様式 C-19

科学研究費補助金研究成果報告書

平成２１年　５月１２日現在

研究種目：若手研究（A）
研究期間：2006～2008
課題番号：１８６８０００３
研究課題名（和文）　プログラム検証による情報保護の統一理論とその応用
研究課題名（英文）　A unified theory and application of information hiding by program verification

研究代表者
住井　英二郎（SUMII EIJIRO）
東北大学・大学院情報科学研究科・准教授
研究者番号：００３３３５５０

研究成果の概要：

コンピュータプログラムやネットワークにおける暗号化や抽象化など、さまざまな形の情報保護の統一的基礎理論を研究した。特に、ループないし再帰関数、再帰型（リストや木など）、多相型ないしジェネリックス、抽象データ型ないしオブジェクトなど、幅広い現実的機能を有する計算体系における情報保護の数理論理学的証明手法を世界で初めて確立し、Journal of the ACM や IEEE LICS など最高水準の国際論文誌・国際学会に採録・発表された。

交付額

（金額単位：円）

	直接経費	間接経費	合　計
２００６年度	4,800,000	1,440,000	6,240,000
２００７年度	3,900,000	1,170,000	5,070,000
２００８年度	3,500,000	1,050,000	4,550,000
年度			
年度			
総　計	12,200,000	3,660,000	15,860,000

研究分野：プログラミング言語理論
科研費の分科・細目：情報学・ソフトウェア
キーワード：プログラム言語、情報セキュリティ、プログラム等価性、双模倣、ラムダ計算、パイ計算、高階計算、型理論

１．研究開始当初の背景

交通機関や医療機器、電子政府、電子商業システムなどの社会基盤がコンピュータに依存する現代社会において、それらを実際に制御するソフトウェアの信頼性向上は最重要課題である。特に偶然の事故だけでなく不正侵入など意図された攻撃に対するセキュリティは、一見すると些細な欠陥が問題となるケースがほとんどで、重要かつ困難な緊急課題となっている。研究開始の前年だけでも、一般紙の第一面で報道されるほどの重大な問題が毎月のように続発した。

暗号に代表される様々な技術にもかかわらず、問題が続発する根本要因として、暗号などの技術を正しく用いることの難しさが挙げられる。実際に、いわゆるセキュリティホールの大半は暗号アルゴリズムや認証デバイスの問題ではなく、それらを利用・制御するソフトウェアの欠陥が原因である。しかし人間の注意やテストのみによって、ソフトウェアの欠陥を十分に防止することは困難であり、またセキュリティの欠陥は非常に微

保護の方式	事前検査	安全の保証	検証手法の主要研究
暗号化	**不要**	**システム全体としては保証されない**	spi計算の双模倣など（1990年代後半～）
抽象型	**必要**	**数理論理学的に保証**	多相λ計算の論理関係など（1970年代～）
情報流解析	**必要**	**数理論理学的に保証**	slam計算など（1990年代後半～）

妙な条件で起こることも多く、「プログラマやエンジニアが注意する」「テストのプロセスを改善する」といった対策だけでは解決しない。

そこで、情報処理システムの欠陥を発見・防止する手法として、型理論やプログラム等価性など、プログラミング言語の基礎研究を応用し、特定の欠陥（情報漏洩など）が絶対に発生しないことを数理論理学的に検証するアプローチが注目されている。

本研究代表者は (1) 科学研究費補助金 特定領域研究「社会基盤としてのセキュア・コンピューティングの実現方式の研究」に領域代表者（東京大学 米澤明憲教授）研究室助手として参加、(2) ペンシルバニア大学 Visiting Scholar および Research Associate として、Benjamin C. Pierce 教授ら国内外の研究者と緊密に連携 などして、型理論やプログラム等価性といった数理科学的アプローチによるソフトウェア安全性検証について研究してきた。この研究により、コンピュータサイエンス分野全体のトップレベルにランクされる国際会議・学術雑誌（http://citeseer.ist.psu.edu/impact.html における estimated impact が上位 1%～3%程度）に多数の査読論文を採択された。

２．研究の目的

上述の研究をふまえ、本研究課題では「暗号化」「抽象型」「情報流解析」といった様々な情報保護の方式を検証する統一理論を確立し、さらにそれを利用して一つの方式における知見を他の方式へ応用することを目指した。

暗号化は、情報処理システムの実行時に実際にデータを変換することにより、アクセスを制限する方式である。暗号化は、事前検査されていない攻撃者からのアクセスも制限できる一方で、使用法は開発者にまかされており、誤って用いると（たとえ暗号自体が安全であっても）情報漏洩が発生する。

一方で、抽象型と情報流解析は、実行前の型検査や静的解析により、検査を通過したプログラムが情報を漏洩しないことを保証する方式である。抽象型と情報流解析は、防御側だけでなく攻撃者のプログラムも事前検査する必要があるが、事前検査さえ通過すれば情報漏洩は発生しないことが数理論理学的に保証される。また、抽象型を使用したプログラムの性質は、1970 年代より活発に研究されており、いわゆるオブジェクト指向としても利用され、理論・応用の両面が発達している。

