Safety-IからSafety-IIへ
―レジリエンス工学入門―

Erik Hollnagel

Perceive those things which cannot be seen
Miyamoto Musashi (1584–1645)

安全は伝統的に「物事が悪い方向へ向かわない状態」(Safety-I) として定義され，それに対する多種多様な取り組みがなされてきた．しかし，日々複雑さを増している現代の社会工学的システムを鑑みると，このような安全のとらえ方は不十分であると言える．レジリエンス工学が提唱することの一つは，安全を伝統的な旧来の考え方から，「物事が正しい方向へと向かうことを保証する」(Safety-II) という新たな考え方への変革を促すことである．本稿では，安全に対する考え方の歴史的変遷を実例を交えつつ紹介し，レジリエンス工学の目指すところを解説する．

キーワード：レジリエンス，安全，安全管理，リスク管理

はじめに

安全とは，いかなるものも悪い方向に向かわない状態として，伝統的に定義されてきた．より厳密に言うと，いかなるものも悪い方向へ向かわないことを保証することなどは不可能であることを我々はわかっているので，悪い方向に向かうものの数が許容できる程度に少ないときに，そのような状態は安全であると定義することができる．これは，以下の各種の定義からも見て取ることができる．

- 安全とは許容できない危機が存在しないことである．（アメリカ標準化協会）
- 安全とは不慮の事故による損害が存在しないことである．（合衆国医療研究・品質調査機構）
- 安全とは，危険の特定と危機管理の継続的なプロセスを通し，人への危害や財産への損害が許容できるレベルと同等かそれ以下に減らされ，そして維持されている状態である．（国際民間航空機関）

物事が悪い方向へ向かう状況は当然のことながら期待されていない状況であり，またそのような状況は，意図されなく，望まれない損害や損傷に繋がるかもしれないという二つの理由のため，人間の活動に関して，物事が悪い方向へ向かう状況に焦点を合わせるのは良い実践感覚であると言える．物事が悪い方向へ向かう事象は，当初は「神の所行」あるいは「天災」として説明され，それ故，人類の制御を超えたものであるとされてきた．（皮肉にも，「天災」は人間がそれを克服するたびにさらに大きくなっていくように思える．）このような考え方は，人類が徐々に技術を極めるとともに，特に 1750 年頃の第 2 次産業革命[1]の後，変遷していった．人間が行っていた作業の急速な機械化は，その副作用として事故の増大を引き起こした．これらの事故の共通の要因は，科学技術の機能停止，故障，および不具合に帰するものであった．そのため，安全に関する懸念事項は，機械類の保護，爆発の阻止，および構造物の崩壊防止に集中した．問題の発生源，および各種ソリューションの主たる源としての科学技術へのこれらの意識は，1979 年までは成功裏に維持されてきた．しかし，この年のスリーマイル島における原子力発電所の事故は，安全防護に関する技術は不十分であることを実証することとなった．この事故は，人的な要因にスポットライトを当て，潜在的なリスクとして，人的な失敗や人の不調を考慮することの必要性を明らかにした．そのわずか 7 年後の 1986 年のスペー

Erik Hollnagel（エリック・ホルナゲル）
Professor, University of Southern Denmark
Chief Consultant, Centre for Quality Improvement, Region of Southern Denmark
E-mail: hollnagel.erik@gmail.com

[1] 何を“産業革命”と見なすかについては，いくつかの考え方が存在している．ある一つの考え方では，紀元前 3,000～5,000 年の農耕の出現を第 1 次産業革命（これは新石器革命とも呼ばれている）とみなし，18 世紀中盤の蒸気機関の実用化を第 2 次産業革命と見なしている．本稿はこの考え方に基づいて記述している．

スシャトル・チャレンジャー号の爆発事故は，チェルノブイリの事故も相まって，安全の考え方に関して，さらなる変革を迫ることになった．このときは組織的エラーの影響，および経験から得る共通知識に関する安全文化も含まれた．

歴史的に言って，新たなタイプの事故は，因果関係の基本的な仮定の正当性に疑問を呈することなく，新たなタイプの原因（金属疲労，ヒューマンエラー，組織的エラー，複合システム）と適合してきた．我々は事故を原因と結果の関係から説明することに慣れきってしまっているので，もはやそのことを意識することはない．我々はこの伝統に強固にしがみついており，現実と調和させることはますます難しくなってきている．

