戦略的創造研究推進事業　CREST
研究領域
「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」
研究課題「利用者指向ディペンダビリティの研究」

研究終了報告書

研究期間　平成20年10月～平成26年　3月

研究代表者：木下佳樹
（神奈川大学理学部、教授）

§1. 研究実施の概要

(1)　実施概要

オープンシステムディペンダビリティの概念規定を DEOS 研究開発センターと共同で行った。それを反映させたライフサイクルにおけるアシュランスに関する国際標準を出版し、さらに本格的なオープンシステムディペンダビリティの要件標準策の新作業項目を IEC 内で開始し、今後十年以上にわたってオープンシステムディペンダビリティの国際標準を保守し続ける体制を国際標準団体 IEC の中に築いた。一方、アシュランスケースの構築によるオープンシステムディペンダビリティ評価法の研究を行い、アシュランスケースの自動的な整合性検査を可能にする形式アシュランスケースの定式化、それに基づいたアシュランスケース構築支援および整合性検査を行うソフトウェア研究開発、オープンシステムディペンダビリティ実現のためのガイダンス策定などを行った。以下では上記で下線を施した四つの小項目について実施内容と経緯、成果を記す。

概念規定　概念規定にあたっては、チーム内のみならず、研究領域サブコアチームに参加、連携して議論を重ね、研究領域全体による[19][25]の執筆に参加、貢献した。標準化作業からのフィードバックも有効に作用した。

標準化　本プロジェクトにおける標準化活動には、成果普及の目的以外に、プロジェクトが提出する概念の評価を、産学官の各視点からの総合的な判断能力を持つ国際標準化団体に求める、という目的がある。前者の目的のためには、まず概念を確定させた後に標準化を行うことになるが、後者の観点から、概念確定の研究と標準化を並行して行い、後者の作業からオープンシステムディペンダビリティの概念定義へのフィードバックを得ることができた。

De jure 標準については、ISO/IEC JTC1 SC7 Systems and software engineering および IEC TC56 Dependability において活動し、本チームと DEOS 研究開発センターによる研究成果をアシュランスに関する標準 ISO/IEC 15026 Systems and software assurance に反映させたほか、新作業項目 IEC 62853 Open Systems Dependability を提案し、TC５６の承認を得て成立させ、プロジェクトリーダを派遣した。さらに IEC 62853 策定作業を遂行する Working Group 4 の convenor を本プロジェクトから派遣して、オープンシステムディペンダビリティ関連標準の開発保守の長期的な環境を整備した。

また、Object Management Group (OMG) System Assurance Task Force (SysA) においても活動、Machine-checkable Assurance Case Language の標準制定活動を開始させた。

アシュランスケース研究　当初は本プロジェクトが提出する標準への適合性評価技術を一般に研究する計画であった。しかし、適合性評価技術のうち、アシュランスケースと呼ばれる文書に関する論理学的分析に絞ることとした。その経緯は以下の通りである。研究開始後約半年から一年で、ディペンダビリティをはじめ安全性やセキュリティなどのシステムの属性一般について、その評価結果をアシュランスケースによってまとめることが世界的に受け入れられつつあり、しかも膨大なアシュランスケース文書の整合性検査技術の研究が急がれることがわかった。研究領域全体としても、D-Case という形でアシュランスケースが DEOS プロセスにとりいれられた。

我々は、アシュランスケースを数理論理学における形式理論とそこでの命題及びその証

明の三つ組で表現する形式アシュランスケース(formal assurance case)に関する理論を構築し、それをもとにアシュランスケースの整合性を機械的に検査する方法を考案し、ソフトウェア D-Case in Agda によって実装して無償公開した。

ガイダンス策定　アシュランス達成のための一般的なシステム構築ガイダンスの項目を ISO/IEC 15026-4 の内容として標準化した。 また、受発注に関する D-Case 運用・保守のガイダンス[26]およびオープンシステムの合意形成に関するガイダンス[27]を発表した。これらの成果を得るために、研究チームおよび DEOS 研究開発センターにおける議論の結果に対する国際標準化委員会からフィードバックを獲得し、またアシュランスケース記述実験を行った。

(2)　顕著な成果

① 優れた基礎研究としての成果

1. D-Case in Agda の研究開発と公開

概要 : 依存型付プログラミング言語を用いてアシュランスケースを形式的に記述することによって、アシュランスケースの整合性検査を自動的に行うことを可能にする方式を考案し、形式アシュランスケースと名付けた[23]。並行して、D-Case の形式記述支援と整合性検査を行うソフトウェア D-Case in Agda を研究開発して無償公開した。この技術を D-Case のみならず一般の文書に適用させる特許を申請した[8]。

② 科学技術イノベーションに大きく寄与する成果

1. 受発注(supply chain)における D-Case の運用・保守に関するガイダンス提供

概要:システムの運用･保守過程における D-Case 文書の変更への対応が必要である。一年間の準備実験と一年半の D-Case 記述実験の結果、受発注における D-Case 文書の運用・保守に関するガイダンスをまとめて発表した[26]。受発注に限らず、アシュランスケースの変化対応の手順をまとめたものは、我々の知る限り、世界的に初めてのものである。システムライフサイクルの現場への D-Case の適用には、このようなガイダンスが不可欠であると予想され、今後現場での利用を見込む。

2. IEC TC56 における WG4 convenor ポストの獲得および新作業項目の開始

概要 : IEC TC56 Dependability WG4 System aspects of dependability の convenor (主査) を派遣することができた。主査は長期的に活動して TC の運営に参加する。したがって、このことは今後、長期にわたって、オープンシステムディペンダビリティ関連標準の開発保守の長期的な環境が整備されたことを意味する。

3. 国際標準 ISO/IEC 15026 の出版

概要 : ディペンダビリティに極めて近い意味をもつシステムアシュランス（安心・安全）を担保し、評価するための初めての国際基準 ISO/IEC 15026 の第二部から第四部までについて執筆者を派遣した。本標準は、米国 DoD、DHS などが採用に向けて準備を進めているため、今後わが国にも大きな影響を与えると予想される。

§２． 研究構想

（1） 当初の研究構想

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に立って how ではなく what を論じる観点から、システムの社会的責任への考慮を含めた総合的なディペンダビリティを、国際標準とその適合性評価ガイドライン、および規格に適合するためのシステムライフサイクルのガイドラインの形で表現することを目標とした。

「利用者指向ディペンダビリティの概念規定と規格策定」を唯一の研究項目として、利用者指向ディペンダビリティの概念規定、標準化活動、適合性評価法の研究、システムライフサイクル技術の研究などを行い、あわせて本領域のコアチームでの活動に参加し、研究開発センターで進められるオープンフレームワークの構築に関する共同研究を行う。一方、国際的に機能する標準を構築するため、ISO および IEC などの dejure 標準化団体および OMG などのフォーラム標準作成団体などに参加しながら国際的コミュニティ形成を図ることとした。

概念規定　チーム内での研究討論を出発点とするものの、標準化団体やコアチームなど、いろいろな場を利用して産業の現場での経験を取り入れるように努めることとした。

従来議論されているディペンダビリティは、既に記したように開発者の視点からみた色彩が濃く、要素還元主義的に構成要素を細分化し、その要素のディペンダビリティを向上すればシステム全体のディペンダビリティが向上するというどのように作るのかといった立場での議論が主であった。ネットワークで接続され、更新も頻繁に行われるなど複雑な現在のシステムには通用しない点がある。これに加え、コスト・納期等全要素が複雑に絡む要因を考慮しなければならない現実的な制約を考えると従来と違った視点でディペンダビリティを議論することとした。

そこで我々は「利用者」の立場からのディペンダビリティを議論したい。利用者の立場から「サービスの質」や「ユーザビリティ（使いやすさ)」、アカウンタビリティを取り入れてディペンダビリティ概念を考察していく。これはソフトウェアのみならず（人を含めた）システムのディペンダビリティの研究である。

システム分析、リスク評価、機械安全、機能安全などのエキスパートを集めたチームを形成し、に本計画に参加してもらい、月一回程度の打ち合わせを通じ、IEEE, IEC などのディペンダビリティに関する国際的活動に参加しながら議論を重ねて利用者指向ディペンダビリティの概念を規定することとした。

標準化　標準を de jure で開発するか de facto で開発するかの意志決定は中間審査までに行うこととした。De jure 標準化を行うとすれば IEC が一般のシステムに関するディペンダビリティ管理を規定した IEC60300 (Dependability management)を参照して情報処理システムのライフサイクルに特有の事情を反映した標準を作成することとなる。

