[解説]

事故とエラーのモデルに基づく安全・セキュリティのための個人及び組織の在り方

Requirement on Personnel and Organization for Safety and Security Improvement by Accident and Error Model

キヤノングローバル戦略研究所　　氏　田　博　士
Canon Institute for Global Studies　　Hiroshi UJITA

要　旨

巨大複雑システムにおいて、技術の巨大化・複雑化と高度化に伴い、安全・セキュリティ問題がハードウェアから人間そして組織の問題へと、次第に社会化する現象があらゆる技術分野で発生している。これに伴い、事故やエラーの形態や社会的な受け止め方、またその分析方法も時代とともに変化している。当初はドミノ事故モデルとヒューマンエラー、次いでスイスチーズ事故モデルとシステムエラー、そして最近のとらえ方は組織事故と安全文化の劣化、である。これらの事故の分析から安全を議論する方向に対し、新たな動向として、様々な事象の良好事例に着目して分析するレジリエンス・エンジニアリング、高信頼性組織、リスクリテラシーなどの研究手法も盛んとなりつつある。また、情報セキュリティ分野を中心に、人間の持つ本質的な弱さを利用してその人をある行動へと誘導する方法とその対策を検討するソーシャル・エンジニアリングも最近の研究テーマとして検討が始まった。

キーワード

事故モデル、人的・組織的要因、レジリエンス・エンジニアリング、ソーシャル・エンジニアリング

1.　まえがき

巨大複雑システムにおいて、技術の巨大化・複雑化と高度化に伴い、安全・セキュリティ問題がハードウェアから人間そして組織の問題へと、次第に社会化する現象があらゆる技術分野で発生している。安全･セキュリティの達成のために､人々の価値観・倫理観や行動様式(安全文化)だけでなく、社会的受容や事故への社会・環境への影響も、考慮することが不可欠になりつつある。その一方、リスクを含まない科学技術はないが、リスクを上回る効用があるからこれまで受け入れられてきたことも事実である[1][2]。

プラントシステムが現代ほど複雑でなかった時代には、技術の欠陥が問題の発生源であり、技術的対応によって事故を防止できると考えられていた。システムがより複雑になるにつれて、それを操作する人間の能力限界に突き当たるようになり、ヒューマンエラーによる事故が起きるようになった。その典型が1979年にスリーマイル島（TMI）原子力発電所で起きた事故である。このため、エラーを犯す個人

が問題の発生源と考えられ、要員の適切な選抜と訓練によって要員の能力向上を図り、またインタフェース設計を適切に行うことがエラー防止に有効と考えられるようになった。

その後、技術、人間、社会、管理、組織などの要素の複雑な相互関係による事故が発生するようになり、次に問題となったのが社会と技術の相互作用である。更には、プラントや企業の内部だけでなく、外部の関係者や組織との関係不全が問題の発生源である事故が目立つようになり、組織間関係も含めた包括的問題解決の枠組みが必要になってきた。事故の形態が、複合要因により発生しその影響が社会的規模に至るいわゆる組織事故が最近の事故の特徴である。

1986年のチェルノブイリ原子力発電所の爆発・放射能汚染事故は、社会と技術の相互作用の時代に発生したものであるが、不全な組織間関係により安全文化が劣化するという特徴も備えた新しいタイプの事故の前兆である[3]。1999年に我が国で発生したJCO臨界事故は、組織事故の典型である。そしてこの2011年3月11日には、大規模天災が引き金とは言いながら、安全文化の劣化により事故の想定を誤り大規模な事故に至った福島第一原発事故は、日本の原子力の安全神話を根底から崩してしまった。

