「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 20 年度採択研究代表者

平成 20 年度
実績報告

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

本プロジェクトの目的は、情報処理システムのディペンダビリティ評価の手法を確立することである。DEOS 研究領域全体で開発するオペレーティングシステムのディペンダビリティを、この手法によって評価し、どのような意味で「ディペンダブル」なオペレーティングシステムを提供しようとしているのかを明確にすることにより、新たな価値を付加することを狙う。 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。

- ✧ 「利用者指向ディペンダビリティ」の概念規定
- ✧ 上の概念に基づいた国際規格策定
- ✧ この規格に対する適合性評価技術の研究
- ✧ 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確定について。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ながら精読し、日本語の用語確定を目指すとともに、継続可能なサービスの提供を保証するために必要なライフサイクルの過程について考察を進めている。
- ✧ 国際規格策定について。コミュニティ形成および de jure 規格策定準備の観点から ISO/IEC JTC1/SC7/WG7 および IEC TC56 の活動に参加することとした。2009 年 1 月より木下が JTC1/SC7/WG7 委員に、4 月からは高井が同 WG のテクニカル・エキスパートに、また木下と高村が IEC TC56 委員に、それぞれ就任した。一方、
- ✧ 適合性評価について。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（請合申立、保証事項の説得材料一式）の考え方を調査し、City University, London や CMU/SEI を中心とした International Working Group に参入するほか、JTC1/SC7/WG7 における ISO15026 System and Software Assurance の改訂検討をリードするなどしている。

✧ ライフサイクル技術に関しては、AIST 包括フレームワークを用いた事例作成と調査活動を開始し、全ライフサイクルを通じてのシステムのディペンダビリティの担保について研究活動を開始した。

3. 研究成果、今後の見通し

全般に、研究開始後六ヶ月であり、しかも他分野からディペンダビリティ規格の分野へ参入して間もないため、成果はまだ殆どなく、研究発表もポジション発表の程度にとどまっている。しかし、六ヶ月の試行錯誤によって、

1. 概念規定と用語確定に関しては古典的論文の分析、
2. de jure 規格活動に関しては JTC1/SC7 への参加、
3. 適合性評価に関しては assurance case の国際作業グループへの参画、
4. ライフサイクル技術に関しては産総研でこれまで続けてきた包括フレームワークを保守・更新・廃棄の全ライフサイクルに適用できるように拡張する

など、四つのサブテーマの進め方に見通しが得られた。また、

5. コアチームの活動およびオープンフレームワーク開発に二名の若手研究員を派遣して領域の他グループや研究開発センターとのアイディアの流通を図る
6. 産総研計算センターのシステム更新の過程を観察してディペンダビリティ確保上の問題点を探る
7. 英国の主要ディペンダビリティ研究サイト(Newcastle, York, Bath, City University London, Edinburgh, Swansea)を歴訪して、最新の研究動向を調査する

などを行った。今後も上記 5. 6. を続けるほか、7. の延長として

8. 欧州（大陸）および米国の主要ディペンダビリティ研究サイトを訪問して、最新の研究動向調査を続ける。

また、

9. 2009 年夏前にディペンダビリティ規格の草案を出して、領域の他グループからの意見を請う。
10. また、ディペンダビリティ評価の対象をどうするのかの議論、つまり OS そのもののディペンダビリティ評価を行うのか、OS の上で動くシステムの評価基準と評価法を与えるのかについての議論を開始する。
11. ディペンダビリティ評価指標の研究を assurance cases, safety cases などの知見をふまえて発展させ、適合性評価が厳正に行えるような規格づくりへ還元する。このことは利用者指向ディペンダビリティ概念と密接に関連する事柄である。

2. 研究実施内容（文中にある参照番号は 4.(1)に対応する）

1. 研究目的

情報処理システムのディペンダビリティ評価の手法を確立することである。DEOS 研究領域全体で開発するオペレーティングシステムのディペンダビリティを、この手法によって評価し、どのような意味で「ディペンダブル」なオペレーティングシステムを提供しようとしているのかを明確にすることにより、新たな価値を付加する。

2. 方法

✧ DEOS プロジェクト内での共同研究

DEOS 研究開発センターにおいて行われている、ネットワークにつながり、ユーザが直接触れる組み込みシステム(「Open Embedded System」と呼んでいる)のためのアーキテクチャを構築する作業に参加している。現在はディペンダビリティに関連する国際規格の調査などを行っている。今後われわれの利用者指向ディペンダビリティ規格の策定作業と協調しながら、共同研究を行う予定である。

