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2回－
Lecture series of risk assessment methodologies for contemporary industrial systems No.2

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１回目では現代の産業リスクの定義と意味について述べた。今回はそのリスクをアセスメントする上での現代の産業システムの特徴について、歴史と実例を交えて解説する。

2．現代における大規模・複雑システム－人間と機械の共存

ナノテクノロジーのような極小の技術が進歩する一方で、航空機、発電システム、交通システム果ては社会システムまで、大規模化、複雑化している。大規模・複雑システムの特徴は、人間と機械が協調して目標を達成するシステムであり、例えば小さな人間のエラーや、機器の軽微な故障が進展して大きな災害に及ぶことである。アメリカスリーマイル島原子力発電所２号機の炉心の損傷事故、様々な航空機事故、国産ロケットの打ち上げ失敗等がある。この意味で、大規模・複雑系を語る際には、人間と機械の共存が問題となる。

従来は、安全達成のために、ハードウェアの信頼性向上に重点が置かれ、研究開発・適用が図られてきた。計装関係では専ら制御器やリレー等の信頼性向上が至上の課題であった。確かに異常状態になれば、自動系が作動して大規模・複雑系を緊急停止させるのは機械（自動システム）であり、安定した状態にプラントを制御するのは、従来は主として人間の役割であった。

さて近年、計算機技術の長足の進歩で、多くの産業分野で人間－機械系に計算機が導入され、人間－機械系での人間の役割は、従来の手動制御者としての役割から、計算機が自動制御する機械システムの状況を監視する監督者の役割（監督制御）に変遷した。[1]

このことは一面では機械システムから人間を疎外する方向に変化したと見なすこともできる。すなわち、「自動化のアイロニー」[2]という言葉で認知心理学者が警鐘を鳴らしたように、人間にとって機械システムがブラックボックス化して緊急時対応での技能低下を招き、これが種々の大事故の原因と指摘され、従来の「技術中心の自動化（Technology Centered Automation）」から最近は、「人間中心の自動化（Human Centered Automation）」への転換が主張されている。

航空機のコックピット、高速鉄道の運転席、発電所や化学プラントの中央制御室は、人間と機械がお互いの役割を分担する「共存空間」と考えられ、その中の人間を人間－機械系と言う全体システムの一要素としてとらえる必要がある。また、その共存空間には、人間と機械の間での情報のやりとりのための接点が必要である。これはヒューマン・マシン・インタフェースと呼ばれるが、人間と機械とでは情報の処理プロセスが異なるので、インタフェースでの情報表示のあり方が問題となる。とくに前述のスリーマイル島原子力発電所２号機事故以降、事故時の情報提示に様々な提案がされている。この詳細説明や設計方法は、しかるべき参考書に譲るとしても、インタフェースは人間－機械系の中で重要な要素であり、特に人間－機械の役割分担がしっかり決められないと実際に役立つものを設計することは困難である。人間－機械系では、人間と機械が共存するシステム全体としてのリスクアセスメントが、インタフェース設計にとどまらず、大規模・複雑系の全体設計の基礎となる。

そこでまず大規模・複雑系のリスクアセスメントの前提知識として、人間と機械のそれぞれの長短、自動化のレベルと自動化のもたらす諸問題への対策を解説する。人間と機械の能力の長所、短所を比較する代表例としてFittsのリストを表－１に示す。[3]

歴史上、18世紀後半の産業革命時代にさかのぼると、蒸気タービンのガバナー弁による回転数制御は自動化の端緒であった。これは蒸気機関の自動制御の強

◆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

力な「ツール」で、それまで人間がなしえなかったことが可能となり、人間の生産活動が一挙に拡大した。この例は表－１のうちの属性の速度、出力、堅実性、検知能力の点で人間には実施しにくいタスクである蒸気タービンの回転数制御を、機械が肩代わりするものであった。その後、Wienerらの提唱したサイバネティクス[4]により自動制御の手法は飛躍的な発展を遂げ、ディジタル計算機の登場で機械システムの自動制御化が長足の発展を遂げた。なお、プログラムを記憶可能な最初のディジタル計算機はアメリカで開発されたILLIACという真空管を無数に使用したもので、1952年９月１日に受け入れ試験が実施された。無数の真空管が使用されたので、その冷却と故障に悩まされ、このことを解決しようという努力が信頼性理論発展の礎となった。その後、計算機はトランジスタの登場によって真空管が置換され、それに続く集積回路技術の進歩によって益々小型化していった。その結果、実際にプロセス制御用の計算機が現れたのは、1960年代になってからである。いわゆる、プロセス制御用マイコン（マイクロコンピューター）DEC PDP－５が最初に市場に登場したのは1963年であった。

