米国における有力組織との意見交換

SECシステムグループ 主任 八嶋 俊介　SEC研究員 峯尾 正美
SEC研究員 小崎 光義　SEC職員 山田 彩歌

1 はじめに

IPA/SECでは、国際連携活動の一環として、米国の有力なソフトウェア技術拠点であるNIST（米国商務省国立標準技術研究所※1）、SEI（カーネギーメロン大学ソフトウェア工学研究所※2）と定期協議を行っている。今回もこの2組織を訪問し、最新の取り組み事項について意見交換を行った。2017年1月23日から1月27日にかけての上記米国出張について、その内容を報告する。

2 NISTとの意見交換

写真1　NISTとの意見交換の様子

（1）NISTの活動状況について（NIST）

NISTの関連活動として、セキュリティを中心としたITL※3の取り組み、EL※4のスマートグリッドへの取り組みとCPS Frameworkの最新状況に関する説明が行われた。昨年度も伺ったスマートグリッドに加えて、スマートシティに向けたフレームワークの検討が進められていることが分かった。また、現在発行されているCPS Frameworkではセーフティに関しては今後の検討となっていたが、米SAE※5と連携して自動車分野への機能安全を考慮した適用について取り組み、その結果のフィードバックが計画されていることが分かった。その他、テストベッドの検討や、UMLでモデル化するためのオープンソースツールの検討が行われていることが分かった。

（2）つながる世界の開発指針に関連する活動状況について（IPA/SEC）

IPA/SECが取り組んでいる、つながる世界の開発指針、開発指針に基づいた実証実験、及び開発指針の普及状況について説明した。IPA/SECもNISTもそれぞれ、IoT、CPSをSystem of Systemsとして捉えていることについて共通理解が得られた。

IPA/SECからは、とくに、日米独での安全安心なIoTについての国際標準化についての連携について提案した。現在、IoTに関して、日米独で、それぞれ個別に標準の整備が行われており、それらをすり合わせて国際標準化を進めることが必要である。一方で、そのためには、コモンランゲージ（共通の用語）がないと、それぞれの標準の差異の明確化が進まないことが想定されるため、NIST CPS Frameworkは、OSIの7層モデルのように、標準化する場合の共通モデルとして使って欲しいという立場であることが分かった。今後は、開発指針の国際標準化にあたってNIST CPS Frameworkのモデルを意識して提案するなど、引き続き相互に連携して進めていく予定である。

3 SEIとの意見交換

写真2　SEIとの意見交換の様子

（1）ソフトウェア開発データ分析にかかわる意見交換

一昨年、NDAを締結して送付したIPA/SECデータ白書のデータに基づいたSEI側の研究テーマ内容に関して、状況確認と意見交換を行った。

SEI側の研究テーマは、「IPA/SEC、TSP（Team Software Process）データにおける因果関係モデリングツールを用いた因果関係の分析」であり、分析項目として、昨年IPA/SECより送付した「ソフトウェア開発データが語るメッセージ2015」で述べた分析項目のうち、IPA/SEC、TSPで共通に収集している項目が候補となる。訪問時点では、プレ分析を実施済みで、幾つかの項目では、IPA/SEC側と同様な相関関係が得られているとの報告があった。

今後は、ツールを用いて、それらの間の因果関係を分析するとのことで、データの更新を含め、協力して研究を推進したい。

（2）システムズエンジニアリング推進の取り組み状況について

IPA/SECが行っている、システムズエンジニアリング推進のための活動や、欧州における導入状況（IESE※6への委託調査結果）について紹介し、意見交換を行った。SEIにおけるシステムズエンジニアリングに対する考え方の概要は、以下の通りである。

- システムは複数の観点から、検討されるべきである。
- 今や、ソフトウェアに関係しないシステムはあり得ない。
- システムズエンジニアリングには、以下の3つのタイプが存在する。
  ①要求をいかに実現するかの「プログラム型」
  ②実現可能性を検討する「発見型」
  ③論理的なアプローチを取る「アプローチ型」
- システムズエンジニアリングの考え方は、万国共通的なものである。
- 米国の、とくに大企業では、システム全体を見る専門の組織があって、すべてのインターフェースに責任を持つという点で、日本とは組織構成上も大きな違いがある。
- システムズエンジニアリングのエンジニアは、技術的だけでなく、人間的な面にもかかわる場合がある。
- システムズエンジニアリングのエンジニアは、自分の専門的知識を深く学ぶ一方で、多方面の知識を広く浅く学び、「T字型」の知識を持つ必要がある。更に、最近のソフトウェア、セキュリティに関しては、双方向に幅広く知識を持つ必要がある。こうした人材の育成については、米国でも大きな課題となっている。

