様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　５ 年　 ６ 月 １３ 日現在

機関番号：３２６８９
研究種目：基盤研究(B)（一般）
研究期間：2017～2021
課題番号：１７Ｈ０１７２０

研究課題名（和文）高階・再帰的データ構造への破壊的代入を含む高レベル言語プログラムの高精度な検証

研究課題名（英文）Verification of high-level programs containing mutable higher-order recursive data structures

研究代表者

寺内　多智弘（Terauchi, Tachio）

早稲田大学・理工学術院・教授

研究者番号：７０４４７１５０

交付決定額（研究期間全体）：（直接経費）　　13,980,000円

研究成果の概要（和文）：以下の研究成果を得た。(1)高階プログラムの時相的仕様についての研究成果。(2)再帰的(帰納的・余帰納的)な述語定義を書くことのできる一階不動点論理や関連する数学的帰納法の形式化である循環証明体系についての研究成果。(3)破壊的代入など様々な計算効果を統一的に扱える先進的言語機能である代数的エフェクトハンドラについての研究成果。(4)サイドチャネルやReDoS攻撃の検出・防衛などプログラム検証・合成技術のセキュリティへの応用に関する研究成果。(5)後方参照、先読みといった拡張機能を含む拡張正規表現の形式言語理論についての研究成果。

研究成果の学術的意義や社会的意義
非決定的動作を含む高階プログラムについて初の相対的完全な検証を実現するリファインメント型システムの提案、様々な問題の解決に応用できる一階不動点論理の妥当性判定のための新しいアルゴリズムを提案、深刻なセキュリティ脅威であるReDoS脆弱性を修復するため初のプログラム合成手法の提案など、本研究はこれまでのプログラミング言語・形式検証・定理証明・セキュリティの研究を大きく飛躍させた。よって、本研究の成果は極めて高い学術的および社会的意義を持つと考える。

研究成果の概要（英文）：We have achieved the following research results. (1) New methods for temporal property verification of higher-order programs. (2) New results on cyclic proof systems, formal deduction systems for mathematical induction, and new methods for deciding validity of formulas in first-order fixpoint logic with background theories. (3) A new type and effect system for verifying temporal properties of programs with algebraic effects and handlers, an emerging programming language feature for uniformly expressing a variety of computational effects including destructive updates. (4) Research achievements on the application of program verification and synthesis techniques to security, such as a method for repairing real-world regular expressions vulnerable to ReDoS attacks. (5) New results on the formal language theory of regular expressions extended with real-world features such as backreferences and lookaheads.

研究分野：コンピュータサイエンス

キーワード：プログラム検証　不動点論理　型システム　自動定理証明　分離論理　循環証明

※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、研究者個人に帰属します。

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

今日の情報化社会において、コンピュータソフトウェアは生活基盤のいたる所に活用されており、その重要度は計り知れない。また、ソフトウェアシステムの不具合は社会的に大きな問題として取り沙汰され、ソフトウェアプログラムの検証が非常に高い関心を集めてい。特に、ソフトウェアモデル検査など高精度な自動検証は、2007 年にモデル検査の提唱者の Clarke らがコンピュータ科学におけるノーベル賞といわれるチューリング賞を受賞し、Microsoft 社がソフトウェアモデル検査に基づく検証ツールを開発・公開するなど、学術界・産業界双方から高く注目されている。

従来のソフトウェアモデル検査は C 言語など低レベル言語を対象としていたが、近年、代表者らをはじめ国内外の研究グループが関数型言語のための自動検証の研究を推進し、関数型言語のための自動検証は急速な進化を遂げている。例えば、プログラミング言語分野最難関の国際会議である POPL 2016 に採録された代表者らの研究では、リファインメント型という関数型プログラムのプログラム断片の動作を精密に表すことのできる型システムを用いた関数型言語プログラムのための線形時相論理仕様の(相対)完全な検証手法が提案されている。

