

ソフトウェア検証、高信頼 AI 技術および形式化された数学の確立

① ビジョンの概要

未来社会においては、誰もが安全性を確信できるソフトウェアと AI の信頼性の高い基盤技術が必要となる。その実現には、誤りや脆弱性を排除し、数学的に保証された知識と技術を社会に浸透させることが不可欠である。本構想は、演繹的検証、自動検証、証明付きソフトウェア構成、数学基盤形式化の 4 本の柱を並行的に推進し、安全で持続可能な社会を下支えする学際的研究を展開する。

② ビジョンの内容

誰もがソフトウェアや AI を安心して利用できる未来社会の実現には、複雑なシステムや新しい技術基盤から誤りや脆弱性を根本的に排除する仕組みが不可欠である。一方で、ソフトウェアの複雑化に加え生成 AI や量子計算が普及する中、従来のテスト中心の方法では信頼性の担保に限界がある。重大な事故やリスクを防ぎ持続可能な社会を築くには、数理論理による厳密な保証技術が求められる。

そのため本構想では、プログラム検証技術を演繹的手法と自動化手法の両面から発展させ、それを証明付きソフトウェア構成や数学基盤形式化へと展開することで、次世代の高信頼基盤を築くことを目指す(図 1)。

演繹的検証は、多様化する計算モデルに対応した理論体系を与え、自動検証は大規模ソフトウェアを人的コストなく扱える技術を提供する。証明付きソフトウェア構成は、検証技術そのものの正当性を保証し、社会に直結する重要システムの信頼性を高め、数学基盤の形式化は、計算機による厳密な検証と学術的成果の精密な共有を実現する。これらの柱は互いに密接に関連し、循環的に発展することで強固な基盤を形成する。

本ビジョンは、計算機科学と数学の架橋を促進し形式的手法の新潮流を牽引する。プログラム検証に用いた数学の形式化の知見を数学界にも還元し、双方の発展に寄与することを目指す。また、重要インフラの安全性を根本から支え、生成 AI や量子計算といった新技術の健全な応用をも可能にする。さらに、検証と形式化を基盤とした技術は教育や人材育成にも大きく寄与し、国際共同研究の推進や国際競技会を通じて世界に発信されることで、日本が分野融合研究の中心的役割を担うことが期待される。

③ 学術研究構想の名称

ソフトウェア検証、高信頼 AI 技術および形式化された数学の確立

④ 学術研究構想の概要

自動運転や手術ロボット、電力網等の安全性が重視されるソフトウェアには、クラッシュや情報漏洩を一切起こさない完全な検証が不可欠である。昨今の生成 AI の進化によりプログラム作成は容易になったものの、誤りを含む可能性があり、安全性が重視されるソフトウェアへの利用には課題が多い。

この問題を解決するソフトウェア検証技術は現在も国内外で盛んに研究が続けられている。静的解析ツールや証明支援系の発展により実用化は進んでいるが課題も多く、量子計算機の登場に伴う新理論の確立も急務である。また、検証に利用される証明支援系は国際的に活躍する数学者らにも注目され、数学の形式化が進められている。同様の形式化はソフトウェア検証の基盤となる数学的な定理についても必要である。

ソフトウェア中心の現代社会において、本課題の解決は避けて通ることができない。その達成には、情報科学のみならず数学や物理学といった広範な分野における、大規模かつ国際的な連携が不可欠である。

⑤ 学術的な意義

演繹的検証は、数理論理に基づきプログラムの正しさを厳密に保証する。これは言語や計算の理論を深化させ、並行・量子・AI 等の新モデルにおける安全な設計基盤となる。単なる解析技術を超え、計算の一般理論を発展させる点に大きな学術的意義がある。自動検証は多様な手法を統合し、人手を伴わない大規模ソフトウェアの検証を実現する。SAT/SMT ソルバ等の限界に挑む過程で革新的なアルゴリズムを生み、機械学習との融合は探索の柔軟性と適応性を高めることが期待される。この研究は検証の効率化に加え、最適化や AI 分野へも広く波及する。さらに、演繹的検証を AI 技術に応用し、ブラックボックス的な深層学習の安全性や頑健性を数理的に解析することによって、高信頼 AI の実現を可能にする。証明支援系によるプログラム検証の

