（様式４）

二国間交流事業 共同研究報告書

令和６年４月26日

独立行政法人日本学術振興会理事長　殿

［日本側代表者所属機関・部局］
群馬大学・情報学部
［職・氏名］
准教授・浜名　誠
［課題番号］
JPJSBP　　120223201

1. 事業名　相手国：フランス　（振興会対応機関：MEAE-MESRI　）との共同研究

2. 研究課題名
（和文）機械証明と高階書換え理論によるソフトウェア安全性保証技術の高度化
（英文）Advanced High-Assurance Software Technology by Proof Assistants with Higher-Order Rewriting

3. 共同研究実施期間　令和4年4月1日 ～ 令和6年3月31日（２年０ヶ月）

【延長前】　令和4年4月1日 ～ 令和6年3月31日（２年０ヶ月）

4. 相手国側代表者（所属機関名・職名・氏名【全て英文】）
INRIA・Researcher・ Frederic Blanqui

5. 委託費総額（返還額を除く）

本事業により執行した委託費総額		1,950,000　円
内訳	1年度目執行経費	950,000　円
	2年度目執行経費	1,000,000　円
	3年度目執行経費	－　円

6. 共同研究実施期間を通じた参加者数（代表者を含む）

日本側参加者等	9名
相手国側参加者等	7名

＊ 参加者リスト（様式 B1(1)）に表示される合計数を転記してください（途中で不参加となった方も含め、全ての期間で参加した通算の参加者数となります）。

7. 派遣・受入実績

	派遣		受入
	相手国	第三国	
1年度目	0	0	2(0)
2年度目	2	0	2(0)
3年度目			( )

＊ 派遣・受入実績（様式 B1(3)）に表示される合計数を転記してください。

派遣：委託費を使用した日本側参加者等の相手国及び相手国以外への渡航実績（延べ人数）。

受入：相手国側参加者等の来日実績（延べ人数）。カッコ内は委託費で滞在費等を負担した内数。

8. 研究交流の概要・成果等

(1)研究交流概要(全期間を通じた研究交流の目的・実施状況)

情報システムが重要な社会基盤の一つとなるにつれ、ソフトウェアの安全性保証 が大きな課題となっている。しかしコンピュータ・ソフトウェアは、構築する事も、その安全性を保証することも大変難しい。 個々の問題毎に対応するのではなく、ソフトウェア一般に高い信頼性保証を与えるには、適用範囲が広く、厳密な理論に基づくソフトウェア技術が必要である。 本課題は、ソフトウェアのための安全性保証技術のために、 定理証明支援システムを発展、応用し、フランスとの二国間交流研究として次のテーマを研究する。

＊ 日本の SOL システムと、フランスの Dedukti システムの融合

＊ 高度定理証明支援システム実現のための高階書換え理論と型理論の融合

＊ 高度ソフトウェア検証技術のため、書換え技術を関数型プログラミング言語、定理 証明支援システム Isabelle/HOL、および Coq システムへ導入し、合流性や停止性の性質 を自動証明する

(2)学術的価値(本研究交流により得られた新たな知見や概念の展開等、学術的成果)

＊ SOL システムと Dedukti システムの統合
日本の SOL とフランスの Dedukti の統合をフランス側代表者 Blanqui と行った。 このために、Dedukti システムのための TRS フォーマットの出力と整形を SOL システムに実装した。高階の TRS フォーマットの仕様策定を新しく行った。フランス側代表者 Blanqui と議論と共同作業を行ないつつ、そのためのパーサと変換器を作成した。さらに Dedukti システム、LambdaPi システムのための Web インターフェースを構築し、大幅にその利便性を向上させることに成功した。

＊ 高度定理証明支援システム実現のための高階書換え理論と型理論の融合
λΠ modulo 計算のための合流性条件を詳しく研究し、合流性を含意する他の書換え 論的性質を明らかにした。また高階書換えと型理論の融合のために、多相型停止性基 準判定方を、General Schema の理論と判定条件を多相に拡張することで完成させた。 また高階書換えの新しい合流性判定法の可能性を追求した。