しかし、代表者らの研究を含め、従来の関数型言語プログラムのための検証技術は主に純粋関数型言語を対象としており、破壊的代入を含むプログラムを直接的に扱うことは困難である。特に、Java、C++などオブジェクト指向言語におけるオブジェクトなど破壊的代入を行える高階・再帰データ構造の扱いは課題である。

２．研究の目的

本研究では、オブジェクト志向言語におけるオブジェクト等、高階・再帰データ構造に対する破壊的代入を含む高レベル言語のための高精度な自動検証手法の確立を目指す。その手段は、リファインメント型によるソフトウェアモデル検査など高階関数型言語の自動検証の研究と分離論理など破壊的代入を含むプログラムの検証の研究の融合である。

研究の背景でも述べたように、既存のリファインメント型による高階関数型言語のためのソフトウェアモデル検査は破壊的代入を直接扱えない。対して、分離論理など既存の破壊的代入を含むプログラムの検証のための枠組は自動検証に適しておらず、また、高レベル言語機能の扱いが不十分である等の課題がある。そこで、本研究の主要目標として以下を設定する。

(1) リファインメント型システムや分離論理など、既存の検証枠組みを融合・昇華させ、高階・再帰データ構造に対する破壊的代入を含むプログラムの自動検証に適した新たな検証の枠組み（プログラム論理・型システム）を構築する。

(2) 上記の枠組みをベースとした検証アルゴリズムを開発する。代表者らのこれまでの研究でもある CEGAR・制約解消による型推論・述語推論の研究や分離論理のための自動定理証明の研究などを基にアルゴリズムを考案する。また、時相論理仕様など、幅広い仕様のクラスに対しての検証アルゴリズムの実現も目指す。

(3) 検証ツールを作成し、Java 言語、Swift 言語等で記述された高階・再帰データ構造への破壊的代入を含むプログラムに対しての検証実験を行う。

３．研究の方法

研究目的(1)については、代表者らの先行研究であるリファインメント型システムの研究や分離論理および分離論理の型システム版ともいえるエイリアス型の研究などを参考に研究を行う。
研究目的(2)については、まず安全性仕様の検証ための検証アルゴリズムを開発することを目指す。リファインメント型システム・分離論理などの検証枠組みは、それ自身がすでに演繹的に安全性仕様を検証するための枠組みであるため、演繹推論アルゴリズムが検証アルゴリズムとなる。代表者らの先行研究を含めた既存のリファインメント型システムのための型推論アルゴリズムや分離論理のための自動演繹アルゴリズムの研究を参考に研究を進める。加えて、線形時相論理(LTL)など時相論理で記述される仕様の検証できるように検証アルゴリズムを拡張する。代表者らの先行研究であるリファインメント型を用いた線形時相論理仕様の検証などの研究を参考に研究を進める。研究目的(3)の検証ツール作成および検証実験は、研究期間全体を通して行う。

４．研究成果

以下の成果を得た。

(1) 高階プログラムの時相的仕様についての研究成果を得た。具体的には、非決定的な動作を含む高階プログラムの相対的完全な検証を実現するリファインメント型システムを開発した。この研究の成果をまとめた論文はプログラミング言語分野最難関国際会議である The 45th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL 2018)に採録された。加えて、この研究を拡張して、再帰的(帰納的・余帰納的)な述語定義を書くことのできる一階不動点論理の論理式をリファインメントとして使えるリファインメント型システムを提案し、この型システムを用いた非決定性を含む高階プログラムの時相仕様の相対的完全かつモジュラーな検証手法を示した。この研究の成果をまとめた論文は理論計算機科学分野最難関国際会議である The 33rd Annual ACM/IEEE Symposium on Logic in Computer Science (LICS 2018)に採録された。

