



高度技術システムの安全に関する一考察

原, 拓志

(Citation)

神戸大学経営学研究科 Discussion paper, 2016・10

(Issue Date)

2016-04

(Resource Type)

technical report

(Version)

Version of Record

(URL)

<https://hdl.handle.net/20.500.14094/81009472>



Graduate School of
Business Administration

KOBE
UNIVERSITY



ROKKO KOBE JAPAN

2016-10

高度技術システムの安全に関する一考察

原 拓志

Discussion Paper Series

1. はじめに

現代社会では、非常に複雑で、複合的で、統合的で、しばしば強力な技術システムが増えている。たとえば、原子力発電、高速鉄道、航空機、コンビナートである。さらに、現在進んでいる IoT (the Internet of Things) と呼ばれる人工物のネットワーク化によって、自動運転車走行システムなども新たに加わる可能性がある。これらを、高度技術システムと呼ぶ。これらは、大変便利であるが、いったん事故が起こると従来以上の被害をもたらす潜在的な危険性を有している。

したがって、高度技術システムの安全¹は、供給側にとっても利用側にとっても極めて重大な問題である。そして、こうしたシステムの開発、生産、販売、利用には、多くの企業や組織が関わり、その安全形成もそれらの相互作用の下になされるがゆえに、これは経営学にとっての研究対象であると同時に、経営学も安全形成のために貢献すべきである。

本稿は、そうした問題意識に立って、高度技術システムの安全について考察するが、特に論じたいことは、この領域で著名なジェームズ・リーズン (James Reason) のスイスチーズ・モデル (the 'Swiss Cheese' model) の通俗的な理解と、一般的に事故リスクの定義に用いられる定量的リスク・アセスメントの公式 (Hammer 1980, 邦訳, 187-201 頁) に潜んでいる前提が、競争優位やコスト削減への圧力が強く働く環境においてもたらずバイアスについてである。本稿では、新幹線と航空管制の経験的データを用いて、そのバイアスの存在を示唆し、既存の安全に関わる議論の相対化を図る。

2. リーズンのスイスチーズ・モデル

リーズンのスイスチーズ・モデル (Reason 1997, pp. 7-18, 邦訳, 11-23 頁) は、安全や事故防止に関わる近年の多くの研究に影響を与えている (中西 2007; 谷口 2012; 樋口 2012 など)。リーズンが注目しているのは、個人レベルの事故ではなく、多くの人々が原因に絡み、めったに起こらないが、ひとたび起こると甚大な被害をもたらす「組織事故 (organizational accidents)」である (Reason 1997, p. 1, 邦訳, 1 頁)。原子力産業、航空産業、石油化学産業、鉄道産業などの例から判断しても、これは本稿で扱う高度技術シス

¹ 本稿では「安全」とは、事故を起こさないこととして把握している。しかし、一般的に、安全には、事故が起こった後の対処 (被害の拡大防止やシステムの回復など) の側面もある (Hollnagel 2008)。高度技術システムの事故は、まずは起こさないことが優先されるべきだという考えから、本稿は、さしあたり、事故防止の側面に限定して議論している。

テムにおける事故と同義とみてよいだろう。

スイスチーズ・モデルの概要としては、潜在的な危険性 (hazards) によって生じるかもしれない損害を防ぐために防御壁 (defences) を置くが、防御壁は本質的に不完全であるため、それを多重に設置するというものである。不完全な防御壁は、ちょうど穴の開いたスイスチーズのようなものであり、それがモデルの名前の由来であるが、穴があっても多重にすることで、一つまたは複数の防御壁をすり抜けても危険性を封じ込めることができるという考え方である。

防御壁は、「ハード面」と「ソフト面」との混合からなっている。ハード面の防御壁とは物的な設備等であり、ソフト面の防御壁とは規則や訓練、資格などの制度や人間主体の活動である。これらの防御壁は、安定的なものではなく常に揺れ動く (in constant flux) (Reason 1997, p. 9, 邦訳, 11 頁)。変化の原因として、リーズンが注目しているのは、一つは、現場オペレーターのエラーや規則違反などの不安全行為 (unsafe acts) であり、彼はこれを「能動的 (な働きをする) 失敗 (active failure)」と呼んでいる。しかし、それだけでは事故の説明はできない。彼が防御壁の変化の原因として挙げているもう一つは、個人の心理的要因に帰属できない、関係組織が長年にわたって蓄積してきた病原体的存在である「潜在的諸条件 (latent conditions)」である。それには、貧弱な設計、監督の不備、検出されなかった製造の不良や保全の不良、使えない手順、ぎこちない自動化、訓練不足、不適切な道具や設備などが含まれる。これらの潜在的諸条件が、特定の環境の下で、能動的失敗と重なることによって、スイスチーズの穴が偶発的に揃って、潜在的危険性が損害を伴う事故を引き起こすというのである。

能動的失敗と潜在的諸条件の両方を高度技術システムの防御壁に生じる脆弱性の原因とするリーズンの議論の重要な含意は、事故が注目されやすい個人のミスだけでなく、様々な組織的状况が陰で関係しているということである。個人的責任の追及や不安全行為の撲滅だけではシステムの安全性向上につながらないということを主張 (Reason 1997, pp. 14-15, 邦訳, 18-19 頁) するとともに、事例でも示している。つまり、事故には、能動的失敗につながる不安全行為の原因となる、作業現場における要因や組織的要因が、潜在的諸条件として階層をなして関わっている (Reason 1997, p.17, Figure 1.6, 邦訳, 21 頁)。また、組織的要因や作業現場の要因は不安全行為を経ずに直接に防御壁を壊すこともあるとしている (Reason 1997, pp.17-18, 邦訳, 22 頁)。

なお、スイスチーズ・モデルの図式に比べると一般的に注目されていないリーズンの主張に、防御壁がむしろ危険をもたらすという命題がある。その論理としては、①特定のヒューマンエラーを減らすための方策 (たとえば作業と検査との分離) がシステムの他の部分でのエラー (たとえば品質管理の形骸化) をもたらしてしまう、②防御において獲得された利得が生産性向上に向けられ却って危険性を増してしまう、③冗長性及び多様性に基づく深層 (多重) 防御壁がオペレーターにとってシステムを見えにくくし潜在的諸条件が知らぬ間に蓄積する、④警報や警告が頻発することで本当の緊急時に効果がなくなる、⑤

