組込みソフトウェア技術研究会

「STAMP Workbench ハンズオンセミナー」

～STAMP 理論に基づく効率的な安全分析を体験する～

（セミナー概要）

近年の IoT の進展に伴い大規模・複雑化するシステムでは、複数の異なるシステムが相互接続されるようになり、システム障害も複数の要素間の相互作用に起因するものがしばしば発生しています。そのような中、システムの相互作用に着目した新しい安全分析方法論 STAMP*1 が幅広い産業界で注目されています。

STAMP は事故原因分析に用いられるだけでなく、将来的なリスクを回避するための安全分析（この分析手法を STAMP/STPA*2 と呼びます。）にも用いられます。特に、後者の目的で活用する際には、STAMP/STPA の習熟や経験に基づくノウハウが必要となります。

そこで、IPA は、STAMP 独自の作業手順や用語、表記法に馴染みが無くても安全分析ができ、分析者は思考に重点をおくことができるツール「STAMP Workbench」を作成し、2018 年 3 月より公開しています。

本セミナーでは、STAMP/STPA の概要と「STAMP Workbench」の特徴を紹介します。また、グループ演習では、簡易なシステムを題材に、「STAMP Workbench」を用いた効率的な安全分析の手順と分析のポイントをステップごとに解説しながら、STAMP/STPA による安全分析を体験します。

また、アーキテクトには複雑なシステムの開発における多くの場面で、システム思考に基づいてシステム全体を俯瞰したアーキテクチャーを描くことが要求されるようになっています。STAMP/STPA はまさにシステム思考に基づいて安全に関するシステム全体のアーキテクチャーを描き、安全分析に活用する手法なので、本セミナーではシステム思考についても概説します。

*1 STAMP（System-Theoretic Accident Model and Processes）：マサチューセッツ工科大学(MIT)の Nancy Leveson 教授が提唱した「アクシデントはシステム構成要素間の相互作用から創発的に発生する」という理論。

*2 STAMP/STPA（STAMP/System-Theoretic Process Analysis）：STAMP 理論に基づく、相互作用する 機能単位でリスクを考える安全分析手法。

グループ演習ではパソコンを使用しますので、ご自身のパソコンをご持参ください。（ＰＣが準備できない場合は、お申し込み時にその旨ご連絡ください。）

パソコンの OS は Windows に限ります（Mac は不可）。

※事前に IPA 提供ツール「STAMP Workbench」のダウンロードをお願いします。

主催	静岡大学 情報学部 組込みソフトウェア技術（HEPT）コンソーシアム
開催日時	2019 年 11 月 6 日（水）13:30～18:00　4.5 時間
開催場所	静岡大学情報学部 1 号館 1 階　情報科学第 1 実験室 (静岡県浜松市中区城北 3-5-1 静岡大学浜松キャンパス)
定員	20 名
参加費	無料
募集対象	● STAMP に関心があり、STAMP ツールを用いた効率的な分析方法を知りたい方 ● 安全分析に STAMP/STPA の導入を検討している方 ● システム開発における、安全分析の工数、分析結果の漏れ・誤りなどを低減したい方 ● システム思考に基づくアーキテクチャー構築に関心があり、実践したいと考えている方 ● システム企画、システム設計、ソフトウェア設計担当、システム運用、品質保証を担当している方
セミナーで学べること	1.　「STAMP Workbench」の操作方法を学ぶことで、効率的な安全分析方法を習得できます。 2.　簡易なシステムを題材として、STAMP/STPA の理解を深め、実践的な分析のコツをつかむことができます。
配布物	・小冊子「はじめての STAMP/STPA」 ・書籍「はじめての STAMP/STPA（実践編）」 ・書籍「はじめての STAMP/STPA（活用編）」 ・事業成果集 DVD「IPA ソフトウェア高信頼化 早わかり 2018」

時刻	プログラム概要
13：00	**受付**
13：30～ 14：00 （30 分）	**IoT 時代に適した安全分析手法 STAMP/STPA** **～STAMP 支援ツール STAMP Workbench の特徴～** Society5.0 の実現に向けて益々必要性が高まるシステム思考に基づくアーキテクチャー構築とその活用について概説した後、STAMP/STPA の概説と「STAMP Workbench」ツールについて以下を解説します。 ・システム理論に基づく新しい事故モデル STAMP とは？ ・従来の安全分析の考え方と STAMP の考え方の違い ・STAMP に基づく安全分析手法 STPA と概略手順 ・STAMP Workbench の特徴と使い方 <講師> IPA 社会基盤センター 調査役　石井　正悟
14：00～ 18：00 （240 分） 適宜休憩	**【グループ演習】STAMP 理論に基づく効率的な安全分析を体験する！** 人とソフトウェアと機器から成る簡易なシステムを題材として、「STAMP Workbench」を用いた以下の分析の手順とこつを体験することにより STAMP/STPA の本質を理解します。 (1) アクシデント、ハザード、安全制約の識別 解説、演習、発表、討議 (2) 登場人物の抽出（コンポーネント抽出表） 解説、演習、発表、討議 (3) コントロールストラクチャーの構築 解説、演習、発表、討議 (4) 非安全なコントロールアクションの抽出 解説、演習、発表、討議 (5) 非安全なコントロールアクションのハザード要因特定とハザード発生シナリオ作成 解説、演習、発表、討議 演習の各 Step でグループごとに分析結果を発表していただき、参加者全員で討議します。 <講師> IPA 社会基盤センター 研究員　向山　輝／調査役　石井　正悟