2.　人的･組織的要因の考慮

2.1 ヒューマンエラーとは何か

所謂オミッション、コミッションなどのヒューマンエラーの分類は存在するが、実はエラーであるか否かの判断は視点により大きく異なる。

a. 安全と品質保証と性能と経済性

安全と品質保証とはよく似ているように見えるが、必ずしも同じではない。品質保証とは、基本的には物の性能を良くすることであり、通常は性能が上がれば信頼性も安全性も上がるが、そうならない場合もある。信頼性には、システムの信頼性（常用系の信頼性）、システムが壊れた際のバックアップシステムの信頼性（安全系のアベイラビリティ）、システムを動かす人間の信頼性という3つが絡んでくるが、システム信頼性への影響は人間信頼性が最も大きい。

一般に、システムの信頼性について品質保証を実施しまた性能を上げれば、経済性も上がることから、多くの場合、企業はこの部分に傾注する。しかし、これに偏ると、安全性が弱くなってしまう恐れがある。事故を分析すると、品質保証が良いにもかかわらず、事故を起こしている例（例えば JCO 事故のように）が少なからず見受けられる。また今回の福島第一原発事故事例のように、経済性を重視すると、頻度は低いが一旦事故が起こればその影響が大きい事象、いわゆるレアイベントに対する備えが不十分となる可能性も否めない。

b. 刑法（ケア、性悪説、規範的人間像）と人間工学（アテンション、性善説、もろい人間像？）

ある事故が起こった場合に、警察が捜査で誰に刑事責任があるのかその主体を追及することと、今後の事故防止のために何をすべきかを考えることとでは全く視点が異なる。刑法では、注意力「ケア」が足りないという観点からエラーを定義している。他方人間工学では、基本的に人間は注意力「アテンション」を継続することはできず、エラーを起こすものであることを前提に、そうならないために何をすべきか、という観点でものを見ている。「To err is human, to forgive divine」は、人間工学で必ず出てくるキーワードである。

刑法の視点を重視すると、指示やマニュアル遵守の主体性のない対応となり、安全性の劣化につながる恐れがある。脆いが無限の可能性を期待できる人間をいかに支援できるかの視点が安全性・セキュリティ向上のために大切である。

c. 文脈の中での限定合理性と神の目から見た判断

認知科学や認知システム工学の分野では、人間は必ず情報制約がある中で、文脈（コンテキスト）に沿って考え合理的に判断している。それを

外部から後付で見るとエラーであると判断されることがある。これを、「文脈の中での限定合理性」と呼んでいる。

したがって、これからの人間を対象とする工学では、エラーの起こしやすい社会の文脈を見つけていく必要がある。つまり、エラーとは何かを分析するのではなく、エラーを起こす社会の文脈を分析する方向に考え方が変ってきている。この方向は、エラーの内容を基本的に扱う従来の人間工学の範囲を超えているから難しいのは事実である。しかし現在は、安全やセキュリティと人間を取り巻く環境要素との関連性の視点でエラーを分析しなければ対策に結びつかない時代になってきていると認識すべきであろう。

d. 標準（スタンダード：慣例・道徳）と基準（ルール：法・規制）

エラーの定義に大きな違いが現れるのは、法や規制から逸脱しているかと、慣例や道徳に反するのではないか、とが一致しない場合である。最近では、法律には触れていなくとも倫理的には問題があると糾弾されることも少なくない。

e. エラーの定義も社会の要請で変化する

昨今問題となっている企業等の個人情報の漏洩は、今に始まったことではなく以前からあったのであろう。食品問題が典型的だがその安全性が社会との関係で決まるのと同様に、最近になってセキュリティ問題も社会との関係で問題として報道にされるようになったというのが実際のところではないかと思われる。

今回の福島第一原子力発電所事故では、当事者である一企業が責任追及されているが、個人や組織のエラーと言うよりは、業界全体の判断誤り、さらには大規模災害が起因することを鑑みれば国の政策の誤りと考えるべきであろう。国家政策と営利企業の活動との狭間の「国策民営化」の概念の共通認識の誤りと言うべきかもしれない。