過去の事故の顕著な原因を排除するために取り入れた対策が、システムの複雑性、不確実性を増して却って次の事故につながる、⑥防御壁などが新たな部品や関係を生み出すと、それらは複雑性を増すだけでなく、それら自体の故障がシステム崩壊の引き金となる、などである (Reason 1997, pp. 41-60, 邦訳, 61-89 頁)。

同様の論理は、チャールズ・ペロー (Charles Perrow) やスコット・セーガン (Scott D. Sagan) など、高度技術システムの安全と組織についての論者にも見出すことができる。ペローは、よく知られているように、構成要素間関係が複雑で、緊密な連結に基づいたシステムにおいては、システム事故は、いわば当然のことであり、「通常事故 (normal accidents)」だとしている (Perrow 1999; 原 2010)。彼は、システムにおける安全装置 (リーズンによるところの防御壁) について、以下のように論じている。

安全装置を含む安全策は、ときに新たな事故を生み出す。それらはしばしばシステムの運営者やオペレーターに、より高速にとだけでなく、より危険な状況においてでも、あるいは、より多くの危険を携えてでも、システムを稼働するように仕向ける (Perrow 1999, p. 11, 著者訳、一部意識)。

さらに以下のようにも述べている。

安全装置は (システムの) 部品やユニットの機能不全から防御することだけでなく、その機能不全を隠蔽しようとする力に対処するためにも必要である。これは、すでに十分に複雑なシステムをさらに複雑にし、システム自体が崩壊する前に不具合から回復する可能性を著しく制限する。この複雑性と緊密性の増大には際限がないようにみえる (Perrow 1999, p. 292, 著者訳、カッコ内は著者による補足)。

つまり、安全装置の増強自体が、運転者やオペレーターが受容する潜在的危険性を増やし、また、システム自体の複雑性を増すことで、システムの制御を難しくし、事故を引き起こす潜在的条件を構成してしまうというのである。また、セーガンも、このペローの議論を、「冗長性は、相互作用の複雑性と不透明性を増し、リスクテイクを促進することで、しばしば事故を引き起こす」と定式化し (Sagan 1993, p. 46)、それが歴史的な証拠によって支持されているとしている (Sagan 1993, p. 252)。

以下の節においては、日本における新幹線システムと航空管制システムを事例として、リーズンのスイスチーズ・モデルの通俗的な理解にあるような「スイスチーズの穴が揃う可能性を低下させるためには防御壁を増強すればよい」という考えが現実の高度技術システムの形成において浸透しているかどうか、またその結果、リーズンらの本来の主張にあるように、「防御壁の増強こそが危険を増す可能性がある」が実際に起こっているかについて確かめることとする。

3. 新幹線システムの安全形成とその動向

新幹線は、時速 200km を超える高速²で、総計 2500 km以上（2014 年 10 月現在³）の距離を、毎日往復計 800 本以上⁴が運行している高度技術システムだといえるが、長期間にわたりシステム事故⁵を起こしていない。とくに、東海道新幹線では、1964 年 10 月の営業運転開始以来 50 年以上にわたってシステム事故を起こすことなく、今では短いときは 3~4 分程度の間隔で臨時列車も含めると 1 日 350 本を超える本数が運行している。その安全の形成には、さまざまな物的要因、制度的・構造的要因、組織的・主体的な要因⁶（防御壁）が貢献している。

新幹線の安全の原則は、鉄道の安全原則である閉塞や危険時の停止に加えて、攪乱要因を徹底的に排除することである。そのために、物的要因に関わるものとして、専用の線路を使い、車両の種類や列車の種類も少なくシンプルにすること、道路等とは立体交差として踏切を一切設けていないこと、線路内に人が立ち入らないように防護柵を設けたり、雪の対策としてスプリンクラーを設けることなどの対策が図られている。また、車両、架線、路盤、トンネル、プラットホームなどにも数知れない対策が設けられている。さらに、自動列車制御装置（ATC）や列車集中制御装置（CTC）、地震を早期検知し自動的に送電停止して緊急停車させるシステムが採用されている。加えて、保線産業には、様々な高効率の機械が導入され、軌道や架線、信号電流の検査測定には新幹線電気軌道総合試験車（通称ドクターイエロー）が投入されている（山之内 2005; 斉藤 2006; 新星出版社 2007; 原 2008）。

また、制度的・構造的要因としては、線路内への立ち入りを防ぐための「新幹線鉄道の列車運行の安全を妨げる行為の処罰に関する特例法」の制定・施行や、毎日深夜 0 時から早朝 6 時までの列車の運行を止めての保線作業、定期的実施される車両検査、大雨や暴風などの状況で列車運行を取りやめる基準などが挙げられる。また、中央指令室の所在地

² 新幹線区間のみ。山形新幹線や秋田新幹線の在来線区間は最高速度が時速 130 kmと定められているので、本稿の議論には含めない。

³ 営業キロで東海道新幹線 552.6、山陽新幹線 622.3、九州新幹線（博多・鹿児島中央間）288.9、東北新幹線（東京・新青森間）713.7、上越新幹線（東京・新潟間）333.9、長野新幹線（東京・長野間）222.4（JR 時刻表，2014 年 10 月号）。

⁴ ここでは、臨時列車を除いて数えているが、東海道新幹線などでは、実際には毎日相当数の臨時列車が運行されている（JR 時刻表，2014 年 10 月号）。

⁵ 意図せざる出来事であり人間や物財の被害を伴い、システムの継続中ないし将来の成果に重大な打撃を与えるもの（Perrow 1984, pp. 63-65）。さらに、本稿では、システムの構造自体に被害を引き起こす内在的要因が認められるものとする。たとえば、新幹線でいえば、自殺行為による人身事故などによる遅延は、システム事故からは除外される。

⁶ 物的な要因、制度的・構造的要因、組織的・主体的要因に分けて防御壁を整理しているのは、筆者の分析枠組みである「技術の社会的形成アプローチ」（原 2007）に基づくものである。今後、筆者の他の議論との接合を図るため、その枠組みで整理した。