因果律信条 (causality credo)

事故がどのようにして起こるのかといういかなる説明も，原因が結果にどのようにしてつながるかに関するいくつかの仮定を必ず含んでいる．これは，しばしば事故モデルと呼ばれるものである．最も単純な事故モデルは Domino モデル [1] であり，この考え方はおそらく人類の歴史と同じくらい古くからあるものである．このドミノモデルはシンプルな線形の因果関係を表現しており，それはドミノが次から次へと倒れることと似通っている．これらのモデルのロジックによると，事象解析の目的は，損害から逆方向に推論し，“根本原因”を発見することである．同様に，リスク解析とは何かがそれ自身によって，あるいはほかの失敗や機能不全との組み合わせによって，“壊れる”かどうかを明らかにすることである．ここで，“壊れる”とは，特定の構成要素が失敗したり機能不全に陥ったりすることを意味している．

シンプルな線型モデルは 1980 年代に，複合線形モデルに取って代わられた．複合線型モデルで最も有名なものはスイスチーズモデルである．これらのモデルでは，有害な結果は，能動的な失敗（または安全でない行動）と潜在的な条件（危険）との組み合わせによって説明される．したがって，事象解析とは，低下した防壁や弱くなった防御力が，能動的な（人間の）失敗とどのように組み合わさるのかを探求することである．同様に，リスク解析とは，単独の失敗や潜在的な条件の組み合わせが有害な結果につながる条件を探しだすことに焦点を当てる．ここで，潜在的な条件は，低下した防壁や弱くなった防御力と考えることができる．

ドミノモデルやスイスチーズモデルは事故モデルの典型的な実例であるが，ほかの事故モデルも数多く存在する．これらのすべてのモデルに共通することは，結果はそれに先立つ原因から生ずるものであると理解することができるという暗黙の仮定である．この仮定は因果律の法則における信念，あるいは信条に相当するものであるので，これを因果律信条 (causality credo) と呼ぶことができる．因果律信条は以下のように表現することができる．

- 有害な結果は，何かが悪い方向へ向かうから起こる．有害な結果は原因を持つ．
- 十分な証拠が集められると，これらの原因を発見することが可能となる．ひとたび原因が判明すると，その原因を取り除いたり，隔離したり，あるいは，無力化することができる．
- すべての有害な結果は原因を持っており，また，すべての原因は発見することができる．したがって，すべての事故は防止することができることになる．これは，多くの企業が魅力的だと考える，事故ゼロ，損害ゼロというような構想である．

このような方法での推論は比較的シンプルなシステムにとっては妥当であるかもしれないが，より複雑なシステムにとっては十分とは言えないものである．そして，現代のほとんどのシステムは複雑でないというよりは複雑であるので，1984 年に Perrow が指摘したように [2]，因果律信条はもはや有効とは言えない．

Safety-I: 物事が悪い方向へ向かうのを避ける

安全の考え方の歴史的な発展は，因果律信条と相まって，図 1 で示される考え方につながっていく．この考え方によると，許容できない結果はそれに先行する失敗や機能不全が原因で発生し，その一方，許容できる結果は人を含めたすべてのものが期待どおりに機能しているから起こると見ることができる．これは，“相違原因仮説 (hypothesis of different causes)”と呼べるものである．つまり相違原因仮説とは，有害な事象の原因や“メカニズム”は，うまくいった事象のそれとは異なっているという仮説である．うまくいかないケースに該当しない場合，このような原因の除去やメカニズムの無効化は，物事が正しい方向に向かう確率を下げることにもなり，つまり逆効果になってしまう．

安全は伝統的に有害な結果（事故，偶発的な事象，ニアミス）が可能な限り少ない状態であると定義されてきた．これは，Safety-I と呼ぶことができる．安全管理の目的は，結果としてこのような状態を達成し維持することである．この安全の定義はシンプルである．しかしながら，安全でない状態，つまり安全が達成でき