2.2 不安全行為と組織過誤の分類

これまでの事故モデルは、故障やエラーの因果関係を分析し対策するドミノモデルである。そのモデルで、現場の作業で発生する不安全行為の分類として使われる、スリップ、ラプス、ミステイクは、従来のヒューマンファクタで扱っていた。これらは基本的エラータイプに属し、規則違反を認識した上で行った行為は、バイオレーションと呼ばれ、JCO事故を含め最近起きた社会的事故を契機として、考慮せざるを得なくなってきた[3]。

- 日常的違反、合理化違反、創意工夫違反からなる規則逸脱｛刑法の過失相当｝と消極的違反の誤規則遵守｛認識ある過失｝と積極的違反の規則無視｛未必の故意｝

最近発生する事故は、深層防護の設計思想が確立されたこともあり、多様なシステムのエラーの重畳が原因となっている。このスイスチーズ事故モデルによる分析には、従来のエラー分析に加え、組織過誤の分析も必要となる。それには、管理職の違法性認識の観点が重要である。過誤はまず責任／権限の有無で判断され、そのエラーモードは予見性に基づき分類される[2]。

- 能力･経験不足｛過失｝､注意力不足･看過｛過失｝､努力不足･無責任(誤規則放置)｛認識ある過失｝､怠慢・放置(不作為)｛未必の故意｝､意図的違反(隠蔽・改竄)｛故意｝

この分類に従って、組織過誤の原因を、組織のピラミッドの頂点から底辺まで分析する。底辺の数層では、組織過誤の分類に加え、不安全行為の分類が適用される。対策立案においては、リスク評価によりシステム全体のバランスを取ることが重要である。

2.3 組織事故と不祥事の相違

組織事故は組織内部の問題であり、その原因は基本的に良かれと思いしたことの蓄積が結果的に組織を揺るがすまでに至るものであり、安全問題（善意の行為だがエラーとなる）との関連性が高い。組織事故は、深層防護の誤謬により、組織の内部あるいは組織間における相互依存が累積されひいては安全

文化の劣化の問題となる。この対策には、行動科学などの組織分析に基づく組織管理が必要となろう。

これに対し、不祥事には倫理的問題を含んでいる点と社会的問題とみなされ、セキュリティ問題（本質的に悪意があると社会から指弾された）との関連性が高いところに相違がある。ソーシャル・エンジニアリングなどの社会心理学的対処が必要となろう。

3. レジリエンス・エンジニアリング、高信頼組織の方法論

最近になりレジリエンス・エンジニアリング、高信頼性組織など新たな研究方法が提言され、様々な個人や組織の能力の分類が提言されている。システムの安全性を維持向上させるには、また緊急時の適切な対応を期待するには、安全意識の高い人間に頼らざるを得ないとの仮説に基づき、組織として必要となる個人や組織の能力を分析する試みである。

3.1 レジリエンス・エンジニアリング（RE：Resilience Engineering）

レジリエンス・エンジニアリングの研究方針はまだ、定まったものではない。以前のレジリエンス・エンジニアリングは、危機対応に重点を置いていた。最近の定義では[4]、個人の判断を排除しまたヒューマンエラーを生じさせないようにロバストなシステム設計を目標とするストラテジに対して、システム状態の変化がやむをえない場合に個人の状況判断を許容し（結果としてのヒューマンエラーの発生は許容した上で）、変化するシステム状態への人の対応を期待して、システムが定常に収まるようにしようとするストラテジのことである。

ホルナゲルが通常運転時への注目を強調したのもそのためである。レジリエンス（柔軟で強靭）とは、組織が本来的に持っている能力であり、環境変化や外乱に応じて組織機能を事前にその最中にまたは事後において調整する能力である。これにより組織は想定内または想定外の変動条件下で日常の業務を失敗することなく遂行できる。この調整自体は通常行われるものであり、この調整が上手くいかなかったときに失敗が発生する。

人間は行動を最適化しようとしたときに、効率性と完全性の間の許容できるバランス、すなわちトレードオフを達成しようとする。レジリエンスな組織とは、この調整する能力が組織の全階層で実行でき、バランスの取れた効率性－完全性のトレードオフができる組織である。