が秘密にされ、バックアップの司令室も置かれるなど、テロリストの攻撃や不測の事態への一定の備えもなされている。さらに、日本社会の特性ともいえる相対的に良好な乗客マナーや治安の良さ⁷なども定時走行を容易にして、結果的に攪乱要因の低減に貢献しているといえよう（三戸 2005; 斉藤 2006; 新星出版社 2007; 原 2008）。

組織的・主体的要因としては、在来線とは別個の組織とされて、高い使命感を有した成員は、選抜や教育にも注意が払われるとともに、開業当初からの小事故や故障、トラブルの経験と対策の積み重ねによって、システムの安全性が高められてきたことが明らかにされている（斉藤 2006; 原 2008）。このように、新幹線は営業当初から、物的あるいは制度的・構造的、そして組織的・主体的な要因⁸によって安全のための防御壁が数多く設けられ、その結果、長期間にわたり安全が確保されてきたといえる。このことは、「スイスチーズの穴が揃う可能性を低下させるためには防御壁を増強すればよい」という考えが実際に適用されている例と理解できる。

では、リーズンらのあまり知られていない方の主張「防御壁の増強こそが危険を増す可能性がある」については、どうであろうか。新幹線の実現自体がこの主張を裏付けているともいえる。つまり、在来線よりはるかに高速の鉄道を運転するにあたって、防御壁を多く設けることで、潜在的には危険性の高いシステムを実現したからである。さらに改善されていく防御壁のもとで、新幹線システムは、どのように変化してきたのか。本稿で注目するのは、速度の増加と、列車本数の増加である。開業当初、東京・新大阪間の所要時間は4時間で運行され、列車も30分おきであった。その後、1966年からは、同区間の所要時間は3時間10分となり、新列車「のぞみ」が登場した1992年からは2時間30分となった（図1参照）。ちなみに、新幹線導入前の東京・大阪間の所要時間は6時間30分であった（Hood 2006, p. 29）。列車本数も次第に増加し、往復で開業当初60本程度だったものが、今では、区間運行や臨時列車を併せると350~400本以上となっている（各年時刻表）。この期間中、新車両導入など安全のための防御壁も改善されてきた。「防御壁の増強こそが危険を増す可能性がある」という命題は、新幹線システムにおいて例証されているといえよう。ただし、同時に注目しておきたいことは、列車本数の増発は、安全のための防御壁が改善されたことだけでなく、安全な運行実績の蓄積、輸送需要の増加、飛行機との競争、運営組織の民営化なども大きく関連していると思われる。それぞれの寄与度については、今後の研究に委ねるが、少なくとも新幹線のように数多くの防御壁が用意された高度技術

⁷ 治安の良さといっても、今後社会不安が高まれば続くとは限らない。2015年6月30日に男が新幹線車内で焼身自殺を図り、他の乗客にも死傷者が出た。放火が、システム構造も関係して乗客の不慮の死や負傷を招いたということでは、システム事故の面もあるかもしれない。この防止策として現在図られているのは、車内の防犯カメラの設置と可燃物持ち込みの禁止・制限（2016年3月31日発表、4月28日適用）である。

⁸ 物的要因、制度的・構造的な要因、組織的・主体的な要因は、便宜上、分類して説明したが、現実には分かちがたく結びついていることには注意されたい。たとえば、保線作業一つとっても、制度も物も組織も全てが一体となって実施されている。

システムで、速度と密度が時間とともに増して、潜在的な危険性を増す方向にシステムが変化したことは明らかとなった。

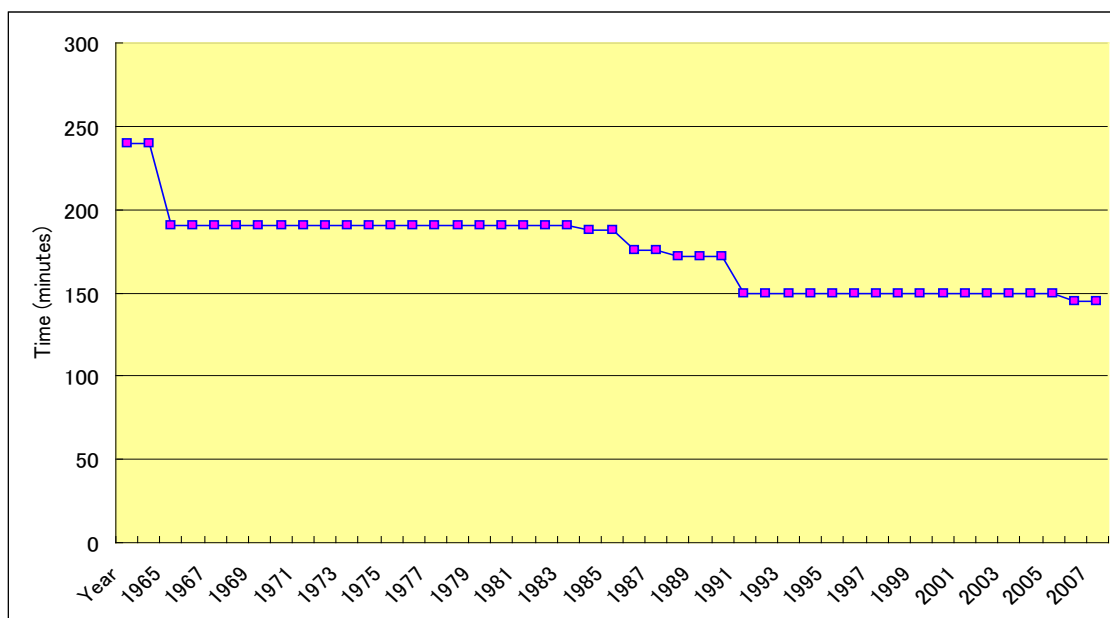


図1：東海道新幹線における速度の推移（東京・新大阪間の所要時間）（各年時刻表）

4. 日本の航空管制における安全形成とその動向

次に日本の航空管制における安全形成の事例を検討する。日本の航空管制は、1959年にアメリカ軍から日本政府に移管され、現在は国土交通省航空局管轄下で運営されている。航空管制は、人間と揮発性燃料を乗せて地上と上空を高速で移動する航空機を安全に運行させるための高度技術システムであり、機能不全が、航空機の墜落や衝突、爆発などのシステム事故を引き起こす潜在的危険性を孕んでいる。そこで、安全のための防御壁も多重に備えられている。その結果、日本では1960年に小牧空港で全日空機と自衛隊機との衝突で3名が死亡した事故以降、50年以上にわたり、航空管制が原因での死者を伴う飛行機事故は起こっていない。この事例における防御壁も、物的、制度的・構造的、組織的・主体的な要因から成り立っている。