(2) 上記の研究と関連して、一階不動点論理や関連する数学的帰納法の形式化である循環証明(cyclic proof)体系についての研究成果を得た。具体的には、分離論理のための循環証明体系のカット除去性について研究を行いこの体系ではカット除去が不可能であることを示した。この研究成果をまとめた論文は国内雑誌コンピュータソフトウェアに掲載された。加えて、一階不動点論理の妥当性判定を、述語制約解消問題に帰着してモジュラーに解く手法を提案し、この妥当性判定アルゴリズムが様々なプログラム検証の問題に応用できることを示した。これらの研究成果をまとめた論文は形式検証最難関国際会議である The 33rd International Conference on Computer-Aided Verification (CAV 2021)とプログラミング言語分野最難関国際会議である The 50th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL 2023)に採録され、Distinguished Paper Award も受賞した。

(3) 破壊的代入など様々な計算効果を統一的に扱える先進的言語機能である代数的エフェクトハンドラ(algebraic effect handlers)についての研究を行い成果を得た。具体的には、代数的エフェクトハンドラを含むプログラムの時相仕様検証のための型エフェクトシステムを提案した。この研究成果をまとめた論文はプログラミング言語分野の国内ワークショップ第 25 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(PPL 2022)に採録され、最優秀論文賞も受賞した。

(4) 加えて、プログラム検証・合成技術のセキュリティへの応用に関する研究を行い成果を得た。具体的には、プログラミング検証・合成によるタイミング攻撃などサイドチャネル攻撃の検出・防衛に関する研究、正規表現処理の振る舞いを悪用した DoS 攻撃である ReDoS 攻撃の防衛に関する研究などを行い成果を得た。これらの研究成果をまとめた論文はプログラミング言語分野最難関国際会議 The 38th ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI 2017), セキュリティ分野国際会議 The 6th International Conference on Principles of Security and Trust (POST 2017), The 8th International Conference on Principles of Security and Trust (POST 2019)、セキュリティ分野国際ジャーナル Journal of Computer Security、セキュリティ分野トップ国際会議 The 32nd IEEE Computer Security Foundations Symposium (CSF 2019)、セキュリティ分野最難関国際会議 The 43rd IEEE Symposium on Security and Privacy (S&P 2022)に採録された。

(5) 加えて、後方参照(backreference)、先読み(lookahead)といった拡張機能を含む拡張正規表現の形式言語理論についての研究を行い成果を得た。これらの研究成果をまとめた論文は理論計算機額分野国際会議 the 7th International Conference on Formal Structures for Computation and Deduction (FSCD 2022)とプログラミング言語分野の国内ワークショップ第 26 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(PPL 2023)に採録され、最優秀論文賞も受賞した。

５．主な発表論文等

〔雑誌論文〕　計21件（うち査読付論文　21件／うち国際共著　9件／うちオープンアクセス　11件）

１．著者名 Hiroshi Unno, Tachio Terauchi, Yu Gu, Eric Koskinen	４．巻 7
２．論文標題 Modular Primal-Dual Fixpoint Logic Solving for Temporal Verification	５．発行年 2023年
３．雑誌名 In Proceedings of the 50th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL 2023), PACMPL 7(POPL)	６．最初と最後の頁 2111～2140
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3571265	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 該当する

１．著者名 Hiroshi Unno, Taro Sekiyama	４．巻 7
２．論文標題 Temporal Verification with Answer-Effect Modification: Dependent Temporal Type-and-Effect System with Delimited Continuations	５．発行年 2023年
３．雑誌名 In Proceedings of the 50th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL 2023), PACMPL 7(POPL)	６．最初と最後の頁 2079～2110
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3571264	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 Yu Gu, Takeshi Tsukada, Hiroshi Unno	４．巻 7
２．論文標題 Optimal CHC Solving via Termination Proofs	５．発行年 2023年
３．雑誌名 In Proceedings of the 50th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL 2023), PACMPL 7(POPL)	６．最初と最後の頁 604～631
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3571214	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 Nariyoshi Chida, Tachio Terauchi	４．巻 228
２．論文標題 On Lookaheads in Regular Expressions with Backreferences	５．発行年 2022年
３．雑誌名 In Proceedings of the 7th International Conference on Formal Structures for Computation and Deduction (FSCD 2022)	６．最初と最後の頁 15:1~15:18
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.FSCD.2022.15	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 Nariyoshi Chida, Tachio Terauchi	4．巻 S&P 2022
2．論文標題 Repairing DoS Vulnerability of Real-World Regexes	5．発行年 2022年
3．雑誌名 In Proceedings of the 43rd IEEE Symposium on Security and Privacy (S&P 2022)	6．最初と最後の頁 2060~2077
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/SP46214.2022.9833597	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Hiroshi Unno, Takeshi Tsukada	4．巻 6
2．論文標題 Software model-checking as cyclic-proof search	5．発行年 2022年
3．雑誌名 In Proceedings of the 49th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL 2022), PACMPL 6(POPL)	6．最初と最後の頁 1～29
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3498725	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 Hiroshi Unno, Tachio Terauchi, Eric Koskinen	4．巻 12759
2．論文標題 Constraint-Based Relational Verification	5．発行年 2021年
3．雑誌名 In Proceedings of the 33rd International Conference on Computer-Aided Verification (CAV 2021), Lecture Notes in Computer Science	6．最初と最後の頁 742～766
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-81685-8_35	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 該当する