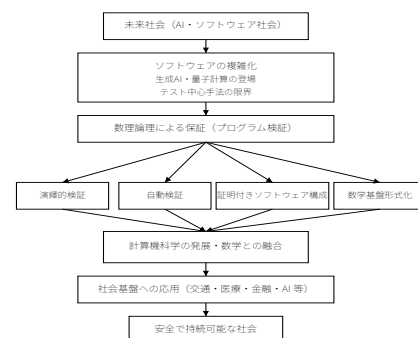


図1 数理論理による次世代高信頼基盤

形式化は、高信頼ソフトウェア開発において重要な役割を果たす。証明支援系（Rocq や Lean 等）は、定義や定理を形式化し機械的に検証するツールであり、コード抽出もサポートされているため、上述の検証技術を実開発に応用でき、高信頼なソフトウェア構築が実現できる。証明支援系による数学の形式化では、定義・定理・証明を検証済みプログラムとして言語化し、再現可能なライブラリとして保存・伝達を促進することを目指す。数学的知識の保存は、国際数学連合においても重要な課題として認識されており、近年では著名な数学者による実践も始まっているが、専門知識と労力を要する点が課題である。本研究提案では、これまでの経験を活かして形式化の生産性を向上させ、誰もが手軽に数学的知識の保存・共有できる環境を目指す。

⑥ 国内外の研究動向と当該構想の位置付け

プログラム検証や数理的基盤の形式化に関しては、欧米を中心に活発な研究が進められている。演繹的検証では、分離論理や依存型システムを拡張した多様な論理体系の提案が続き、量子計算や AI に対応する形式手法の萌芽的研究も見られる。自動検証の分野では、SAT/SMT ソルバやモデル検査、抽象解釈を基盤とした技術が国際的に標準化され、さらに機械学習を活用した探索戦略の改良など新しい方向性が模索されている。証明付きソフトウェア構成については、CompCert 等の検証済みコンパイラや、証明支援によるアルゴリズム実装の実用化が現実味を帯びている。また数学基盤の形式化では、大規模な証明ライブラリの構築が進められ、国際数学連合においても数学知識の保存手段として重視されている。本構想は、これらの潮流を踏まえつつ、演繹的検証と自動検証を統合し、さらに証明付きソフトウェア構成と数学形式化へ展開することで、国際的な研究動向に呼応すると同時に、日本独自の学術的強みを発揮するものである。

⑦ 社会的価値

本構想の社会的価値は、ソフトウェアの信頼性を根本から高める技術確立し、その成果を社会基盤に還元できる点にある。インフラや医療等の重要分野では、検証技術による厳密な保証は、国民の安全・安心を支える基盤となる。また、証明付きソフトウェアの実現は、テスト依存の開発から脱却し、高信頼ソフトウェアの効率的な構築を可能にする。さらに、数学基盤の形式化を通じた知識の保存と再利用により、知的資産の永続的な蓄積を促す。これは学術的価値のみならず、開発コスト削減や新産業創出など経済・産業面にも大きく貢献する。また、整備された証明ライブラリやオープンソースの検証基盤は教育資源としても活用でき、次世代人材の育成に寄与する。加えて、本構想は SDGs における「産業と技術革新の基盤構築」や「持続可能な都市・社会インフラの実現」にも直結し、持続的かつ安全な社会の実現に大きく貢献する。

⑧ 実施計画等について

・実施計画・スケジュール 本計画は 10 年を目途とし、演繹的検証、自動検証、証明付きソフトウェア構成、数学基盤の形式化という 4 つの柱を並行的に推進しつつ、時期に応じて重点を変えて進展させる。前期（1～3 年）では、各柱の基盤整備を行う。演繹的検証ではプログラム論理の拡張を進め、並行・確率・量子計算に対応可能な推論体系を構築する。自動検証では SAT/SMT ソルバ、抽象解釈、モデル検査を組み合わせた自動化技術を開発し、評価用ベンチマークを整備する。証明付きソフトウェア構成では検証アルゴリズムの小規模実装を証明支援系上で試行し、数学基盤の形式化では基本的な定義・定理のライブラリ構築を開始する。中期（4～6 年）では、各柱を発展させ相互に連携させる。演繹的検証と自動検証の成果を統合し、効率性と精密性を兼ね備えた検証基盤を構築する。証明付きソフトウェア構成では実用規模のソフトウェアを対象に高信頼実装を行い、数学基盤の形式化ではライブラリの拡充と応用範囲の拡大を図る。後期（7～10 年）では、4 つの柱を統合的に展開し、学術的・社会的応用へ結実させる。検証基盤を医療・金融システムに応用し、国際競技会を通じた評価基盤の運用に参画する。また、数学形式化の大規模プロジェクトに参加し、国際的に共有可能な知識基盤を整備する。これらを通じて日本が分野融合研究の拠点として国際的に主導的役割を果たすことを目指す。

・実施機関と実施体制 関連する主要分野で十分な研究実績を有する東北大学電気通信研究所が中心となり研究を開始する。同研究所が共同利用・共同研究拠点として国内外の情報通信分野の研究促進の役目も担っていることも活用しながら、国内外の研究機関との共同研究を広げ実施してゆく。10 年間の総経費として 8,000 百万円（設備費 3,200 百万円、人件費 3,200 百万円、事業推進費 1,600 百万円）を計上する。

⑨ 連絡先

海野 広志、中野 圭介（東北大学電気通信研究所）