さて、ここでその後、このような計算機の登場により、人間と機械のタスク割り当て問題がどのように変遷してきたかを展望しておこう。

表－１　Fittsのリスト

属性	機械	人間
速度	非常に優れている.	比較的緩慢，秒単位で測定可能
出力	レベルの点でも一貫性の点でも非常に優れている.	比較的弱い．短時間全出力で約1500Wまで．持続時間が1時間を超えると150W未満．
堅実性	変化のない反復運動に理想的.	信頼性が低い．必ず習得してマンネリ化と疲労感を起こす.
情報処理能力	多重チャンネル処理が可能．速度Ｍbit/秒で伝送可能.	主に単一チャンネル．情報伝送速度は遅く，通常は10 bits/秒以下
記憶容量	逐次再生の場合は理想的．アクセスが限られ形式的.	原則や戦略の場合は，人間の方が適する．アクセスは融通性があり，創造的.
推論計算	十分に演繹的．プログラミング作成は困難であるが，推論計算は速く，的確．エラー補正能力は不十分	十分に帰納的．プログラミング再生が容易．推論計算は緩慢で不正確．エラー補正能力は十分
検知能力	専門的で範囲が比較的狭い．定量的評価は十分パターン評価能力は劣る	検知エネルギー範囲が広く，場合によっては多重機能を有する
異常時対応能力	情報源に文書と音声が混在する場合の対応能力が不十分．ノイズがある場合のメッセージ検出能力が不十分	情報源に文書と音声が混在する場合においても対応能力が十分にある．ノイズがある場合のメッセージ検出能力が機械同様，不十分

- （19世紀初頭－1970年代に盛んとなり現在でも産業基幹部分での採用が見られる）：人間機械系のタスクの割当てが考えられた第１段階では、技術的・経済的理由で機械に割当てることができないタスクを人間に残した。この段階での至上命題は与えられた目標を如何に早く、効果的に達成するかということであった。主要な関心は、機械の性能であって、人間は機械に付属するものととらえられる傾向があったと考えられる。発電所、航空分野、生産ラインにおいて、人間は効率向上（少しは安全性の向上について考えられたかも知れない）に、時として問題を起こすものの必要なものと見なされた。人間－機械系のタスク分配は、「機械とその弱点を所与とし、人間を使って機械の弱点を補わせ如何に効率的に仕事を進められるか」という点に専ら注意が向けられた。またそれに沿って「人間工学」が登場してきた時代である。
- （1970年代から提唱され始め、1980年代に盛んとなって現在に至る）：次の段階は、ある作業における人間機械系の効率に注意が払われた。ディジタル計算機が科学技術に欠かせないツールとなり、計算機との関わりが重要な要素になってきた。人間機械系におけるタスクの割り当ては、「人間と機械の相互作用（Human Computer Interaction: HCI）」として扱われ人間機械系のタスクの割り当ては、Fittsのリストに沿ってお互いの弱点を如何に補償するかに注意が向けられてタスク設計が行われた。このような展開は、基本的には産業基盤が個別の機械装置にディジタル計算機を組み込んで高機能化させる方向に移った時代である。
- （1982年に提唱され、現在に至る）：昨今の高度情報技術の発展は目覚ましい。その結果、単なる計算の道具に過ぎなかった計算機が「知能化」してきた。現在、知能化した計算機が、航空機、プロセス制御の重要な要素となっている。そこでは、人間と機械の間に一定の境界線を設けてタスク配分を設計するよりも、寧ろ、共通の目標を達成する人間と機械の結合系（Human Machine Joint System）として捉える方向に発展している。HCIの負の側面に注目して、それを軽減する方向で、その効率あるいは容易さを改善するのではなく、HCIの両者間のコミュニケーションで新たな機能を発現させることで、この結合系が一体となって設計目標を達成することを問題とする。いわばHCIの正の側面に注目する。制御の維持は、効率向上と生産の継続に常に必要であ

