「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

H24 年度
実績報告

木下佳樹

(独)産業技術総合研究所セキュアシステム研究部門・主幹研究員

利用者指向ディペンダビリティの研究

§1. 研究実施体制

(1)「木下」グループ

①研究代表者:木下　佳樹　(産業技術総合研究所情報技術研究部門、主幹研究員)

②研究項目

1. 開放情報系ディペンダビリティの概念確定
2. 開放情報系ディペンダビリティに関する規格制定
3. 適合性評価技術(D-Case)
4. ライフサイクル技術ガイドライン

§2. 研究実施内容

(文中に番号がある場合は(3－1)に対応する)

木下チームは全体で一つのグループとして活動している他、24年度はDEOSプロセス/アーキテクチャ会議と連携しながら活動した。4つの研究項目についてそれぞれ研究のねらい、これまでの研究の概要、研究進捗状況、研究成果、今後の見通しを説明する。

2.1. 開放情報系ディペンダビリティの概念確定

2.1.1. 研究のねらい

D-Caseの記述として結晶するオープンシステムディペンダビリティの静的側面の研究については、22年度までにほぼ終了しており、その成果はテーマ②の国際標準規格策定に受け継いでいる。
23年度からは残された課題である動的構造の研究を、rebuttal(反論)に基づくD-Caseの発展、進化、変化の研究に焦点を絞って進めてきた。

2.1.2. これまでの研究の概要

合意形成のダイナミズムを生むのは、D-Case 文書に対する反論 (rebuttal) である、との立場から、当初、いくつかの研究項目を設定したが、特に

① D-Caseの主張に対する反論(rebuttal)とそれを受けての修正とは、どのようなことなのかについての論理的分析とその支援システム

についての研究が進んでいる。

2.1.3. 研究進捗状況

①に関して、次の二つの研究を行った。

1. Dung が開始した「攻撃」(rebuttal に相当する) に基づく議論の解析を AI の研究者と研究交流しながら続けている。Dung による「議論フレーム」を、形式理論がつくる半順序集合あるいは圏に置換えて考えるアプローチをとっている。
2. また、このようなテーマに対しては従来、推論のための論理そのものを変更するアプローチ(non monotonic logic や description logic)が多かったが、我々は、論理は一階述語論理等の通常のものに固定し、その上の理論(公理系)が変化していくという立場から反論のモデルを作成した。

2.1.4. 研究成果

前項2.の成果発表が[2]である。

2.1.5. 今後の見通し

2.1.3 節1.については、我々のアプローチを、その簡単な適用結果とともにまとめて発表することが、プロジェクト終了前にできそうである。

2.2. 開放情報系ディペンダビリティに関する規格制定

2.2.1. 研究のねらい

Open Systems Dependabilityの概念の規格化はIEC TC56 Dependabilityで行う。ISO/IEC JTC1 SC7 Software and System Engineeringではシステムアシュランス(ディペンダビリティとほぼ同義語だが、米国でより多く使われる語)に関する先行活動にOpen System Dependabilityの概念を注入する。米国国防省が、四軍に対して「調達基準にISO15026-4を使ってもよい」との通達を出しており、この規格は今後注目されていくと思われる。また、D-Case周りのツールにつながる規格をOMG System Assurance Task Forceで構築する。

2.2.2. これまでの研究の概要

IEC TC56 では Open Systems Dependability の概念の説明を国内委員会で繰り返し行い、浸透を図った。ISO/IEC JTC1 SC7 WG7 では ISO/IEC 15026 Systems and software assurance の coeditor をプロジェクトから派遣し、Open Systems Dependability の概念を規格に埋め込むことができた。