✧ 包括フレームワークの試用

AIST 包括フレームワークの feasibility を確かめるため、システム検証研究センターで設立する連携検証施設のクラスタシステムの予約システム構築作業において、その試用(主に用件定義作業)を行っている。業務専門家であるシステム検証研究センターの倉垣に AIST Workflow エディターを使ってワークフローを書いてもらい、その作業の観察、および概念図の作成にかかわり、feasibility の調査を行っている。作業全体を AIST 包括フレームワークの専門家であるサービス工学センターの清野に見てもらっている。AIST 包括フレームワークは、現在システムの用件定義、開発を主に扱っている。今後特にシステムの運用において拡張を行い、われわれの利用者指向ディペンダビリティにおけるライフサイクル技術のベースとすることを計画している。

✧ コアチームでの活動

本領域のコアチームの活動に研究員を参加させ、規格策定の観点から開発オペレーティングシステムの要素技術に関して調査するとともに、本年度のコアチームの成果物である DS Benchmark, Configuration の執筆を一部担当した。またディペンダビリティ メトリックスの議論に参加し、ディペンダビリティ評価指標のための知見を得た。

✧ 規格策定のための活動

国際規格化のためのコミュニティ形成として、JTC1/SC7, IEC TC56 の活動に参加し、来年度より委員として我々の提案する利用者指向ディペンダビリティを基礎とする規格の策定への活動の足場をつくった。

✧ 先行研究プロジェクト訪問

今年度はイギリスのディペンダビリティに関する先行研究プロジェクトを実施した組織を訪問した。ニューキャッスル大では Cliff Jones 教授・Brian Randell 教授 他 6 名から PDCS 、DIRC、DEPLOY、ReSIST プロジェクトについて報告を受けた。エジンバラ大学では Don Sannella 教授、David Aspinall 講師から彼ら周辺でのディペンダビリティ関連研究を紹介され MRG 、Mobius、ReQueST プロジェクトの概要説明を受けた。ヨーク大学では Jim Woodcock 教授・Tim Kelly 講師他 5 名から同大計算機科学科 High Integrity Systems Engineering グループの研究紹介を受けた。Praxis-HIS 社の Managing Director Keith Williams 氏他 Praxis-HIS 社 3 名と、Martyn Thomas Associates 社の Martyn Thomas 博士から、Praxis-HIS 社 の活動について紹介を受けた。Robin Bloomfield 教授他から同大 Centre for

Software Reliability と Adelard 社の研究紹介を受けた。具体的には、医療分野の computer-aided decision making、Honeynet ネットセキュリティ データ収集、クリティカル・インフラの Preliminary Interdependency Analysis、DBMS の diverse redundancy、diverse redundancy 数理モデル、 Multi-legged argument の信頼性の Baisian Belief Net による分析、電子投票の dependability case、Adelard 社の Assurance case 関連の活動、ツール、適用事例紹介等。

✧ 総括への定例報告会

本プロジェクトは本領域の他のチームと性質が異なりオペレーティングシステムの開発を担当せず、規格策定を主に本領域の全体に関係をもつ。そのため定期的に領域総括との意思の疎通を図ることが重要である。本プロジェクトの方向性を議論する場として定例報告会を三回実施した。うち一回はディペンダビリティ関連規格である ISO/IEC 12207 の説明を行った。

✧ 基本参照論文の翻訳

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出版する予定である。当初は2008年12月に終了する予定であったが、2009年3月現在未完成であり、4月はじめに集中翻訳合宿を実施して加速する。

✧ ソフトウェア認証に関して

法定計量の分野ではソフトウェア認証が進んでおり、法定計量分野のソフトウェア規格では、OIML D 31 ソフトウェア制御の計量器の一般要求事項」が最先端の規格であるのでそれを調査した。具体的には、ディペンダブル規格でも要求事項として検討の対象になり得る、「監査証跡」、「分離」などの計量器ソフトウェアに対する具体的な要求事項例に関して調査した。

✧ 機能安全に関する活動

機能安全の国際規格である IEC 61508 ははじめてソフトウェアに関する要求事項がもうけられた国際規格である。ディペンダビリティに関する規格を策定するにあたり、適合性評価という観点からも IEC 61508 は重要な規格である。現在改定に向けての作業が行われているが、第2版におけるソフトウェアに対する要求事項（パート3）の詳細を理解し検討した。IEC 61508-3 第2版CDVの翻訳（コメント、注釈つき）を作成した。これはJIS化の際の原案となる。

✧ 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。

3. 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

4. 研究成果の発表等

特許出願

平成 20 年度 国内特許出願件数：0 件（CREST 研究期間累積件数：0 件）