米国の NIST、MIT、SEI の３組織を訪問して

SEC ソフトウェアグループ リーダー
中尾　昌善

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）、MIT（マサチューセッツ工科大学）、SEI（カーネギーメロン大学ソフトウェア工学研究所）と定期的に意見交換を行っている。今年度も 12 月８日から 12 日にかけて３組織を訪問したので、その模様を報告する。

2. NIST

（1）CWE（Common Weakness Enumeration：ソフトウェアにおけるセキュリティ上の脆弱性の種類を識別するための共通の基準）

NIST 側からソフトウェアの脆弱性情報を取りまとめた CWE、CVE※1、CAPEC※2 に関する取り組みの紹介があった。色々な組織から集めている情報のため定義があいまいで、３つのデータベース間の整合性がないなどの問題もあるが、ベンチマーク用の情報として活用されているようである。今後は、CWE の項目間の関係からソフトウェアの欠陥パターンを導出することや、形式記述での表現の仕方などについて検討を進めるとのことである。IPA/SEC からは、コーディング作法ガイド（ESCR）へのセキュリティ項目の取り込みの活動を紹介し、その内容について確認してもらうこととした。

写真１　厳重な NIST の正面入り口：ここからシャトルバスに乗って目的の建物に行くくらい構内面積が広い。

写真２　NIST メンバとの議論模様：この後、NIST 職員のクリスマスパーティにも飛び入り参加させていただいた。

（2）SAMATE（Software Assurance Metrics And Tool Evaluation）

産業界や政府など様々な機関から提出してもらったソフトウェアの Assurance 情報を集めた SARD（Software Assurance Reference Dataset）というデータベースの紹介があった。これもベンチマーク用に活用されており、3,000 ダウンロード / 月程度のアクセスがあるとのことである。

【脚注】
※１　Common Vulnerabilities and Exposures
※２　Common Attack Pattern Enumeration and Classification

(3) 医療機器のインタオペラビリティ

IoT 時代における医療機器のインタオペラビリティに関する取り組みの説明（接続テストやデータログの取得など）があった。IHE（Integrating the Healthcare Enterprise）など色々な機関との関係についても解説があり、NIST が各機関のハブとなって、この取り組みを推進していることがわかった。IPA/SEC からは、ソフトウェアサプライチェーンと品質に関する取り組み、及び障害事例に基づく教訓集作成の取り組みを紹介した。教訓集の取り組みには NIST も関心があるようで、今後意見交換を継続していく必要があると感じた。

いずれに関しても活発な質疑応答があったため、予定時間をオーバーしての終了となった。

3. MIT

MIT 訪問の主要目的は、ナンシー・レブソン教授にお会いし、彼女が創始者である STAMP 技術に関する情報交換を行うことであった。STAMP とは Systems Theoretic Accident Model and Processes の略であり、システム理論に基づく事故モデルの構築手法のことである。JAXA「こうのとり」の事前ハザード分析や中国高速鉄道の事故分析に適用されたことで知られている。

IPA/SEC も STAMP 技術の有用性に着目し、その導入推進に力を入れていこうと考えており、その活動を開始している。

当方から直前に多くの質問事項を送付したにもかかわらず、教授はそれらの一つ一つへの回答資料を数 10 ページにわたって用意して下さっており、その誠実さが窺えた。主な質問は、STAMP の実際の適用域に関する事項、具体的な技術内容の確認、今後の活動予定等であった。

写真３　雪の舞う MIT 校内移動：後ろに見える建物でミーティングを実施した。

まず、STAMP 技術が既に幅広い分野で利用されていることを具体的に示していただいた。更に、大規模システムは色々な専門家が個々にいるほど複雑なので、すべてを理解して見通すのは難しいのではないかという質問にも、まずはステップ 1 で共通的な事項に取り組み、ステップ 2 で領域毎の技術に取り組んでいくとの回答であった。色々な自動化ツールを開発中であり、その 1 つは既に 1,000 ダウンロード以上に及び、また STAMP のワークショップには 25 カ国からの参加があり、関心の高さと適用活動の多さを感じ取れた。

STAMP の新たな研究動向として、自動化ツールやコンセプトレベルでの安全要件・モデル作成の手法、STPA-Sec と呼ぶサイバーセキュリティへの活用などのトピックを紹介いただいた。とくに、セキュリティに対しても因果関係分析の STAMP モデルが適用できるとの見解は興味深いものであった。

お忙しい身でありながら、30 分以上も超過して我々の更なる矢継ぎ早の質問に答えて下さったレブソン教授に感謝を申し上げたい。

写真４　レブソン教授とのミーティング：左奥の女性がレブソン教授

4. SEI

SEI のあるピッツバーグは氷点下であった。そんな寒い朝の 8 時半に始まったミーティングは、途中 SEI 所長であるニールセン氏との昼食を挟み、夕方 4 時半まで続いた。

（1）Assurance

SEI の主な活動分野は、Software Engineering, Assurance, Specific Capabilities, Cyber Security の 4 つであるが、最近は Assurance に関する要求が高まっているとのことである。サプライチェーンにおける Software Assurance では、プロダクト自身のセキュリティ設計だけでなく、どういう状況で使われるのかといった System Assurance の考え方が重要とのことである。IPA/SEC からは、ソフトウェアサプライチェーンに関する取り組みと、障害事例に基づく教訓集作成の取り組みを説明した。教訓集の米国における活用の是非について聞いたところ、適用環境が異なるとなかなか難しい面はあるが、マインド醸成には有効で、学校等で教えるのが良いかもしれないとの意見だった。

（2）Software Quality & SME

SEI では以前 CMMI（ソフトウェア開発プロセスの改善モデルと評価手法）を SME（中小企業）へ適用する検討を行ったが、SME は品質への関心が薄く、リソースも限られることから、なかなかうまくいかなかったため、現在はとくに SME 向けの活動は行っていないとのことである。INCOSE（システムエンジニアのための国際団体）では、VSME（Very Small and Micro Entities）の WG でシステムズエンジニアリングの観点での取り組みが行われているようである。

（3）Agile in Government

SEI がかかわっている国防総省の開発プロジェクトを短縮化する目的で、アジャイル開発の適用を進めており、現在では約 30％近くをアジャイルで開発しているとのことである。費用が固まらないと政府系では適用が難しいのではないかと質問したところ、要件リストを作り、総量で管理するようにすれば可能であるとのことだった。

（4）TSP（Team Software Process：ソフトウェア開発工程の分析 / 改善手法の一つ）

TSP の適用は 250 以上のプロジェクトに広がり、ソフトウェアの欠陥を中心として分析を始めているとのことである。IPA/SEC で発行しているソフトウェア開発データ白書が対象としているプロジェクトと規模的にも似ているため、相互にデータを比較して日米の違いを明らかにすべく、秘密保持契約を結んで今後共同で検討を進めることとした。

写真５　SEI 入り口：カーネギーメロン大学の一画にある。

写真６　先方のプレゼン模様：それぞれが持ち時間をオーバーして説明するほど熱の入ったものであった。

5. おわりに

訪問した３組織とも、国際的な意見交換や共同作業の重要性を強調しており、今後も引続き連携を進めていくことで一致した。また、いずれにおいてもセーフティとセキュリティは一体であるとの認識であり、IPA も SEC と ISEC（セキュリティセンター）で一体となって対応していく予定である。