2.2.3. 研究進捗状況

ISO/IEC JTC1 SC7 WG7では、ISO/IEC 15026 System and Assurance Case Part 4 Assurance in System Life Cycle のcoeditor(木下)を派遣して執筆し、IS (International Standard)として出版された。この規格は、システムライフサイクルの各過程でhigh assurance (= dependability)実現のために何を行うべきかについてのガイダンスを記したもので、我々の計画にとってはテーマ2.4の主要な成果ともなる。ISO/IEC 15026 System and Assurance Case Part 3 Integrity Levelsの改訂が25年に開始されそうなので、適応できるよう準備している。さらに、ISO/IEC 15026-2 Assurance caseの翻訳JIS化のための委員会活動が経済産業省からの日本規格協会への平成25年度委託事業として成立した。規格の国内普及の推進が見込まれる。

IEC TC56では、Open Systems Dependabilityの概念を記した新しい規格策定のNWIP (New Work Item Proposal)を提案し、当初の目論見よりは半年程度おくれたものの、投票の結果NWIとして認められ、しかも十分な数の国からexpert派遣を得て、規格作成プロジェクトがIEC TC56 PT4.8として2013年1月に成立した。当研究プロジェクトからPT4.8プロジェクトリーダ(木下)を派遣している。また、TC56 WG4 のconvener 辞任に伴い、当研究プロジェクトからTC56 WG4 convenerを派遣し(木下)2012年10月に任命された。

OMG (Object Management Group)のSystem Assurance Task Forceには、D-Case/Agdaが他に先駆けて実現しているassurance caseの整合性検査の機能について、それを可能にするための言語機能を規格化する計画MACL (Machine-checkable Assurance Case Language)を本プロジェクトから提案(武山、木下)、現在CFI の段階にある。

2.2.4. 研究成果

本年度の研究の最も顕著な成果は ISO/IEC 15026-4:2012 の出版[ISO/IEC 15026:2012 Information technology - Systems and software engineering - Systems and software assurance - Part 4 Assurance in the life cycle]である。2 名の editor (Project editor: K. Richter, coeditor: 木下佳樹)のうちの 1 名を本プロジェクトから派遣した。また、[武山誠、DEOS 実用化のためのオープンシステムディペンダビリティ国際標準化戦略、ET2012 カンファレンス スペシャルセッション C-8、

「オープンシステムディペンダビリティが世界を変える～DEOS（変化しつづけるシステムのためのディペンダビリティ向上技術）、いよいよ実証フェーズへ！～」、パシフィコ横浜、2012 年 11 月 16 日]などで普及活動を行い、産業界からのフィードバックを得ることができた。さらに、15026-2 の執筆により国際規格開発賞を本プロジェクトのメンバーが受賞し[国際規格開発賞（情報処理学会情報規格調査会）、木下佳樹、2012年 5 月 17 日（ISO/IEC 15026-2 執筆に対して）][国際規格開発賞（情報処理学会情報規格調査会）、高井利憲、2012年 5 月 17 日（ISO/IEC 15026-3 執筆に対して）]、15026-2 の JIS 化委員会活動が成立した[ISO/IEC 15026-2 翻訳 JIS 原案作成委員会、日本規格協会（経済産業省からの委託事業）、平成25年度]。また進捗状況に記したように、IEC TC56 に対して open systems dependability の要件規格化をわが国委員会から提案させ、TC56 のプロジェクトとして成立させ、そのためのプロジェクトチーム PT4.8 のチームリーダ、およびそのプロジェクトを所掌する WG4の convener を派遣することに成功した。

2.2.5. 今後の見通し

IEC TC56 PT4.8 によるOpen Systems Dependability要件規格策定は、早ければ本プロジェクト終了時にCD1が承認される見通しである。

ISO/IEC JTC1 SC7 WG7では当面、15026-3の改訂作業が中心となる。国内では15026-2の翻訳JIS化委員会[ISO/IEC 15026-2 翻訳JIS原案作成委員会、日本規格協会（経済産業省からの委託事業）、平成25年度]が活動する。

MACLのRFIに対する回答が2013年6月にまとめられ、早ければ12月にもRFP（Request For Proposal）OMG System Assurance Task Force 集会に提出することができる見通しである。

2.3. 適合性評価技術（D-Case）

2.3.1. 研究のねらい

D-Case の記述による適合性評価法を研究する。本プロジェクトで当初計画していた適合性評価法の研究を、D-Case の記述および評価法の研究として拡張し遂行している。