適合性評価　システムの標準への適合性評価手法についての研究も行うこととした。本計画で作成する標準はいわゆる評価標準であり、これを有効なものとするためには、適合性評価の方法に関するガイドラインを策定し、評価過程を客観化することが必要である。そこで、以下を行うこととした。

1. 適合性評価のために開発者が提出する文書の様式を規定する。
   提出を求める開発過程の説明、システム・ライフサイクルの各過程におけるディペンダビリティへの考慮がなされていることに関する開発者自身の宣言などに関する文書およびそれぞれに記述すべき項目のリストを作成する。さらに、これらの文書に記されるデータの整合性、完全性の解析の自動化を考慮する。
2. 適合性評価において評価者が用いるべきチェックリストを規定する。
   既に法定計量や機能安全などの世界で作成され、利用されている適合性評価のためのチェックリストを参考に、本計画で策定する規格への適合性評価を求める場合に提出を求めるチェックリストを作成する。

ガイドライン　標準に適合するシステムを開発するために必要な、ディペンダビリティの分析手法、ディペンダブルなシステムの開発･利用手法（運用･保守･廃棄など）を、提出することとした。利用者指向ディペンダビリティ概念に基づき、環境の予期せぬ変化を考慮し、さらに、システムの開発過程の経験が後続システムの改善にどのように影響していくのか、またライフサイクルにおける各フェーズでの項目間の関係性などの構造を詳細化・明確化することで真のライフサイクルをもつ枠組でのディペンダビリティを考察していく。そのために、システムライフサイクルの実地調査を行う。具体的なシステム構築作業の実地調査をとおして、現実的なシステムライフサイクル技術の提案を行う。

(2)　新たに追加・修正など変更した研究構想

①　中間評価で受けた指摘や助言、それを踏まえて対応した結果について

研究領域全体での調整により、本プロジェクトで「利用者指向ディペンダビリティ」と呼んできたものも､「オープンシステムディペンダビリティ」に統一することとなった. 従って、本報告書でもこの用語に従う。

「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。Open Systems Dependability ならびに DEOS プロセス・アーキテクチャ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。」との指摘を受けて、以下のように戦略を定めた。

DEOS プロジェクトの成果は、大きく分けて二通りある。DEOS プロセス、D-Case 記述などの、システムライフサイクルプロセスを新しく規定することを通して、オープンシステムディペンダビリティ達成の要件を規定するものと、これらのプロセスを実現するための D-ADD, D-RE, D-Script, D-Case editor, D-Case in Agda などのツール群である。前者を規定するのが要件標準、後者を規定するのがツール標準である。

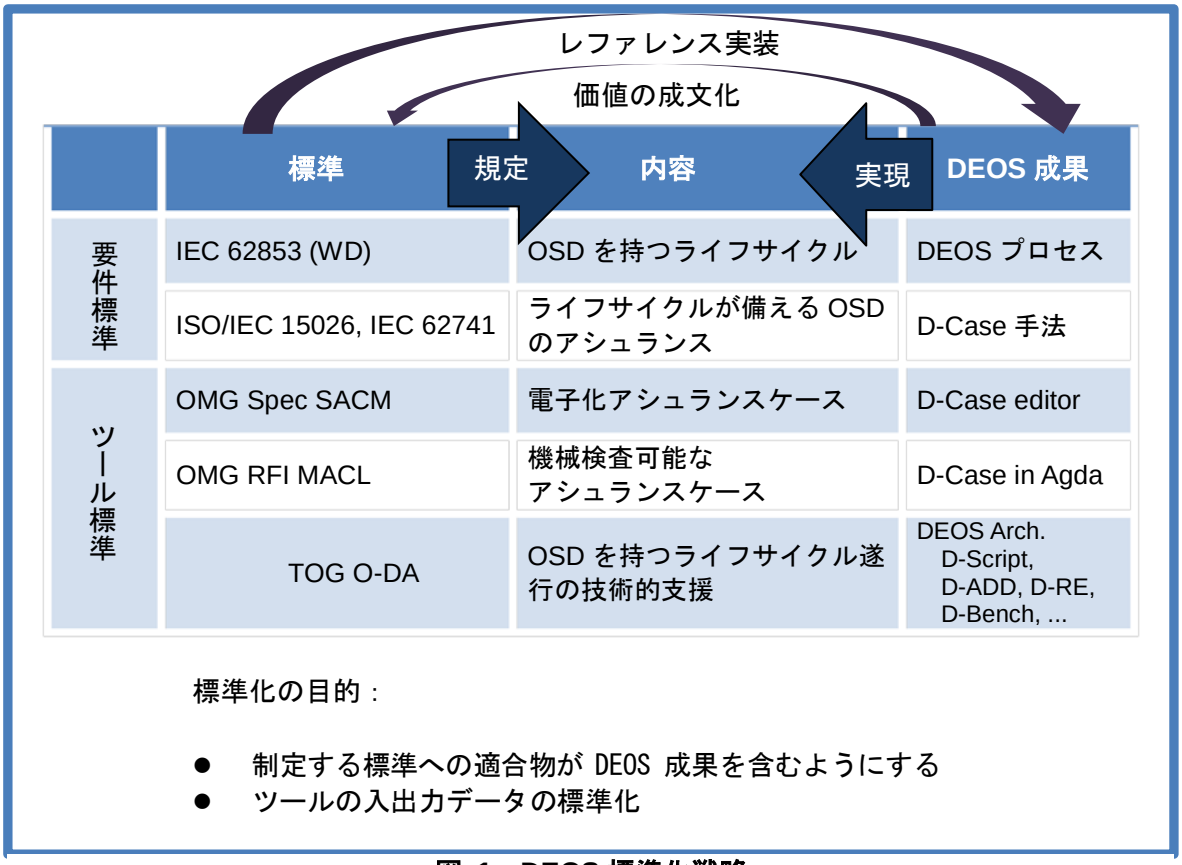

図 1　DEOS 標準化戦略

要件標準制定の場は、ISO および IEC におくこととした。これらはいわゆる de jure 標準制定団体である。具体的には ISO/IEC JTC1 SC7 Systems and software Engineering と IEC TC56 Dependability において活動することとした。

一方、ツール標準制定の場を OMG（Object Management Group）および TOG（The Open Group）におくこととした。これらはいわゆる forum 規格制定団体である。具体的には OMG System Assurance Task Force (SysA)などである。(TOG での活動は DEOS 研究開発センター。)

中間評価では、特に「Open Systems Dependability ならびに DEOS プロセス・アーキテクチャ」を国際標準に盛り込むことが求められた。前者についてはその後、IEC TC56 国内委員会を通して提案した IEC 62853/NP Open Systems Dependability が投票の結果採択され、各国からの専門家派遣をえて策定プロジェクトが 2013 年 1 月似発足し、3 年以内に標準が発行されることとなった。後者については、制定された TOG O-DA がそれに相当するものとなった。

中間評価ではさらに、「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」が求められた。IEC60300 については、その Part 1 が、現状では IEC TC56 活動の基幹標準として位置づけられており、数年ではそれを変更することは不可能である。しかし TC56 WG4 convenor を派遣して、TC の運営に参加したため、長期的な視野で 62853 を 60300-1 の上に位置づける、あるいはオープンシステムディペンダビリティの考えを次期

60300-1 の改訂に反映させる、などのことを容易にする環境を整えた。IEC61508 については、これは E/E/PE 機器の機能安全に限定した規格であり、オープンシステムという広範囲のシステムを対象とする我々の規格によってこれを置き換えるのは適当ではないと考える。

中間評価ではさらに「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」との指摘を受けた。これに対し、ISO 15026-4[4]策定、受発注における D-Case 運用保守のガイドライン[26]、オープンシステム達成のための合意形成手法の提示[27]などを行ったが、全体をまとめたガイドライン執筆にはいまだ至っていない。しかし、[26]などは、二年半にわたる D-Case 記述実験の成果であり、現場運用への橋渡しが十分にできるレベルの活動であると自己評価している。

② 中間報告書§7．今後の研究の進め方、および研究成果の見通しの記載事項に関し、研究を進めた結果について

今後の研究の進め方では『今後重点化すべき科学技術研究は「２．適合性判定技術」である。いっぽう、本プロジェクトの成果による社会貢献を「４．規格標準化」という形で進めていく。「３．ライフサイクル技術」は、規格標準化活動の一部として、産業の現場における知識を体系化して規格にするという形で進める。「１．ディペンダビリティの概念確定」は、求められるディペンダビリティ概念が開放系のディペンダビリティという形で明らかとなりつつあり、ほぼ終了した。』と記した。この点に関して、以下のように研究を進めた。