る。特に異常な状況（事故や緊急事態）の場合では、効率が安全達成に十分に寄与しなければならないので、状態を制御し、維持することが極めて重要である。この結合系にあっては、様々な人間－機械系の従来の縦割り的な考えにとらわれず、両者が協調して結合系がプロセス制御の維持という共通の目標を達成することを可能にする。このように知能化した計算機を活用し、HCIの正負の側面を総合的に考慮した「人間中心の自動化」を指向している。

人工知能分野で、「機械学習」や「知識発見」が注目されている現在、想定内のことであれば、機械が意思決定を行うことも可能となっている。人間はさらに、長期的、戦略的な意思決定を行うことが必要となってくるのであろう。従って、人間－機械系の各々の役割も日進月歩で変化していると言っても言い過ぎではない。しかし、実際の適用においては、原子力発電所の保守支援ロボットも放射線レベルの強いところに行き、人間の保守業務（タスク）を完全に代行する総合的なものは、実用化には至っていない。ハードウェアに限って言えば、2足歩行で、階段の昇降を人間のように移動したり、小走りができる一種のマニピュレータのプロトタイプが完成したというところであろう。

3．現代の自動化とリスク低減

人間機械系のタスク配分を機械の自動化のレベルという別の視点から見た提案がなされている。[5]機械がどこまで人間の代行をするかに注目して大略下記のように分類するものである。

レベル－1．機械（計算機）は何の支援もしない。人間が全てのタスクを処理する。

レベル－2．機械は採るべき別のタスクを適当な表示によりその意思を人間に伝える。

レベル－3．機械は採るべきタスクを選択し、意思を人間に伝える。

（ここまでは、機械は何の制御操作も行わない）

レベル－4．機械は人間の同意があれば、機械自身の行ったレベル－3の意思決定どおりに実行する。

（この場合、厳密には複数の提案が機械よりなされる）

レベル－5．機械は操作実行前に最終意思決定のために予め定められた時間を人間に与える、即ち与えられた時間に人間が意思決定を行わない場合、機械が提案した操作をそのまま実行する。

レベル4、5の相違は、意思決定権限の大きさがレベル－4では人間側が強いのに対し、レベル－5では明らかに機械側が強くなっている。レベル－4は英語で、“management by consent”と言い、レベル－5では、“management by exception”と言われる。これから明らかなように、医療で使われる“informed consent”という言葉の裏には、医者が複数の提案を行い、それを患者やその家族が選択するという意味がある。

（ここまでは人間－機械の合意のもとに機械が操作を行う）

レベル－6．機械は自動的に制御操作を実行するが、実行したことを全て人間に報告する。

レベル－7．機械は自動的に制御操作を実行するが、実行したことを人間に要請されれば報告する。

レベル－8．機械が意思決定を行い、制御操作を実行する。人間を無視する。

しかし、この方法は、大規模・複雑系全体として統一的にどのように自動化レベルを設定するのがふさわしいか、という問題に直接答えるものではないことに注意して欲しい。

そこで状況に応じて自動化レベルを変えるというアイデアも提唱されている。[6]このことを現実の原子力発電所に当てはめて考えてみよう。

原子力発電所ではタービン出力を一定に制御する自動化は従来から採用されてきた。この自動化はあるローカル制御の制御目標値を別のローカル制御の信号から採るというように総合化したもので、レベル－6に近いものである。又、最近では、起動・停止をプログラム制御によって自動で行うというプラントもある。これはレベル－4に近いものである。廃棄物処理や水処理の補機関連の自動化も同様である。

一方、事故時の運転については、原子力発電所は独特の設計思想を採用している。いわゆる「止める」、「冷やす」という機能的なタスクについて、基本的には人間のタスクの介入を「事故後一定の時間（日本では10分、ドイツでは30分）は期待しない」自動化設計としていることである。解釈によっては、レベル－8の自動化が行われていると考えることができる。「期待しない」ということは、「人間によるタスク介入」を禁止しているわけではない。しかし、スリーマイル島の事故では、「冷やす」機能を持った緊急炉心冷却装置の正しい自動動作に対して、運転員が状況の理解

を誤り、返って自動系に介入してそれを止めた結果、破局的な事故に至った。その後、機械による自動的な「止める」、「冷やす」の機能的なタスクに人間が介入することをかなり制限している。基本的には事故時には、人間も混乱しているであろうから、その間に人間がタスクを行うことを期待しないという姿勢である。