航空管制における安全の原則は、航空機相互あるいは航空機とその他の物体との間の安全間隔（垂直間隔：Vertical Separation、縦間隔：Longitudinal Separation、横間隔 Lateral Separation など）の確保（中野 2014, 81-92 頁；園山 2010, 27-28 頁）である。その意味では、航空機も鉄道と同様に一種の「閉塞」を作り出すことが安全原則となるが、線路がなく自由な空間であるがために「閉塞」の維持は、制度（たとえば、航空管制と航空機との間の取り決めやコミュニケーションなど）に鉄道よりも大きく依存する。さらに、この取り決めやコミュニケーションに関しては、航空管制と航空機運航が別の主体によって運

営されていること、また国際路線になると、制度や文化、言語の異なる主体が混在すること⁹も考慮しなければならない。また、航空機の場合、危険時に運航を停止することはできない。安全に着陸をしようとするれば、場所や条件を確保しなければならないため飛び続ける時間が必要になる(園山 2010, 21-26 頁)。この点も鉄道の安全原則とは異なる。他方で、線路がないため、空間的により自由な危険回避ができるという面もある(園山 2010, 27 頁)。このように、航空管制の安全原則は、間隔の維持とそれを実現するための、位置の測定と航空機側との意思疎通が基本となる。したがって、航空管制システムにおける防御壁も、そうした要因からなっている¹⁰。

まず、物的には、航空機の位置を特定するための航空路監視レーダー (Air Route Surveillance Radar: ARSR)、洋上航空路監視レーダー (Oceanic Route Surveillance Radar: ORSR)、空港監視レーダー (Airport Surveillance Radar: ASR)、精測進入レーダー (Precision Approach Radar: PAR)、二次監視レーダー (Secondary Surveillance Radar: SSR)、空港面探知レーダー (Airport Surface Detective Equipment: ASDE) など各種レーダーや GPS (Global Positioning System)、運輸多目的衛星 (Multi-functional Transport Satellite: MTSAT)、自動従属監視 (Automated Dependent Surveillance: ADS)、空港監視のための管制塔などがある。また、航空機側が、自機の位置を把握するための設備として、超短波全方向式無線標識施設 (VHF Omnidirectional Range: VOR)、距離情報提供装置 (Distance Measuring Equipment: DME)、無指向性無線標識施設 (Non Directional Radio Beacon: NDB)、計器着陸装置 (Instrument Landing System: ILS)、航空灯火、GPS、ADS、慣性航法装置 (Inertial Navigation System: INS)、航空機衝突防止装置 (Airborne Collision Avoidance System: ACAS)、高度計などがある。そして、航空機と航空管制とが意思疎通するために、遠隔対空通信施設 (Remote Center Air-Ground Communication: RCAG)、遠隔空港対空通信施設 (Remote Air-Ground Communication: RAG)、着陸誘導管制業務 (Ground Controlled Approach: GCA)、管制官・パイロット間データリンク通信 (Controller Pilot Datalink Communication: CPDLC) などがある。さらに、これらの探知機器や通信機器、入力装置などから集められた膨大な情報を処理するための情報処理システムとして、飛行計画情報処理システム (Flight Data Processing System: FDP)、飛行情報処理管理システム (Flight Data Management System: FDMS)、航空路レーダー情報処理システム (Radar Data Processing System: RDP)、ターミナルレーダー情報処理システム (Automated Radar Terminal System: ARTS)、ターミナルレーダー・アルファニュ

⁹ 1977年3月27日カナリア諸島テネリフェ島のロス・ロディオス空港(当時)における航空機衝突事故の一因は、英語を母国語としない管制官とパイロットとの間の異常事態時のコミュニケーション不良にもあったとされる(藤田 2005, 89-121 頁; Weick 1990)。

¹⁰ 現在の日本の航空管制の概略的な設計思想としては、機器的な情報システムを中心とした防御壁がプライマリーとバックアップの2重にあり、さらに組織がカバーするマニュアルの防御壁があつて、最後が個人の臨機法変な判断に基づく防御壁の4重であるという(大阪航空局保安部管制課長(当時)三田公靖氏インタビュー、2008年8月27日)

ーメリック表示システム (Terminal Rader Alphanumeric Display System: TRAD)、洋上管制データ表示システム (Oceanic ATC Data Processing System: ODP)、空域管理システム (Air Space Management System: ASM)、航空交通流管理システム (Air Traffic Flow Management System: ATFM)、運行情報提供システム (Flight Service Information Handling System: FIHS)¹¹、以上の情報処理システムの各種バックアップシステム¹²、情報システムと管制官ら人間とのインターフェイスである航空路管制卓システム (Integrated En-route Control System: IECS) などがある (中野 2014; 国土交通省航空局管制保安部 2008; 国土交通省 2016a)。

次に、組織的・主体的要因としては、まず、高度に訓練され高い職業意識を備えた管制官、管制技術官、運行情報官、航空機パイロットが重要である¹³。また、航空灯火や電気施設の管理や保全、飛行検査、衛星運用などを担う人々の努力や注意も重要である。また、「危険因子 (ハザード) を特定し、そのリスクを評価したうえで受容できるまで低減する対策を事前予防的な取り組みを PDCA サイクルに則って体系的に実行しようとする管理手法」(国土交通省航空局管制保安部 2008) としての安全管理システム (Safety Management System: SMS) への組織的取り組み、管制官同士あるいは管制技術官同士、運行情報官と各種関係者との間、管制官と管制技術官と運行情報官との間の良好な関係とチームワーク¹⁴、より広範な職務間・組織間における連携を目指した協調的意思決定 (Collaborative Decision Making: CDM) への取り組み (国土交通省航空局管制保安部 2008; 国土交通省 2016b) などが挙げられる。