1．著者名 Naoki Kobayashi, Taro Sekiyama, Issei Sato, Hiroshi Unno	4．巻 12913
2．論文標題 Toward Neural-Network-Guided Program Synthesis and Verification	5．発行年 2021年
3．雑誌名 In Proceedings of the 28th International Symposium on Static Analysis (SAS 2021), Lecture Notes on Computer Science	6．最初と最後の頁 236～260
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-88806-0_12	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Tachio Terauchi and Timos Antonopoulos	4．巻 28
2．論文標題 Bucketing and information flow analysis for provable timing attack mitigation	5．発行年 2020年
3．雑誌名 Journal of Computer Security	6．最初と最後の頁 607-634
掲載論文のDOI（デジタルオブジェクト識別子） 10.3233/JCS-191356	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Tachio Terauchi, Timos Antonopoulos	4．巻 11426
2．論文標題 A Formal Analysis of Timing Channel Security via Bucketing	5．発行年 2019年
3．雑誌名 In Proceedings of the 8th International Conference on Principles of Security and Trust (POST 2019), Lecture Notes in Computer Science	6．最初と最後の頁 29～50
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-17138-4_2	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 該当する

1．著者名 Timos Antonopoulos , Tachio Terauchi	4．巻 CSF 2019
2．論文標題 Games for Security Under Adaptive Adversaries	5．発行年 2019年
3．雑誌名 In Proceedings of the 32nd IEEE Computer Security Foundations Symposium (CSF 2019)	6．最初と最後の頁 216～229
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/CSF.2019.00022	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Daisuke Kimura, Koji Nakazawa, Tachio Terauchi, Hiroshi Unno	4．巻 37
2．論文標題 Failure of Cut-Elimination in Cyclic Proofs of Separation Logic	5．発行年 2020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 1_39～1_52
掲載論文のDOI（デジタルオブジェクト識別子） 10.11309/jssst.37.1_39	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 Naoki Kobayashi, Takeshi Nishikawa, Atsushi Igarashi, Hiroshi Unno	4．巻 11822
2．論文標題 Temporal Verification of Programs via First-Order Fixpoint Logic	5．発行年 2019年
3．雑誌名 In Proceedings of the 26th International Symposium (SAS 2019), Lecture Notes in Computer Science	6．最初と最後の頁 413～436
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-32304-2_20	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Yuki Satake, Hiroshi Unno, Hinata Yanagi	4．巻 AAAI 2020
2．論文標題 Probabilistic Inference for Predicate Constraint Satisfaction	5．発行年 2020年
3．雑誌名 In Proceedings of the 34th AAAI Conference on Artificial Intelligence (AAAI 2020)	6．最初と最後の頁 1644～1651
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 オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Terauchi Tachio、Antonopoulos Timos	4．巻 11426
2．論文標題 A Formal Analysis of Timing Channel Security via Bucketing	5．発行年 2019年
3．雑誌名 Proceedings of the 8th International Conference on Principles of Security and Trust (POST 2019), Lecture Notes in Computer Science, Springer	6．最初と最後の頁 29～50
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-17138-4_2	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 該当する