2.3.2. これまでの研究の概要

22 年度に D-Case/Agda システムを稼動開始させた。これに伴い、D-Case の様式を Agda 言語におけるデータ型およびその周辺の宣言として定式化した。23 年度には、D-Case 記述実験を開始し、D-Case 記述の方法論構築の試みを続けている。23 年度には、Web による架空の販売サイトの信頼性に関する D-Case 記述、X 社におけるソフトウェアバージョン運用ガイドラインの安全性に関する D-Case 記述などの記述実験を行った。

2.3.3. 研究進捗状況

24 年度は D-Case 記述実験を続けた。特に、本年度からは、記述に D-Case/Agda を用いることが可能になった。研究室のファイルサーバについて、設計、開発、運用、保守などの、システムライフサイクルの各フェイズでの D-Case 記述の実験を詳細に行った。

2.3.4. 研究成果

D-Case 記述実験の結果に基づき、記述方法についての試論を展開し、

[木下佳樹, 武山誠, 平井誠, 湯浅能史, 木藤浩之, D-Case/Agda によるアシュランス・ケース記述, JST CREST DEOS project technical report DEOS-FY2012-SV-01, 2012.]
[木藤浩之, 平井誠, 湯浅能史, 事例研究:高信頼なファイルサーバのためのアシュランスケースに基づく開発, Dependable Systems Workshop 予稿集, 日本ソフトウェア科学会, 2012.]

に記している。

2.3.5. 今後の見通し

上記に試論を記した D-Case 記述の方法論を完成させて、出版することがプロジェクト終了前に可能であると見通しを立てている。

2.4. ライフサイクル技術ガイドライン

2.4.1. 研究のねらい

Open Systems Dependability を達成するために、システムライフサイクルの各プロセスでどのようなことをなすべきか、を記したガイドラインを作成することとした。

2.4.2. これまでの研究の概要

ガイドラインを国際規格 ISO/IEC 15026-4 として標準化した。この規格では特に Open Systems Dependability の語は用いていないが、これまでの我々の研究成果を反映させている。一方、我国の産業界作成の、「IT 化の原理原則 17 ヶ条」にも、open system の立場から見て重要な条項が多数含まれているので、15026-4 執筆にとりいれた。

2.4.3. 研究成果

ISO/IEC 15026-4 の出版[ISO/IEC 15026:2012 Information technology - Systems and software engineering - Systems and software assurance - Part 4 Assurance in the life cycle]。また、この ISO 規格への日本委員会からの貢献の内容を記した「IT 化の原理原則 17 ヶ条」を英訳する活動に参加した。

2.4.4. 今後の見通し

ISO/IEC SC7 WG7 では、システムライフサイクルに関する基本規格 ISO/IEC 15288 および 12207 の改訂を開始しようとしており、これまでの我々の活動も、新たな 15288, 12207 に適応するよう、規格の保守を続けていく必要がある。

§3. 成果発表等

(3－1) 原著論文発表

・論文詳細情報

[1] Yoshiki Kinoshita and John Power, “Category Theoretic Structure of Setoids”, Theoretical

Computer Science, Elsevier, to appear.

[2] Yoshiki Kinoshita and Makoto Takeyama, “Assurance Case as a Proof in a Theory: towards Formulation of Rebuttals”, in *Assuring the Safety of Systems Proceedings of the Twenty-first Safety-Critical Systems Symposium, Bristol, UK.*, (Chris Dale and Tom Anderson, eds.), ISBN 978-1-4810-18647, CreateSpace Independent Publishing Platform, pp. 205-230, Dec 2012.

[3] Takeyama M, Kido H, Kinoshita Y (2012) Using a proof assistant to construct assurance cases, Fast Abstract in Proceedings of Dependable Systems and Networks (DSN), May 2012.

（3－2） 知財出願

① 平成 24 年度特許出願件数(国内　0 件)

② CREST 研究期間累積件数(国内 1 件)