「２．適合性判定技術の研究」は、アシュランスケース（特に D-Case）の整合性自動検査技術の研究に集約し、D-Case in Agda の研究開発[1]および形式アシュランスケースの研究[23]を行った。また、「３．ライフサイクル技術」とも関連して、D-Case 記述実験を行い、システムライフサイクル現場への D-Case 適用にあたっての知見を蓄え、一部をガイドライン[26][27]として提供した。

「３．ライフサイクル技術」は上述の D-Case 記述関連のガイドラインに加え、ライフサイクルのプロセス一般に関するガイドライン ISO 15026-4[4]の執筆に参加、同標準を出版した。また IEC 62853[5]、OMG MACL の規格策定プロジェクトを開始した。

「1．ディペンダビリティの概念確定」がほぼ終了、と記したが、実際にはその後、IEC での規格制定活動からフィードバックを得て、概念規定の見直しを続けている。これは今後も続けるべき活動であろう．

次に研究成果の見通しでは『D-Case/Agda による assurance case 記述のテンプレートや、書き方のノウハウを集積し、assurance case 技術と呼ぶべき一つの技術分野を創出する、という方向に研究を進め、その成果を、ソフトウェア工学、ディペンダビリティなどの分野の規格活動を通して、社会に普及させていくことができると考えている。規格活動は爆発的なインパクトを社会に与える種類のものではなく、この方法では、中長期的に着実な活動を進めていく必要がある。一方、Argumentation 理論、法令工学、数理議論学、Toulmin model などの研究分野との交流から、新たな学問分野の創出につながる可能性が十分にあると考えられる。』と記した。これらの点に関して、以下のように研究を進めた。

D-Case in Agda (D-Case/Agda を改名)による D-Case 記述ノウハウを集積し、特に受発

注と合意形成についてガイドライン[26][27]を提供した。テンプレートの作成には至っていないが、そのためのデータ、材料を集めることができた。

標準化の中長期的活動については、IEC TC56 WG4 への convenor 派遣を達成し、そのための環境を整えた。

Argumentation 理論、法令工学、数理議論学、Toulmin model などの研究分野との交流については、国立情報学研究所公募型共同研究「議論の発展過程の数理科学的研究」(研究代表者: 木下佳樹)の 2012 年度からの実施、1st Intenational Workshop on Argument for Agreement and Assurance の 2013 年に実施、さらに国立情報学研究所湘南セミナー「Logical Desription Methods」の提案（採択決定、2015 年実施予定）などの進展を得た。

③　上記①②以外で生まれた新たな展開について

特になし。

§３．研究実施体制

(1)　研究チームの体制について

① 神奈川大学 木下グループ

研究参加者

氏名	所属	役職	参加時期
木下 佳樹	神奈川大学	教授	H20.10～
武山 誠	神奈川大学	研究員	H20.10～
平井 誠	神奈川大学	研究員	H24.4～
湯浅 能史	神奈川大学	研究員	H23.3～
中原 早生	神奈川大学	研究員	H25.4～
森口 草介	神奈川大学	研究員	H25.4～
水口 大知	産業技術総合研究所知能システム研究部門	研究員	H20.10～
渡邊 宏	産業技術総合研究所計測標準研究部門	研究員	H20.10～
山田 陽滋	名古屋大学大学院（産業技術総合研究所知能システム研究部門）	教授（産総研産学官制度来訪者）	H20.10～
和泉 憲明	産業技術総合研究所知能システム研究部門	主任研究員	H20.10～
岸本 充生	産業技術総合研究所安全科学研究部門	研究グループ長	H20.10～
田口 研治	産業技術総合研究所セキュアシステム研究部門	招聘研究員	H22.4～
木藤 浩之	産業技術総合研究所セキュアシステム研究部門	産総研特別研究員	H23.10～H25.2
後藤 里香	産業技術総合研究所セキュアシステム研究部門	テクニカルスタッフ	H23.11～H25.3
高井 利憲	産業技術総合研究所情報技術研究部門	研究員、テクニカルスタッフ	H20.10～H24.3

青峰　亮子	株式会社　東芝	社員	H22.11～H23.3
渡邊　竜明	株式会社　東芝	社員	H22.11～H23.3
長尾　洋平	株式会社　東芝	社員	H22.11～H23.3
小森　誠司	株式会社　東芝	社員	H22.11～H23.3
髙村　博紀	産業技術総合研究所システム検証研究センター	特別研究員	H20.10～H22.3
松野　裕	産業技術総合研究所システム検証研究センター	特別研究員	H20.10～H22.3
國定　美佐子	産業技術総合研究所システム検証研究センター	テクニカルスタッフ	H20.10～H22.3
松岡　聡	産業技術総合研究所計測標準研究部門	研究員	H20.10～H22.3
冨松　美知子	産業技術総合研究所システム検証研究センター	テクニカルスタッフ	H20.10～H22.3
岡本　圭史	産業技術総合研究所関西産学官連携センター組込みシステム技術連携研究体	招聘研究員	H22.11～H23.3
松崎　健男	産業技術総合研究所関西産学官連携センター組込みシステム技術連携研究体	テクニカルスタッフ	H22.10～H23.10

研究項目

・　「開放系ディペンダビリティの概念規定と規定策定」

（2）　国内外の研究者や産業界等との連携によるネットワーク形成の状況について

国際的な人的ネットワークを

- アシュランスケースの研究コミュニティ
- ディペンダビリティの国際標準化コミュニティ
- ソフトウェア工学、とくにアシュランスの国際標準化コミュニティ

にまたがって形成することができている。このような横断的活動において、我々はリーダシップを獲得しつつある。

アシュランスケースに関しては、アシュランスケースに関する初めての国際ワークショップ ASSURE 2013 にパネリストとして招聘された他、University of York、London City University, NASA Ames, SRI International などの研究者との間で、学会及び非公式な訪問を重ねて、新たな研究コミュニティを形成しつつある。また、国内外においてアシュランスケースと議論の論理に関する研究コミュニティを形成しつつあり、

- 国立情報学研究所公募型共同研究「議論の発展過程の数理科学的研究」(研究代表者: 木下佳樹) 2012-2013（延長の可能性あり）
- 1st Intenational Workshop on Argument for Agreement and Assurance, 2013.
- 国立情報学研究所湘南セミナー「Logical Desription Methods」の提案（採択決定、2015年実施予定）

などの活動に繋がっている。

ディペンダビリティに関する国際標準は IEC Technical Committee 56 （TC56） Dependability の管轄下にあり、この委員会のコミュニティに参加しはじめた。この委員会は機械やプロセス技術の専門家が集まっており、情報技術の観点が弱いが、下記の SC 7 との間のリエゾン委員を本チームから派遣するなど、ディペンダビリティ技術と情報技術の橋渡し役を国際標準の場で務めつつある。

ソフトウェア工学に関する国際標準は ISO/IEC Joint Technical Committee 1 (JTC1) Information technology SubCommittee 7 (SC7) Systems and software technology の管轄下にある。ISO/IEC 15026 のエディタチームへの参加を通じてこのコミュニティに参加し、IPA SEC (Software Engineering Center)においてまとめられたソフトウェアライフサイクル向上に関する知見を ISO/IEC 15026 に反映させるなど、既存の国内コミュニティと既存の国際コミュニティの橋渡し役を果たすことができている。

§４． 研究実施内容及び成果

本チームは一つの研究グループとして活動した。以下では四つのサブテーマ毎に研究実施内容と成果を説明する。

(1) 開放系ディペンダビリティの概念規定

ディペンダビリティの分野で基本とされる参照論文を翻訳して、用語語集の作成も含めて対訳版として公表した[28]。

オープンシステムディペンダビリティに関する議論をチーム内で重ね、オープンシステムでは、

- 予測不能(何が起こるか分からない)
- 利害関係者間の意思疎通の齟齬
- 経時的変化への追随の必要
- 全体像の把握が困難なこと

などの課題があること、これらの課題解決のためには

- 危機管理、
- 合意形成

の二つが重要であること、などを明らかにした。この結果をディペンダブル組込み OS 研究開発センターのコアチームに提出し、コアチームにおいて議論を重ねてさらに考察を加えた結果、[25]におけるオープンシステムディペンダビリティの基本概念として研究領域全体で共有できる概念となった。

このようにして、領域全体で確立したオープンシステムディペンダビリティの概念を、システムが達成するための要件を、国際標準化の立場から、さらに考察した。その結果、ISO/IEC 15288 における「プロセスビュー」の考えを用いて要件を表現することとし、またアシュランスケースに関するアシュランスケースをメタアシュランスケースと呼ぶことにした。要件を四つのプロセスビュー

