研究課題別事後評価結果

1. 研究課題名： 利用者指向ディペンダビリティの研究

2. 研究代表者名及び主たる研究参加者名（研究機関名・職名は研究参加期間終了時点）：
研究代表者
木下　佳樹　（神奈川大学理学部情報科学科　教授）

3. 事後評価結果

かねてより研究代表者らが中心となって開発してきた形式的手法によるVerification & Validation技術を、変化し且つ不定性を含むオープンシステムのアシュランス記述に用いるべく変更し、D-Case in Agdaを開発した。具体的には、アシュランス記述の追加や変更に伴い発生する矛盾を自動的に検出する機構を考案し、D-Case in Agdaシステムに実装した。これを用い、実際にファイルサーバシステムの開発においてアシュランス記述の追加や変更の履歴を含む2000ノードを超えるD-Caseを記述し、実用的な規模においてその有効性を示した。特許出願や多数の国外・国内原著論文の発表をしたのち、本システムを一般公開した。これまで形式的手法は静的システムを対象として研究がなされてきたが、本研究の成果により、初めてオープンシステムへの応用を可能とした点は極めて高く評価できる。この成果をMachine-Checkable Assurance Case として国際標準とすべく、標準化団体OMGにおいて精力的に活動している。

加えて本研究チームは、本研究領域全体の課題であるオープンシステムディペンダビリティの概念規定の作成に貢献し、その精緻化に中心的な役割を果たした。これを反映したアシュランス記述の方法を国際標準規格（IEC 15026)に含めた。また、オープンシステムディペンダビリティの概念そのものを、現在の機能安全規格（IEC 61508）に変わる将来に向けたディペンダビリティの最上位概念規定として国際標準化すべく、本研究代表者がIEC TC56のコンビーナとして委員会を立ち上げ、IEC62853 として成立させるべく研究メンバーとともに精力的に活動している。

すなわち、本研究チームは形式的手法の新たな実用的応用分野を開拓し、その有効性を示すとともに、オープンシステムディペンダビリティと言う新しい概念規定の作成に貢献し、精緻化に中心的役割を果たし、次世代に向けた新たなディペンダビリティの国際標準化に向けて精力的に活動しており、期待通り、そして一部については期待以上の成果を挙げており、大変高く評価できる。