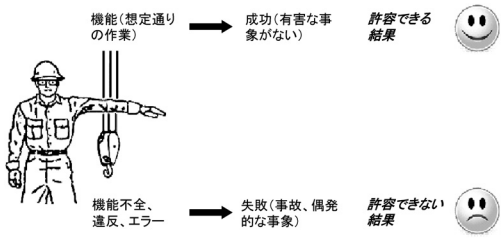

図 1　Safety-I における失敗と成功の考え方

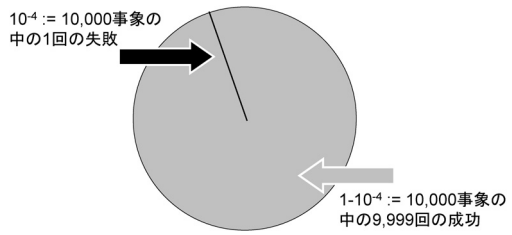

図 2　正しい方向へ向かう事象と間違った違った方向へ向かう事象の不均衡

ていない場合に何が起こるかによって安全が定義されているので，この定義は問題をはらむこともある．またこの定義において，安全はその存在ではなく，またその質でもなく，安全でない場合に引き起こる結果によって間接的に評価される．

Safety-I においては，システムはうまく設計され，また細心の注意を払って維持管理されており，各種の手順や手続きは完全で正しく，設計者は比較的重要でない偶発的な事象さえも前もって予測し見通すことができ，人々は期待されたとおりに行動するので（さらに重要なことだが，人々は教育されたとおりに，あるいは訓練されたとおりに行動するので），システムは正しく機能するということを暗に仮定している．これは，仕事が実施される方法において，コンプライアンスが重要視されることに不可避的につながっている．

何が正しい方向に向かうかを見るよりも，何が悪い方向に向かうかを見る

レジリエンス工学では，Safety-I の考え方は簡略化しすぎであり，間違っていると考える．レジリエンス工学は，相違原因仮説は採用せず，その代わりに，物事が正しい方向へ向かうことと，物事が悪い方向へ向かうこととは，基本的に同じ方法で起こると考える [3, 4]．つまりこれは，許容できる結果がどのようにして起こるかをまず最初に理解しなくては，許容できない結果がどのように起こるかを理解することなどできないということを意味する．図 2 は，物事が正しい方向へ向かうことを観察することよりも，物事が悪い方向へ向かうことを観察した場合の帰結を示している．この図は，失敗の（統計的な）確率が 10,000 分の 1 の場合の例を示している．言い換えると，何かが悪い方向へ向かうこと（黒い線の部分）が一度起こるごとに，物事が正しい方向へ向かい，望ましい結果につながること（灰色の部分）が 9,999 回発生することになる．

悪い方向へ向かうものへ焦点を当てることは，規制をかける者や，権威ある者によって求められている．また，数え切れないほどのデータベース，論文，書籍，また学術会議の予稿集に記載されているモデルや方法論によっても支持されている．これらの最終結論は，どのようにして物事が悪い方向へ向かうかについてと，このような出来事を避けるために何をなすべきかについての両方に関する情報であふれている．また，これらの方策は，失敗と機能不全を見つけ，原因の究明に努め，原因を取り除き，また障害を改善することに努めるということであり，つまりそれは“発見と修正”として知られる単純な原理原則である．

何かが正しい方向へ向かうとき，つまり 10,000 事象のうちの 9,999 事象の場合になると，状況は大きく異なってくる．物事が正しい方向へ向かうことへ焦点を当てることは，ほとんど奨励されない．それは，権威ある者によって要求されることはなく，人間や組織的なパフォーマンスがどのように成功するかに関する理論やモデルはほとんどない．また，どのようにしてそれが起こるのかを研究するための手助けになる方法論もほとんどない．実データを見つけるのは困難であり，論文や書籍，またほかの形式の科学的な文献を見つけるのも難しく，それに価値を見いだしている人もほとんどいない．別の言い方をすると，なぜ物事が悪い方向へ向かうのかを理解するための取り組みには多くの時間が費やされてきたが，なぜ物事が正しい方向へ向かうのかを理解するための取り組みはほとんどなされてこなかったということである．我々は，安全の存在よりも，安全の不在について研究しているのである！

なぜ物事は正しい方向へ向かうのか？

レジリエンス工学では，システムが正しく機能するのは，人々が作業内容を作業環境に合わせて調整することができるからであると提唱する．人々は，設計上の不備や機能上の欠陥を特定し，問題を解決する方法を習得する．そして，実際の要求を認識し，自らの行動をそれに合わせて調整し，また，条件に合わせるように手順や手続きを解釈し適用する．さらに，何かが

