平成 21 年度
実績報告

「実用化を目指した組込みシステム用
ディペンダブル・オペレーティングシステム」
平成 21年度採択研究代表者

木下 佳樹

(独)産業技術総合研究所 システム検証研究センター・研究センター長

利用者指向ディペンダビリティの研究

§1. 研究実施の概要

(1) ねらい

現代社会の情報処理システムに対応するディペンダビリティの概念を確立し、それを反映した規格策定、適合性評価法の検討、システムライフサイクル技術の検討などを行う。以下の4つのサブゴールを設け、プロジェクトを遂行している。

1. 「利用者指向ディペンダビリティ」の概念規定
2. 上の概念に基づいた国際規格策定
3. この規格に対する適合性評価技術の研究
4. この規格に適合したシステムライフサイクルを実現するシステムライフサイクル技術の研究

(2) これまでの研究の概要と進捗

- 利用者指向ディペンダビリティの概念規定: オープンシステムのディペンダビリティを考える上では、システムに関する情報を全て持つとは限らない利用者の視点から考えることが有効ではないかという予想から出発し、現代的なディペンダビリティの概念確立を目指している。
    ① ディペンダビリティの概念規定を試みた古典的論文を翻訳しテクニカルレポートとして5月に出版した。
    ② 7月には、利用者指向ディペンダビリティの問題意識や今後の研究の方向性について論文にまとめ、ディペンダブルシステムに関するワークショップにて発表した。
    ③ 9月と2010年2月に合宿を行い、概念規定を進めている。9月の合宿で議論された内容は、12月のサイトビジットの際に高村が発表した。来年度前半で3回程度の合宿を集中的に行い、利用者指向ディペンダビリティの概念を提案し、開放情報系との

関連を論じる論文を執筆する予定である。

- 国際規格策定:コミュニティ形成および de jure 規格策定準備の観点から、以下の標準化団体等で活動している。
  - ISO/IEC JTC1/SC7(Software engineering) WG7(system and software lifecycle)(木下、高井)
    5月のISO/IEC JTC1/SC7 のハイデラバードでの国際会議に参加し、木下および高井が改訂中であるISO/IEC 15026(system and software assurance)のcoeditorに就任し、現在草稿執筆作業に従事している。
  - IEC TC56(Dependability) WG4(System aspects of dependability)(高村)
    ディペンダビリティ関連規格の改定に対して、専門家の立場からコメントしている。
  - IEC TC65a(System aspects)(水口、木下)
  - OIML(International Organization of Legal Metrology) TC5/SC2(Software)(木下、松岡、水口、渡邊)
  - OMG(Object Management Group)(松野)
    Assurance case の記法に関する標準化を議論するSystem Assurance Platform Task Forceに2度参加し、今のところ、情報収集や、DEOS-CRESTプロジェクトの紹介などを行っている。

  以上の活動を通じて、安全性、ソフトウェア信頼性、ソフトウェアライフサイクル、オブジェクト指向などの標準化活動への浸透を図っている。利用者指向ディペンダビリティの概念が確立し次第、その規格化を適切な組織を通じて図る。
- 適合性評価:当初の計画で重要だと考えていた適合性審査は、責任を転嫁するシステムであるが、むしろ、assurance case(具体的にはD-case)などによって、リスクコミュニケーションを促進し、責任を利害関係者の間で共有するシステムのほうが有効であると現在では考えている。従って、assurance case、 特に、D-caseの研究を進めている。具体的な活動としては、適合性審査申請書類の内容及び様式を検討する立場から、assurance caseの考え方をコアチームに紹介した。その後、コアチーム内で松野が中心となり、オープンシステムに対する assurance case を目指して、D-case としてまとめた。また、assurance case の機械的な処理を目指して、assurance case を形式的な証明とみて機械処理するというアイディアをテクニカルレポートとしてまとめ、assurance case の国際ワークショップにて発表した。
- ライフサイクル技術
  ライフサイクル全般にわたってディペンダビリティを確保する技術の提供を目指す。当初は、今年度は開始しない予定であったが、前倒しして運用プロセスのライフサイクル技術の調査を開始した。GUD(guideline for user-oriented dependability)。まずは運用プロセスに注目し、ソフトウェア受発注時のガイドラインであるAIST包括フレームワークをもとに、運用プロセスにおけるガイドライン作成を目指す。今年度は、運用プロセスにおけるディペンダビリティ確保のための活動を調査するため、2社からのインタビューおよび産総研イントラシステムの運用の

調査を行い、今後作成するガイドラインの方向性について考察した。

§2. 研究実施体制

(1)「木下」グループ

①研究分担グループ長:木下 佳樹((独)産業技術総合研究所、研究センター長)

②研究項目

利用者指向ディペンダビリティの研究

§3. 研究実施内容

(文中に番号がある場合は(4－1)に対応する)

