産業発展を支える安心・安全なシステム開発手法の科学技術

①　計画の概要

現在、IT システムがあらゆる産業基盤・社会基盤を支えている。そのような中、セキュリティ脆弱性に起因するサイバー攻撃や情報流出が絶え間なく発生している。これらは取引サイトからの会員情報流出や仮想通貨取引所サイトでの仮想通貨の盗難など多岐にわたっている。これらの原因は、サイバーセキュリティ上、高度な技術を駆使したものというよりも、よく知られている脆弱性と攻撃技術を用いたものであり、システム開発の段階での問題点に起因することが多い。システム開発においては、安心・安全なシステムとなるように、設計・実装・テスト・保守などの開発過程において安心・安全なシステム開発に対応したものにならなければならない。高品質なソフトウェアを生産するためにこれまでさまざまな開発手法が研究されてきた。これに加えて、安心・安全なソフトウェアを開発するための手法、セキュリティ向上のためのソフトウェアテスト手法等、最近研究された様々な成果を整理・体系化し、新たな研究を推進することが重要である。さらに研究のみならず、これらの技術をソフトウェア生産に適用できるように人材育成のための教育カリキュラムの開発を行うことが必要とされている。そのために教育研究組織「安心・安全システム開発教育研究センター」を設立する。

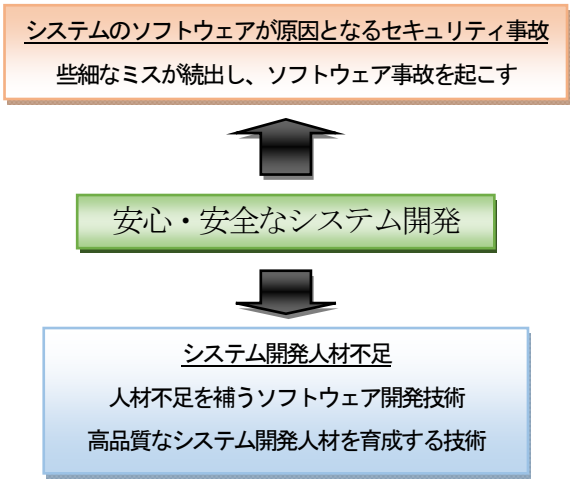

図１　産業発展を支える安心・安全なシステム開発

高品質・高効率なシステム開発手法や安心・安全なシステム開発手法を学術研究を推進する。Digital Software Expert Engineer の実現や形式的証明により保証された安心安全なシステム構築技術等の研究に取り組む。そしてそれと同時に、最新の開発手法に対応した教育カリキュラムを確立し、大学院で PBL 授業を授業カリキュラムを実践する。その経験を通して、開発手法および教育カリキュラムの改善を行い、研究への相乗効果が期待される。

②　学術的な意義

ソフトウェア開発手法の研究をはじめとしたソフトウェア工学における研究は、単に、手法の提唱と有効性の検証のみならず、その手法を実際のソフトウェア開発において浸透させるためには技術者への教育が重要となる。したがって、ソフトウェア開発手法に関する研究は、研究と共に教育カリキュラムの整備と教育の実践が必要不可欠と言える。そのようにソフトウェア開発手法と教育カリキュラムの整備・教育の実践が同時に実行することは学術的に意義深いものである。

ソフトウェア開発は、量的には産業界が中心となっているが、Mach カーネル等のオペレーティングシステムや Kyoto Common Lisp や SML#などのプログラミング言語処理系等、大学においても先進的かつ高品質なソフトウェアが開発されてきた。また今日、大学においても数多くの情報システムが利用されている。学生・教員・事務職員が教務用情報システムおよび研究用情報システム等、大学が提供する情報システムの利用者となっている。大学は、情報システムの提供者と多数の利用者を抱えるソフトウェア開発手法の研究の場としての可能性を有している。一方、大学の計算機ネットワーク利用者は身分・年齢・能力・経験において多岐にわたる。実際、CTF での成績優秀者である学生がいる一方、学士課程新入生は、多くが素人である。このようなことからも、サイバーセキュリティの実践の場としても、大変良い場所であると言える。

それらのことから、大学は、ソフトウェア開発手法を研究する場であると同時に、ソフトウェアを開発する現場という側面を持っている。このことから考えても、大学は、ソフトウェア開発手法の研究とソフトウェア開発教育・ソフトウェア開発の実践を行う場としてふさわしい場所であると考えられる。

③　国内外の動向と当該研究計画の位置づけ

これまで、国内外において、ソフトウェア開発手法は 1960 年代から現在に至るまで、様々な研究がなされている。それは、ハードウェアの進歩、ネットワークの進歩、利用者の変化、これらのソフトウェアを取り囲む環境により、ソフトウェア開発手法も変化・発展し、現在も研究が推進されている。