悪い方向へ向かおうとしているとき，人々はそれを検知し，修正することができる．そのため，状況が深刻になる前に，介入することができる．これは，行動の可変性として説明することができる．行動の可変性とは，規範や標準からの逸脱といった悪い意味ではなく，安全や生産性にとって必要なスムーズな調整という良い意味あいである．

行動の可変性，あるいは行動の調整は，今日の社会工学的システムの機能にとって必須の要件である．行動の可変性は，望ましく許容できる結果に作用する．したがって，行動の可変性を取り除いたり制約をかけたりすることによって，許容できない結果や失敗を防ぐことはできない．それに代わり，ある状況におけるリソースや制約を明確に提示し，また，行動の結果をより予測しやすくすることによって，必要となる行動の調整を促進するための取り組みが必要となる．行動の可変性は，それが間違った方向へ進んでいると思われるときは弱める方向に，またそれが正しい方向へ進んでいると思われるときは強める方向に管理されるべきである．それを達成するためには，まず最初に行動の可変性が避けられないことであり，必要であることを認識し，次に監視し，そして制御することが必要である．

Safety-II: 物事が正しい方向へ向かうことを保証する

とりわけ強力な情報技術の魅力のおかげで，私たちを取り巻く社会工学的システムは発展し続け，より複雑になってきている．そのため Safety-I のモデルや方法論によって必要とされ，また熱望されている“安全な状態”を実現することは，ますます難しくなってきている．Safety-I における各種手法をさらにいっそう無理に使い続けるよりも，安全の定義を“何かが悪い方向へ向かうのを避ける”から，“すべてが正しい方向へ向かうことを保証する”へと変えることもできる．より正確に表現すると，意図され許容できる結果（これは日々の活動と言うこともできる）の数をできる限り高められるように，変わりうる状況下で成功する能力を伸ばすことに注力するということである．これを Safety-II と呼ぶことができる（図 3）．安全の基礎，安全管理は，今日に至っては，なぜ物事が正しい方向へ向かうのかを理解することになっている．つまりこれは日々の活動を理解することを意味する．

結果によらず，基本的にすべてのことは同じ方法で起こっているので，物事が悪い方向へ向かうこと（事故や偶発的な事象）と，物事が正しい方向へ向かうこと（つまり日々の作業）とに異なる原因やメカニズムを考えることはもはや必要ない．安全管理の目的は，後者（物事が正しい方向へ向かうこと）を保証することである．そして，そうすることによって前者（物事が悪い方向へ向かうこと）を減少させることである．したがって，Safety-I と Safety-II は，いずれも望まれざる結果を減少させることにつながる．しかし，それらは根本的に異なるアプローチを取っており，生産性や質はもちろんのこと，どのようにプロセスが管理され評価されるかに重大な影響を及ぼす．

Safety-II の考え方によると，安全管理の目的はできるだけ多くのものが正しい方向へ向かうことと，毎日の作業が所期の目的を達成することを保証することである．これは，何かに反応するだけでは達成することはできない．なぜなら反応とは，起こったことを修正するだけだからである．そうではなく，安全管理は事前対策的でなければならない．これを機能させるためには，許容できる見込みのもとで何が起こりうるかを

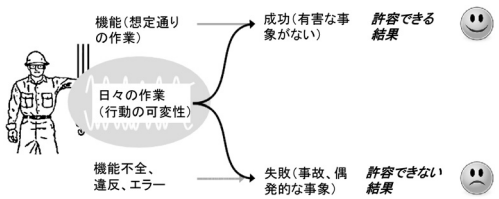

図 3　Safety-II における失敗と成功の考え方

表 1　Safety-I と Safety-II との主要な差異

	Safety-I	Safety-II
安全の定義	悪い方向へ向かう物事ができるだけ少ないこと	できるだけ多くのことが正しい方向へ向かうこと
安全管理の原則	何かが起こったときに，反応し，応答する．	事前対策的，発展や事象を予期するように努める．
事故の説明	事故は失敗や機能不全が原因で起こる．	結果によらず，物事は同じ方法で起こる．
ヒューマンファクターの見方	責任	資源