最後に制度的・構造的要因としては、航空管制そのものがあり、それを実現可能にするための制度として管制区、飛行情報区、航空路、飛行計画、最低安全間隔、計器飛行方式、飛行高度、出発・到着経路などが制度化されている。鉄道と比較すると経路について線路という物的な制約がないため、機能代替的に制度的制約によって安全がコントロールされている。そうした制度は、国内の法規則である航空法、航空法施行規則などで定められ、

¹¹ FDMS、FIHS 及び全国の空港等に設置された端末等を網羅する情報通信ネットワークが航空交通情報システム (Common Aeronautical Data Interchange Network: CADIN) である。CADIN は、本文中に列挙した各種の管制情報システムなど航空局内のシステムをはじめとして、気象庁、防衛省、海上保安庁、航空会社、空港会社、海外管制機関などの外部システムと接続されており、多種多様な情報の収集、編集、管理、中継、提供を行っている (国土交通省 2016a)。

¹² システム開発評価・危機管理センター (SDECC) に設置されているシステムは、航空交通管制情報処理システムのプログラム等を開発及び評価するシステムであり、同時に管制部等に設置された運用システムのバックアップとして危機管理を実施する機能も果たしている (国土交通省 2016a)。

¹³ 巻末謝辞に挙げた管制官、管制技術官、運行情報官、航空機パイロットへのインタビューからは、いずれの職種においても職業意識の高さが感じられた。

¹⁴ 関西空港管制官 (当時) 岩田氏、宮坂氏へのインタビュー (2008 年 10 月 28 日) および管制技術官 (当時) 伊地知氏、阪氏、運行情報官 (当時) 金子氏、村松氏へのインタビュー (2008 年 10 月 14 日)。また、月刊エアライン 2010 年 5 月号、25 頁参照。

その監督機関として国土交通省航空局などが存在するが、国際交通を含むため、それらの制度はまた、国際民間航空条約や国際民間航空機関（ICAO）およびそれが制定する国際標準および勧告方式といった国際的な制度にも強く制約される。また、既述の航空交通流管理（ATFM）や協調的意思決定（CDM）も、気象庁や航空会社、自衛隊や米軍、海外管制機関との情報提供や調整を制度的に実施している。そして、主体的要因である管制官、管制技術官、運行情報官の養成についても航空保安大学校やそれぞれの国家資格によって制度化されている（中野 2014；国土交通省航空局管制保安部 2008；国土交通省 2016a）。

以上のように、物的、組織的・主体的、制度的・構造的な要因による多重的な防御壁が航空管制システムにも備えられている。典型的には、注9で述べたように、2重の物的・機器的なシステム、それを補う組織・人間によるマニュアルのシステム、さらに最後には個人的判断に基づく包括的な緊急措置という4重の防御壁が設計思想となっていた。特に物的・危機的なシステムは、近年ますます高度化、精緻化、統合化され増強されている。こうした実践は、「スイスチーズの穴が揃う可能性を低下させるためには防御壁を増強すればよい」という考えに基づいているといえるであろう。