総じて計算機技術や、ソフトウェア、ハードウェアの信頼性向上の恩恵で、状況により影響を受けにくい定型的なタスクは自動化の方向にある。この場合、人間のタスクは機械（自動制御）を監視し、定められた範囲からプラントプロセスが逸脱した場合、機械にオーバライドして操作をすることが求められ、人間に課せられたタスクは自動系の動作監視バックアップである。

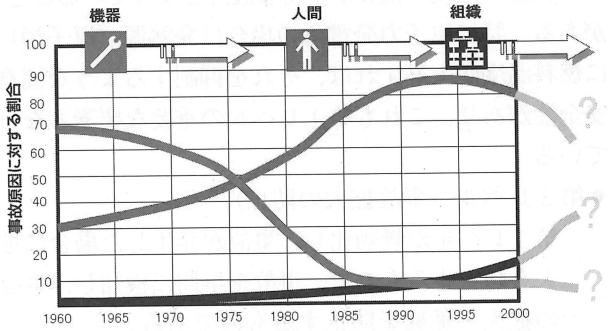
つまりプラントの個々の状況に応じて対処すべきプラント「機能」を確実に達成する上で機械（自動系）の信頼性に応じて、また人間サイドの信頼性に応じていずれかの自動化レベルにするという個別問題の設計の集積である。また自動系の機能喪失時のバックアップは人間に委ねられている。

航空機は、離陸、発進は、管制塔とパイロットの間で、ほぼ人間の技量（制御）で行われる。一旦、離陸して、着陸態勢に入るまで、オートパイロットのモードに入れば目的地まで何もなければ、ピッチ、ロール制御等は、人間に代わり完全に自動で行われる。ただし、一旦不具合が起こると人間が問題を同定し、機体を安定させなければならない。様々な指示系、CRTからの情報を咀嚼し、状況を把握する必要がある。高速鉄道にしても大型船舶にしても同じである。

破局的な災害事象に至るリスクは、（機械に起因するリスク）＋（人間に起因するリスク）と単純に考えそうであるが、実際にはそう簡単ではない。両者は複雑に絡み合っている。それらを的確に評価できるのが、PRAのフレームワークの大きな特徴であり、多くの産業分野の産業リスクアセスメントに適用可能な理由である。プロセス計算機の故障率、MTBFやソフトウェアで生ずるエラーについてのオーソライズされたデータベースは現在未だ存在しないが、もし計算機関係の故障率データベースが整備された場合には、多くの産業で直面している災害リスクを最小化する自動化のレベルを、PRAを適用して評価できる可能性がある。さらにそれに要するコスト等を勘案しての意思決定も可能となる。

最近の技術革新に伴うハードウェア信頼性の改善は著しい。原子力発電所も80年代から、安定運転時のハードウェア単体による事故件数は激減している。航空機と同じように、起動・停止時に事故が集中している。さらに最近では、世界の産業災害の原因の変遷を見ると、図－１に示すように一連の日本国内の電力の不祥事や災害のように組織の脆弱性が事故に発展するケースも世界的に増えている。

人類は信頼性理論や厳正な品質管理方法を確立し、ハードウェアの信頼性向上に徹底的に取り組んできた。それにも拘わらず、産業災害の件数は著しく減少したものの、オフセットは残り、これを現在のところ、様々な試みにも拘わらず減少することができない。このオフセットを生じさせている事故を子細に観察してみると。人間の状況認識の失敗や、人間－機械間での意思疎通の不具合が大きな原因の要素となっていることに気づく。従って、リスク低減の方法も、従来の信頼性理論で得られている方法以上に人間のエラー予測とその対策、人間の認知ミスを防ぐ方策、人間－機械間のインタフェース改善に向けられるべきであろう。



図－１　産業災害原因の変遷 [7]

4. 原子力発電所における安全思想

大規模・複雑系において、原子力発電所は「管理されない放射能が環境に放出されることを防ぐ」ということが社会から要求され、防止策が初期の段階から設計に盛り込まれてきた。他の産業分野でも破局的な災害を防止するための方策は講じられているものの、原子力の災害防止のための設計思想は体系立っており、分かりやすいので、ここで紹介しておく。原子力の「深層防御（defense in depth）」と呼ばれる、いわゆる安全設計思想がそうであり、その思想の概略は次の通りである。

- 第１レベル（余裕をもった設計、入念な点検による故障／破損の防止、厳しい品質保証（事故の発生防止）

これらを保証するための方策としては、

・余裕を持たせた設計とすること－例えば設計で評価した最大内圧が、X(Pa) とした場合、1以上の係数 k をかけた値、$k \cdot x$(Pa) を最大耐圧として設計を行う

