

令和 2 年 6 月 29 日現在

機関番号：11301

研究種目：基盤研究(B)（一般）

研究期間：2015～2019

課題番号：15H02681

研究課題名（和文）高階・型付きの計算体系に基づくプログラミングの理論と応用の展開

研究課題名（英文）Development of theory and application of programming based on higher-order/typed calculi

研究代表者

住井 英二郎（Sumii, Eijiro）

東北大学・情報科学研究科・教授

研究者番号：00333550

交付決定額（研究期間全体）：（直接経費） 13,700,000円

研究成果の概要（和文）：主に関数型言語ないしそれに近い研究コミュニティで発展してきた、プログラミング言語理論（特に高階計算および静的型システム）をさらに発展・応用することにより、研究成果報告書の本文に列挙のとおり、多岐にわたる成果や新たな理論を得た。研究の一部は、コンピュータサイエンス分野で重要視される、水準の高い査読付国際会議にフルペーパーが採択・発表されるなど、良い評価を得た。

研究成果の学術的意義や社会的意義

広義の「計算」の記述としての高水準プログラミング、ひいては情報処理システムの生産性・信頼性を向上させる分野の研究成果である。研究計画に明記したとおり、本研究は学術的基礎理論研究であり、「201X年YY月にZZZ理論を着想する」といった具体的計画をあらかじめ立てることはあり得ないため、研究計画もあくまで例示である旨を明記した上で採択されたが、研究題目に沿った多数の予見し得なかった成果が得られ、研究者自身の発想による自由な研究の重要性が再確認された。

研究成果の概要（英文）：As enumerated in the report, a variety of results and new theories have been obtained by developing and applying programming language theory (in particular, higher-order computation and static type systems) studied in functional languages and related research fields. Some of our research has been accepted as full papers and presented in refereed, high-quality international conferences.

研究分野：プログラミング言語理論

キーワード：プログラミング言語理論 関数型プログラミング 高階計算・計算（ラムダ計算）型システム 情報セキュリティ・情報流解析 並行・分散計算 形式的（機械的）定理証明・検証 環境双模倣

科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属されます。

様式 C - 19 , F - 19 - 1 , Z - 19 ( 共通 )

## 1 . 研究開始当初の背景

関数型プログラミング(functional programming)とは、式の値を計算(評価)する以外の「副作用」をなるべく避けるプログラミングスタイルである。関数型プログラミングをサポートするプログラミング言語を、関数型プログラミング言語(略して関数型言語)という。関数型言語の歴史は古く、1950年代のLISPひいては1930年代の計算まで遡る。関数型言語はその単純さと強力さのため、しばしば高階計算や多相型推論といった先進的プログラミング言語機構の研究の基礎として用いられてきた。それらの先進的機構の多くは最近になってC++, Java, Python, Ruby等の「テンプレート」「ジェネリックス」「型推論」「ラムダ式」「クロージャ」等として、関数型以外のプログラミング言語にも広く取り入れられている。

Haskell, MLといった現代的な関数型言語自体も注目され、国内外での応用が急速に進んでいる(日経コンピュータ2012年9月27日号特集『次の主流は「関数型」 覆る言語選定の常識 Javaはもう古い』, 日経ソフトウェア2014年11月号特集1「オブジェクト指向のウソ 関数型のウソ」他。商業誌のため、扇情的な表現も見られる一方、研究代表者のコメントや記事も掲載されている)。関数型言語に関する国際会議ICFP(ACM SIGPLAN International Conference on Functional Programming)等も参加者が急増するとともに、Google, Microsoft, Mozilla, Oracle, Standard Chartered, Bloomberg, Credit Suisse, Facebook, Twitterといった著名IT企業や金融関連企業等がスポンサーに名を連ねている。