他方の「防御壁の増強こそが危険を増す可能性がある」に関しても、新幹線の事例と同様、航空管制システムにおいても見出される。図2はそれを顕著に示している。

航空管制取扱機数と航空管制官等定員の推移

国土交通省

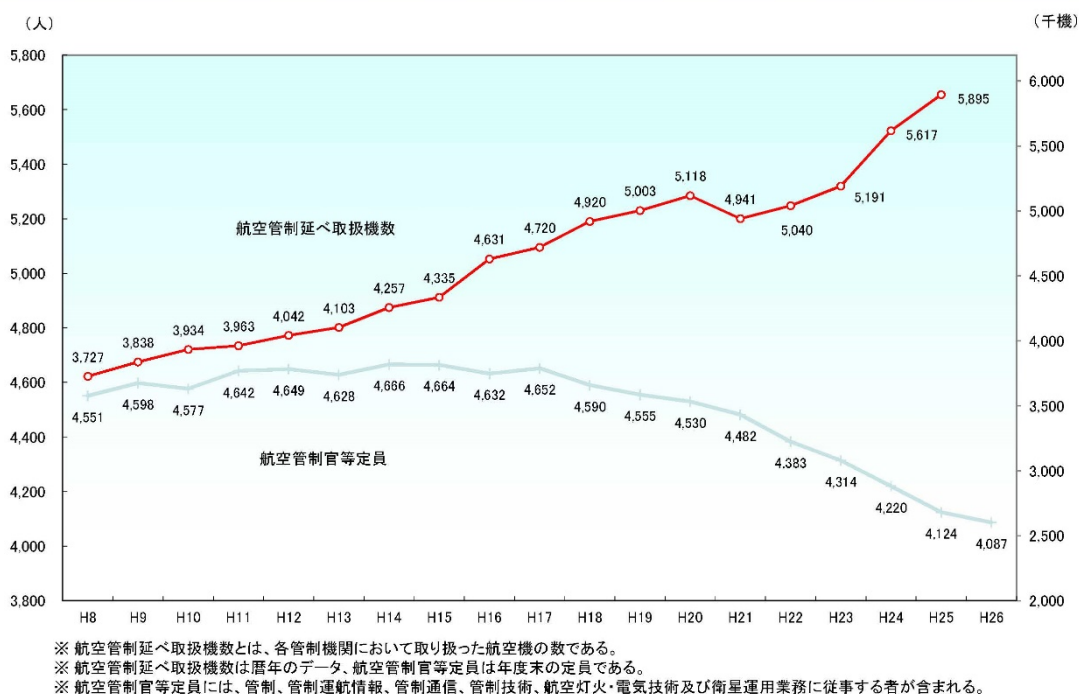


図2：航空管制取扱機数と航空管制官等定員の推移

(出所) 国土交通省ホームページ, <http://www.mlit.go.jp/common/001081154.pdf>

図2によれば、最近の18年間（1996年-2014年）において、取扱機数は増加しているにも関わらず、管制官等の人員は減少している。定員削減は財政上の理由が大きいであろうが、各種情報システムやデータリンクなどの自動化がその背景にあることは各種資料から明らかである（中野 2014；国土交通省航空局管制保安部 2008；国土交通省 2016a；月刊エアライン 1995年7月号，2001年11月号，2010年5月号）。航空管制の効率化が進んでいることは間違いない。航空管制による事故が増えたわけではないので、安全性が損なわれているかどうかは可視的ではない。しかし、システムが抱える潜在的危険性（取扱機数）は増大していることは確かである。そのことは、最低安全間隔における制度変更にも見出される。たとえば、国内空域における垂直管制間隔については、かつては29000フィートを超える高度では2000フィートであったものが、航空機搭載機器の性能向上によって、2005年に1000フィートに短縮された¹⁵（中野 2014, 88頁）。また、洋上管制間隔についても、人工衛星を活用した通信・航法の監視機能の強化によって、現行10分～15分（80海里～120海里相当）の縦間隔、50海里的横間隔を、縦横ともに30海里まで短縮する目標が掲げられている¹⁶。また、空域、特に空港付近の空域の混雑状況の悪化に伴い、たとえば成田空港では、新たな離陸方式の導入、航空機監視装置の導入によって、発着枠の容量拡大を実現したり、地方空港等では、GPSや高性能な機上装置を活用して山岳地帯に沿った着陸方式を実現したりしている。さらに、2010年9月に策定された「将来の航空交通システムに関する長期ビジョン（CARATS）」では、安全性の向上などとともに、就航率、速達性、効率性の向上が謳われている。また、空域を飛行フェーズに応じて上下分離することで、効率性向上と管制処理能力の向上も考えられている¹⁷。

このように、航空管制システムにおいても、「防御壁の増強こそが危険を増す可能性がある」ことが見受けられる。もちろん、取扱機数の増加は、航空管制システムが求めたものではない。むしろ、増える航空機を安全に交通整理するために、機器の導入などによる防御壁の増強が図られているともいえる。また航空管制官等の定員の減少も航空管制システムが求めたものではない。国の予算で決められているものであり、むしろ航空管制側からは望まないことであろう。そういう意味では、新幹線システムとは、防御壁の増強を促進する論理には違いも存在している。しかし、競争や需要増加、予算削減などはいずれも効率性向上の圧力となっており、機器などの性能向上により安全のための防御壁の増強が可能である場合には、その防御壁が効率性向上と潜在的危険性の増大に結果として利用されていることには違いない。

以上の事例に示されているように、現代の高度技術システムにおいては、安全のために

¹⁵ 国土交通省ホームページ，http://www.mlit.go.jp/kisha/kisha05/12/120930_.html（2016年4月12日閲覧）。

¹⁶ 国土交通省ホームページ，http://www.mlit.go.jp/koku/15_bf_000368.html（2016年4月12日閲覧）。

¹⁷ 国土交通省ホームページ，<http://www.mlit.go.jp/common/001081152.pdf>（2016年4月12日閲覧）。

多くの物的、組織的・主体的、制度的・構造的な防御壁が多く備えられ、特にコンピューター化、システム化、自動化、統合化された防御壁のもとで、高速化、高密度化など効率向上が図られる傾向がある。企業間競争や定員削減などの構造的な圧力が背景にある。圧力の種類がなんであれ、こうした効率向上は、結果的に潜在的危険性を増大させているともいえる。しかし、強力になった防御壁、より穴が少なく小さくなった防御壁によって、事故が起こることは、ほとんどない。日本の新幹線も航空管制も毎日多数の件数を扱いながら数十年間、大きなシステム事故は起こしていない。こうしたことが、こうした動きについて、技術進歩ということで良いこと、あるいは当たり前のこととして一般には受け止められているようである。

しかし、2011年の東日本大震災の際の福島第一原子力発電所の事故は、同様に多重にあって増強されているはずの防御壁も崩れる可能性、つまりスイスチーズの穴が揃う可能性があることを示した。それまで、日本の原子力発電所も何十年もの間、大きなシステム事故は起こしていなかった。原子力発電所の安全は、各防御壁が完璧を目指す前段否定の思想に基づいた防御壁を重ねる深層(多重)防護に基づいていたはずである(佐藤 2006, 54-56頁)。それでも事故は起こったのである。「想定外」という言葉が当時流行った。人知には限界があり、想定には範囲がある。それが、さまざまな領域で共通しているとすれば、他の高度技術システムにも同様の事態が発生する可能性を示唆している。

一般に事故のリスクは、事故の発生確率とそれによって生じる損害の重大性との積でとらえられることが多い(古田・長崎 2007, 13頁; Stewart and Melchers 1997, 邦訳, 3-4頁; Hammer 1980, 邦訳, 187-201頁)。専門的なリスク分析、リスク評価においては、システムの構成要素間のリスクが組み合わされ、評価者によるウェイトの判断もそこに加味されるなどの精緻化が図られる(Wilson and Crouch 2001, pp. 9-10)が、上記のシンプルな式[発生確率×損害の重大性]が事故リスクの定義の中核となっている。この式によれば、事故リスクは、発生確率を小さくすれば、損害の重大性が増したとしても大きくはならず、結果的に社会で受容されることになる。新幹線や航空管制、原子力発電所などの高度技術システムにおいて実際に見られる展開は、まさにこの式によって説明されるし、正当化される。次節でこの式について、さらに検討を加えたい。

5. リスク数量化の問題

前節で述べたように、安全のための防御壁の増強、あるいは深層防護によって、潜在的危険性の増大も受容できるという考えの論拠に、事故リスクの「数量化」[発生確率×損害の重大性]がある。通俗的な「スイスチーズの穴が揃う可能性を低下させるためには防御壁を増強すればよい」という考えや、専門家による「やみくもに防御壁を増やしても意味はない。前段否定の思想に基づいて深層防護を図るべき」という考えにも共通しているのは、防御壁がしっかりしていれば、潜在的危険性を増しても構わないという、この式に隠