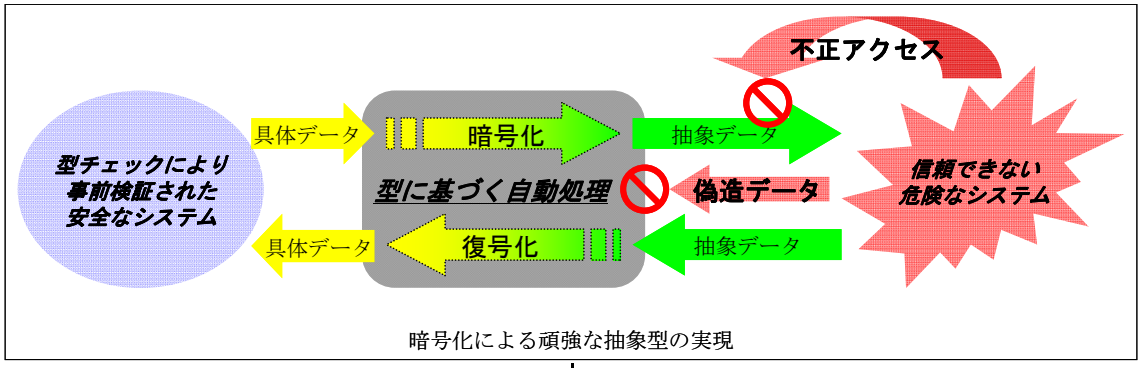
本研究課題では、これらの方式の利点・欠点を相互に応用・補完するために、特に次のテーマに取り組んだ。(1) 暗号化を中心に研究されてきた双模倣という検証手法と、抽象型を中心に研究されてきた論理関係という検証手法の両方の長所をそなえ、様々な情報保護に適用できる、統一された検証手法を確立する。(2) その知見を利用して、たとえば暗号化における復号化に対して抽象型における「具体化」を考え、抽象型の単純さと暗号化の柔軟さを兼備した言語機構を実現するなど、一方の手法を他方へ応用していく。

３．研究の方法

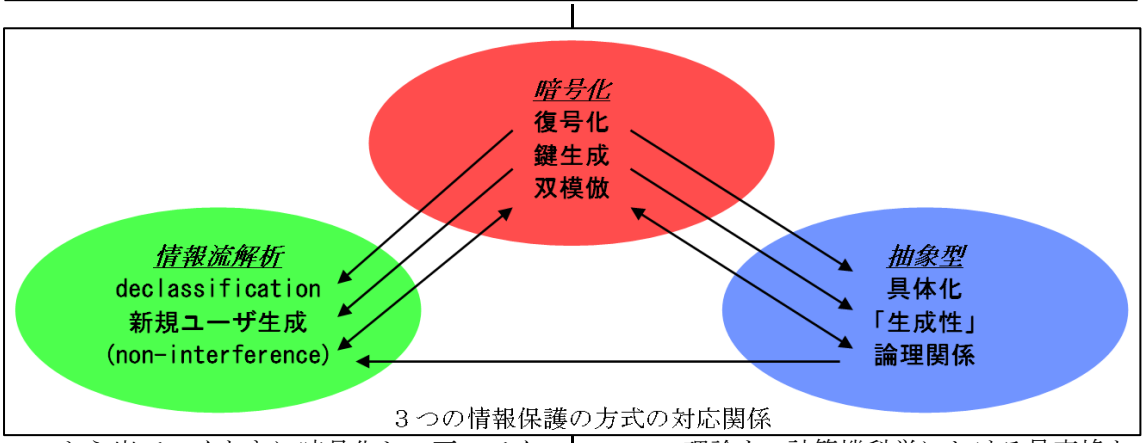
以下の計画に従い研究を行うことを目指した。

平成 18 年度　既存の論理関係と双模倣を比較・検討し、両者の特長を兼備した検証手法を確立する。特に、研究代表者による「抽象型のための双模倣」において、高階関数の場合に必要であった「インデックス」（計算ステップ回数）についての複雑な条件を取り除く。この複雑な条件は、実際の実行では常に満たされることが直観としては予想され、等価性に対する健全性を示す証明に織り込んでしまえば、双模倣の条件としては要求しなくても済むと考えられる。これにより、型に基づくシンプルな議論が可能で、かつ、再帰関数や再帰型・並列性など、現実で必要な機構に対応した検証手法が可能になると期待される。

それと並行して、抽象型を暗号化によって実装し、型検査されていない攻撃者からも情報を保護する通信ライブラリをプログラミング言語 Objective Caml で実現することを目指した。具体的には、抽象型の値がモジュ



