IoT時代の安全安心に向けて

システム理論に基づく新しい安全性解析手法STAMP/STPA

SEC調査役 三原 幸博　SEC調査役 石井 正悟　SEC調査役 十山 圭介
SEC研究員 松田 充弘　SEC調査役 三縄 俊信　SECシステムグループ主任 八嶋 俊介
SEC研究員 金子 朋子

近年の我々の生活に満ちあふれている車や列車、航空機、ロボット、家電製品などの工学システムは、その内部にコンピューターと無線ネットワーク機能を持ち、高度なソフトウェアによって制御されているが、これらはますます大規模化・複雑化しつつある。IoT、AI※1の時代と言われるゆえんである。しかし既存の安全性解析手法や安全規格は、このような複雑システム、とくにソフトウェアの安全性評価に対応できていない。そこで、マサチューセッツ工科大学(MIT)のNancy Leveson教授は2012年に、新しい安全性解析手法としてSTAMP/STPAを提唱した。欧米では産業界へのSTAMP普及が進みつつあるが、日本では認知されているとは言えないのが現実である。そこで、IPA/SECではIPA/SECでは日本でのSTAMP普及を目指して活動している。

1 STAMP/STPAとは

従来のシステムの多くは、ハードウェア機器がシステムの基幹を担う要素となっていた。それ故、アクシデントは、機器の故障や人間のオペレーションミスが根本原因であり、それがほかの機器や人間に伝搬し、最終的にアクシデントに至るものと捉えられていた。その延長で、従来の安全分析では、システム構成機器を組み合わせたものをシステム全体と捉えて分析していた。

しかし、近年は、システムの基幹を担う要素がソフトウェア中心に変化すると共に、システムにかかわる要素(人、ソフトウェア、ハードウェア)も爆発的に増大してきた。そのため、要素間の相互作用も複雑になり、個々の要素の役割を理解しただけでは、もはやシステムを理解できなくなった。そして複雑なシステムにおけるアクシデントの原因は、一つの構成要素に限定できる要因だけではなく、複数の要素間の相互作用による要因も考えなければならなくなった。

このような状況において、Leveson教授は、現代のシステムのアクシデントの多くは、システム構成要素の故障によって起きるのではなく、システムの中で安全のための制御を行う要素と制御される要素間の相互作用が働かないことによって起きるという「STAMP：システム理論に基づくアクシデントモデル」を提唱した。

STAMPはアクシデントを説明するモデルである。STPAはSTAMPをベースとしたハザード分析手法である。従来のハザード分析手法と比べて**STPAは、複雑なシステムの「ソフトウェアの要求・設計ミス」を識別するのに適したもの**とされている。

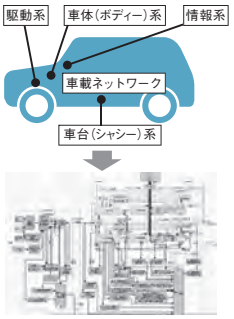

図1　システム中心の安全分析

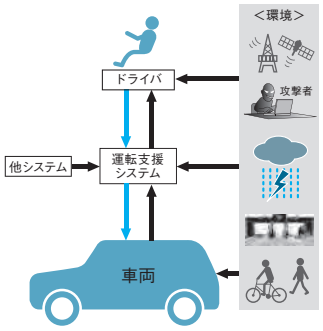

図2　システム理論に基づく安全分析

2 はじめてのSTAMP/STPA

IPA/SECは、2016年4月にSTAMP初心者向けにSTPA手順を解説する「はじめてのSTAMP/STPA」を発行し※2、多くの産業界の方々に参考にされている。

本書では、国内で実際に運用されている鉄道踏切制御装置にSTAMP/STPAを実施し、勘違いしやすい点や理解しにくい点についての注意や導入の勘どころをSTAMP/STPAの手順に沿って具体的に解説しており、初心者向け入門解説書として有用な一冊である。

図3　はじめてのSTAMP/STPA

3 はじめてのSTAMP/STPA(実践編)

「はじめてのSTAMP/STPA」では基本的な考え方と教科書に近い応用事例を中心に解説したが、2017年3月に公開した「はじめてのSTAMP/STPA(実践編)」※3では、産業界でのニーズを考慮した多様な事例についての安全分析を試みた。ここで取り上げた事例は、いずれも教科書で例示されているような標準的な制御構造とは異なっており、それぞれに分析の工夫をしている。

図4　はじめてのSTAMP/STPA(実践編)

3.1. フィードバックがない「とりこ検知」事例

Control loopに着目すべしと言われても、Feedbackがないからloopがないんですけれど・・

この事例の安全制御構造にはフィードバックがほとんど存在しない。フィードバックを持たないことは、一般的に安全の阻害要因であるが、その逆にもなり得る。この分析結果は、その両面を考えるきっかけになるであろう。この事例では、フィードバックがないことがむしろ安全上の強みになっている。

