# タイトル:STAMPはSTPAによる安全分析だけではない

**まえがき**

STAMP(システム理論に基づく事故モデル)では、STPAという新しい安全分析手法に注目が集まっており、日本の中で公開されている応用事例は、そのほとんどがSTPAに係るものである。ナンシーレブソン教授の著書(邦題:システム理論による安全工学、共立出版、2024年)の第8章にあるように、

「STPAを開発した最大の理由は、STAMPで識別された、旧来の手法(補記:FTA, ETA, HAZOP, FMEAなどを指す)では扱えない新たな因果要因を含めるためである。具体的には、**ソフトウェアの欠陥も含む設計エラー、コンポーネントの相互作用による事故、認知的に複雑な人間の意思決定エラー、事故に影響する社会的、組織的、管理的要因**などをハザード分析手法に含めるためである。」

とあるのが大きな理由である。

一方で、同著書の第14章では、米国海軍の原子力潜水艦のSUBSAFEプログラムがSTAMPの思想を体現した大きな成功事例として紹介されている。このSUBSAFEは、1963年の原子力潜水艦スレッシャー号での民間人まで巻き込んだ沈没事故を契機に開発された安全管理プログラムで、STAMP理論の発表よりはるかに前に開発されたものである。事故後半年足らずで開発されたプログラムにも関わらず、その後の80年にわたって、原子力潜水艦の致命的な事故を防いでいる。このプログラムの大きな特徴は、潜水艦の設計・製造に係る機械的な安全機構だけでなく、設計から運用まで含めた安全管理の組織的要因まで立ち入って、事故の分析結果に基づいた安全管理システムを構築していることである。

このSUBSAFEで、STAMPの安全思想を体現していることは既に述べたが、その中でSTPAのような安全分析手法の全ては使われていない。ここで述べられているのは、安全目標の峻別と、個々の組織・コンポーネントの安全責任と相互の関係だけである。つまりは、安全目標と安全責任を明示化した制御構造図が、複雑で大きなシステムの安全を保つために必要ということであり、STPAの第3、4ステップまで立ち入らなくても、十分にSTAMP理論の利用価値があるということである。

SUBSAFEプログラムの成功の要点

SUBSAFEの成功の基礎となる考え方で大事なものの一つは、システムの安全目標を次のように絞り込むことであった。

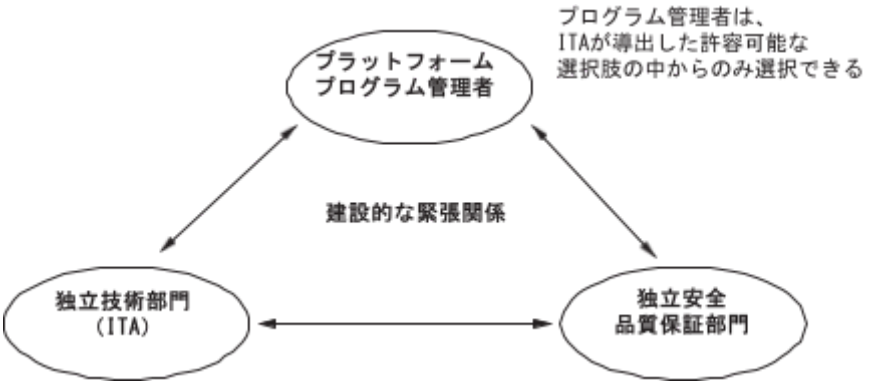
- 潜水艦の船体の防水の完全性
- 浸水ハザードのコントロールと回復のために重要なシステムの運用性(operability)と完全性(integrity)(注:ここでのサブシステムの運用性と完全性とは、事故の際に中央制御室から遠隔で制御できることと考えてよい)

この安全目標を峻別することの大事さを、上記著書では、以下のように表現している。

『焦点を絞ることによって、SUBSAFEプログラムは、この明記された目的以外に焦点を広げたり弱めたりすることはない。たとえば、ミッションの達成は大事ではあるが、SUBSAFEの焦点ではない。同様に、火災安全、兵器の安全、労働者の安全衛生、原子炉システムの安全はSUBSAFEには**含まれない**。』