- consensus formation
- accountability achievement
- failure response
- adaptation

を備え、かつ、システムのアシュランスケースが以下の四つの性質を満足していることであると表現した。

- intra-system consistency
- inter-system consistency
- validity
- confidence

このディペンダビリティの概念は、経時的変化や多様な価値観を考慮している点で、IEEE の提示した概念や IEC TC56 Dependability の定義にはなかったものである。特に、ニーズや要求の変化やシステムの環境の変化を考慮し、事前措置よりも事後措置に重点を置く点で、従来のディペンダビリティがリスク管理であったのに比べ、いわゆる危機管理を必要とするものである。

上記のようなオープンシステムディペンダビリティの要件の妥当性は、今後の実用化を待たなければならない。国際標準団体の有識者による判断もそのための一つの有効な指標であり、[36]の場で検討されている。

(2)　標準化

まず、本プロジェクトにおける標準化活動の位置づけについて記す。

現代のシステムでは、対象システムのディペンダビリティ達成だけに目的を絞っても、うまく行かず、関連するシステムを一緒に考慮にいれることが、対象システム自身のディペンダビリティ達成のためにはどうしても必要である。また、直接の利害関係者（stakeholders）だけではなく、周辺の組織や個人のことも考えにいれなければ、ディペンダビリティが長期的には達成できない。これがシステムのオープン性である。

周辺が皆でうまく行くようにするためには、システムについての基準を共有しなければならない。どの程度のコストをかけて、どこまで対策を講じなければならないのかが明らかにならないと、詳細を決めようがない。しかし、「ここまで対策しさえすればよい」という命題は論理的、科学的に客観性をもって結論できるものではなく、その基準は、社会常識あるいは世間一般の通念や評価によって決められるものである。

社会的通念がきめる基準は、通常曖昧で暗黙的なものだが、ディペンダビリティ達成のためには、明確な基準が必要である。曖昧で暗黙的な基準を標準化し、明文化することによって、社会全体が共有する基準を明確にすることができる．これによって初めてしてディペンダビリティ達成活動の出発点が得られる。

標準化は、社会全体でディペンダビリティを達成するための手段であり、その意味でオープンシステムディペンダビリティ達成のための要素技術である。つまり、技術の成果を普及するだけではなく、ディペンダビリティ達成のための一連の過程の一つとして標準化活動を捉えている。

以上のような位置づけのもと、標準活動の場を de jure に求めるのか de facto ないし forum 規格制定団体に求めるのかを決める必要があったが、研究総括と相談の上、中間審査時まではその決定を持ち越すこととした．一方、de jure 標準活動をもし展開するとすれば、委員会に加入して人的ネットワークを築くのに時間が必要なので、プロジェクト開始後すぐに ISO/IEC JTC1 SC7 Systems and software engineering と IEC TC56 Dependability に委員を派遣した。オープンシステムディペンダビリティは情報システムのディペンダビリティであるが、TC56 では情報システムに疎く、SC7 では情報システムの専門家は多いがディペンダビリティに疎いため、双方の委員会にまたがった活動が必要だと判断した。

JTC1 SC7 に参加したところ、ちょうどアシュランスケースに関する[2]を策定している最中であった。システムアシュランスとディペンダビリティは極めて近い考えであるので、コエディタを派遣し、[2][3][4]の執筆に参加した。

中間報告の前に、de jure 活動はいずれにしても必要であるという判断をして、TC56 にオープンシステムディペンダビリティの要件規格を提案することとした。しかし、提案をしても各国委員会の投票で承認されなければならない上、たとえ投票で可決されても、五ヶ国以上の委員会から専門家のプロジェクトチームへの派遣がなければ、規格制定のプロジェクトは成立しない。そのため、TC56 の国際委員会の場で周到な準備が必要であった。2010 年の年次集会で非公式に打診し、2011 年の年次集会でアイディアについてのプレゼンテーションを行い、2012 年夏に新規作業項目を提案して直後の年次集会で提案についてのプレゼンテーションを行ったところ、十分な理解を得て投票による承認および七ヶ国（日本を含む）からの専門家派遣を得て、プロジェクト[5]が成立した。

[5]は TC56 内部でも、今後のディペンダビリティ標準のあるべき方向性を示しているとの認識が広がりつつあり、特にオーストラリア、中国からの強い支持を得ている。

中間報告の後、要件規格は de jure で、ツール標準は forum で行う方針を定めた。以下、OMG におけるツール標準の我々の活動を記す。

アシュランスケースについては、[2]があるが、その形式についての詳細な標準が Forum 標準制定団体である OMG において審議されており[6]、これにコメントを送付して策定に貢献した。

さらに、我々のソフトウェア D-Case in Agda に関連する標準[7]の策定提案活動を OMG において行っており、現在 Call For Information を行っている段階である。

最後に関連標準について説明する。ライフサイクルに関する ISO/IEC 15288 と ISO/IEC 12207 は SC7 における基幹標準である。また、TC56 における基幹標準は、ディペンダビリティ管理に関する IEC 60100-1 である。[5]の案は IEC 60100-1 を参照しながら、ISO/IEC 15288 に規定されているライフサイクルに関してオープンシステムディペンダビリティ達成の要件を定義するものである。　IEC 60100-1 には独自の「ディペンダビリティライフサイクル」の定義があり、これが ISO/IEC 15288 のシステムライフサイクルと必ずしも整合しない。これは今後の課題を生んでおり、オーストラリア委員会とともに解決のための作業を進めている。

(3)　アシュランスケース

アシュランスケースの論理学的およびプログラミング言語論的な分析を行って、DEOS

研究開発センターによる D-Case の概念構築に貢献した。その成果は国際標準[2]および提案準備中の[7]に反映されている。

また、プログラミング言語によるアシュランスケースの記述を支援するソフトウェア D-Case in Agda を証明支援系 Agda の上に実装し、無償公開した。この方式ではプログラミング言語によってアシュランスケースを記述するため、プログラム構成・管理の豊富な機能（バージョン管理やモジュール機能、抽象化、構文拡張機能など）をアシュランスケースの管理・構築のために用いることができるのが特長である。

プログラミング言語によるアシュランスケース記述を以下に簡単に説明する。

アシュランスケースは、その語彙と基本的前提（公理）の記述部分と、議論の記述からなる。語彙の記述はプログラミング言語における変数や定数、関数、データ型などの宣言に相当する。基本的前提は公理に相当するが、Agda 言語のような構成的型理論に基づくプログラミング言語では、論理式やその形式証明も記述することができるため、公理も記述することができる。

一方、議論は Claim, argument, evidence からなるが、これらが丁度、厳密な意味で、形式証明の帰結、証明規則、証明規則適用の前提に対応する。この対応のもとで、Agda 言語の形式証明の記述機能を用いて、議論を記述することができる。

D-Case in Agda は、型検査機能を用いて、アシュランスケースの整合性検査機能の他、プレースホルダーの機能を用いた記述支援機能を提供する。

D-Case エディタや各種の GSN 記述支援環境では、アシュランスケースへの操作がソフトウェアで規定されているため、新たな操作を加えたり、既存の操作の変更をするにはソフトウェアを改版する必要がある。しかし、D-Case in Agda ではアシュランスケースへの操作をユーザがプログラムとして実現できるため、アシュランスケース操作の実験には有利である。一方、このようなジェネリックなツールをエンドユーザにそのまま提供すべきかどうかについては疑問が残る。今後の研究課題である。

(4)　開放系ディペンダビリティ達成のためのガイダンス

システムライフサイクルがオープンシステムディペンダビリティを達成するためのガイダンスを提供した。ガイダンスのための材料は、国際標準委員会における識者との討論と、D-Case 記述実験のふたつから得た。

[4]は、システムアシュランス達成のためのガイダンスで、システムアシュランスとディペンダビリティの概念が近いことから、オープンシステムディペンダビリティ達成のための要件を多数、[4]に埋め込むことができた。ガイダンスの内容は、本チームのみならず、国内委員会および国際委員会における識者との討論による。

一方、企業のシステムライフサイクル現場においけ D-Case 記述実験を繰り返し、そこから本チームが材料を抽出してガイダンスを提供した。実験は大きく分けて三つある。まず T 社における組込みシステム開発ライフサイクルに D-Case を適用する実験を一年間にわたって行い、ライフサイクルの各過程における D-Case 関連のタスクを考察した. しかしこれは、T 社自身の企業秘密と抵触する場合があって、余り自由な実験ができなかった。