研究代表者は高階かつ静的型付きの関数型言語の理論と応用に関する研究を行ってきた。特に、再帰関数や繰り返し(ループ)、リストや木などの再帰型、破壊的代入の可能な状態変数や参照(ポインタ)等を持つ現実的な関数型言語において、二つのプログラムの振る舞いが等しいことを数理論理的に証明する「プログラム等価性」の健全・完全かつ初等的な証明手法を世界で初めて確立した。この業績はプログラミング言語理論分野において最も水準が高いとされる国際会議POPL(ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages)に採択率16~18%の査読を経て2004~2005年の2年連続で発表、計算機科学分野において最も水準が高いとされる論文誌Journal of the ACMに全43頁の論文が採録され、欧米の多数のグループにより追従研究がおこなわれるなど、国際的に高く評価されている。国内においてもマイクロソフトリサーチ日本情報学研究賞、日本IBM科学賞(コンピューター・サイエンス分野)、船井学術賞、日本学術振興会賞などを受賞した。

研究代表者は関数型言語の教育用コンパイラMinCamlも開発し、東京大学や英国ケンブリッジ大学などで採用され、また、プログラミング言語理論分野の著名な教科書(Types and Programming Languages, Benjamin C. Pierce, MIT Press)を監訳(オーム社、2013年)、Amazon.co.jpにおいて雑誌や漫画・小説等も含む新刊全体で専門書としては異例の42位にランクインした。2011年ICFPプログラミングコンテスト委員長、日本ソフトウェア科学会プログラミング論研究会主査、同研究会主催・ACM他協賛FLOPS2014(Symposium on Functional and Logic Programming)プログラム共同委員長をはじめ、多数の学会委員等を務め、国内外の多数の優れた研究者・技術者らと積極的な活動を行なっている。

## 2 . 研究の目的

本研究では、主に関数型言語ないしそれに近い研究コミュニティで発展してきた、プログラミング言語理論(特に高階計算および静的型システム)とその応用のさらなる展開を目指す。

## 3 . 研究の方法

背景および目的の項で述べたようなプログラミング言語理論をさらに発展・応用することにより、新たな理論や成果を得る。

#### 4. 研究成果

多岐にわたるが、一部を以下に列挙する。これらは研究協力者（当時の大学院生・学部生を含む）との共同研究である。

- 機械学習による関数型プーリアンプログラムの型推論
- 多相関数のインライン展開による特殊化に関する研究
- Up-to context technique を用いた環境双模倣の準判定器
- セキュリティ型付きラムダ計算のための環境双模倣
- データ構造の低水準操作に関する分離論理を用いた定理証明
- MinCam1 の K 正規化の形式的検証
- 非限定継続を扱えるラムダ計算における文脈等価性のための健全かつ完全な双模倣
- ロボット制御プログラム生成のための関数型 DSL
- 情報流解析のための環境双模倣
- ロックフリーアルゴリズムの形式的検証
- 必要呼び意味論と名前呼び意味論の対応の形式的検証
- NetKAT with Cryptography（暗号プリミティブを追加した NetKAT）
- メモリ使用量比較のための環境双模倣の拡張
- $F^*$  による高階関数の等価性の証明
- ブロックチェーン合意形成プロトコルの Coq による証明からのコード抽出
- セキュリティ型付き 計算の環境双模倣の検証と改良
- 並行性・非決定性・状態・暗号を備えた NetKAT
- Polymorphic gradual typing with holes
- 型システムを用いたロックフリースタックの検証

以上の研究の一部は、コンピュータサイエンス分野で重要視される、水準の高い査読付国際会議にフルペーパーが採択・発表されるなど、良い評価を得た。それら以外の研究の多くも、2020 年度より採択された後継プロジェクトにおいて発展・継続中である。

研究計画に明記したとおり、本研究は学術的基礎理論研究であり、「201X 年 YY 月に ZZZZ 理論を着想する」といった具体的計画をあらかじめ立てることはあり得ないため、研究計画もあくまで例示である旨を明記した上で採択されたが、研究題目に沿った多数の予見し得なかった成果が得られ、研究者自身の発想による自由な研究の重要性が再確認された。

