IoT時代を迎え、従来個別のシステム／サービスだったものがネットワークを通じて連携し、利用者にとって便利で高価値な新しいサービスとして提供される事例が増えている。一方、それに伴ってシステム相互間での複合的な原因による障害も増加しているが、従来型の安全性分析手法では限界があり、新たな安全性分析手法としてSTAMPが提唱され、活用が期待されている。

特集にあたって

SEC調査役　三原 幸博

現在の複雑なシステムは、故障しないソフトウェアや動作に不確定性のある人間を含むサブシステムコンポーネントで構成されており、故障は構成要素間の相互作用で発生するものが中心となる。従って、事前の安全性解析や事故の原因分析には、従来型の「ハードウェア中心」「動作が確定的」「事故は構成要素の故障に帰着できる」ことを前提とした分析手法では限界がある。

こうした背景から、本特集では、新たな事故発生メカニズムに基づくハザード要因解析手法として米国で提案され、欧州を含めて数々の実績を上げている「STAMP（System Theoretic Accident Model and Process：システム理論に基づく事故モデル）」が提唱している安全性解析手法ついて紹介する。この手法は、新たに登場しつつある複雑なシステムに対して、安全性の事前解析・事故原因の分析が可能である。IPA/SECにおいて設置したWGを核に推進してきた普及のための継続的な取り組み内容と、産業界及び学界における先進的な取り組み事例を紹介する。

本特集では、次の記事を掲載している。

会津大学の兼本による「これからの複雑システムの安全分析STAMP/STPA」では、人と高度なソフトウェアが連携・協調して高度な機能を提供する、これからの複雑な工学製品で期待されている安全分析法STAMP/STPAの応用可能性について解説すると共に、故障をなくすのではなく、安全を制御するというパラダイムシフトの重要さを指摘し、複雑システムの安全論証のあり方について解説している。

仙台高等専門学校の岡本、株式会社チェンジビジョンの平鍋による「安全性モデリングとSTAMP/STPA、その最新ツール紹介」では、モデルベース手法一般に必要な機能・性能とSTAMP支援ツールで実現したいコンセプトと機能について、既存の支援ツールとIPA/SECが実現しようとしている支援ツールを対比して解説している。

東日本旅客鉄道株式会社の北村による「JR東日本におけるSTAMP活用の取り組み」では、鉄道における各種信号保安システムが、情報通信技術の採用による技術革新に伴って発生し始めた、装置単体レベルでは説明ができないような複雑な事象に対応するために、新たな安全解析手法STAMPを活用した取り組みについて紹介している。

日本電気株式会社の向山による「エンタープライズ系システムを対象としたSTAMP/STPA分析試行」では、仕様をデータ処理の観点で表現することが一般的であり、制御が明示的ではない業務系システムでも、ハザードにかかわる処理に着目することによりSTAMP/STPAの適用が可能であり、更には業務仕様に欠けていた安全要件の導出まで得られた知見を解説している。

仙台高等専門学校の岡本、信州大学の岡野による「STAMP海外事例の紹介：STPA-SafeSec」では、米国における広域送電網とローカル送電網の接続に関するセキュリティ面のリスク分析をSTPA（STAMP based Process Analysis）の拡張手法である“STPA-SAFETY-SEC”を使って行った事例について解説している。

有人宇宙システム株式会社の野本による「STAMP初心者を卒業する」では、与えられた制御構造をSTAMPのお作法に従って分析するだけでは、安全が実現できない事例として航空機事故を取り上げ、分析から一歩踏み込んで真に安全な制御構造を設計できる能力（システムズエンジニアリング）について解説している。

IPA/SECによる「STAMPワークショップに関する活動報告」では、2017年9月にアイスランドで開催されたEuropean STAMP Workshop2017と同じく11月に東京で開催された第2回STAMPワークショップの模様を中心に最近のイベントを紹介している。

読者の方々には、本特集で紹介した事例などを参考に、各社・組織で開発あるいは運用されているシステムの特性を勘案し、安全性の向上・確保にSTAMPの活用を進めていただくことを期待する。また、IPAで開発してきたSTAMP支援ツール“STAMP Workbench”の公開・無償提供の開始を2018年4月に予定している。併せて活用いただきたい。