そこで、本プロジェクトが出資する自前の小さなライフサイクルを計画し、それに関する D-Case 記述実験を二年半にわたって行った。研究室のファイルサーバがそのライフサイクルの対象である。要求抽出から始め、仕様記述から開発のみでなく運用や保守の過程についても実験ができた。実際の開発運用は経験豊富な企業との協力体制をとり、従来の開発運用のノウハウも取り入れた。特にチームの産総研から神奈川大学への移動は、ファイルサーバに関する大掛かりな保守案件を生み、よい実験材料を提供した。DEOS プロセスの全てのアクティビティに関して、そこでの関係者合意を記述するための実践的な D-Case パターンを確立した。これら一連の実験の結果、[16][19][26][39][66]などの成果を出した。

また、オープンシステムの開発運用における、権限委譲と説明責任に関する研究を行った。このようなシステムでは、環境の変化や想定外の障害に対応できる体制を、如何に実現するかが、従来から重要な問題とされてきた。我々は連鎖する複数の業務委託での権限委譲と説明責任の事前合意により解決する方法を提示し、ファイルサーバ運用開を題材に適用実験を行った[26]。

さらに、(株)Symphony における放送業務への D-Case 適用事例を解析し、オープンシステム関する合意形成の方法論[27]を提供した。

[4]のようなライフサイクル一般のガイダンスは、既に[35]などがあるが、国際規格とした点に意義がある。

[26]のようなアシュランスケースに関するライフサイクルのガイダンスは、我々の知る限り、前例がない。実用を前提とした DEOS システムを、ゼロから開発、長期に渡って運用した事例は、世界初といえる。今後、ライフサイクルの他の過程にもこのようなものが提供されていくべきである。

[27]のように、合意形成に関するガイダンスを情報システムに関して記したものも、我々の知る限り前例がない。合意形成は既にいろいろなところで論じられているが、多くは社会システムにおける合意形成に関するものであった。DEOS では合意形成を重視するので、今後この方向の考察を進めて行くべきである。

§ 5． 成果発表等

(1) ソフトウェア/ハードウェア

[1] D-Case/Agda: D-Case の整合性を検査するツール。2011 年 10 月に Windows 用のインストーラとともに無償公開。URL: http://wiki.portal.chalmers.se/agda/pmwiki.php?n=D-Case-Agda.D-Case-Agda

(2) 国際標準

[2] ISO/IEC 15026 Systems and software engineering -- Systems and Software Assurance -- Part 2 Assurance Cases, 2011 年 2 月 2 日発行.
本プロジェクトより Coeditor を派遣。

[3] ISO/IEC 15026 Systems and software engineering -- Systems and Software Assurance -- Part 3 Integrity levels, 2011 年 12 月 16 日発行.
本プロジェクトより Coeditor を派遣。

[4] ISO/IEC 15026 Systems and software engineering -- ystems and Software Assurance -- Part 4 Assurance in the life cycle, 2012 年 9 月 28 日発行.
本プロジェクトより Coeditor を派遣。

[5] IEC 62853:NP Open Systems Dependability,
本件は標準は未発行。各国の投票による承認および7ヶ国からの専門家の派遣を得て IEC TC56 PT4.8 においてプロジェクトを 2013 年発足させた段階。本プロジェクトより Project leader および project member、また DEOS 研究開発センターより project member を派遣。

[6] Object Management Group Standard, “Structured Assurance Case Metamodel (SACM), Version 1.0,” OMG Document Number: formal/2013-02-01, Standard document URL: http://www.omg.org/spec/SACM, 2013.
本プロジェクトよりコメント提出の形で策定に貢献。

[7] Object Management Group Standard, “Machine-checkable Assurance Case Language (MACL),” OMG CFI (Call for Information).
本プロジェクトから CFI の内容を提供。本プロジェクトが推進した。

(3) 知財出願

①国内出願 (1 件)

[8] 1. アシュアランス・ケース文書の整合性の機械的検査を、定理証明支援系によって行う手法、発明者:木下佳樹、武山誠、出願人:野間口有、平成 23 年 9 月 6 日、特願 2011-193452

②海外出願 (0 件)

③その他の知的財産権

なし

(4) 原著論文発表 (国内 (和文) 誌 4 件、国際 (欧文) 誌 1 5 件)

1. 著者、論文タイトル、掲載誌 巻、号、発行年

[9] Yoshiki Kinoshita, Yutaka Matsuno, Hiroki Takemura, Makoto Takeyama, Toward User Oriented Dependability Standard for Future Embedded Systems, First International Workshop on Software Technologies for Future Dependable Distributed Systems (Stfssd 2009), IEEE, March 1 2009.

[10] 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.

[11] Kenji Taguchi, Nobukazu Yoshioka, Takayuki Tobita, Hiroyuki Kaneko. “Aligning Security Requirements and Security Assurance Using the Common Criteria”, In Proc. Fourth International Conference on Secure Software Integration and Reliability Improvement, SSIRI 2010, Singapore, June 9-11, 2010. IEEE, pp69-77.

[12] Yoshiki Kinoshita and Toshinori Takai. “A field-scientific approach to Clinico-Informatics”, Synthesiology English edition, Vol. 3, No. 1, pp.64-76, ISSN 1883-0978 (Print), ISSN 1883-2318 (Online), July 2010.

[13] Keishi Okamoto, Yoshiki Kinoshita, Takahiro Seino, Noriaki Izumi, Koiti Hasida and Hiroki Takamura. “A Design for an Assessment Process for Dependability based on a Formal Model”, Proceedings of the IASTED International Conference, Advances in Management Science and Risk Assessment (AMSRA 2010).

[14] Yutaka Matsuno, Jin Nakazawa, Makoto Takeyama, Midori Sugaya, Yutaka Ishikawa. Toward a Language for Communication among Stakeholders. In Proc. The 16th IEEE Pacific Rim International Symposium on Dependable Computing, IEEE, Dec. 2010.

[15] Takashi Kitamura, Keishi Okamoto, Makoto Takeyama. Formal validation and requirements management based on the Jackson's reference model for requirements and specifications (Fast Abstract). In Proc. The 16th IEEE

Pacific Rim International Symposium on Dependable Computing, IEEE, 2010.
[16] T. Komoto, K. Taguchi, H. Mouratidis, N. Yoshioka, K. Futatsugi, A Modelling Framework to Support Internal Control, 2011 Fifth International Conference on Secure Software Integration and Reliability Improvement - Companion, pp187-193, IEEE, 2011.
[17] Yutaka Matsuno and Kenji Taguchi, Parameterised Argument Structure for GSN Patterns, Proceedings of the 11th International Conference on Quality Software, Jul., 2011.
[18] Hiroyuki Kido, Katsumi Nitta: Toward Justifying Actions with Logically and Socially Acceptable Reasons, Lecture Notes in Artificial Intelligence, Proc. of 10th Mexican International Conference on Artificial Intelligence, Part 1, 7094, pp. 52-64, 2011.
[19] DEOS プロジェクト White Paper, Version 3.0, November, DEOS レポート DEOS-FY2011-WP-03J, 2011, URL: http://www.dependable-os.net/osddeos/data/DEOS-FY2011-WP-03J.pdf
[20] 大畠明, 田口研治, 松野裕, 中坊嘉宏, 消費者機械安全性・信頼性保証の国際標準化, SEC Journal, 7, 4, IPA, Jan., 2012.
[21] 木藤浩之, 新田克己: Pareto 最適な撤回可能帰結を軽信的に正当化する実践的議論意味論, 人工知能学会論文誌, Vol. 27, No. 2, pp. 52-60, 2012.
[22] Yoshiki Kinoshita and John Power, “Category Theoretic Structure of Setoids”, Theoretical Computer Science, Elsevier, to appear.
[23] 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.
[24] 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.
[25] Mario Tokoro (ed.), Open Systems Dependability, CRC Press, ISBN 978-1-4665-7751-0, 2013.
[26] Makoto Hirai, Yoshifumi Yuasa and Yoshiki Kinoshita, A Chain of Accountabilities in Open Systems based on Assured Entrustments, The 3rd International Workshop on Open Systems Dependability: Adaptation to Changing World (WOSD 2013), Nov. 2013.
[27] Yukiko Yanagisawa, Takashi Ito, Makoto Takeyama and Yasuhiko Yokote, A New Method of Consensus Building for Open Systems Dependability, The 3rd International Workshop on Open Systems Dependability: Adaptation to Changing World (WOSD 2013), Nov. 2013.