## 5. 主な発表論文等

〔雑誌論文〕 計8件（うち査読付論文 7件/うち国際共著 0件/うちオープンアクセス 8件）

1. 著者名 Mizuno Masayuki, Sumii Eijiro	4. 巻 11893
2. 論文標題 Formal Verifications of Call-by-Need and Call-by-Name Evaluations with Mutual Recursion	5. 発行年 2019年
3. 雑誌名 Programming Languages and Systems - 17th Asian Symposium, APLAS 2019, Nusa Dua, Bali, Indonesia, December 1-4, 2019, Proceedings. Lecture Notes in Computer Science	6. 最初と最後の頁 181 ~ 201
掲載論文のDOI (デジタルオブジェクト識別子) <a href="https://doi.org/10.1007/978-3-030-34175-6_10">https://doi.org/10.1007/978-3-030-34175-6_10</a>	査読の有無 有
オープンアクセス オープンアクセスとしている (また、その予定である)	国際共著 -

1. 著者名 Masayuki Mizuno, Eijiro Sumii	4. 巻 10818
2. 論文標題 Formal Verification of the Correspondence Between Call-by-Need and Call-by-Name	5. 発行年 2018年
3. 雑誌名 Functional and Logic Programming - 14th International Symposium, FLOPS 2018, Nagoya, Japan, May 9-11, 2018, Proceedings. Lecture Notes in Computer Science	6. 最初と最後の頁 1 ~ 16
掲載論文のDOI (デジタルオブジェクト識別子) 10.1007/978-3-319-90686-7_1	査読の有無 有
オープンアクセス オープンアクセスとしている (また、その予定である)	国際共著 -

1. 著者名 Ryohei Tokuda, Eijiro Sumii, Akinori Abe	4. 巻 241
2. 論文標題 Specialization of Generic Array Accesses After Inlining	5. 発行年 2017年
3. 雑誌名 Proceedings ML Family / OCaml Users and Developers workshops, ML Family/OCaml 2015, Vancouver, Canada, 3rd & 4th September 2015, Electronic Proceedings in Theoretical Computer Science	6. 最初と最後の頁 45-53
掲載論文のDOI (デジタルオブジェクト識別子) 10.4204/EPTCS.241.4	査読の有無 有
オープンアクセス オープンアクセスとしている (また、その予定である)	国際共著 -

1. 著者名 Taichi Yachi, Eijiro Sumii	4. 巻 10017
2. 論文標題 A Sound and Complete Bisimulation for Contextual Equivalence in $\lambda$ -Calculus with Call/cc	5. 発行年 2016年
3. 雑誌名 Programming Languages and Systems - 14th Asian Symposium, APLAS 2016, Hanoi, Vietnam, November 21-23, 2016, Proceedings, Lecture Notes in Computer Science	6. 最初と最後の頁 171-186
掲載論文のDOI (デジタルオブジェクト識別子) 10.1007/978-3-319-47958-3_10	査読の有無 有
オープンアクセス オープンアクセスとしている (また、その予定である)	国際共著 -

1. 著者名 水野 雅之, 住井 英二郎	4. 巻 印刷中
2. 論文標題 無限の入出力を行う関数型プログラムのK正規化の形式的検証	5. 発行年 2017年
3. 雑誌名 コンピュータソフトウェア	6. 最初と最後の頁 印刷中
掲載論文のDOI (デジタルオブジェクト識別子) なし	査読の有無 有
オープンアクセス オープンアクセスとしている (また, その予定である)	国際共著 -

1. 著者名 Akinori Abe, Eijiro Sumii	4. 巻 198
2. 論文標題 A Simple and Practical Linear Algebra Library Interface with Static Size Checking	5. 発行年 2015年
3. 雑誌名 EPTCS	6. 最初と最後の頁 1-21
掲載論文のDOI (デジタルオブジェクト識別子) 10.4204/EPTCS.198.1	査読の有無 有
オープンアクセス オープンアクセスとしている (また, その予定である)	国際共著 -