二つ目の大事な特徴は、「**権力の分離**」と呼ぶ独自の管理体制である(原著　図14.2)。わかりやすく言い換えると、**3本脚の腰掛**のように、独立した脚(権力)で安全を支える仕組みである。安全管理の責任は3つの組織に分割され、チェックアンドバランスシステムを可能にする。相互に独立というだけでなく、「建設的な緊張関係」という協調関係もある。権力的に上位に見えるプログラム管理者は、ITAと呼ばれる技術部門が導出した許容可能な選択肢の中からのみ選択するような縛りをいれることで、独裁的な管理を防ぐことができる。

図14.2　SUBSAFE 権力の分離「3本脚の腰掛」



三つ目の大事な特徴が、「SUBSAFEコンプライアンスコントロールストラクチャーにおける責任の割り当て」である。（原著　図14.4）これが、STAMPの制御構造図に相当する。各コンポーネント（組織）の安全責任が明記されている。原著の中ではその詳細が述べられているが、ここでは朱筆で記した請負業者および造船所の「地方政府の監督権限への認証作業」という安全責任に着目したい。これは、上位にあたる地方政府の監督部門への下位からの制御指示（コントロールアクション, CA）である。下位から上位への制御指示をSUBSAEF安全管理プログラムに明記することは、現場と管理部門の風通しを良くする画期的な方法ともいえる。日本的な管理では、「目安箱」や「相互交流」といった形で、本社―元受け―孫請けなどの組織の間の風通しを良くする方策が良く見られるが、これを制御指示（CA）という形でより能動的にしたものである。能動的な指示であれば、これに対する明確な回答（フィードバック）が必要となり、場合によっては、安全管理違反という過失責任が問われる。第三者の立ち入り調査による指摘ではなく、組織自身による安全管理責任が明記されているところが大きな特徴といえよう。

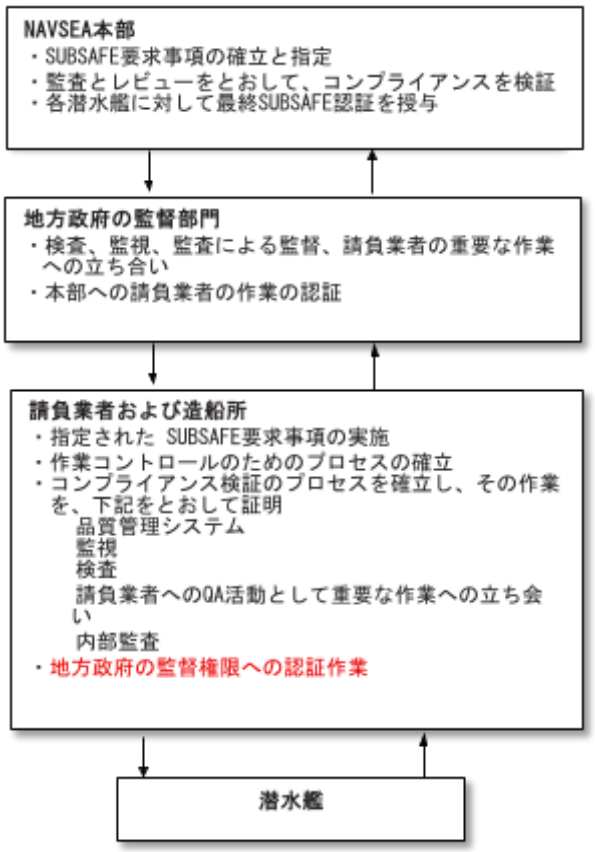



図14. 4　SUBSAFEコンプライアンスコントロールストラクチャーにおける責任の割り当て

## あとがき

安全目標と安全責任を明示化した制御構造図だけでも、複雑な組織・システムの安全管理に大きき寄与できる事例を示した。第1～4ステップまであるSTPAの手順の一部だけを使うことで、システム全体の安全管理を俯瞰的に可視化でき、安全管理に大きく寄与できると考えられる。大きなシステムに係る組織構成員全員が、このような安全目標と制御構造図を用いて安全責任を共有することが大事ということである。

STPAのステップ3、4、さらに、これに続く安全方策の立案を実行するのはかなり大変な作業になるし、その推論過程を組織全員で共有するのは極めて困難になるが、最初のステップ1、2から取り掛かることで、組織全体での安全意識を共有可能になるのではないか。

以上（2025/8/22　兼本　茂）