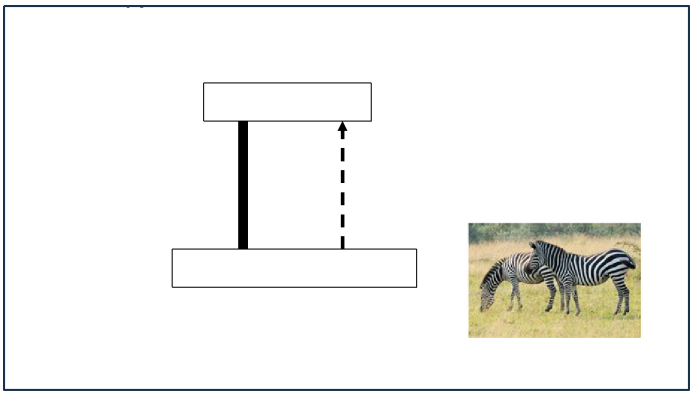
タイトル：STAMPのキーワード　複雑性と創発とは？

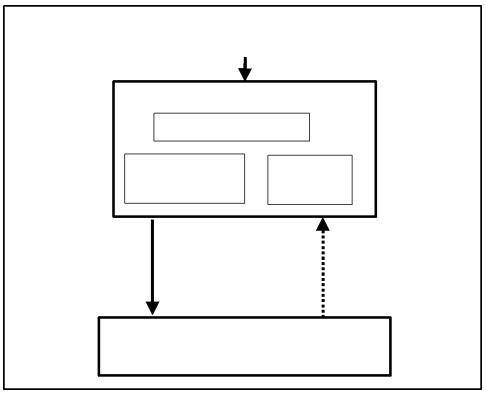
まえがき

STAMP(システム理論に基づく事故モデル)の名称に込められた「システム理論」の意味を紹介したい。ナンシーレバソン教授のSTAMPの講演が日本で初めてなされた2015年頃、「創発とは何か？」「複雑システムと何か？」という疑問が多くなされた。同教授の著書（邦訳：システム理論に基づく安全工学、2024年）の第3章には、システム理論の発祥の経緯と概要がまとめられているが読み飛ばされた人も多いのではなかろうか。システム理論は、熱力学で言うエントロピー増大の法則（閉システムにおいては全ての秩序は無秩序に向かう）に反して、「生物は何故安定した秩序を伴う形態を維持できるのであろうか？」という疑問へ応えるための学問体系といえる。開放系（エネルギーの流出入がある系）においては、エントロピー増大の法則に反してある秩序を持った形態を維持できるというシステム理論の考え方が1950年前後に、ルートヴィヒ・フォン・ベルタランフィにより提唱され、ノーバート・ウィーナーはこのアプローチを制御・通信工学に適用し注目されている。また、イリヤ・プリゴジンは、非平衡熱力学の体系をまとめ、特に散逸構造の理論で1977年のノーベル化学賞を受賞している。

創発と安全性

前記の第3章には、創発の例として、何故リンゴは硬い実を持つのかという疑問にならって説明をしているが、もう少しわかり易い例として、「何故シマウマは縞々の模様を持っているのか（下図）」という例で説明したい。シマウマの表面の色素細胞は、それぞれの細胞での色素の生成反応と、色素の細胞間の拡散による散逸の相互作用で縞模様のパターンが出来上がる。これは、「反応拡散モデル」としてモデル化され、発生したマクロなパターンは、自己組織化や創発（Emergence）現象と呼ばれる。このようなマクロなパターンが環境に隠れやすく生存競争に適しているということは、シマウマの個々の細胞自体は全く意識していないが、細胞全体としては、マクロな特性が出現するため、これを「創発」と呼んでいるのである。一方で、このような特性のシマウマが生き残ってきたのは、自然界の進化という上位のシステムからの要求（安全制約）でもある。これが、STAMPのコントローラと被コントローラの間のコントロールアクションとフィードバック（含む創発特性）という基本モデルになっている（下図右側）。