ソフトウェア工学分野の教育は、欧米では、ソフトウェア工学を専攻とする修士課程が設置されている。また、サイバーセキュリティにおいてもそれを専攻とする修士課程が設置されている。(例えば、カーネギーメロン大学やオックスフォード大学等) 国内の大学においても、サイバーセキュリティを専門とする大学院プログラムが設置されている事例が少なくない。

そのような中、本計画では、研究と教育カリキュラム開発とを両輪として推進することを提唱する。

④　実施機関と実施体制

本計画は、東京工業大学において、学士課程と大学院課程を有する組織である情報理工学院が中心となり、学術国際情報センターおよび工学院を初めとする関連組織の協力の下で推進していくことを計画している。

これまで、情報理工学院では、「IT 特別教育プログラム」と呼ばれる、システム開発に関する特別教育プログラムを大学院修

士課程に設置している。また、サイバーセキュリティ分野においては情報理工学院を中心とし、工学院・学術国際情報センターが協力して、「サイバーセキュリティ特別専門学習プログラム」を設置している。これらのプログラムでの経験と成果を生かして、「安心・安全システム開発教育研究センター」を設置し、研究と教育に取り組んでいく。

⑤ 所要経費

大型施設計画の場合、建設費(装置、設備等を含む)及び運営費（研究費を除く）を明記。
大規模研究計画の場合、研究費（設備費・人件費等を含む）を明記。
総経費　35 億円
（1）設備費: 2億円（内訳　20、000 円×10 年）
（2）人件費 : 30 億円（内訳　300、000 千円×10 年、教員・研究員・事務補佐員）
（3）旅費 : 2億円（内訳　20、000 千円×10 年、国内・国外出張費）
（4）その他 : 教材資料作成費 1 億円　（内訳　10、000 千円×10 年）

⑥ 年次計画

2019 年度
【事前調査】
国内外の大学におけるシステム開発手法の研究活動と、それらの研究グループにおいて取り組まれている教育活動に関して調査を行う。さらに、サイバーセキュリティ教育について調査を行う。特に、システム開発手法に関する教育とどのように関連付けてサイバーセキュリティ教育を行っているのかという点について調査を行う。
第 1 期（2020 年度～2025 年度）
【安全安心なシステム開発手法に関する研究の推進】
開発するシステムの安全性を向上させる開発手法、例えば、Robotic Process Automation (RPA)、Digital Labor によるソフトウェア開発支援、セキュリティ・安全性の検証に関する研究に取り組む。
【教育カリキュラム開発】
システム開発に関係し、必要となるサイバーセキュリティに関する知識を教授する科目や、セキュリティテストやセキュリティ評価等を含むようなチーム開発に関する PBL 演習科目、それらの基盤となるソフトウェア検証技術に関する演習を備えた教育カリキュラムを開発する。そのカリキュラムを大学院教育で実施し、その効果を検証する。
第 2 期（2026 年度～2029 年度）
【教育カリキュラム改良】
第 1 期に行った研究成果を教育カリキュラムに反映させることにより改良する。
【教育カリキュラム適用拡大】
開発した教育カリキュラムを、他大学や企業等への適用を行い、再検討を行う。

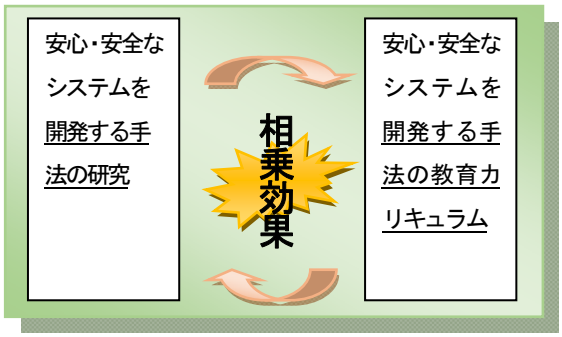

図２　安心・安全システム開発教育研究センター

⑦ 社会的価値

情報システムは、現在、社会を支える基盤であり、システム開発手法はそのような基盤を造成する技術である。情報システムは適切な仕様に従って効率よく動作することが望まれてきた。あらゆる情報システムがインターネットを介して相互接続し、また、多様なデバイスが接続することにより、サイバーセキュリティの見地に立ったシステム開発が重要となっている。

現在、さまざまなサービスがインターネットに接続された情報システムにより提供されているが、セキュリティ・インシデンスは止むことはない。その理由はセキュリティ・インシデンスを引き起こす攻撃が高度化しているというよりも、システム開発の過程で、サイバーセキュリティの観点における注意の欠如が原因になっていることが多い。サイバーセキュリティの観点を備えたシステム開発手法を確立し、その教育カリキュラムを整備し、対応する人材が養成されることにより、状況は劇的に改善される。

⑧ 本計画に関する連絡先

西崎　真也（東京工業大学学術国際情報センター）