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　システムグループ　研究員　峯尾　正美
SEC　ソフトウェアグループ　研究員　小崎　光義

1 はじめに

IPA/SECでは、国際連携活動の一貫として、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。また、IV&Vの専門家として以前からIPA/SECの活動にご協力いただいているCukic博士（昨年ウェストバージニア大学からUNC（ノースカロライナ大学※3）に移籍）を訪問し、最近の取り組み内容について意見交換を行うと共に、米国の業界団体等を訪問し、IPA/SEC活動成果の普及を図った。本稿では2016年１月４日から１月10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

(1) CPS PWG※4の活動状況について

CPS PWGの関連活動として、スマートグリッド、CPS Framework概要、及びCPS PWGの５つのサブグループ（SG）のうち３つ（リファレンスアーキテクチャSG、ユースケースSG、タイミングSG）に関する情報を収集した。

本WGの取り組みとして、コモンランゲージ（共通の用語）、クロスドメインのテストベッド、ビジネスモデルを重視しているという説明があった。従来はドメイン内のデバイス間通信であったが、今後はドメイン間のインターオペラビリティが重要と考えられており、そのためにFrameworkが必要であるということであった。CPS Frameworkでは、OSIの７層モデルのようなものを目指すという説明もあった。また、具体的な事例をユースケースとして収集し議論しているということであった。

CPS FrameworkとIIC※5のリファレンスアーキテクチャとの関係について質問したところ、CPS Frameworkは実行可能なアクティビティから成る構造であるのに対し、IICのリファレンスアーキテクチャは、実際の使い方までは明確になっていないとのことであった。

また、ほかの標準類とCPS Frameworkとの関係については、標準類は指示的なものであるのに対し、CPS Frameworkは枠組みであることから、相互のギャップを埋めるため、NISTとしてもIoTの標準であるIEEE P2413やISO/IEC 30141の策定に参加し、密接に活動しているということであった。

写真１　NIST SSD（Software and Systems Division）チーフのRam D. Sriram氏と

(2) つながる世界の開発指針検討WGの活動状況について

IPA/SECが策定に取り組んでいる、「つながる世界の開発指針」について説明した。本開発指針では、つながる世界における安全安心（セキュリティ、セーフティ、リライアビリティ）について検討しており、NIST CPS FrameworkのTrustworthiness（セキュリティ、セーフティ、リライアビリティ、プライバシー、レジリエンス）と関連性が高いこと

を双方で共有した。

(3) ESCR※6とCWE※7の対応について

前回訪問時(2014年12月)、IPA/SEC内に設置されたWGで検討中のESCRとCWEの対応表を説明し、コメントをいただいた。今回の訪問では、協力に感謝すると共に、いただいたコメントをWGで議論し、対応表を公開した旨を報告した。また、引き続きESCR C++版についても同様の議論を進めていく予定であることを報告した。

3 AHAM(米国家電製品協会※8)との意見交換

AHAMは、DoE(エネルギー省※9)に対するロビー活動や、家電製品の性能に関する標準化や認証を行っている団体である。ここでは、IPA/SECの事業概要と、組込み分野への取り組みとして、ESCRの紹介を行った。

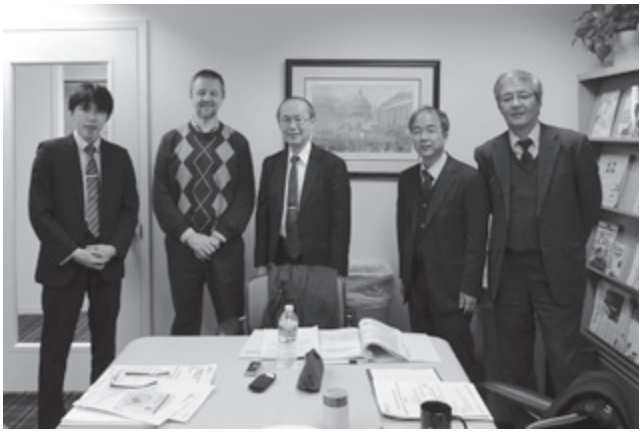

写真2　AHAM 標準化担当部長のMatthew B. Williams氏と

家電同士がつながるスマートハウスに関連して、日本においては、家電同士をつなげる標準プロトコルとして、ECHONET Liteが挙げられるが、米国ではSEPプロトコルが最も使われているとのことである。ただし、IoTへの対応はこれからという印象で、IICの動きもとくに気にしていない様子であった。

家電同士の相互接続性に関しては、5年前にAHAMからホワイトペーパーが発行されている。その中で、各プロトコルの比較表を作って評価しているとのことであった。また、標準化に関しては、家電制御の共通コマンド標準を作成しており、現在はユースケースの標準化に取り組んでいるとのことである。