された「価値観」である。この式によれば、典型的には、損害の重大性を補償金額で表したならば、リスクを金額で定量的に捉えることができる。そうすることで、技術的、社会的に質の異なる代替的な安全策について同列に並べて経済的に評価することが可能になる。こうした把握方法が、ビジネスや財政の立場からは、実用性が高いことは明らかである。

だが、このようにリスクを捉えるのは、いわば保険会社の価値観であって事故被害者の価値観とは異なるものである。前者では「大数」の中の 1 件の生命であるが、後者にとっては唯一無二のものである。現代社会において、この根本問題は競争上「不都合な」こととして排除される。利便性のためには仕方のないこととされる。めったに起きないので無いこととされ、起こった時にも時間がたてば忘れ去られていく。少数の被害者の声は圧倒的多数の享受者の声にかき消されてしまう。しかも、被害に遭うまでは通常の間人は後者の側にいる。しかし、高度技術システムの安全について、学問的に論じるために、我々は「数量化」の隠された価値観を相対化しなければならない。

もし、システム事故の発生確率が低くてもゼロではないということで、つまり、防御壁を深層防護でいくら増強したところで想定外の事態で穴が揃う確率がゼロではなく、いつか必ず起こるものと考え、被害者となる可能性のある立場からは、受容しがたい深刻なシステム事故をもたらす潜在的危険性そのものがリスクとみなされる。これも一つの代替的な「価値観」である。この価値観に基づくと、確率について考えることは不要で、被害者となる可能性がある人々が受容できない深刻なシステム事故をもたらす潜在的危険性は、無条件に回避されるべきということになる。注意しなければならないのは、この考えは「絶対安全」を求めるものではない。利便性や他の代替策と比較して受容できる潜在的危険性か否かということである。たとえば、自動車などは、毎日死亡事故があり、相当の危険を伴うシステムであるが、自らが危険をコントロールできる納得感があり、しかも便利なので、多くの人々がこれを受容している。また、航空機については、自らはシステムに安全を任せることになるが、とにかく速い遠距離移動が可能なので、これも受容される。しかし、新幹線にしても航空管制にしても、あるいは原子力発電所にしても、これ以上にそれらの潜在的危険性を増すことは、被害者になる可能性のある人々によって、本当に支持されているのだろうか。被害者になる可能性のない人々も含めて受容度を測ることは、この場合、正しくない。あくまでも、リスク評価において、特に重大なシステム事故を起こし、被害者になる可能性のある人々から受容されないような潜在的危険性の増大は避けべきとする価値観である。

この価値観によれば、[一定の発生確率×受容できる損害重大性] は、[極めて低い発生確率×被害者になる可能性のある人々にとって受容できない損害重大性] と同じになることは決してない。両者は質的に異なるからである。これが、前述の一般的なリスクの数値化に潜んだ価値観との違いである。リスクの数値化の価値観に基づけば、[極めて低い発生確率×被害者になる可能性のある人々にとって受容できない損害重大性] と [一定の発生確率×受容できる損害重大性] がリスクとして等値であると見なされる時には、市場競争

や予算削減で有利となる前項が選ばれる。これが、事例で確認された状況だといえる。この選択は、リスクを増すことではないと見なされているため、「安全に効率向上が図られている」ということになる。しかし、我々が示した代替的な価値観においては、前項と後項は等値ではなく、明らかに前項のリスクは大きくて受容できない。この立場からすれば、市場競争や予算削減を理由に前者を選ぶことは、「効率のために安全を損なう」行為であり、「防御壁の増強こそが危険を増す可能性がある」ということを体現するものだと言える。

このように、一般的なリスクの数量化である〔事故発生確率×損害の重大性〕には、特定の価値観が潜んでおり、それは競争圧力や原価低減圧力のもとで、潜在的危険性を増すバイアスをもたらす。そのバイアスは、潜在的被害者の価値観からすれば、受容できないリスクをもたらすものである。

6. むすびにかえて

現代の高度技術システムには、競争やコスト削減の圧力のもとで、特に自動化の範囲や精度、信頼性が高まると、システムの高速化、高密度化、複合化、巨大化がもたらされ、潜在的危険性が増大するという傾向がある。それを支え正当化するのが、スイスチーズ・モデルの通俗的理解「スイスチーズの穴が揃う可能性を低下させるためには防御壁を増強すればよい」と、定量的リスク・アセスメントの公式〔事故発生確率×損害の重大性〕に潜む「損害重大性は同一数直線上にある数値で表される」という前提である。こうした傾向は、本稿において、新幹線システムや航空管制システムの事例研究で明らかにされた。

しかし、エネルギーの増加と高密度化は明らかに潜在的危険性を増す。一般的なリスク評価の価値観とは異なる潜在的被害者の価値観に基づけば、致命的、不可逆的な被害を増すような高度技術システムはそもそも構築すべきではない。防御策の増強は、「安全な効率化」ということで正当化されているが、実は「防御壁の増強こそが危険を増す」可能性もあるので慎重に考えるべきである。リーズン、ペロー、セーガンなどのあまり知られていない方の主張をもっと議論すべきである。

なお、リーズンは能動的失敗と潜在的諸条件ということで、主に主体の失敗と戦略的・組織的決定の失敗に注目している（Reason 1997, pp.10-11, 邦訳, 12-14 頁）。物的存在への考慮も見られるが、どちらかといえば、誤った物的存在の選択などに注目され、物的存在自体の劣化については、十分に言及されているとはいえない。また、制度的・構造的要因についても、不十分な訓練や使えない手順など、完全な制度が想定されたうえで、それに達しないために事故の潜在的諸条件とされている。しかし、社会的構築物である「制度」に完全や絶対ということは論理的にありえず、制度が設計通りに適用されても、失敗することはある。たとえば、ルールの肥大化による処理の遅れなどである。これらも防御壁の増強に潜む脆弱性の可能性に関わる要因であり今後の議論に加えるべきである。