＊ 高階書換え系の標準フォーマットの仕様策定
国際書換え系コンペティションでは、合流性、停止性ともにコンペティション用のフォーマットが未成熟である。これについて Blanqui、日本側メンバと議論を深め、高階書換え系には、標準フォーマットを策定した

(3)相手国との交流(両国の研究者が協力して学術交流することによって得られた成果)

フランスとの交流により(2)で述べた成果に加えて、次の成果を得た。

＊ 高階書換え系の標準フォーマットの仕様策定

国際書換え系コンペティションでは、合流性、停止性ともにコンペティション用のフォーマットが未成熟である。これについて Blanqui、日本側メンバと議論を深め、高階書換え系には、標準フォーマットを策定した。

(4)社会的貢献(社会の基盤となる文化の継承と発展、社会生活の質の改善、現代的諸問題の克服と解決に資する等の社会的貢献はどのようにあったか)

本研究により、ソフトウェア自動検証のための理論と技術を構築し、 情報技術の信頼性と安全性の向上に貢献した。 具体的には、定理証明システムと書換え系を用いた自動化技術が開発され、合流性と 停止性の確保を目指す先進的な方法論が提案された。これにより、ソフトウェア開発 プロセスにおけるバグの早期発見と修正が可能となり、社会生活の質の向上に寄与す ると期待できる。

さらに、関数型言語を活用した実装は、教育や研究の分野でのプログラミング教育を 充実させる効果も持つ。関数型言語はその数学的な特性から、正確で信頼性の高いソ フトウェア設計を促進するための理想的なツールである。この言語を用いることで、 将来のソフトウェア開発者たちは高度なプログラミング技術を身につけることができ、 社会のデジタル化推進に貢献すると考えられる。

また、この研究成果は、公共の安全を確保するためのシステムや、環境保護を支援す るアプリケーションの開発にも応用が可能である。自動検証技術を活用した環境監視 システムは、異常が発生した際に迅速に対応を行うことが可能であり、これが現代の 諸問題への解決策として機能すると考えられる。

総じて、本研究はソフトウェアの信頼性向上による社会基盤の強化、教育の質の向上、 環境及び公共安全への貢献、そして文化の発展といった多角的な社会的貢献を実現す ると期待できる。

(5)若手研究者養成への貢献(若手研究者養成への取組、成果)

山田はフランス INRIA を訪問することで書換え系と証明支援系の境界領域について、訪 問先研究者と深く議論し、新たな研究の萌芽となるアイデアを取得した。 今後の書換え系を基礎とした定理自動証明研究への発展が期待できる。 池渕はエコールポリテクニークと INRIA を長期訪問することで、 最新の書換え理論、特に高次元書換え系を訪問先の研究者と深く議論し、理解を深め ることができた。 書換え系の次世代の理論である高次元書換えは、証明支援系やプログラム検証をさら に高度化させる将来性がある。 これらにより、ソフトウェア科学分野の若手を海外での研究経験を与えて国際化と研究能力の養成ができたと考えられる。

(6)将来発展可能性(本事業を実施したことにより、今後どの様な発展の可能性が認められるか)

本研究で開発された自動検証技術は、特に安全性が重要な自動車、航空宇宙、医療機器業界のソフトウェア開発に重要な役割を果たすことが予測される。自動運転車の制御システムや人工知能を用いた診断支援システムなど、新技術の安全性確保には本研究の成果が不可欠である。 また、サイバーセキュリティの分野では、セキュリティプロトコルや暗号アルゴリズムの検証に自動検証技術を応用することで、より堅牢なデジタルセキュリティシステムを構築し、サイバー攻撃への防御能力を向上させることが期待される。これにより、経済や国家の安全保障に大きく貢献する。 本研究は理論の進展に加えて、実践的な応用でも広範な影響が期待され、経済全体の生産性向上に寄与する潜在力を持っている。

(7)その他(上記(2)～(6)以外に得られた成果があれば記載してください)

受賞: 浜名誠、日本ソフトウェア科学会第 40 回大会 優秀発表賞, 東京大学, 2023.10.