

研究課題別中間評価結果

1. 研究課題名：利用者指向ディペンダビリティの研究

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

3. 研究概要

ディペンダビリティに関する従来の議論では、システムを **white box** としてとらえ、開発者の立場から **how** を論じることが多かった。我々はシステムを外界との関係において **black box** としてとらえ、利用者や運用者の立場から **what** を論じる観点を重視する。本研究領域が初めて提唱し、研究開発の目標とするオープンシステムディペンダビリティは我々の視点と一致している。主に他の研究チームにより行われている **DEOS** プロセス・アーキテクチャー実現に関する研究開発と並行して、本チームがオープンシステムディペンダビリティの概念を明らかにし、これを規格として策定し標準化し、具体的かつ標準的な手法を提供することは、今後の我々の生活の重要な基盤である巨大情報システムの開発から運用に至るディペンダビリティ確保のため極めて重要であると考え

る。

オープンシステムディペンダビリティの規格はいわゆる製品規格ではなく、**ISO9000** や **ISO14000**、**IEC61508** などと同様に、複雑な適合性評価の過程が必要な評価規格である。そのためには適合性評価技術とライフサイクル技術を与える必要があり、それらの開発を並行して行っている。具体的な活動としては、**ISO/IEC JTC1 SC7** に委員を送って活動し、**DEOS** プロセスの基本方針を取り入れた **assurance case**、**integrity level**、**assurance in life cycle** の規格を発行した。また **IEC TC56** に委員を送って活動し、新規検討項目 (**New Work Item**) 候補として **Open Systems Dependability** の議論が開始されており、2012 年春には **New Work Item Proposal** として最初のドラフトが提出される運びとなっている。

同様に **OMG** においても **ARM (Argumentation Metamodel)** や **SAEM (Software Assurance Evidence Metamodel)** などの規格を策定中である。加えて、**D-Case** 記述の論理的整合性を検査するための **D-Case/Agda** を開発し、無償公開した。

4. 中間評価結果

4-1. 研究の進捗状況及び研究成果の現状

標準化活動はこれまで研究とは異なるものであると考えられることもあったが、実用化を目標とした工学的分野の研究開発においては研究と標準化は一体として行うべきである。本チームは本プロジェクトの全体方向を理解し、これまでの研究並びに標準化活動の経験を活かして、標準化団体に委員を出して **Open Systems Dependability** 並びに **DEOS** プロセス・アーキテクチャーの規格化、国際標準化を行っている。実際に **Open Systems Dependability** ならびに **DEOS** プロセスに関するいくつかの成果が国際標準化案に組み込まれており、また、他のいくつかの成果が新たな国際標準化の新規検討項目 (**New Work Item**) として今春、日本から提案される予定で、本チームはそこで中心的役割を果たしている。規格化・標準化に向けた作業が開始されており、活動が着実に進んでいると考えられる。このチームがこれまで継続的に行ってきた **Agda** に関する研究成果は **DEOS** プロセスにおける **D-Case** の検証系として統合され、これに関する特許が出願され、無償公開されている。一部の規格化・標準化項目に関して、実際のシステムへの応用からのフィードバックが必要な部分もあり、企業との共同研究などによりこれが進められている。

一方で、**Open Systems Dependability** (概念) と **DEOS** プロセス・アーキテクチャー (具体的仕様) の規格化・標準化に関する全体像や標準化に向けた戦略がやや不明確な面もある。今後これをより一層明確にし、

活動を進める必要がある。

標準化作業は時間のかかる社会的な行動であり、まだそのスタートラインに着いたところである。Open Systems Dependability ならびに DEOS プロセス・アーキテクチャーが国際標準に盛り込まれれば非常に高いレベルの成果になる。今後の進展を大いに期待したい。

研究体制並びに研究の進め方については、規格化・標準化のそれぞれの項目に対して、経験者・専門家がその作業にあたっており、活発に標準化活動が行われていると考えられる。また、プロセス・アーキテクチャー・チームと融合して活動し、他のチームとの連携も良くとれている。研究費の執行状況についても特段の問題は無いと考える。

4-2. 今後の研究に向けて

これまでは主に Open Systems Dependability (概念) と DEOS プロセスにおける D-Case に関する部分について活動を行ってきた。今後は規格化・標準化の全体像をより一層明確にして、DEOS プロジェクトが出願している特許なども勘案し、戦略的に行動する必要があると考える。より具体的に言えば、Open Systems Dependability の概念を IEC60300 の下に置くのではなく、より上位の概念として位置づけることはできないか、DEOS プロセスを IEC61508 の置き換えとして位置づける可能性は無いのか、などの検討である。また、応用分野別の実現系となる DEOS アーキテクチャをどのように標準化の中に組み入れて行くかも今後検討する必要がある。ライフサイクル技術に関しては、規格策定にとどまらず、ガイドラインなどの策定を通して、企業など現場における運用や第三者認定への橋渡しができるレベルの具体的な研究活動を期待する。

4-3. 総合的評価

ネットワークで接続され、ますます複雑化する巨大ソフトウェアシステムのディペンダビリティの向上は人類・社会の喫緊の課題である。この課題の解決には、新たな概念の下で、具体的なプロセスとアーキテクチャを与え、国際標準規格によってその効果が担保されていることが必須である。本研究課題はオープンシステムディペンダビリティの概念ならびにこれに基づいた DEOS プロセス・アーキテクチャーを標準化することによってこの課題を解決しようとする世界で初めての試みである。本研究課題に関する国際標準化が達成できれば、ソフトウェア工学における我が国初ともいえる大きな国際貢献になり、関連する産業の競争力の向上に大いに寄与することができる。本チームは実際に国際標準機関に委員を送ってその作業を積極的かつ着実に進め、既にいくつかの標準化案に本研究領域の成果が組み入れられ、新たな標準化検討項目としても取り上げられていることは高く評価できる。標準化活動は人と時間のかかる作業であり、これからが成否を決める本番であるともいえる。今後、規格化・標準化の全体像をより一層明確にして、戦略的にその作業を遂行し、大きなスケールで国際標準に貢献することを期待する。