準を定めて対応すれば、これまで以上に安全性が高まることは明らかである。失敗に学ぶ再発防止の考え方である。しかし、現在の構造や考え方をそのままにして安全性を上げるというモグラたたき的対応の延長線上で、わが国の原子力発電がこれからも認められるだろうか。わが国や世界の民衆の価値観に依存する大きな今後の課題である

リスクは危害の発生確率と危害にひどさの組み合わせであるが、危害が極めて大きな場合には、前述したように発生頻度がいくら小さくてもそのリスクは認められないという考え方はあり得る。確率よりもひどさを優先するという価値観に基づくもので、確率的には極めて稀であるという意味で数値的には安全であっても、安心が得られないからである。安心は個人の、または社会の価値観に依存し、安全が実現されている構造が理解でき、安全を確保している人間、組織、機関を信頼することから醸成されるのだろう。フェールセーフに基づくアプローチは確定論に基づく考え方であり、リスクが極めて高いシステムに対する安全設計思想の一つの候補である。構造がよく理解でき、本質的に安全が確保されているので安心につながる。この際、原子力発電は安全の基本に戻り、安全確保の構造と論理に戻る必要があるだろう。原子力発電に関しては、わが国の技術力をフェールセーフな原子炉の開発に集中し、原子力発電の高度な安全性確保の技術の開発を通して、わが国は安全立国として世界に貢献して行くという選択枝もあり得て、それができないならば、地震や津波が多いわが国では、長期的には原発ゼロという選択枝もあり得るだろうということを提案したい。

参考文献

1) 向殿政男、北野大、他、安全学入門～安全の確立から安心へ～、研成社、2009

おかいどの●まさお

1970年明治大学大学院工学研究科博士課程修了。工学博士。同年明治大学工学部電気工学科専任講師、78年同大学工学部電子通信工学科教授、89年から同大学理工学部情報科学科教授。経済産業省 消費経済審議会委員(製品安全部会長)、国土交通省社会資本整備審議会委員(昇降機等事故調査部会長)。消費者庁参与、(公)私立大学情報教育協会会長。