前記のナンシーレバソン教授の著書では、下記のように複雑システムの安全性に関する基本的な考え方が述べられている。

「安全性は,システム全体の状況（context）を考えることによってのみ定義可能なのである.たとえば,あるプラントが安全性の許容範囲を満たすかどうかは,バルブ1つ1つを調べてみても判断できない.バルブがどのような状況で使用されているかという情報なしに,「バルブの安全性」について述べても意味がない.安全性は,バルブと他の構成機器との関係性によって決まるのである.別の例を挙げると,たとえばパイロットが着陸時に行う手順がある.その手順が,ある航空機やある状況下では安全であったとしても,状況が違えば安全とは言い切れない.」

プラントの安全性は個々のバルブを調べても判断できず、バルブと他の構成機器の関係性によって決まるという主張を、前記の創発特性と重ねると、「安全性は創発である」ということが理解できよう。

ただし、実務的にこの創発特性を扱おうとすると、もう少し正確に理解しておく必要がある。米国のモビリティ専門家を会員とする非営利団体SAE（米国自動車技術者協会）が発行している安全規格レポートSAE J3187では、事故を下記のように分類している。Known Knownsとは、自身が知っていると認識している知識（事故に関する）のことで、下記の四つに分類できる。このレポートでは、(B)-(D)を創発事象と考え、この領域の事故をできるだけ少なくすることが大事であり、そのためにSTAMPの理論を役立てることを目指している。ナンシーレバソンの著書には、様々の現実の事故事例が、その分析結果とともに紹介されているが、そのほとんどは、（B）や（C）に分類される。つまり、事故が起こってみれば、「なんだ、知っていたことではないか（ポカミス）」(C)とか、「未知の領域があると知ってはいたがまさかそれが起こるとは思っていなかった」（B）といったことに気づく。しかし、た

まに、「想定外のことが起こるとは知らなかった」(D)もあり、その原因究明には多大な時間や再現実験が必要とされることもある。いずれにしても、我々は多くの事故から学んで、安定したシステムを作ってきたことも事実である。「創発事故だから仕方ない」と単純にあきらめてはいけない。

- 既知の既知（Known Knowns）：知っていると知っていること
- 既知の未知（Known Unknowns）：知らないと知っていること
- 未知の既知（Unknown Knowns）：知っていると知らないこと
- 未知の未知（Unknown Unknowns）：知らないと知らないこと

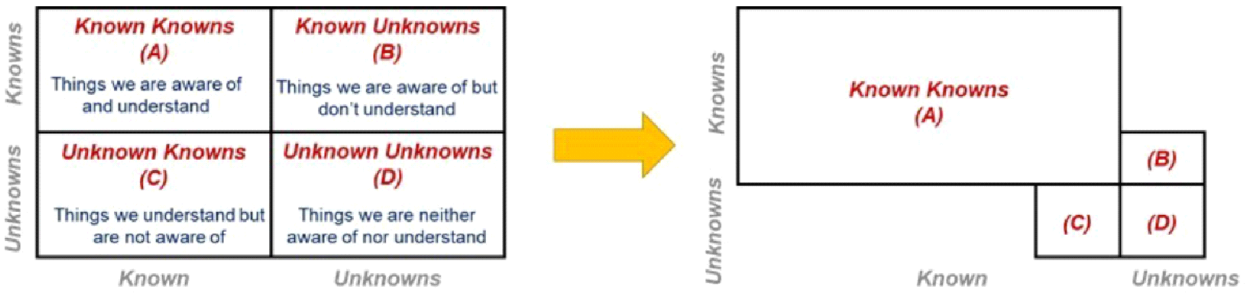


Figure 20 - Scenario quadrant with understanding and awareness as axes

<u>複雑性と安全性</u>

まえがきで述べたように、「複雑性とは何か？」という質問を多く受けたことがある。人によって受け止め方が違うことを実感したが、前記の著書第1章では、近年の大規模システムの複雑性に関して、次のように述べている。