レジリエンスな組織となるための能力は以下の 4 つであり、この能力を組織の安全文化として醸成することにより、安全の向上と管理能力の向上を同時に実現でき、予測・計画・生産の力量を強化することができる。

① 学習力（Factual）：何が発生したかを理解する（過去の事象から、何が原因だったかを正しく学ぶ）
② 予測力（Potential）：何が起こりそうか判断でき、承知する
③ 監視力（Critical）：何に眼を光らせるべきか分かる
④ 即応力（Actual）：何をすべきか分かり、対応する実行力がある（通常または通常以外の状況変化発生時に効果的かつ柔軟に対応する）

トラブル事例を分析し、トラブルの起因となった効率性、更にはそれを補完すべきレジリエンス能力について分析・評価することにより、組織として通常必要なレジリエンス能力を明らかにし、高めていくことができる。

3.2 高信頼性組織（HRO：High Reliability Organization）

高信頼性組織の研究分野でも組織の能力を研究している[5]。平時には、些細な兆候も報告する「正直さ」、念には念を入れる「慎重さ」、操作に関する鋭い感覚である「鋭敏さ」を、有事には、問題解決のために全力で対応する「機敏さ」、最も適した人に権限を委ねる「柔軟さ」を、挙げている。またこれらを統合する中核として、「マインド」を持つ人とプロセスを開発し、彼らを支える組織マネジメン

ト、組織文化を作ることを提案している。

高信頼性組織は、REでは事故やトラブルにおける良好事例から教訓を得るという立場とは対照的に、緊急時組織（例えば原子力空母）の現場観察から良好事例を見いだすという立場であるが、事故やトラブルを少なくするという目標では共通しており、方向性は一致している。安全文化も組織の安全に関する能力を議論していると考えれば、やはり方向性は同じであろうし、実態として安全文化とHROを同時に議論する人は多い。REやHROとは目的は異なるが、組織のリスクマネジメントとして要員はリスク対処能力、リスクリテラシー(RL、後述する)を持つべきと林は考えている[6]。

事故トラブルを調査すると、かなりの事例で、エラーや規則に違反した行為に気がついている人、すなわちサトクリフがいうところのマインドフルな人がいる。彼らを強化し適切に支える仕組みができれば、事故トラブルを低減する新たな枠組みができるであろう。

4. 事故対応能力の考察

レジリエンス・エンジニアリング（RE）[4]、高信頼性組織（HRO）[5] などの新たな研究方法に基づいて、福島第一原子力発電所事故の対応における成功事例と失敗事例を、対応能力の個人レベル、組織レベル、外部対応に関連つけて分析し課題を摘出した。本分析では、主に東京電力（株）の「福島原子力事故調査報告書」[7]を基にして、1 号機における注水の経緯、特に海水注入継続判断を中心に検討した。

1号機の注水経緯について、RE、HRO、RLの各々の観点で分析した。その例として、表1にはRLの観点での分析結果を示す。横軸には提案されている対応能力を通常時と緊急時に分けて示す。縦軸には個人、組織（さらに現場と管理部門に分割した）、外部対応の各レベルを置いている。また、ゴチック体は良好事例、イタリック体は失敗事例を示している。

表 1 に示すように、事故対応能力については個人や組織のレベルと国家や業界レベルとの間に相違が見られる。

個人ベースや組織ベースではレジリエンスの良好事例が多くみられる。現場において良好事例が多くみられる根底には、現場における当事者としての使命感があり、常日頃から問題意識を持っていることまた対象範囲は異なるがアクシデントマネジメント訓練を経験していたことが緊急時に有効に働いたと考えられ、これこそが安全文化醸成の意義であろう。特徴的な良好事例として、中越沖地震の経験を反映して、整備された非常用電源・空調のある免震重要棟を緊急時対策室として有効活用し、また配備された消防車を海水注入等に有効活用したことが挙げられる。これから、平時における**「組織としての学習（フィードバック）システムの確立」**が重要であると提言できる。また、通常時において、苛酷な事象進展を想定した緊急時訓練を継続することが有効であろう。