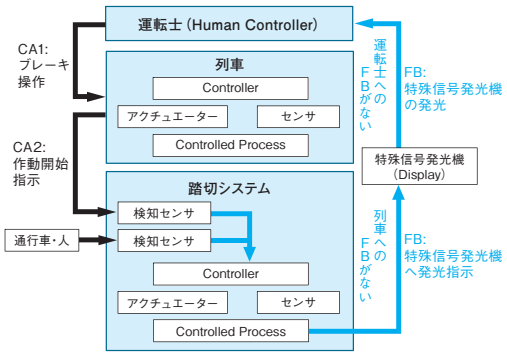

図5　フィードバックのない事例

3.2. 組織や人が絡む業務ワークフロー事例

心配なのはコンピューターやメカじゃないんですけれど・・

安全分析したい対象システムが必ずしもコンピューターシステムとは限らない。この事例では、踏切工事にかかわる人・組織、そしてその業務を分析対象とした。この事例では、コントロールストラクチャー図を書くことによって、制御行動の抽出不足に気づきやすくなった。

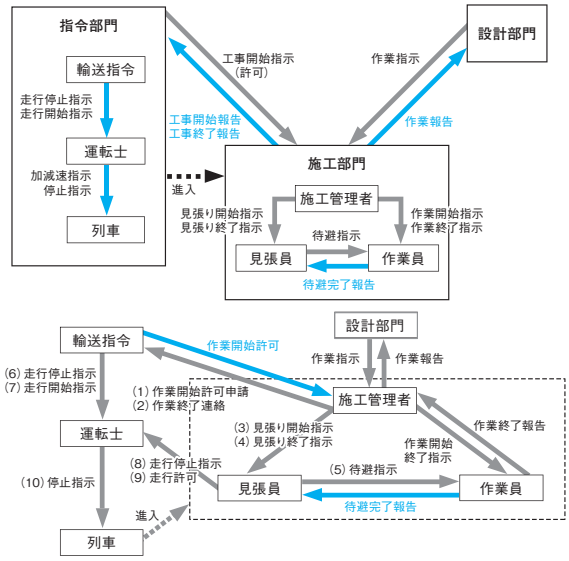

図6　視点を変えた2つのコントロールストラクチャー

3.3. エンタープライズ系の「ネット通販」事例

STAMPを適用したいのは制御系じゃないんですけれど・・

この事例の分析では、識別された2つのコントロールアクションが、別々のアクションのままでは安全ではなく、1つの不可分なアクションにまとめられる必要があるという結論に至った。この分析の結果、「損失防止」のための新たな制御行動の欠陥を見つけることができた。

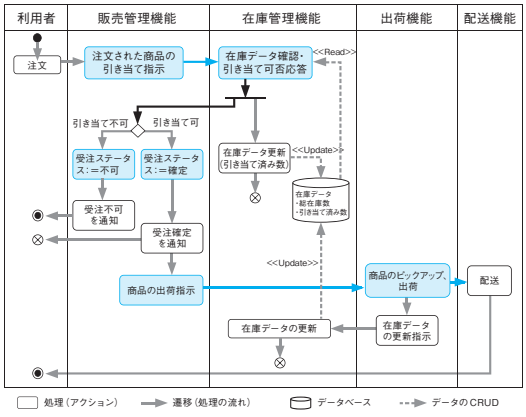

図7　ネット通販の事例

3.4.「機械 対 機械」以外の要素に対するヒントワード

「人」へのヒントが「生成の欠陥」？　「組織」へのヒントが「コンポーネント故障」？　そう言われても・・

現状STPAが提供する、HCF※4特定のためのガイドワードは、制御機械と稼働機械の組み合わせのみであるが、今後、人・組織・機械が協調動作するシステムの安全性解析がますます重要になると考えられることから、それらの組み合わせに適合したガイドワードをヒントワードと呼称することとした。

表1　HCF特定のためのヒントワードの種類

制御＼被制御	人	機械	組織
人	人 対 人	人 対 機械	人 対 組織
機械	機械 対 人	機械 対 機械	
組織	組織 対 人		組織 対 組織

4　STAMPワークショップ in Japan

2016年12月には、第1回STAMPワークショップin Japanを開催し多様な産業界からの参加を得て、多くの参加者が、新しい時代の安全性をどうやって確保していくか悩んでいる現状を目の当たりにした。2017年11月には、第2回を東京地区にて開催の予定である※5。

欧米では日本よりも早くからSTAMPワークショップが定期開催されている。IPA/SECは、欧米と連携してSTAMPワークショップを開催していく所存である。

図8　日米欧が連携するSTAMPワークショップ

5　まとめと今後の取り組み

STAMPに限った話ではなく、実際の開発現場では「手法適用が教科書通りにいかない」ことはよくあることで、また「立て板に水」のごとく定石通りに分析を進めるだけでは安全化を達成できない場合もあるため、分析の工夫が必要であることを「はじめてのSTAMP/STPA(実践編)」に示した。

今後IPA/SECは、更なる工夫によってSTAMP理論の進化に貢献し、STAMP/STPAの解析能力拡大・活用容易化に向けた活動を進めていく。

脚注

※1　IoT(Internet of Things)：物のインターネット
　　AI(Artificial Intelligence)：人工知能
※2　http://www.ipa.go.jp/sec/reports/20160428.html
※3　http://www.ipa.go.jp/sec/reports/20170324.html
※4　HCF(Hazard Causal Factor)：ハザード誘発要因
※5　2nd JSW, Tokyo(第2回STAMPワークショップ)
　　http://www.ipa.go.jp/sec/events/20171127.html