(5) その他の著作物（総説、書籍など）

[28] 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.
[29] 木下佳樹, 高井利憲, 田口研治, 武山誠: オープンシステムディペンダビリティに関する考察～「視点の動的網」による解決～, 算譜科学研究速報 AIST01-J00022-103, PS-2010-003, 産業技術総合研究所, 2010 年 5 月 13 日.
[30] 木下佳樹, 高井利憲: 情報システムディペンダビリティ認証項目について, 算譜科学研究速報 AIST01-J00022-104, PS-2010-004, 産業技術総合研究所, 2010 年 7 月 13 日.
[31] 木下佳樹, 高井利憲: 記述の科学-第 1 回 記述とは. 情報処理、Vol.51、No.8,

pp. 1049-1057、2010 年 8 月.
[32] 木下佳樹, 高井利憲: 記述の科学-第 2 回 視点と形式的体系. 情報処理、Vol.51、No.9, 2010 年 9 月.
[33] 木下佳樹, 高井利憲: 記述の科学-第 3 回 記述の構成と利用. 情報処理、Vol.51、No.10, 2010 年 10 月.
[34] Makoto Takeyama, “A note on `D-Cases as proofs as programs”’, 算譜科学研究速報 AIST01-J00022-107, PS-2010-007, 産業技術総合研究所、2010 年 10 月 28 日.
[35] IPA (Information-technology Promotion Agency, Japan, Software Engineering Center, Development Process Sharing Committee, “The seventeen principles for system development – a ‘cho-joryu’ approach”, http://www.ipa.go.jp/sec/reports/20120502.html
[36] IEC 56/1482/NP, New work item proposal, Open Systems Dependability, Proposed by Japan, 2012.
[37] 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.
[38] 木下佳樹 武山誠(産業技術総合研究所), 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, JST CREST DEOS project technical report, DEOS-FY2012-SS-01J, 2012.
[39] 湯浅 能史, 木下 佳樹. システムのコンポーネント構成に着眼した CD ネット販売における障害対応の Assurance Case 作成, 算譜科学研究速報, 産業技術総合研究, 2012.5.
[40] Makoto Hirai, Hiroyuki Kido, Yoshiki Kinoshita, Makoto Takeyama, Yoshifumi Yuasa. D-Case in Verification and Validation, 産業技術総合研究所, 2013.3.

(6) 国際学会発表及び主要な国内学会発表

① 招待講演 (国内会議 0 件、国際会議 2 件)

[41] Yoshiki Kinoshita、 Fieldwork and the 4:6 Principle-Introduction to the Research Center for Verification and Semantics、12th IEEE International Symposium on Object/component/service-oriented Real-time distributed Computing (ISORC2009)、 AIST、 March 19 2009.
[42] Yoshiki Kinoshita. Verifying Open Systems Dependability, Verifying Reliability (Dagstuhl Seminar 12341), Schloß Dagstuhl, 2012.8.23.

② 口頭発表 (国内会議 １９件、国際会議 ２２件)

[43] Makoto Takeyama, Formalization of System LSI Specification and Automatic Generation of Verification Items, Newcastle CSR-AIST meeting, The Centre for Software Reliability, the Dept. Of the University of Newcastle, Newcastle, UK, February 24, 2009.
[44] Makoto Takeyama, Formalization of System LSI Specification and Automatic Generation of Verification Items, York HISE-AIST meeting, High Integrity Systems Engineering, the University of York, York, U.K., February 27, 2009.
[45] Makoto Takeyama, Formalization of System LSI Specification and Automatic Generation of Verification Items, Bath-AIST-Swansea workshop, the Dept. of Computer Science, Swansea University, Swansea, U.K., March 4, 2009.
[46] Makoto Takeyama, Formalization of System LSI Specification and Automatic Generation of Verification Items, CUL CSR-AIST meeting, The Centre for Software Reliability, City University London, London, U.K., March 6, 2009.

[47] Yoshiki Kinoshita, Yutaka Matsuno, Hiroki Takamura, Makoto Takeyama, Toward User Oriented Dependability Standard for Future Embedded Systems, First International Workshop on Software Technologies for Future Dependable Distributed Systems, IEEE, the Okubo Campus of the Waseda University, March 17 2009.
[48] 武山誠、岡本圭史、DEOS (Dependable Embedded OS) Project and Assurance Cases、 Assurance Cases for Software-based Systems in a Regulatory Environment、Chuck Weinstock 、米国、2009 年 05 月
[49] 木下佳樹、User oriented dependability、第 7 回ディペンダブルシステムワークショップ、北海道大沼、2009 年 7 月
[50] 武山誠、岡本圭史、An approach to assurance cases、第 7 回ディペンダブルシステムワークショップ、北海道大沼、2009 年 7 月
[51] 中澤仁（慶應義塾大学）、松野裕、菅谷みどり（JST）、塙敏博（筑波大学）、前田俊行（東京大学）、石綿陽一（デジタルヒューマン研究センター）、杵渕雄樹（早稲田大学）、高村博紀、藤田肇（東京大学）、三浦信一（筑波大学）、山田浩史（慶應義塾大学）、ディペンダビリティメトリクス、 第 7 回ディペンダブルシステムワークショップ、北海道大沼、2009 年 7 月
[52] 加藤真平、藤田肇、中澤仁、松田元彦、前田俊行、杵渕雄樹、塙敏博、三浦信一、石綿陽一、松野裕、高村博紀、山田浩史、吉田哲也、倉光君郎、菅谷みどり、石川裕、ディペンダブルシステム向けベンチマークフレームワークの提案、第 7 回ディペンダブルシステムワークショップ、北海道大沼、2009 年 7 月
[53] 武山誠、Assurance cases in Agda: Incorporating informality、5th Theorem Proving and Provers (TPP) Meeting、関西学院大学 神戸三田キャンパス、2009 年 11 月
[54] 松野裕、Dependability Case for Embedded Systems in DEOS project、OMG technical meeting、ロングビーチ、米国、2009 年 12 月
[55] 高井利憲、高村博紀、Dependability standards and our challenge to establish new standard for open systems、57th IFIP WG 10.4 Meeting、石垣島、2010 年 1 月
[56] 中澤仁（慶應義塾大学）、松野裕、Dependability Case and Metrics for Open Systems Lifecycle、57th IFIP WG 10.4 Meeting、石垣島、2010 年 1 月
[57] 高井利憲: DEOS プロジェクトの国際標準化への取組み紹介, JASA 安全性向上委員会、2010 年 4 月.
[58] 岡本圭史、木下佳樹、清野貴博、和泉憲明、橋田浩一、高村博紀. “形式モデルに基づくディペンダビリティのアセスメントプロセスの設計”, 第 42 回情報システム研究会, 大阪府立大学, 2010 年 5 月 28 日.
[59] 和泉憲明, 岡本圭史, 木下佳樹, 高井利憲, 高村博紀, 田口研治, 武山誠, 水口大知. “オープンシステムディペンダビリティと利用者指向 ～課題と解決へのアプローチ～”, ディペンダブルシステムワークショップ（日本ソフトウェア科学会ディペンダブルシステム研究会主催）, 大沼, 2010 年 7 月 22 日.
[60] 高井利憲, 伊東敦, 武山誠, 上野肇, 高村博紀, 松野裕: D-Case を用いた保証プロセスについて, ディペンダブルシステムワークショップ（日本ソフトウェア科学会ディペンダブルシステム研究会主催）, 大沼, 2010 年 7 月 21 日.
[61] 高井利憲: 事故は避けられない---そこから始まるディペンダビリティ, RT 機能安全研究専門委員会、2010 年 9 月.
[62] Makoto Takeyama. “Assurance Cases in Agda”. 3rd Wessex Theory Seminar. 14 April 2010.
[63] Makoto Takeyama. “D-Case graphical editor to Agda connection”. AIM 12, Nottingham, 1 September 2010.
[64] K. Taguchi, Meta-modeling approach to Safety Standards for Consumer