本稿は、高度技術システムの安全において、特定の価値観と特定の社会構造のもとにお

いては、防御壁の増強と潜在的危険性の増大へのバイアスがかかることを論じた。新幹線や航空管制の事例をエビデンスとしたが未だ不十分である。それぞれの事例において、本稿の主張をさらに強く支持するエビデンスを探る必要がある。また、他の高度技術システムにおいても同様の傾向はあるのかについても吟味する必要がある。さらに、防御壁の増強と潜在的危険性の増大が、避けられたはずのシステム事故の発生や悪化につながることの直接のエビデンスも示せていない。これらは、今後の研究課題である。

(謝辞)

本研究は JSPS 科研費補助金 (基盤研究 (C)) 19530333、同 22530407、科研費助成金 (基盤研究 (C)) 15K03657 の助成を受けている。

また、航空管制に関しては、大阪航空局保安部管制課長 (当時) 三田公靖氏、航空管制調査官 (当時) 永藤成明氏へのインタビュー (2008 年 8 月 27 日)、関西空港管制業務見学及びインタビュー (2008 年 9 月 2 日)、航空保安大学校見学及び校長 (当時) 高岡信氏、管制科長 (当時) 稲光裕士氏、航空管制科副長 (当時) 本庄大輔氏、総務課長 (当時) 古舘康男氏、研究調整官 (当時) 高下尚史氏へのインタビュー (2008 年 9 月 2 日)、大阪航空局保安部技術企画調整課長 (当時) 小笠原弦氏のご調整による大阪空港管制業務およびシステム運用管理センター、飛行援助センターの見学および次席航空管制技術官 (当時) 伊地知章氏、阪康行氏、次席航空管制運行情報官 (当時) 金子勝秋氏、航空管制運行情報官 (当時) 村松敬介氏へのインタビュー (2008 年 10 月 14 日)、航空局システム開発評価・危機管理センターの見学および所長 (当時) 加藤信男氏、統括開発評価管理官 (当時) 畠中耕作氏へのインタビュー (2008 年 10 月 14 日)、関西空港次席航空管制官 (当時) 鳥井良平氏、主幹航空管制官 (当時) 岩田氏、主任航空管制官 (当時) 宮坂氏へのインタビュー (2008 年 10 月 28 日) を実施し、上記各位にご協力をいただいた。記して謝意を示したい。また、神戸大学大学院経営学研究科教授 (当時) 故・村上英樹氏には、上記の大阪航空局における調査について紹介と同行をいただいた。昨年あまりに若く鬼籍に入ってしまった氏のご冥福を心より祈るとともに深く感謝を表したい。

参考文献

Hammer, W. (1980), *Product Safety Management and Engineering*, Englewood Cliffs: Prentice Hall. (高橋恒彦監訳, 小竹重信・杉渕斉訳『製品安全の考え方: 安全を問われる製品責任』, 鹿島出版会, 1988 年)

Hollnagel, E. (2008), "Risk + Barriers = Safety?" *Safety Science*, Vol. 46: 221-229.

Hood, C. (2006), *Shinkansen: From Bullet Train to Symbol of Modern Japan*, London and New York: Routledge.

Perrow, C. (1999), *Normal Accidents: Living with High-Risk Technologies*, Princeton:

Princeton University Press

Reason, J. (1997), *Managing the Risks of Organizational Accidents*, Aldershot: Ashgate (塩見弘監訳, 高野研一・佐相邦英訳『組織事故』, 日科技連, 1999年)

Sagan, S. D. (1993), *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons*, Princeton: Princeton University Press.

Stewart, M. G. and R. E. Melchers (1997), *Probabilistic Risk Assessment of Engineering Systems*, London: Chapman & Hall. (酒井信介監訳, 小林英男ほか訳『技術分野におけるリスクアセスメント』, 森北出版, 2003年)

Weick, K. E. (1990), "The Vulnerable System: An Analysis of the Tenerife Air Disaster," *Journal of Management*, Vol.16, No. 3: 571-593.

Wilson, R. and E. A. C. Crouch (2001), *Risk-Benefit Analysis*, Cambridge (MA): Harvard University Press.

国土交通省 (2016a), 国土交通省ホームページ「航空: 航空保安業務の概要」, http://www.mlit.go.jp/koku/15_bf_000316.html (2016年4月11日閲覧)

国土交通省 (2016b), 国土交通省ホームページ「航空: 関係者の連携~協調的な意思決定(CDM)」, http://www.mlit.go.jp/koku/15_bf_000349.html (2016年4月11日閲覧)

国土交通省航空局管制保安部 (2008), 「航空保安業務の概要 (2008)」。

齋藤雅男 (2006), 『新幹線: 安全神話はこうしてつくられた』, 日刊工業新聞社。

佐藤一男 (2006), 『改訂 原子力安全の論理』, 日刊工業新聞社。

新星出版社 (2007), 『徹底図解: 新幹線のしくみ』, 新星出版社。

園山耕司 (2010), 『図解よくわかる航空管制』, 秀和システム。

谷口勇仁 (2012), 『企業事故の発生メカニズム: 「手続きの神話化」が事故を引き起こす』, 白桃書房。

中西晶 (2007), 『高信頼性組織の条件』, 生産性出版。

中野秀夫 (2014), 『航空管制のはなし (七訂版)』, 成山堂。

原拓志 (2007), 「研究アプローチとしての『技術の社会的形成』」, 『年報 科学・技術・社会』, 16巻, 37-57頁。

原拓志 (2008), 「安全の社会的形成に関する予備的考察」, 『国民経済雑誌』, 197巻, 4号, 31-44頁。

原拓志 (2010), 「技術システムの安全と組織理論」, 『国民経済雑誌』, 201巻, 3号, 31-44頁。

樋口晴彦 (2012), 『組織不祥事研究: 組織不祥事を引き起こす潜在的原因の解明』, 白桃書房。

藤田日出男 (2005), 『あの航空機事故はこうして起きた』, 新潮社。

古田一雄・長崎晋也 (2007), 『安全学入門』, 日科技連。

三戸祐子 (2005), 『定刻発車: 日本の鉄道はなぜ世界で最も正確なのか』, 新潮文庫。

山之内秀一郎 (2005), 『なぜ起こる鉄道事故』, 朝日文庫。

[2016.4.18 1222]