・誤操作、誤動作を防止する設計－フェールセーフ、フールプルーフ設計（fail safe, fool proof）と呼ばれ、前者は安全維持に関わる機器の駆動電源、制御電源や制御空気等が喪失した場合に、プラント全体がより安全な状態となるように機器機構を設計しておくことを言う。空気弁、電動弁等では、fail safe, fail open, fail as is（電源、空気喪失時自動的に閉止、開放、直前の状態を維持）を言う。後者は人間がエラーを犯した場合、プラント全体がより安全な状態となるように機器機構を設計しておくことを言う。

・システムが多重性、多様性を有しており、各々が独立・分離されていること。

・機器の点検・検査が容易な設計となっていること。

がある。特に原子力発電所の場合は発熱源（原子炉）に燃料温度が上昇すれば、それを抑制するような固有安全性があり、これも第1レベルの重要な要素となっている。

●第2レベル（事故拡大の防止）

・第1レベルが無効化し、事故が発生した場合に拡大を防止するもので、事故を早期に検知し、事故の拡大・進展を防止するものである。

・安全保持に必要なパラメータが異常な値を示した場合、原子炉に制御棒を全部挿入して、原子炉を停止する原子炉保護系や、原子炉の空炊きを防止する緊急炉心冷却装置（ECCS：emergency core cooling system）は第2レベルのシステムに該当する。

●第3レベル（事故影響の緩和）

・第2レベルでも事故が収束しない場合に第3レベルに移行する。原子力発電所の場合は、旧ソ連のチェルノブィル原子力発電所のように大量の放射能を環境に放出し、環境を汚染するのが、想定する最悪の事故であるが、加圧水型原子力発電所（PWR）の場合、その放射能の最終の閉じこめの防壁である格納容器を中にある主要機器の健全性をも犠牲にして守る「格納容器スプレー系（格納容器圧力低減系）」が第3レベルに該当する。格納容器の内圧を下げるために、水酸化ナトリウムを含んだ水を格納容器上部からスプレーする。これにより格納容器に充満した水蒸気を凝結させ、内圧を下げると共に、ヨウ素131（呼吸等により体内に取り込まれると甲状腺に沈着し、ガンを誘発することが知られている）を除去する。

・さらに原子力発電所の建設にあたっては、人口密集地域から十分な距離を取ることを設計段階で考慮する。

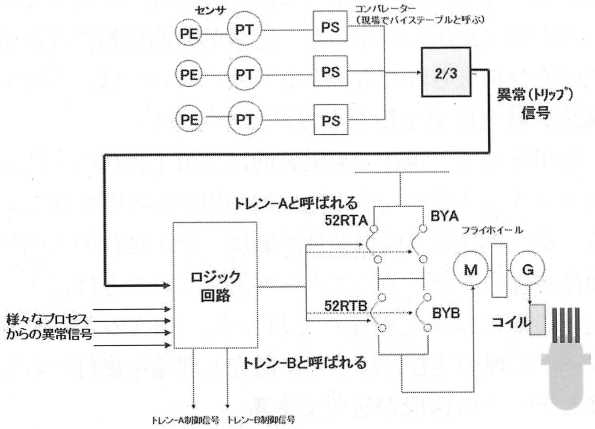
一般に公衆向きには、燃料は安定にペレット化され、さらに燃料ペレットは被覆管で覆われ、それを覆うのが原子炉、原子炉は格納容器で覆われているという多重の物理障壁により、原子力発電所の安全は担保されていると説明されているが、原子力発電所の安全思想の基本は「深層防御」である。

この安全思想は他の産業でも適用されている。原子力発電所のように明確には謳っていないが、航空機産業でも、第1レベルは十分に配慮されている。第2レベルは、様々な警報システム、激突防止のための自動化システムで守られている。第3レベルは、明確にはされていないが、どのような努力によっても墜落が避けられない場合は、家屋の殆ど見あたらない場所に、パイロットは出来るだけソフトランデイングで胴体着陸を試みるであろう。

5. ハードウエアにおける信頼性理論からのリスク低減

前章の具体的な説明を行っておこう。原子力発電所の制御システムでの、安全設計の第1レベルの典型例である原子炉保護系の簡単なダイヤグラムを図－2に示す。多様性、多重性、独立性を持たせ、第1レベルが無効になるリスクを低減するような工夫を盛り込んだ設計としている。