その一方で、管理部門や国家レベルでは危機対応の不備が多々見られる。管理部門においては、緊急時の責任分担、事態の深刻度の評価と平時から有事へのモード切り替え、などの訓練が欠かせない。国家レベルや業界ベースで、レアイベントの認識の課題と組織文化の課題とにおける失敗事例が多くみられる。これらは限定合理性の考えかた[8]によれば、限定された環境の中で限定された情報に基づいて合理的に判断したが、神の目から見れば失敗だったと解釈される。対策としては、限定合理性を破壊すること、すなわち、有事における**「現場判断を優先する（命令違反を許容する）システムの確立」**が重要である。海水注入継続判断における、官邸及び本店からの注入停止の指示にもかかわらず現場判断を優先し注入継続した行動は、その典型例と言えるであろう。

5. セキュリティに及ぼす人間特性とその対策

情報システムなどの工学分野では、一般ユーザの心理的な弱点を利用する「ソーシャル・エンジニア

リング」と呼ばれる攻撃が増加傾向にあり、情報セキュリティなどの技術的対策のみでは、信頼性を確保することが難しくなっている。ソーシャル・エンジニアリングの主な手法としては、他人になりすまして必要な情報を収集するなりすまし、ゴミとして廃棄された物の中から目的の情報を取得するゴミ箱漁り、清掃員、電気・電話工事人、警備員等になりすましてオフィスや工場等へのサイト侵入、後ろからPC情報を取得するのぞき見、などがある。

ソーシャル・エンジニアリングは、人間の持つ本質的な弱さを利用して人をある行動へと誘導することであるが、情報セキュリティ分野以外でも多くの研究がある。その1つに、チャルディーニの研究[9]で、人間の弱さについて、体系化を図っている。チャルディーニは承諾誘導の戦術として「返報性」、「コミットメントと一貫性」、「社会的証明」、「好意」、「権威」、「希少性」の6つをあげている。ソーシャル・エンジニアリングにおいて、犯罪心理学などを適用して、その対策も現在検討されている。

プラントや輸送システムにおけるヒューマンファクタについての研究の歴史は長く、人間工学、行動認知学、認知心理学など多方面から研究がなされており、近年は、情報セキュリティ分野においても、ゲーム理論やインセンティブメカニズムなどの心理学や経済学知見を活用する動きがある。しかし、人に由来する主観の問題を扱うため、活用の困難さも指摘されている。また、システムのリスク管理の観点からは、人に心理や行動に由来するリスクを低減するだけでなく、リスクの変化を制御して、システム全体のパフォーマンスの変動を抑制するなど、復元性（レジリエンス）の高いシステムの実現が期待されている。

6. あとがき

巨大複雑システムにおいて、技術の巨大化・複雑化と高度化に伴い、安全・セキュリティ問題がハードウェアから人間そして組織の問題へと、次第に社会化する現象があらゆる技術分野で発生している。これに伴い、事故やエラーの形態や社会的な受け止め方、またその分析方法も時代とともに変化している。当初はドミノ事故モデルとヒューマンエラー、次いでスイスチーズ事故モデルとシステムエラー、そして最近のとらえ方は組織事故と安全文化の劣化、である。これらの事故の分析から安全を議論する方向に対し、新たな動向として、様々な事象の良好事例に着目して分析するレジリエンス・エンジニアリング、高信頼性組織、リスクリテラシーなどの研究手法も盛んとなりつつある。また、情報セキュリティ分野を中心に、人間の持つ本質的な弱さを利用してその人をある行動へと誘導する方法とその対策を検討するソーシャル・エンジニアリングも最近の研究テーマとして検討が始まった。

安全やセキュリティの達成のために、人々の価値観・倫理観や行動様式(安全文化)だけでなく、社会的受容や事故への社会・環境への影響も、考慮することが不可欠になりつつある。その一方、リスクを含まない科学技術はないが、リスクを上回る効用があるからこれまで受け入れられてきたことも事実である。そのためにも、安全問題とセキュリティ問題を統一的に扱うことができる安全学の体系化の早急な確立が望まれる。

参考文献

[1] 氏田　博士：安全と信頼とリスク～安全・安心な社会を目指して、「安全･安心を実現する専門家･組織･社会のあり方」、信頼性学会誌、Vol.26, N0.6, 2004.