IPA/SECの提供資料(ESCRの紹介など)は、約150社の会員企業に展開していただけることになった。

4 SAE International※10との意見交換

SAE Internationalの、主に自動車向け組込みソフトウェアの標準化を行っている委員会の担当者と電話会議を行った。当方からは、IPA/SECの事業概要と、組込み分野への取り組みとして、ESCRの紹介を行った。

先方の組込みソフトウェアの標準化活動は、現在活動休止中の状態とのことであるが、クライスラーのハッキング事例をはじめとした、セキュリティ対策については重要視しているようで、2016年1月末に、セキュリティに関する標準を出版する予定とのことであった。(後に、「SAE J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems」が発行された。)

IPA/SECの提供資料(ESCRの紹介など)は、関係者に展開していただけることになった。

【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　UNC：ノースカロライナ大学(University of North Carolina)は、アメリカ合衆国ノースカロライナ州内16個所に大学を設置する州立大学の総称である。訪問したシャーロット校は、とくに工学、情報技術などの産学協同研究が盛んな大学である。

※4　CPS PWG：Cyber-Physical Systems Public Working Group

※5　IIC：Industrial Internet Consortiumは、インダストリアル・インターネットやIoTの標準化や普及推進を行う国際規模の団体である。

※6　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。

※7　CWE：Common Weakness Enumerationは、ソフトウェアにおけるセキュリティ上の弱点(脆弱性)の種類を識別するために用いられる、共通の脆弱性タイプ一覧である。

※8　AHAM：米国家電製品協会(Association of Home Appliance Manufacturers)は、家庭用電化製品の性能や特性について、一定の基準で測定できるようにその基準を定めているアメリカの団体である。

※9　DoE：アメリカ合衆国エネルギー省(United States Department of Energy)は、アメリカ合衆国のエネルギー保障と核安全保障を担当する官庁であり、主な任務は、核兵器の製造・管理、原子力技術の開発、エネルギー源の安定確保、関連技術の開発である。

※10　SAE International：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。“Society of Automotive Engineers, Inc.”が正式名称だが、“SAE International”と呼称している。

5 SEIとの意見交換

(1) ソフトウェア開発データ分析にかかわる意見交換

前回訪問時（2014年12月）の決定事項としてNDAを締結し送付した、IPA/SEC「ソフトウェア開発データ白書」のデータに基づいた共同でのデータ分析に関して、意見交換を行った。

当方からは、当該データの分析から得られた新たな知見の例を紹介し、先方からは、TSP（Team Software Process）での開発データを収集したSEMPR（Software Engineering Measured Performance Repository）の紹介があった。

双方のデータには共通項目も多いことから、まずは、共通項目が何であるかをお互いに認識し、その上で、何を分析するかをすり合わせることで合意した。双方のデータにて、同じ知見が得られるかなど、今後具体的なテーマに関して検討を進めたい。

写真３　SEIメンバと

(2) つながる世界の開発指針検討WGの活動状況について

IPA/SECが取り組んでいる、「つながる世界の開発指針」について、日本の動向を含めて説明した。日本では産官学が連携したIoT推進コンソーシアムが立ち上がり、今後取り組まれていくことについて、SEIのCTOに伝えていただけることになった。日本のIoTへの取り組みについて、深く興味を持っていただけることが期待される。

また、2016年１月開催予定のSCC（Software Certification Consortium）の会合で、セーフティ設計をテーマに各組織の取り組みが報告されることになっており、その情報を送付していただけることになった（発行日時点で開催済み）。

(3) SEIの研究 “Extending AADL for Security Design Assurance of the Internet of Things” について

アーキテクチャモデルを用いた分析／検証への取り組みとして、２つの取り組みの紹介があった。

① アーキテクチャ記述言語として活用されているAADLに、セキュリティに関する記述を拡張し、モデルを作成して形式的な検証を可能とするための研究の紹介があった。セキュリティの脅威については、STRIDE（なりすまし、改ざん、否認、暴露、サービス不能、権限の昇格）のモデルが利用されている。

本研究は、現段階では記述できる範囲はセキュリティに限られているが、今後はセーフティに関する適用も見込まれる。なお、AADLで脆弱性や安全性を分類するモデルは、MIT[※11]のNancy Leveson教授が提唱しているSTAMP[※12]に似ているのではないかと質問したところ、相互に補完しあうものであるということであった。この点について、関連資料をSEIから受領したので、今後検証したい。

② 上記と併せてDRS（Design Rule Space）を用いることで、ソフトウェアのバグの元となるアーキテクチャの問題点の検証を行う研究についての紹介があった。