1．著者名 Nanjo Yoji、Unno Hiroshi、Koskinen Eric、Terauchi Tachio	4．巻 LICS 2018
2．論文標題 A Fixpoint Logic and Dependent Effects for Temporal Property Verification	5．発行年 2018年
3．雑誌名 Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science (LICS 2018), ACM	6．最初と最後の頁 759～768
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3209108.3209204	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 該当する

1．著者名 Satake Yuki、Unno Hiroshi	4．巻 10981
2．論文標題 Propositional Dynamic Logic for Higher-Order Functional Programs	5．発行年 2018年
3．雑誌名 Proceedings of the 30th International Conference on Computer Aided Verification (CAV 2018), Lecture Notes in Computer Science, Springer	6．最初と最後の頁 105～123
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-96145-3_6	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 Blot Arthur、Yamamoto Masaki、Terauchi Tachio	4．巻 10204
2．論文標題 Compositional Synthesis of Leakage Resilient Programs	5．発行年 2017年
3．雑誌名 Proceedings of the 6th International Conference on Principles of Security and Trust (POST 2017), Lecture Notes in Computer Science	6．最初と最後の頁 277～297
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-662-54455-6_13	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Timos Antonopoulos, Paul Gazzillo, Michael Hicks, Eric Koskinen, Tachio Terauchi, and Shiyi Wei	4．巻 52(6)
2．論文標題 Decomposition Instead of Self-Composition for Proving the Absence of Timing Channels	5．発行年 2017年
3．雑誌名 Proceedings of the 38th ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI 2017), ACM SIGPLAN Notices	6．最初と最後の頁 362-375
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3062341.3062378	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Hiroshi Unno, Yuki Satake, and Tachio Terauchi	4．巻 2
2．論文標題 Relatively Complete Refinement Type System for Verification of Higher-Order Non-deterministic Programs	5．発行年 2018年
3．雑誌名 Proceedings of the 45th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL 2018), PACMPL	6．最初と最後の頁 12:1-12:29
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3158100	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Hiroshi Unno, Sho Torii, Hiroki Sakamoto	４．巻 10427
２．論文標題 Automating Induction for Solving Horn Clauses	５．発行年 2017年
３．雑誌名 In Proceedings of the 29th International Conference on Computer Aided Verification (CAV 2017), Lecture Note on Computer Science	６．最初と最後の頁 571～591
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-63390-9_30	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計19件（うち招待講演　6件／うち国際学会　9件）

１．発表者名 Nariyoshi Chida, Tachio Terauchi
２．発表標題 On Lookaheads in Regular Expressions with Backreferences
３．学会等名 ソフトウェア科学会 第25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 (PPL 2023)
４．発表年 2023年

１．発表者名 Nariyoshi Chida, Tachio Terauchi
２．発表標題 On Lookaheads in Regular Expressions with Backreferences (Poster Presentation)
３．学会等名 ソフトウェア科学会 第25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 (PPL 2023)
４．発表年 2023年

１．発表者名 川原 知真，寺内 多智弘
２．発表標題 Nested Data Type における多相再帰の型推論手法（ポスター発表）
３．学会等名 ソフトウェア科学会 第25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 (PPL 2023)
４．発表年 2023年

１．発表者名
川俣 楓河，海野 広志，関山 太郎，寺内 多智弘

２．発表標題
代数的エフェクトハンドラのための篩型システム（ポスター発表）

３．学会等名
ソフトウェア科学会 第25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（PPL 2023）

４．発表年
2023年

１．発表者名
Hiroshi Unno, Tachio Terauchi, Yu Gu, Eric Koskinen

２．発表標題
Modular Primal-Dual Fixpoint Logic Solving for Temporal Verification

３．学会等名
ソフトウェア科学会 第25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（PPL 2023）

４．発表年
2023年

１．発表者名
野上 大成，寺内 多智弘

２．発表標題
後方参照付正規表現の表現力について

３．学会等名
ソフトウェア科学会 第25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（PPL 2023）

