米国 STAMP Workshop2017参加報告

SEC調査役 十山 圭介　SEC研究員 金子 朋子

2017年3月27日～30日までマサチューセッツ工科大学MIT（ボストン、米国）で開催されたSTAMP Workshop2017に参加し、STAMP※1の状況や動向について情報収集を行った。

1 ワークショップの特徴

2012年より始まった本ワークショップは今回で6回目となり、参加数は275～300名で昨年度より12%増えた。参加者は増え続けており、新規参加者は73%を占める。24カ国から参加があり、日本からは15名で、米国に次ぐ参加であった。20程度の産業分野から参加があり、航空宇宙・防衛が40%で最も多く、自動車が20%でそれに次ぐ。多様な企業、政府機関、大学と産官学が参加。Boeing社とEmbraer社はそれぞれMITと共同で分析を行っている。航空機や自動車の事故だけでなく、生産・建設現場での安全性や社会システムの安全性分析、人と自動化のインタラクションに関する分析が出てきている。

2 ワークショップの内容

本ワークショップの講演数は32件、ポスター発表は9件（表1）。ワークショップは、初日のチュートリアルと3日間のプレゼンテーションで構成される。チュートリアルでは基本編としてSTAMP、STPA、CAST※2のイントロダクション、および応用編としてそれぞれの演習を実施。また、拡大テーマとして、今年はヒューマンファクタと作業現場での安全についてのプレゼンテーションが行われた。

Birds of a Featherセッションも開催され、産業別の交流が図られた。当初航空宇宙・防衛と自動車の2グループが設定されていたが、会場で新たにヘルスケア、石油とガス、作業安全も追加され、活況を呈した。

表1　主な発表内容

タイプ	対象	業界
方式（手順）の提案	ハザードシナリオの生成方法	
	MIL-STD-882EとSTAMPとの対応付け	航空宇宙・防衛
	ISO26262との対応付け	自動運転車
	推進のポイント	産業界
STPAの適用	現場安全	航空
	空調制御	航空
	無人航空機システム	航空
	ロータークラフトの設計	航空
	脅威・エラー管理	航空
	フライトテストでの過度の自動化のシナリオ	航空
	電気自動車の高電圧対策	自動車
	レーン保持アシスト	自動車
	建設現場の安全性	建設
	飲用水供給システムのリスク分析	ライフライン
	蝸牛インプラントシステム	医療用ソフトウェア（CPS）
	セキュリティ	航空
		サプライチェーン
	IoTセキュリティ	
	軍事的意思の決定	防衛
	自動運転車	自動車
	海洋石油プラント	石油
STAMPの考えの適用	メンテナンス	鉄道
CASTの適用	ベビーフードによる事故分析	薬品
	自動運転での道路安全	自動車
	航空機事故	航空
	航空機事故	航空
	滑走路侵入	航空

3 注目すべき発表

コンチネンタル社は自動車の機能安全規格であるISO26262に適合した自動運転に対する安全アーキテクチャをSTPAに適用した事例を発表した。ルノー社は自動運転での道路安全に対し、ヒューマンエラーを分類し、CASTを拡張してTesla社の事故を解析した事例を発表した。ほかには、自動運転に伴い課題となるヒューマンエラーに対して、ドライバの注意散漫に着目したレーン保持アシスト、電気自動車の高電圧対策へのSTPAの適用、自動車関連の適用事例が多数発表され、迫力のあるセッションであった。またISO26262の次期バージョンにはSTAMPが入る見込みであり、今後日本でも急速な普及が予想される。

セキュリティに関しては、チュートリアルに加えて事例3件も発表された。Embraer社はフライトマネジメントシステムに対するSTPA-Sec※3を適用。米国の権威ある研究所であるLawrence Livermore National LabはIoTに対するSTPAを適用。IoTのもたらすセキュリティ上の脅威に対してSTPAを利用すると、これまで文献上で得られていた脆弱性が6～10件程度だった事例に対し200以上のセキュリティ上の脆弱性、ハザードなどを発見できた旨を発表した。

4 ポスターセッション

ポスターセッションは、2日目の17：30～20：00で実施された。IPA/SECからの発表タイトルは「A proposal for “hint words” to identify hazard causal factors for systems including human」で、ヒューマンファクタを考慮する際のハザードを導くモデルと「ヒントワード」を提案し、質問やコメントを多くいただいた。

5 日米欧の連携

9月には欧州、11月には日本でワークショップが開催される。STAMP WSは日米欧で3極体制を構築する予定であり、本ワークショップ参加を通じ交流がなされ、日本のIPA/SEC Webサイト（英文版） http://www.ipa.go.jp/english/sec/complex_systems/stamp_workshop.html より、MITと欧州（ESW）のWebサイトに相互リンクが貼られた。

写真1　MIT Nancy Leveson教授と共に

写真2　ポスターセッションでの光景

脚注

※1　STAMP（Systems-Theoretic Accident Model and Processes）とは、MITのNancy Leveson教授が提唱したシステム理論に基づく事故モデルとプロセス

※2　CAST（Causal Analysis based on STAMP）とは、STAMP理論に基づいて、事故後に、なぜ起きたかの検証と分析を行う手法

※3　STPA-Sec（System-Theoretic Process Analysis for Security）とは、STPAをセキュリティに適用した分析手法