(4) IPA/SECの組込み分野への取り組みについて

IPA/SECの組込み分野への取り組みとして、ESCRの紹介を行った。ここでは、関連する規格が常に更新されることなどからくる、コーディングガイドの更新の難しさに関する議論が行われた。（実際にESCRは、ver.1.0（2006年６月公開）、Ver1.1（2007年７月公開）から2.0（2014年３月公開）まで、約８年かかっている。）

また、ESCRの海外展開先としては、ベトナム、シンガポールなどのアジア諸国でも使われている旨を伝えた。

(5) SEIの研究 “Increasing Adoption of Secure Coding” について

複数の静的コードアナライザの結果をマージするツールを作成して、コーディングが終わってからではなく、コーディングをしながらセキュアコーディングに関する的確な診断を実施することで、生産性の向上を図った事例の紹介があった。

また、NISTに紹介したESCRとCWEの対応表については、SEIでもレビューいただけることになった。

6 ノースカロライナ大学（UNC）との意見交換

（1）組織の概要について

College of Computing and Informaticsの学部長から、組織の概要について説明を受けた。

- データサイエンス、データ分析、バイオマティクス（DNAなど）、ヘルスインフォマティクスなどに関連した８つのセンター及び研究所を持ち、約3,400万ドルの予算で運営されている。
- 約28,000人の学生を抱えており（当該学部は約2,000人）、シャーロット地域において最大の研究機関である。
- 情報科学からインフォマティクスへの拡張、T型人材の育成、産業と経済発展のニーズへの適用など、21世紀が必要とするリーダー人材の育成に力を入れている。

写真４　UNCメンバと

（2）最近の研究内容紹介（デモンストレーション含む）

ビッグデータ解析の例として２つの事例紹介（以下①、②）と、企業から実データを収集して行う研究（③）の紹介があった。

① ツイッターの文章を解析し、トピックごとのデータ量の変動をビジュアル化して観測し、更に位置情報と併せて表示することで、その時点でどのような事象がどこで発生しているかを解析するシステム。

② 競合しているチェーン店などに対して、顧客アンケートを実施し、改善点と対策費用などを評価することで対策すべき項目を決定し、顧客満足度を向上させる提案を行うもの。

③ 電力業界や金融業界などのシステムをモデル化してシミュレーションを行うことによって、セキュリティやレジリエンス（復旧性）に関する分析を行う研究。各企業から約10年にわたってデータを収集し、重要インフラ間の相互依存性と時間的波及を精緻にシミュレートすることが可能になっている。UNC及びGeorge Mason大学がハブとなり、NSA※13、Bank of America、MITRE※14などが参画（年間予算50万ドル）。

7 おわりに

NISTに関しては、今回、CPSやIoTに関する取り組みについての相互の活動に理解が深まり有意義であったと考えている。今後はTrustworthinessを中心に協調して活動できるスキームを作っていきたい。

SEIに関しては、ソフトウェア開発データの分析に関する共同研究について、相互のデータベース項目が開示された。窓口担当者の明確化を含め、より具体的なテーマの検討に着手できる状態となり、有意義な訪問であったと考える。

ノースカロライナ大学との議論では、産業界と密に連携して研究を進めている点が非常に印象的であった。研究項目の90％は企業のニーズに基づく研究であり、ベンチャーの支援まで行っている。日本でも産学連携が叫ばれているが、具体的な取り組みにつなげていかなければなかなか“死の谷”は越えられないと感じた。

また、新規開拓として米国の家電の業界団体と、主に自動車を中心とした組込みソフトウェア標準化委員会の担当者とコンタクトを取ることができ、双方ともESCRを広く展開いただけることとなった。このように、各業界のユーザに広く影響を与えることができる方々への紹介活動を通して普及展開を行い、現在はアジア内に閉じているESCRを、米国にも広く展開していきたい。

【脚注】

※11 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。

※12 STAMP：Systems-Theoretic Accident Model and Processesは、複雑なシステムに対する安全性解析の手法であり、人とシステムの間、システムとシステムの間の相互作用に着目して安全評価をするという特徴がある。この手法により、従来では対応が難しかった“システム全体”の安全評価が可能となる。

※13 NSA：国家安全保障局（National Security Agency）は、アメリカ合衆国国防総省（United States Department of Defense, DoD）の内部部局であり、電子機器を使った情報収集、暗号解読、政府情報通信システムの防護、情報分析などを担当する。

※14 MITRE：MITRE Corporationは、アメリカ合衆国政府の支援を受けて、政府向けの技術支援や研究開発を行っている非営利組織である。