４．発表年
2023年

１．発表者名
Nariyoshi Chida, Tachio Terauchi

２．発表標題
Repairing DoS Vulnerability of Real-World Regexes (from IEEE S&P 2022)

３．学会等名
2022年 暗号と情報セキュリティワークショップ（招待講演）

４．発表年
2022年

１．発表者名
Nariyoshi Chida, Tachio Terauchi

２．発表標題
Repairing DoS Vulnerability of Real-World Regexes

３．学会等名
ソフトウェア科学会 第24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 (PPL 2022)

４．発表年
2022年

１．発表者名
川俣 楓河, 寺内 多智弘

２．発表標題
代数的エフェクトハンドラを持つ言語のためのトレースエフェクト

３．学会等名
ソフトウェア科学会 第24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 (PPL 2022)

４．発表年
2022年

１．発表者名
Tachio Terauchi

２．発表標題
Constraint-based Relational Verification

３．学会等名
Workshop on Hyperproperties: Advances in Theory and Practice (HYPER 2021)（招待講演）（国際学会）

４．発表年
2021年

１．発表者名
Yoji Nanjo, Hiroshi Unno, Eric Koskinen, Tachio Terauchi

２．発表標題
A Fixpoint Logic and Dependent Effects for Temporal Property Verification

３．学会等名
Dagstuhl Seminar 19371: Deduction Beyond Satisfiability（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Souta Yamauchi, Tachio Terauchi

２．発表標題
Inferring Simple Strategies for Efficient Quantified SMT Solving

３．学会等名
17th Asian Symposium on Programming Languages and Systems (APLAS 2019)（国際学会）

４．発表年
2019年

１．発表者名
Takashi Nishikawa, Yuki Satake, Yoji Nanjo, Hiroshi Unno, Naoki Kobayashi, Tachio Terauchi, Eric Koskinen

２．発表標題
Solving First-Order Fixpoint Logic for Program Verification

３．学会等名
Third Workshop on Mathematical Logic and its Applications (MLA 2019)（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Koji Nakazawa, Daisuke Kimura, Tachio Terauchi, Hiroshi Unno, Kenji Saotome

２．発表標題
On Cut-Elimination Theorem in Cyclic-Proof Systems

３．学会等名
Third Workshop on Mathematical Logic and its Applications (MLA 2019)（国際学会）

４．発表年
2019年

１．発表者名
Daisuke Kimura, Koji Nakazawa, Tachio Terauchi, Hiroshi Unno

２．発表標題
Failure of Cut-Elimination in Cyclic Proofs of Separation Logic

３．学会等名
日本ソフトウェア科学会 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
Daisuke Kimura, Koji Nakazawa, Tachio Terauchi, Hiroshi Unno

２．発表標題
On Cut-elimination in Cyclic Proof Systems

３．学会等名
The 4th Workshop on New Ideas and Emerging Results in Programming Languages and Systems (NIER 2018)（国際学会）

４．発表年
2018年

１．発表者名
Hiroshi Unno

２．発表標題
Horn Clauses and Beyond for Relational and Temporal Program Verification

３．学会等名
The 5th Workshop on Horn Clauses for Verification and Synthesis (HCVS 2018)（招待講演）（国際学会）

４．発表年
2018年

１．発表者名
Tachio Terauchi

２．発表標題
Information Flow Security and its Applications to Side Channel Attack Resilience

３．学会等名
The 4th Franco-Japanese Workshop on Cybersecurity（招待講演）（国際学会）

４．発表年
2018年

１．発表者名
Tachio Terauchi

２．発表標題
Compositional Synthesis of Leakage Resilient Programs

３．学会等名
NII Shonan Meeting Seminar 115: Intensional and Extensional Aspects of Computation: From Computability and Complexity to Program Analysis and Security（国際学会）

４．発表年
2018年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

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
研究分担者	海野　広志 (Unno Hiroshi) (80569575)	筑波大学・システム情報系・准教授 (12102)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関