1. 著者名 Ryohei Tokuda, Eijiro Sumii	4. 巻 2015
2. 論文標題 Specialization of Generic Array Accesses After Inlining	5. 発行年 2015年
3. 雑誌名 The OCaml Users and Developers Workshop (talk abstracts)	6. 最初と最後の頁 1-2
掲載論文のDOI (デジタルオブジェクト識別子) なし	査読の有無 有
オープンアクセス オープンアクセスとしている (また, その予定である)	国際共著 -

1. 著者名 谷内太一, 住井英二郎	4. 巻 2015
2. 論文標題 Call/ccを含む型無しラムダ計算における文脈等価性の一証明手法	5. 発行年 2015年
3. 雑誌名 日本ソフトウェア科学会第32回大会(2015年度)講演論文集	6. 最初と最後の頁 1-7
掲載論文のDOI (デジタルオブジェクト識別子) なし	査読の有無 無
オープンアクセス オープンアクセスとしている (また, その予定である)	国際共著 -

[学会発表] 計10件(うち招待講演 0件/うち国際学会 4件)

1. 発表者名 Masayuki Mizuno, Eijiro Sumii
2. 発表標題 Formal Verifications of Call-by-Need and Call-by-Name Evaluations with Mutual Recursion
3. 学会等名 17th Asian Symposium on Programming Languages and Systems (国際学会)
4. 発表年 2019年

1. 発表者名 遠藤 侑介, 松本 宗太郎, 上野 雄大, 住井 英二郎, 松本 行弘
2. 発表標題 Progress report: Ruby 3における静的型解析の実現に向けて
3. 学会等名 第21回プログラミングおよびプログラミング言語ワークショップ (PPL2019)
4. 発表年 2019年

1. 発表者名 菅原 慎之介, 住井 英二郎
2. 発表標題 NetKAT with Cryptography
3. 学会等名 第21回プログラミングおよびプログラミング言語ワークショップ (PPL2019)
4. 発表年 2019年

1. 発表者名 木村 朝輝, 住井 英二郎
2. 発表標題 ブロックチェーン合意形成プロトコルのCoqによる証明からのコード抽出
3. 学会等名 第21回プログラミングおよびプログラミング言語ワークショップ (PPL2019)
4. 発表年 2019年

1. 発表者名 Masayuki Mizuno, Eijiro Sumii
2. 発表標題 Formal Verification of the Correspondence Between Call-by-Need and Call-by-Name
3. 学会等名 Fourteenth International Symposium on Functional and Logic Programming (FLOPS 2018) (国際学会)
4. 発表年 2018年

1. 発表者名 水野 雅之, 住井 英二郎
2. 発表標題 無限の入出力を行う関数型プログラムのK正規化の形式的検証
3. 学会等名 日本ソフトウェア科学会大会
4. 発表年 2016年

1. 発表者名 Taichi Yachi, Eijiro Sumii
2. 発表標題 A Sound and Complete Bisimulation for Contextual Equivalence in $\lambda$ -Calculus with Call/cc
3. 学会等名 14th Asian Symposium on Programming Languages and Systems (国際学会)
4. 発表年 2016年

1. 発表者名 Ryohei Tokuda, Eijiro Sumii
2. 発表標題 Specialization of Generic Array Accesses After Inlining
3. 学会等名 The OCaml Users and Developers Workshop (国際学会)
4. 発表年 2015年

1. 発表者名 谷内太一, 住井英二郎
2. 発表標題 Call/ccを含む型無しラムダ計算における文脈等価性の一証明手法
3. 学会等名 日本ソフトウェア科学会第32回大会
4. 発表年 2015年

1. 発表者名 阿部 晃典, 住井 英二郎
2. 発表標題 機械学習による関数型プリアンプログラムの型推論
3. 学会等名 第18回プログラミングおよびプログラミング言語ワークショップ (PPL2016)
4. 発表年 2016年

〔図書〕 計0件

〔産業財産権〕

〔その他〕

<p>Sized Linear Algebra Package (SLAP)  <a href="http://akabe.github.io/slap/">http://akabe.github.io/slap/</a></p>
---

6. 研究組織		
氏名 (ローマ字氏名) (研究者番号)	所属研究機関・部局・職 (機関番号)	備考