このような緊急停止系に一般的に求められるのは、緊急デマンド信号が出た時に原子炉を確実に停止することが必要であり、それに失敗する確率、即ち不動作率（非保護率とも言う）を出来るだけ小さくすることである。逆にデマンド信号が出ていないときに誤動作で緊急停止する確率も考え得る。これを誤動作率というが、原子力発電所ではfail safe設計を採用しているので、これは安全上、問題とされない。しかしながら、商用炉の場合、商業活動も考慮に入れなければならないので、実際には、両者をトレードオフして設計が行われる場合もある。



図－2　原子力発電所の原子炉保護系のブロック図

ここで、図－2のブロック図について簡単に説明を行っておく。これは加圧水型原子炉の場合で、日本の原子力のもう一つの主要な炉型の沸騰水型については割愛するが設計の原理は同じである。図中、PEと書いてあるのは、圧力の検出器（センサ）で、センサー信号は伝送には向かない変位信号、圧力偏差信号等であるので、PT、即ち圧力発信器（pressure transmitter）でこれを電気的信号に変換する。この電気信号を比較器（コンパレータ）の入力とし、ある設定圧力を上回るか下回った時に、異常を1として出力する。この1チャンネル分だけでは、不動作の信頼性として低いので、一般に原子力発電所の原子炉保護系を含めた主要安全計装系では、「多数決原理」を採用している。本例では、2-out-of-3のロジックを採用している。これは、3チャンネルの内、2チャンネルに異常1の信号が立った場合、出力を1とするものである。これらの状態プロセス信号は、ロジック回路の入力となる。ここでは、例えば、状態パラメータXとYのANDで原子炉の異常という論理が設計されている場合、パラメータXの多数決論理回路が1でかつパラメータYの多数決論理が1の場合、緊急停止信号1を出す。

ロジック回路の出口でも信号は多重化、独立化されている。原子炉を緊急停止するための制御棒は機械的な爪で溝を掘った制御棒で電磁石によりグリップされている。緊急停止の場合には、この電磁石での電源を切断することにより、制御棒を重力落下により炉心に挿入させて、核反応を停止する。これを原子炉トリップ遮断器と呼んでいる。図中、52RTA、Bと記してあるのが、原子炉トリップ遮断器である。これは多重化されており、独立した信号（上記信号回路をチャンネルと呼んだが、制御回路の場合は、トレンと呼ばれる－正確にはtrainでトレインと発音するが、発電現場ではトレンと呼ばれている）トレンA、Bの内1つでもトリップ遮断器が開くと原子炉は緊急停止する。各々の制御回路、トレンは電気的に独立であり、供給電源も別となっている。このように独立・分離性により、不動作によって、原子炉に悪影響が及ぶ確率を最小にしている。このように上記の原子炉保護系の他、ECCS等安全維持に関わる制御システムは、基本的にこのような、多重冗長入力、出力の設計となっている。

この中で、バイパスの遮断器BYA、BYBは、定期的な遮断テスト時に使用するものであり、図中M（モーター）、フライホィール、G（発電機）から成立したシステムは電源が瞬間的に落ちても制御棒が落ちないようにするものである。厳密には、これは原子炉の安全保持に関わるものではなく、前述のように誤動作を防ぐものである。

このようなハードウェア上の設計は他の産業でも見られ、実際、このような多重化、独立化された保護システムの信頼性は高く、不動作率も極めて小さい。しかしながら、安全を求められる産業にも災害は起こっている。これは、前節でも言及したように、複雑・大規模系では、人間と機械が共存しており、主に人間のエラーや規定からの逸脱行為が原因の発端となり、災害に至るケースは現在、ニュースで報じられている通り多い。リスクアセスメントにおいて、人間を原因とするリスクアセスメントの方法論の重要性は、現在さらに増している。

6．人間行動の大規模・複雑系の影響評価

ここまで解説を進めてきたように、大規模・複雑系で引き起こされる災害のリスクアセスメントを行うには、設備のアセスメントに加えて人間の行動（パフォーマンス）評価が欠かせない。従来の信頼性理論の適用の範囲外でもあるし、又、心理学等でも適用可能な成果は見あたらなかった。アメリカ、スリーマイル島の事故では、いわば「人災」に近い事故であったため、フォールトツリーを中心とした信頼性評価から大幅な拡張が行われ、人間の行動信頼性に関わるデータベースも、PRAというフレームワークの下に膨大なコス