Devices, Seminar on Systems Assurance & Safety for Consumer Devices: Automotive, Robotics & Building Automation Systems of the Future, 22, June, 2011, OMG.
[65] 木下佳樹, 武山誠, 田口研治, 松崎健男, 湯浅能史, 高井利憲, DEOS-CREST プロジェクト紹介, 形式手法の産業界応用ワークショップ, 大阪, 2011.
[66] 湯浅能史, 木下佳樹: 複合的システムの検証 と Open System Dependability, 日本ソフトウェア科学会第 28 回大会, 沖縄県那覇市, 2011 年 9 月 27 日(火)～29 日(木).
[67] 松野浩, 田口研治, システムのディペンダビリティ、安全保証の現在, 国際標準化セミナー, 計測自動制御学会, 東京, 11, 2011.
[68] 高井利憲, オープンシステムディペンダビリティ国際規格, Embedded Technology 2011 (ET2011), 横浜, 11, 2011.
[69] 木藤浩之, 武山誠: 対話ゲームによる D-Case の妥当性及び正当性の統一的証明法の検討, ディペンダブルシステムワークショップ＆シンポジウム 2011 予稿集, 6 頁, 2011.
[70] K. Taguchi, Meta-modeling Approach to Safety Standards for Consumer Devices, OMG Seminar on Systems Assurance & Safety for Consumer Devices, USA, 6, 2011.
[71] Y. Matsuno, K. Taguchi, Y. Nakabo, A. Ohata, Iterative and Simultaneous Development of Embedded Control Software and Dependability Cases for Consumer Devices, Workshop on Dependable Systems of Systems, UK, 9, 2011.
[72] Toshinori Takai, Yoshiki Kinoshita, Makoto Takeyama, Hiroki Takamura, Evaluation and Standardization of Open Systems Dependability, Open Systems Dependability Workshop II, Tokyo, 3, 2012.
[73] 湯浅能史, 木下 佳樹 ：Agda 言語によるスクリプト検証について, ソフトウェアエンジニアリングシンポジウム 2012, ワークショップ WS-2, 情報処理学会, 2012.
[74] 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.
[75] 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, 日本ソフトウェア科学会ディペンダブルシステム研究会, 2012.
[76] Yoshiki Kinoshita and Makoto Takeyama, “Assurance Case as a Proof in a Theory: towards Formulation of Rebuttals”, *Assuring the Safety of Systems Proceedings of the Twenty-first Safety-Critical Systems Symposium, Bristol, UK.*, December 2012.
[77] Takeyama M, Kido H, Kinoshita Y, Using a proof assistant to construct assurance cases, Fast Abstract Session in Dependable Systems and Networks (DSN), May 2012.
[78] Yutaka Matsuno, Makoto Takeyama, D-Case Editor and D-Case/Agda, 1st International Workshop on Assurance Cases for Software-intensive Systems (ASSURE 2013), California, May 2013.
[79] Makoto Takeyama, Overview of Standardization Efforts, 1st International Workshop on Assurance Cases for Software-intensive Systems (ASSURE 2013), California, May 2013.
[80] Makoto Hirai, Yoshifumi Yuasa and Yoshiki Kinoshita, A Chain of Accountabilities in Open Systems based on Assured Entrustments, The 3rd International Workshop on Open Systems Dependability: Adaptation

to Changing World (WOSD 2013), Nov. 2013.

[81] Yukiko Yanagisawa, Takashi Ito, Makoto Takeyama and Yasuhiko Yokote, A New Method of Consensus Building for Open Systems Dependability, The 3rd International Workshop on Open Systems Dependability: Adaptation to Changing World (WOSD 2013), Nov. 2013.

[82] 武山 誠, 所 眞理雄, 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, ET2013 カンファレンス スペシャルセッション C-7,「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）、いよいよ実用化へ！～」、パシフィコ横浜、2013 年 11 月 22 日.

[83] 武山 誠、Formal Assurance Case in Agda（FACIA）、形式アシュランスケースの Agda 言語による記述、第 5 回 D-Case 実証評価研究会、国立情報学研究所、2014 年 3 月 18 日.

③ ポスター発表 （国内会議 １３件、国際会議 ０件）

[84] 松野 裕, 利用者指向ディペンダビリティ, 第8回 TXテクノロジー・ショーケース in つくば, 2009, つくばサイエンス・アカデミー, 農林水産技術会議事務局筑波事務所本館, 2009 年 1 月 24 日.

[85] 松野 裕（システム検証研究センター）、ディペンダビリティケースを用いた組み込みシステムのディペンダビリティの証拠の提示、「組込みシステム技術に関するサマーワークショップ」、石川県加賀市、2009 年 8 月.

[86] 利用者指向ディペンダビリティの研究---安全・安心社会実現のためのルールつくり: 概念創出・規格策定・ライフサイクル技術・適合性評価技術、組込み総合技術展（ET2009）、横浜、2009 年 11 月.

[87] 武山誠、松野裕. “D-Case エディタ”, Embedded Technology (ET) 2010, パシフィコ横浜, 2010 年 12 月 1 日-3 日.

[88] 木下佳樹, オープンシステムディペンダビリティの国際標準化, Embedded Technology (ET) 2011, パシフィコ横浜, 2011 年 11 月 16 日-18 日.

[89] 松野 裕, 高井 利憲, 山本 修一郎, 田口 研治, 菅谷 みどり, 倉光 君郎, d* フレームワーク: 複数のアクタ間のディペンダビリティ・ケース, ディペンダブルシステムワークショップ＆シンポジウム (DSW2011), 京都, 12, 2011.

[90] 木下佳樹, ディペンダビリティ、システム・アシュランス周辺の国際規格活動, ディペンダブルシステムワークショップ＆シンポジウム (DSW2011), 京都, 12, 2011.

[91] 武山誠、平井誠、湯浅能史、木藤浩之、 D-Case とその Agda による記述、ET2012 (Embedded Technology)、パシフィコ横浜、2012.11.14-16.

[92] 木下佳樹、武山誠、中原早生、平井誠、森口草介、湯浅能史、 D-Case と、その Agda による記述、 SODEC 2013 (ソフトウェア開発環境展)、東京ビッグサイト、2013. 5. 8-10.

[93] 木下佳樹、武山誠、中原早生、平井誠、森口草介、湯浅能史、 D-Case と、その Agda による記述、イノベーション・ジャパン 2013、東京ビッグサイト、2013. 8. 29-30.

[94] 木下佳樹、武山誠、中原早生、平井誠、森口草介、湯浅能史、 D-Case と、その Agda による記述、Embedded Technology (ET 2013)、パシフィコ横浜、2013. 11. 20-22.

[95] 平井誠、湯浅能史、ファイル共有サーバの運用・開発を題材にしたアシュランス ケースの作成について、第 11 回ディペンダブルシステムワークショップ （DSW2013）、2013. 12. 26-27.

[96] [1] 森口草介、D-Case in Agda による議論の段階的形式化、第 11 回ディペンダブルシ ステムワークショップ（DSW2013）、2013. 12. 26-27.

(7)　受賞・報道等

①　受賞

[97]　1. 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）

[98]　2. 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 15026-2 執筆に対して）

②　マスコミ（新聞・ＴＶ等）報道

なし

③　その他

なし

(8)　成果展開事例

①　実用化に向けての展開

[99] JST 研究成果展開事業　研究成果最適展開支援プログラム A-STEP 実用化挑戦ステージ　実用化挑戦タイプ（中小・ベンチャー開発）に、（株）Symphonyが提出している課題「CREST/DEOS プロセスを用いた医療情報プラットフォームの開発とその事業」にシーズの代表発明者として本研究の研究代表者が参画、医療情報処理に本研究領域の成果を実用化しようとしている。2013 年 10 月現在応募済、面接審査をへて引き続き審査中。

[100]　JST 研究成果展開事業　研究成果最適展開支援プログラム A-STEP 本格研究開発ステージ　ハイリスク挑戦タイプによって行われた研究開発課題「モデル化技術による MCU 仕様検証と機能検証の自動化」に研究責任者として本研究の研究代表者が参画、ルネサスエレクトロニクス株式会社と共同研究を行った。とくに本研究によって参加した国際標準化委員会 ISO/IEC JTC1 SC7 から得たシステムライフサイクルに関する知見をもとにルネサスエレクトロニクスにおける不具合実例の解析を行い、同社から高い評価を得た。

[101]　得られた DEOS サイクルに関する成果が、

[102]　ISO/IEC Joint Technical Committee 1 (JTC 1) Information technology, Subcommittee 7 (SC7) Systems and software engineering
この国際標準委員会に IEC TC56 へのリエゾン委員を派遣して活動。オープンシステムディペンダビリティの標準化についてシステム技術の分野において活動容易にする人的環境を整備している。

[103]　IEC Technical Committee 56 (TC56) Dependability, Working Group 4 System aspects of dependability
この国際標準委員会に convenor（主査）および ISO/IEC JTC1 SC7 へのリエゾン委員を派遣することによって、TC56 全体の運営に参画、オープンシステムディペンダビリティの標準化活動を容易にする人的環境を整備している。