> 「複雑性の増加と結合の増加：複雑性にはさまざまな形態があるが、私たちが構築しようとしているシステムでは、そのほとんどが複雑化する傾向にある。たとえば、①**<u>インタラクティブな複雑性</u>**（システムコンポーネント間の相互作用に関連）、②**<u>動的な複雑性</u>**（時間の経過に伴う変化に関連）、③**<u>分解的な複雑性</u>**（構造分解が機能分解と一致しない場合）、④**<u>非線形な複雑性</u>**（原因と結果が直接的または明白な方法で関連していない場合）などがある。システムの運用は、一部の専門家以外には理解できないほど複雑なものもあり、そのような専門家でもシステムの潜在的な振る舞いについては、不完全な情報を持っている場合もある。問題は、私たちが自身の知的管理能力を超えるシステムを構築しようとしていることである。つまり、システムのあらゆる種類の複雑さが増すと、設計者がシステムの潜在的な状態をすべて考慮すること、そして、オペレーターがすべての正常・異常の状況や外乱を安全かつ効果的に処理することが難しくなる。実際、複雑性とは、知的管理能力不能（intellectual unmanageability）と定義することすら可能である。」

システムが大きくなれば複雑になるのは当たり前ともいえるが、近年のシステムの特徴は、コンピュータ（特にソフトウェア）とネットワークが大幅に採用されていること、人と機械の協調制御がより複雑になっていること、社会からの目（監視）がより厳しくなっていることなどである。ただ、このような一般論だけでは複雑性の安全への影響を低減するための手段を設計する参考にはしにくいので、上記の4種の分類にそって複雑性を考えてみよう。

まず、コンピュータとソフトウェアの大幅な性能向上である。これにより、一つのコンピュータで複数の機能を果たすようになり③の複雑性がでてくる。安全分析を従来の構造分解だけに頼れなくなり、機能分解をきちんとし、その機能のあいだの干渉（共通原因故障）への配慮をより慎重に行わなければならない。

また、AI技術などの進展は、人と機械（コンピュータ）の対話を複雑にする（①、②の複雑性）。HMIを、Human-Machine Interfaceから、Human-Machine Interactionへと考え方を変えないといけなくなっている昨今の事情もここにあるといえよう。特に、安全への責任を人と機械のどちらが取るかは、状況により（動的に）変化するので、従来型のFTAのような安全分析では網羅的な予測ができにくくなる。コントローラと被コントローラの役割が動的に逆転するという問題も、自動化の進展で人（運転員）の技能が落ち、並行して、AIやセンサー技術の進展でコンピュータ側の能力が向上してゆくと、人とコンピュータの責任の取り方の考え方を変えないといけなくなる。2002年にドイツで起こったユーバーリンゲン空中衝突事故の事例は、この典型例であり、前記著書でも引用されている。管制官、2機の航空機のパイロット、2機の衝突防止システムTCASの間の相互のインターラク

ションのミスマッチにより発生した。従来型の安全分析でどこまで改善できるか、STAMP／STPAによる安全分析でよりよい改善策が創出できるかなど課題は多い。自動車の自動運転などでは、特に故障などの緊急時に、運転者とコンピュータの間のインターラクションやコントロールアクションの動的な逆転などを可視化して、納得した上での運用に移行することも大事であろう。動的な安全責任の移行は、どんなシステムでも起こり、事故の原因になり得る。

④の非線形複雑性は、原因と結果が明白な形で結びつかない場合で、複雑なソフトウェアで安全を制御する際にしばしば起こり得ると考えられる。特に、AI応用のシステムでは、事故が起こった場合に、その原因にAIアルゴリズムが係っているとしたら、それを明確な形で説明することが大事になる。原因と結果をブラックボックスとして結びつけることだけは避けないとならない。

<u>あとがき</u>

STAMPの基礎となっている「システム理論」について、見逃している人も多いと思い、簡単な解説を試みた。実務的には、創発というキーワードでとどまるのではなく、Known Knownsでの4つの分類のように創発事故をより具体的に分解して考えてみることが大事であろう。また、「複雑性」に関しても、ナンシーレバソン教授の著書にあるような4つの複雑性（もちろん、他にも分類方法はあると思われるが）に着目して、安全設計時の課題を分析してみることも大事な視点かもしれない。

このような課題にはSTAMPの考え方、特に、安全の可視化を通したステークホルダー間での課題の共有が大事になるのではなかろうか。

以上（2025/8/22　兼本　茂）