予見し，何らかの対策を講じるために適切な手段（人と資源）を持つ必要がある．そのためには，どのようにシステムが動作するかを理解し，環境がどのように発展し変わっていくかを理解し，各種の機能がどのように相互依存し影響をしあっているのかを理解する必要がある．この理解は，個々の事象の原因を探求するよりも，複数の事象にまたがるパターンや関係を探求することで深まっていく．このようなパターンを発見し理解するためには，すべての資源を障害からの復旧に使うよりも，何が起こったかを理解することに時間を費やすことが必要である．

おわりに

Safety-I と Safety-II を対照比較させることで，それらに基づく安全管理の結果をより明確にすることができる（表 1 参照）．

Safety-I のアプローチから，Safety-II のアプローチへの発展は，単純でもないし，短時間でなされるものでもない．しかし，どのようにして始めたらよいかの，いくつかの実務的な提案は以下のように与えられる．

- **悪い方向へ向かうものだけでなく，正しい方向へ向かうものを見よ．**人々は状況の求めに応じて目的にかなった調整をするので，物事は正しい方向へ向かう．これらの調整がどのようなものであるかを確かめ，そしてその調整から学べ！
- **何かが悪い方向へ向かったときは，具体的な原因を探すよりも，毎日の行動の可変性を探れ．**何かが達成されたときはいつでも，それは以前に試行されたということを意味し，つまり安全策になる．人々は，どのような行動の調整が正しく機能するかを素早く学び，すぐにそれを信頼するようになる．正確には，行動の調整が正しく機能するからである．したがって，いつもと同じように物事を行う人を非難することは，逆効果と言える．
- **定期的に何が起こっているかを観察し，どのくらい重大かよりも，どのくらいの頻度で起こっているかに基づいて，事象に注目せよ．**まれにしか起こらないものよりも，頻繁に起こるものに対して備えるほうがはるかに簡単である．例外的な行動に関する大きな改善よりも，毎日の行動に関する小さな改善のほうが重要なこともある．
- **考え，学習し，情報交換する時間を考慮に入れよ．**もしすべての時間が収支を合わせるために使われるのならば，（状況をどのように理解するかを含めて）経験を共有したり，リソースを補給したりする時間はない．
- **失敗の可能性に対して過敏であり続けよ，そして気を配り続けよ．**望ましくない状況について考えるように努め，どのようにして望ましくない状況が起こるかについて想像せよ．望ましくない状況の発生を防ぐ方法を考えるか，あるいはそれを認識しそれに対して反応する方法を考える．これは，事前対策的な安全管理の本質である．

我々の存在が依拠している社会工学的システムはますます複雑になり続けており，Safety-I のアプローチを使い続けることは長い目で見れば不十分なものになる．しかしながら，これから先の方法は，Safety-I を Safety-II で完全に置き換えるというよりも，これら二つの考え方を組み合せることにある．Safety-II とは，安全とは何かに関する最初の，そして第一の異なった理解である．したがって，慣れ親しんだ多くの方法論や技術を適用するための異なるやり方でもある．正しい方向に向かう物事を観察し，どのように物事が機能するかを分析し，そして行動の可変性を単に制限するのではなくそれを管理するためには，Safety-I の方法論に加え，Safety-II 自身の方法論も必要になってくるだろう [5]．単に物事が悪い方向へ向かうのを阻止するだけでは，物事を正しい方向へ向かわせることはできない．日々の行動の本質を理解し，直接観察することができない物事を如何にして知覚するかを学ぶことによってのみ，我々は物事を正しい方向へ導くことができるのである．

（訳：吉住貴幸　日本 IBM（株）東京基礎研究所）

参考文献

[1] H. W. Heinrich, *Industrial Accident Prevention: A Scientific Approach*, McGraw-Hill, 1931.

[2] C. Perrow, *Normal Accidents*, New York: Basic Books, 1984.

[3] E. Hollnagel, D. D. Woods & N. Leveson（編著），北村正晴（監訳），『レジリエンスエンジニアリング―概念と指針―』，日科技連出版社，2013（原書 2006）．

[4] E. Hollnagel, J. Paries, D. D. Woods & J. Wreathall（編著），北村正晴，小松原明哲（監訳），『実践レジリエンスエンジニアリング，社会・技術システムおよび重安全システムへの実装の手引き』，日科技連出版社，2014（原書 2011）．

[5] E. Hollnagel，『社会技術システムの安全分析：FRAM ガイドブック』，海文堂出版，2013.