②　社会還元的な展開活動

[104]　2008 年から 2013 まで Embedded Technology (ET) (展示会)に出展、2012 年は約 300 名来訪。

[105]　ソフトウェア開発環境展 (SODEC) 2013 (展示会)に出展、約 400 名来訪。

[106]　イノベーション・ジャパン 2013（展示会）に出展、約 200 名来訪。

§６．研究期間中の活動

（１）主なワークショップ、シンポジウム、アウトリーチ等の活動

年月日	名称	場所	参加人数	概要
2008/10/3	第 1 回チーム全体会議(キックオフミーティング)	産総研千里サイトシステム検証研究センター	13 名	全体研究計画についての内容説明と議論
2008/10/9	第 226 回 計算機言語談話会	産総研千里オフィス	約10名	研究チームが支援した開催談話会。http://cfv.jp/cvs/event/clc/index.html 参照。以下[計算機言語談話会]は全て同様。
2008/10/30	第 227 回 計算機言語談話会	産総研千里オフィス	約10名	
2008/11/7	第 2 回チーム全体会議	同上	9 名	規格と適合性評価に関する議論及び今後の方向性についての検討
2008/11/12	第 228 回 計算機言語談話会	産総研千里オフィス	約10名	
2008/12/11	第 229 回 計算機言語談話会	産総研千里オフィス	約10名	
2008/12/18	第 230 回 計算機言語談話会	産総研千里オフィス	約10名	
2009/1/29	第 231 回 計算機言語談話会	産総研千里オフィス	約10名	
2009/2/24	Newcastle CSR-AIST meeting	The University of Newcastle	10 名	先行ディペンダビリティ研究プロジェクトの調査と本プロジェクトの紹介
2009/2/27	York HISE-AIST meeting	The University Of York	8 名	同上
2009/3/4	Bath-AIST-Swansea workshop	Swansea University	9 名	同上
2009/3/4	第 232 回 計算機言語談話会	産総研千里オフィス	約10名	
2009/3/6	CUL CSR-AIST meeting	City university London	8 名	先行ディペンダビリティ研究プロジェクトの調査と本プロジェクトの紹介
2009/3/31	第 3 回チーム全体会議(20 年度総括ミーティング)	産総研千里サイトシステム検証研究センター	14 名	平成 21 年度研究の計画
2009/4/15	ディペンダビリティ懇話会	産総研千里オフィス	講演者 7 名 聴講者 19 名	ディペンダビリティに関連する研究者によるインフォーマルなワークショップ。主な講演者：神徳徹雄氏（産総

				研)、山田陽滋氏(名古屋大学)、野田五十樹氏(情報技術部門)、高村博紀、武山誠ほか
2009/4/20	第 233 回 計算機言語談話会	産総研千里オフィス	約10名	
2009/6/11	第 234 回 計算機言語談話会	産総研千里オフィス	約10名	
2009/6/18	第 235 回 計算機言語談話会	産総研千里オフィス	約10名	
2009/7/23	第 236 回 計算機言語談話会	産総研千里オフィス	約10名	
2009/8/20	第 237 回 計算機言語談話会	産総研千里オフィス	約10名	
2009/11/30	第 238 回 計算機言語談話会	産総研千里オフィス	約10名	
2009/12/10	第 239 回 計算機言語談話会	産総研千里オフィス	約10名	
2009/12/17	第 240 回 計算機言語談話会	産総研千里オフィス	約10名	
2010/2/4	第 241 回 計算機言語談話会	産総研千里オフィス	約10名	
2010/4/6－7	利用者指向ディペンダビリティセミナー(非公開)	産業技術総合研究所尼崎事業所	8 名	研究チーム内の研究討論
2010/4/7	第 242 回 計算機言語談話会	産業技術総合研究所尼崎事業所	約10名	
2010/4/13	第 243 回 計算機言語談話会	産業技術総合研究所尼崎事業所	約10名	
2010/4/22	第 244 回 計算機言語談話会	産業技術総合研究所尼崎事業所	約10名	
2010/5/17-19	利用者指向ディペンダビリティセミナー(非公開)	産業技術総合研究所尼崎事業所	8 名	研究チーム内の研究討論
2010/5/20	チーム、総括ミーティング(非公開)	産業技術総合研究所尼崎事業所	12 名	研究総括および DEOS センターを交えての研究討論
2010/6/10	第 245 回 計算機言語談話会	産業技術総合研究所尼崎事業所	約10名	
2010/6/14 －17	利用者指向ディペンダビリティセミナー(非公開)	産業技術総合研究所つくば第二事業所	6 名	研究チーム内の研究討論

2010/7/2	第 246 回 計算機言語談話会	産業技術総合研究所尼崎事業所	約10名	
2010/7/12	チーム、総括ミーティング(非公開)	ソニーCSL	7 名	研究総括および DEOS センターを交えての研究討論
2010/7/22	第 247 回 計算機言語談話会	産業技術総合研究所尼崎事業所	約10名	
2010/7/26 - 30	ISO/IEC 15026-4 エディタミーティング(非公開)	Washington D.C.(IDA)	3 名	ISO/IEC 15026-4 執筆のためのエディタチーム打合せ。
2010/8/19	第 248 回 計算機言語談話会	産業技術総合研究所尼崎事業所	約10名	
2010/10/28	チームミーティング(非公開)	産業技術総合研究所尼崎事業所	8名	研究チーム内の研究討論
2010/10/30 - 11/12	アシュランスケースに関する研究討論会(非公開)	NASA Ames	6 名	アシュランスケースに関する研究討論
2010/11/15	第 249 回 計算機言語談話会	産業技術総合研究所尼崎事業所	約10名	
2010/11/16	チームミーティング(非公開)	産業技術総合研究所尼崎事業所	8 名	研究チーム内の研究討論
2010/11/30	チーム、総括ミーティング(非公開)	ソニーCSL	7 名	研究総括および DEOS センターを交えての研究討論
2011/1/6	チームミーティング(非公開)	産業技術総合研究所尼崎事業所	8 名	研究チーム内の研究討論
2011/1/19 - 20	Argumentation seminar	産業技術総合研究所尼崎事業所	11 名	「議論」の論理的および組合せ的研究に関する研究討論
2011/2/7	第 250 回 計算機言語談話会	産業技術総合研究所尼崎事業所	約10名	
2011/2/22	チームミーティング(非公開)	産業技術総合研究所尼崎事業所	8名	研究チーム内の研究討論
2011/2/28 - 3/1	Osaka Workshop on Verification and Validation	産総研尼崎事業所	21 名	検証と妥当性評価に関する研究会
2011/3/12 - 20	ISO/IEC 15026 エディタミーティング(非公開)	Washington D.C.(IDA)	2名	ISO/IEC 15026-4 執筆のためのエディタチーム打合せ。
2011/3/14	第 251 回 計算機言語談話会	産業技術総合研究所尼崎事業所	約10名	

2011/3/17	第 252 回 計算機言語談話会	産業技術総合研究所尼崎事業所	約10名	
2011/3/22	第 253 回 計算機言語談話会	産業技術総合研究所尼崎事業所	約10名	
2011/3/28	チームミーティング（非公開）	産業技術総合研究所尼崎事業所	8名	研究チーム内の研究討論
2011/3/31	第 254 回 計算機言語談話会	産業技術総合研究所尼崎事業所	約10名	
2011/6/1	チームミーティング（非公開）	産業技術総合研究所尼崎事業所	8名	研究チーム内の研究討論
2011/6/21	第 255 回 計算機言語談話会	産業技術総合研究所尼崎事業所	約10名	
2011/6/28	第 256 回 計算機言語談話会	産業技術総合研究所尼崎事業所	約10名	
2011/8/25	第 257 回 計算機言語談話会	産業技術総合研究所尼崎事業所	約10名	
2011/9/7-14	AIM XIV (Agda Implementors Meeting)	湘南国際村センター	17 名	証明支援系 Agda の研究開発に関する研究討論
2011/11/28	第 258 回 計算機言語談話会	産業技術総合研究所尼崎事業所	約10名	
2011/12/2	第 259 回 計算機言語談話会	産業技術総合研究所尼崎事業所	約10名	
2011/12/9	第 260 回 計算機言語談話会	産業技術総合研究所尼崎事業所	約10名	
2011/12/21	第 261 回 計算機言語談話会	産業技術総合研究所尼崎事業所	約10名	
2011/12/22	第 262 回 計算機言語談話会	産業技術総合研究所尼崎事業所	約10名	
2012/2/1	第 263 回 計算機言語談話会	産業技術総合研究所尼崎事業所	約10名	
2012/2/20	第 264 回 計算機言語談話会	産業技術総合研究所尼崎事業所	約10名	

2013/1/15	第 265 回 計算機言語談話会	産業技術総合研究所尼崎事業所	約10名	
2013/10/28	1st Intenational Workshop on Argument for Agreement and Assurance	慶応大学日吉キャンパス来往舎	約20名	

§７． 最後に