目的

オープンシステムに対するディペンダビリティの概念を確定し、それを反映した規格策定、適合性評価法の検討、システムライフサイクル技術の提案などを行う。

方法

(1) コアチームへの参加

松野、高村が参加した。松野が中心となり、9 月 4 日の中間審査のためのデモシステムに対する D-case 作成を行った。

(2) フレームワークチームへの参加

松野、高村が参加した。松野が中心となり、中間審査で用いたデモシステムに関する D-caseを改良した。

(3) 規格活動

ISO/IEC JTC1/SC7/WG7 では、木下および高井が、国内委員会にてそれぞれ委員およびエキスパートとして、ISO/IEC 15026 改訂作業を中心に活動している。具体的には、15026 の共同編集者として草稿の執筆作業、日本から提出する草稿に対するコメント作成、米国から他の共同編集者を日本に招聘しての共同執筆、5 月でのハイデラバード(インド)および 11 月リマ(ペルー)での国際会議参加、毎月の国内委員会参加などである。IEC 56 WG4 では、ディペンダビリティ関連規格の策定におけるコメント執筆、国内委員会でのオープンシステムディペンダビリティの紹介などを行った。

(4) 運用プロセスにおけるディペンダビリティ確保の技術

運用プロセスに対するガイドライン作成を目指して、実際のシステムにおける運用手順など調査した。具体的には、企業 2 社からのインタビューや、産総研次期業務システムの運用マニュアルの調査を実施した。

(5) 合宿形式でのディペンダビリティ概念確定

9 月から 10 月にかけて、4 名で 4 日にわたり、第 1 回目の概念確定のための合宿を実施した。主

に開放情報系に対してディペンダビリティを考える際に問題となることの洗い出しを行った。また、2010 年 2 月には、6 名で 3 日にわたり、第2回目の合宿を行い、第 1 回目の結果を踏まえて、開放情報系のディペンダビリティを考える上で必須となる概念をいくつかまとめつつある（対象化など）。この合宿では、論文化に向けた計画も立てた。

(6) ディペンダビリティの概念規定を試みた古典的論文の翻訳

ディペンダビリティの分野で基本とされる参照論文：Basic Concepts and Taxonomy of Dependable and Secure Computing の翻訳を行い、用語語集の作成も含めて 5 月に出版した。

木下佳樹、松野裕、高村博紀、武山誠、Basic Concepts and Taxonomy of Dependable and Secure Computing ディペンダブル・セキュアコンピューティングの基本概念と用語、算譜科学研究速報、2009 年 10 月

(7) 原子力発電所における開放性の調査

原子力発電所にもオープン性が見いだせるのではないかという所総括の示唆により、調査を開始した。具体的には、原子力発電所はクローズドなシステムと思われがちであるが、システム境界をどこにとるのかを柔軟に考えることによりオープン性を見ることができる。また高い安全性が求められるため、オープンシステムディペンダビリティを考える上で、有益な情報が得られるのはないかという予想があった。まず、システムに係る人として、オペレータから付近の住民まで、また監査機構である原子力安全委員会、保安院など政府の機関も含めて考えることでさまざまな利害関係者の間の合意形成などが大きな課題であることがわかった。また、安全文化に改善プロセスをみることができ、つねに文化を醸成する試みとして完成をみない（完成したと思ったら想定外のことが起こる）ようにすることで閉じさせない不断の努力にオープン性をみることもできる。例えば、原子力に係る法律は問題が生じたあとに、さまざまな意見を取り入れることで改定され、現時点での判断基準が変化することもありうる。

(8) 臨床情報学の提唱

情報処理に関するリスクを抱える現場に対して、情報学の研究成果を用いてそのリスクを軽減する活動に固有の学術としての臨床情報学を提唱した（下記（4－1）原著論文発表の 1）。主に、システム検証研究センターのこれまでの企業との共同研究活動における技術移転についてまとめたものであり、今のところ本 DEOS プロジェクトの他の要素技術などと直接関連づけていないが、情報システムのリスクを扱うディペンダビリティ研究は、情報科学における臨床研究であろうという基本的な考えは、本プロジェクトから得られたものである。

(9) ディペンダビリティ懇話会開催

4 月 15 日に、ディペンダビリティ懇話会と称し、ディペンダビリティ研究に関するインフォーマルなワークショップを開催した。ロボットやサービス工学など様々な分野からの講演者を得て、ディペンダビリティについて議論した。

(10) プロジェクト内定例報告会

本プロジェクトに参加する研究員を集めて、進捗具合や今後の研究方針について議論する場として定例報告会を実施した。機械安全、リスク管理などさまざまな背景をもつ研究者との討論を通じ

て社会的責任を意識した規格策定について、特にディペンダビリティ評価のための研究を行っている。

まとめ
コアチームとの連携においては、assurance case を木下チームから紹介し、松野が中心となりD-case としてまとめた活動が、領域全体を巻き込む活動となった。特に、システムがディペンダブルであることを開発者のみならずユーザーに対して明示化・説得するための手法として D-case を位置付け、これによって、コアチームの成果である DS-Bench、Metrics、Configuration の三部作間の関係が明確になった。

規格活動では、assurance case の規格として改訂作業中の 15026 の共同編集者として活動が中心となりつつある。

§4. 成果発表等

(4－1) 原著論文発表

- 論文詳細情報

1. 木下佳樹、高井利憲、臨床情報学のための野外科学的方法－技術移転の方法論に向けて、Synthesiology、3 巻、1 号、2010 年 3 月