[2] 氏田博士、古田一雄、柚原直弘：組織過誤の分類とソフトバリア概念の提言､ヒューマンインタフェースシンポジウム論文集、2002. 9.

[3] J.Reason: 'Managing the Risks of Organizational Accidents', Ashgate, 1997.

[4] E.Hollnagel, D.D.Woods, N.Leveson (edt.): Resilience Engineering Concept and Precepts, Prentice Hall, 2006.

[5] 中西晶著「高信頼性組織の条件」、生産性出版、

2007.1.

[6] 林 志行、「事例で学ぶリスクリテラシー入門」、日経 BP 社 、2005.

[7] 東京電力(株)、「福島原子力事故調査報告書」、2012.6.

[8] 菊澤研宗、「組織の不条理」、ダイヤモンド社、2000.

[9] ロバート・B・チャルディーニ「影響力の武器」、誠信書房、2007.

(受付日：2014 年 4 月 25 日)

著者略歴

氏田　博士（うじた　ひろし）

昭和 49 年 4 月　(株) 日立製作所入社　原子力研究所（エネルギー研究所からエネルギー・環境システム研究所、現在は日立研究所に名称変更）

平成 23 年 4 月　東京工業大学 大学院理工学研究科原子核工学専攻　特任教授

平成 26 年 1 月　キヤノングローバル戦略研究所上席研究員

日本人間工学会　橋本賞(平成 5)年度最優秀論文)、計測自動制御学会　第 10 回ヒューマンインタフェースシンポジウム　優秀プレゼンテーション賞、人工知能学会　1994 年度研究奨励賞、日本電機工業会平成 8 年度奨励賞、日本原子力学会　平成 15 年度技術開発賞、日本信頼性学会　優秀記事コラム賞、日本原子力学会　社会環境部会　優秀発表賞

東京都市大学、電気通信大学、東京工業大学　非常勤講師

リスクリテラシー ＼ 分析レベル		平時				有事		
		解析力			伝達力		実践力	
		収集力	理解力	予測力	ネットワーク力(情報発信)	コミュニケーション力(影響力)	対応力(今ある危機対応)	応用力(抜本対策)
個人		・津波被害事故例	・津波被害のリスク認識	・電源喪失のリスク認識	—	—	・海水注入継続判断	・緊急時訓練
組織	現場	・事故例収集：貞観津波	・地震・津波PSA実施による影響範囲評価	・事故の大きさの認識	・現場の情報共有	・指揮系統(現場) ・免震棟での一元化 ・中装-緊対室連絡	・淡水・海水注入 ・ベント操作 ・被害の拡大防止	・免震棟を緊対室として活用 ・消防車有効活用 ・指揮系統 ・津波対策 ・AM対策
	管理部門	・事故例収集：貞観津波、JNES津波PSA、ルブレイエ・マドラス炉浸水	・津波被害のリスク誤認識	・電源喪失のリスク誤認識	・本店/現場の情報共有	・TV会議システム(2F) ・本店-現場の指揮系統の乱れ		・教育/訓練システム見直し
外部対応(官邸、等)		・海外テロ対策事例収集：米国9.11テロ-B.5.b.	・事故の重要性分類 ・地震・津波リスク誤認識	・外部事象の重要性 ・インフラ被害リスク誤認識		・メディア、地方自治体、海外広報 ・官邸/本店/現場の指揮系統の乱れ	・初期対応の遅れ ・政府指揮系統	・メーカ・協力企業の支援 ・外部の支援 ・抜本対策：組織改革(規制/電力)