ト、マンパワーがつぎ込まれ整備された。

大きな災害も元を正せば、少しのプロセス偏差であったり、一寸した操作の誤りであることが多い。PRAはそれら機械の故障、人為的ミスがどんどん重なって災害に至るような事象をモデルで表現し、秤量することのできる総合的な評価フレームワークである。PRAでは、前章で述べた機械（設備）の信頼性評価と同じ粒度で人間の行動信頼性を評価できる。機器故障率に加えて、人間の過誤率の膨大なデータベースも整備されている。

ただ、PRAで採用されるべき人間信頼性のモデルは、機械の信頼性評価のように客観的に一意に決まるものではない。非常に多くのモデルが今まで提唱されてきたし、今でも第2世代の人間信頼性評価と称して、定量化の方法が提案されており、議論が絶えない状況である。

実際にPRAに現在適用されているモデル（これを第1世代の人間信頼性評価と呼ぶ）は「構造モデル」と「主観モデル」に大きく分けられる。「構造モデル」は、人間の操作や行動に構造（モデル）を仮定し、行動失敗（基本的な動作の人間過誤率）のデータベースを参照可能なように関連付ける方法である。「主観モデル」はエキスパートの経験から人間の信頼性を求める方法である。「主観モデル」は、アメリカの原子力規制局で、エキスパートの意見は正しいとの見解から、一時適用が推奨されたが、PRAにおける適用例は寡少にとどまっている。

前者については、「タスク型」解析と「イベント型」解析に大別できる。「タスク型」解析はフォールトツリーの考えに類似して、人間の過誤率のデータベース参照が可能なレベルまでに人間の操作を分解していく方法である。「イベント型」解析は、主に人間の操作に要する時間で人間の信頼性を決定しようというものである。J.Rasmussenの提唱した人間の行動形態－スキルベース、ルールベース、知識ベース[8]を考慮にいれることのできるモデルも提唱されている。さらに例えば、操作時に周囲が暗いとか暑いとか、インタフェースが良好であるかの環境条件を勘案するため、性能形成因子（PSF：Performance Shaping Factor）と称する一種の補正係数をタスク個々の基準の人間過誤率に掛けて補正するという考えを採っている。

第2世代の人間信頼性評価は、この補正係数こそ、人間行動の信頼性の帰趨を決定するものであるとの主張に基づくものだが、未だにPRAでの扱いに対する統一的な考えが出ていないし、定量的人間信頼性評価手法が充分検証されたものかどうかについては、今後の議論や研究成果を待たなければならない。

結果として、現在でも実質的には第1世代の方法がスタンダードとして、PRAでは実際に適用されている。第2世代の人間信頼性評価は、第1世代の人間信頼性評価のモデル上の欠点を解決しているとは言え、実証段階には未だ到達しておらず、PRAのフレームワークに埋め込むにはさらに研究と理論を裏付ける実験とデータの採取が必要である。

7. 結び

第2回目の連載では、現代産業システムの特徴とその中に潜むリスク、現在採られている低減の方策について解説した。次回では連載のまとめとして、実際にどのように現代の産業システムのリスクアセスメントを行うかについて概要を解説する。

参考文献

[1]H. Kragt, "Operator tasks and annunciator systems", Eindhoven, Holland, Eindhoven University of Technology (1983).

[2]. L.Bainbridge, "The Ironies of Automation", The Psychologist: Bulletin of the British Psychological Society, 3, 107-108. (1987).

[3]P. Fitts, (Ed), "Human engineering for an effective air navigation and traffic-control system". Ohio State University Research Foundation. (1951).

[4]N. Wiener, "The human use of human beings". Houghton-Mifflin. (1954).

[5]T. B. Sheridan, Supervisory control, Dept of Mechanical Engineering, MIT (1982).

[6]Y. Niwa at al., "Autonomous recovery execution in nuclear power plant by the agent, Cognition, Technology and Work, Springer-London 1 (4) (2000).

[7] E. Hollnagel、横浜国立大学 安心・安全の科学研究教育センター第3回公開セミナー予稿(2006).

[8]J. Rasmussen & M. Lind, Coping with complexity (RISO-M-2293), Riso National Laboratory (1981).

（平成18年2月9日）