（3）IPA/SECの組込み分野への取り組みについて

IoTと深い関係のある組込み分野について、IPA/SECが取り組んでいる活動（ESCR※7）の紹介と、ESCR C++の改訂状況（ver.2.0を発行／公開）の説明を行った。昨年のC言語版（英語版）に引き続き、C++言語版（英語版）の書籍を持参し、成果物の内容について具体的に紹介した。また、C言語版は、SEIから公開されているSEI CERT C Coding Standard※8に対応する形で改訂作業中であることを説明した。SEIでは、SEI CERT C Coding Standardのツールも公開しているとのことで、今後の事業への活用を検討する。

（4）STAMP/STPAを中心とした安全性解析手法についての意見交換

IPA/SECの安全性解析手法普及への取り組みとして、STAMP/STPA※9を用いた日本国内のシステムの安全性解析の事例や、MIT※10の研究者や日本国内の産学の有識者を招いてSTAMP/STPAの活用事例について講演・議論を行ったワークショップ※11などの紹介を行った。SEIからは、STPAとAADL※12を組み合わせた原子力発電所の制御システムや医療システムの安全性解析に関する研究の紹介があった。

（5）SEIの研究“SEI Agile in Government”について

SEIにおける米国政府へのアジャイル普及活動の紹介があった。具体的には、①政府に特化したアジャイルのトレーニング、②アジャイル適用に関する政府組織への指導、③ソフトウェア開発から調達など全ライフサイクルにわたる技術的経験の提供であり、コスト削減のみでなく、早期の価値提供や変化へのリスク低減などのアジャイルの価値を、上層部を含めた関係者に納得してもらい実現しているとのことであった。

また、アジャイル開発の効果を定量的に測定することも行っており、外部関係者に向けた全体システムレベルと、開発管理用のチーム内のレベルでの測定手法があるとの紹介があった。

4 おわりに

NISTに関しては、今回は、CPSやIoTに関する取り組みについて相互の具体的な活動に関して、昨年度以上に理解が深まり有意義であったと考えている。IoTの安全安心に関する国際標準化に向けては、今回の訪問でNIST CPS Frameworkの方針が把握できたように、連携体制の構築には、各国の標準類への取り組みの方針を確認しつつ構築していくことが必要であると感じられた。

SEIに関しては、ソフトウェア開発データ分析における協力研究の進捗とIPA/SECの分析との方向性の一致が確認できた。また、システムズエンジニアリングや組込み分野のセキュアコーディングなどの各分野においても、引き続き協力していくことを確認した。

脚注

※1 NIST：国立標準技術研究所（National Institute of Standards and Technology）は、アメリカ合衆国商務省の技術部門であり、計量、標準化、基礎技術研究などを主な任務としている。

※2 SEI：カーネギーメロン大学ソフトウェア工学研究所（Carnegie Mellon University, Software Engineering Institute）は、アメリカ合衆国ペンシルベニア州に本部を置くカーネギーメロン大学に設置されているソフトウェア開発、ITセキュリティなどの研究機関である。

※3 ITL：情報技術研究所（Information Technology Laboratory）は、国立標準技術研究所に設置された研究ユニットの一つである。

※4 EL：情報技術研究所（Engineering Laboratory）は、国立標準技術研究所に設置された研究ユニットの一つである。

※5 SAE：SAE（Society of Automotive Engineers, Inc.）は、モビリティの専門家を会員とするアメリカの非営利団体である。

※6 IESE：フラウンホーファー研究機構（Fraunhofer-Gesellschaft）実験的ソフトウェア工学研究所（Institute for Experimental Software Engineering）。

※7 ESCR：Embedded System development Coding Referenceは、組込みソフトウェアを作成するにあたって、ソフトウェアのソースコードの品質をより良いものとするために、コーディングの際に注意すべきことやノウハウを体系的に整理したものである。

※8 SEI CERT C Coding Standardは、C言語を使ってセキュアコーディングを行うためのルール（Rule）とレコメンデーション（Recommendation）を定めたものである。

※9 STAMP：System Theoretic Accident Model and Processesとは、マサチューセッツ工科大学（MIT）のNancy G. Leveson教授が提唱したシステム理論に基づく事故モデルであり、STPA：System Theoretic Process Analysisとは、STAMPの理論に基づく、相互作用する機能単位でリスクを考える新しい安全性解析手法である。

※10 MIT：マサチューセッツ工科大学（Massachusetts Institute of Technology）は、アメリカ合衆国マサチューセッツ州に本部を置く私立大学であり、5つのスクールと1つのカレッジ、51の研究機関が設置されている。

※11 「第1回 STAMPワークショップ in Japan」2016年12月5日から3日間、九州大学にて開催。

※12 The SAE Architecture Analysis and Design Language：システムの構造や動作を、処理時間などの非機能的な要素も含めて可視化するアーキテクチャ記述言語。