暗号化による頑強な抽象型の実現



３つの情報保護の方式の対応関係

ールから出ていくときに暗号化し、戻ってくるときに復号化する、という処理を実装する。これは、暗号化・復号化を行う関数を型の表現とするエンコーディングのテクニックによって、Objective Caml を変更しなくてもライブラリとして実現できる。

平成 19 年度以降　平成 18 年度に引き続き、以下の研究を実施する。
(1) 暗号化における鍵生成の手法を応用して、既存の研究では対応していない「新規ユーザ生成」に対応した情報流解析の手法を確立する。さらに declassification（一部の必要な情報を意図して公開する操作）を導入した計算体系において、双模倣による検証手法を確立する。これらにより、新規ユーザ生成や declassification のある、現実のシステムにおいても安全の保証される情報流解析がはじめて可能となる。
(2) 暗号化における復号化の概念を応用し、一種の「秘密鍵」によって抽象データを「具体化」する言語機構を設計・実装する。実装としては前述の Objective Caml のライブラリを拡張し、複雑なデータ通信をする P2P システムやクライアント・サーバシステムなど数種のアプリケーションを試作して、機構設計が適切かどうか確認する。これにより、抽象型の単純さと暗号化の柔軟さを兼備した情報保護の機構が実現できると期待される。

４．研究成果

(1) 抽象型による情報保護のための双模倣の理論を、計算機科学における最高峰とされる論文誌に投稿し、採録された[雑誌論文 4]。また、一種の理想化された暗号化による情報保護のための双模倣の理論を、理論計算機科学において最も著名な論文誌の一つに投稿し採録された[雑誌論文 6]。
(2) プログラム自身を受け渡すことができる「高階言語」では難しいと考えられていた"up-to context"という手法の適用に成功、理論計算機科学において最も権威のある学会の一つである IEEE LICS 等で発表した[雑誌論文 5，雑誌論文 7]。これにより「インデックスについての帰納法」が不要となり、従来より単純かつ強力な双模倣の理論を確立した。
(3) これらの理論をさらに発展させ、等価性以外の性質にも応用する方法を研究し、一部の成果を発表した[雑誌論文 1]。
(4) プログラミング言語 Objective Caml のライブラリとして、「暗号化による抽象化」を実現した[学会発表 1]。
(5) その他、安全な型システムや暗号による情報保護に関連する論文やチュートリアルを発表した[雑誌論文 2，雑誌論文 3，学会発表 2，学会発表 3]。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 7 件）
[1] Eijiro Sumii. A Theory of Non-Monotone

Memory (Or: Contexts for free). Proceedings of 18th European Symposium on Programming, York, United Kingdom, March 22-29, 2009 (Lecture Notes in Computer Science, Springer-Verlag, Germany, vol. 5502), pp. 237-251. 査読あり.

[2] 住井 英二郎. MinCamlコンパイラ. コンピュータソフトウェア, 岩波書店, 25巻2号28-38頁, 2008年4月. 査読あり.

[3] 住井 英二郎. spi計算における暗号プロトコルの形式的検証. 応用数理, 岩波書店, 17巻4号16-26頁, 2007年12月. 査読あり.

[4] Eijiro Sumii and Benjamin C. Pierce. A Bisimulation for Type Abstraction and Recursion. Journal of the ACM, vol. 54, issue 5, article 26, pp. 1-43, October 2007. 査読あり.

[5] Davide Sangiorgi, Naoki Kobayashi, and Eijiro Sumii. Environmental Bisimulations for Higher-Order Languages. Proceedings of Twenty-Second Annual IEEE Symposium on Logic in Computer Science, Wroclaw, Poland, July 10-14, 2007, pp. 293-302. 査読あり.

[6] Eijiro Sumii and Benjamin C. Pierce. A Bisimulation for Dynamic Sealing. Theoretical Computer Science, Elsevier Science, the Netherlands, vol. 375, issues 1-3, pp. 169-192, May 2007. 査読あり.

[7] Davide Sangiorgi, Naoki Kobayashi, and Eijiro Sumii. Logical Bisimulations and Functional Languages. Invited paper in Post-Proceedings of IPM International Symposium on Fundamentals of Software Engineering, Tehran, Iran, April 17-19, 2007 (Lecture Notes in Computer Science, Springer-Verlag, Germany, vol. 4767), pp. 364-379. 査読なし（招待論文）.

〔学会発表〕(計３件)

[1] 須藤 尚稔, 住井 英二郎. 型安全な通信ライブラリQuicksilverとその改良. 日本ソフトウェア科学会 プログラミング論研究会 第9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, 石川県加賀市, 2007年3月8日.

[2] 住井 英二郎. spi計算における暗号プロトコルの形式的検証について（招待講演）. 日本応用数理学会 数理的技法による情報セキュリティ研究部会 第二回研究集会, 東京大学駒場キャンパス, 2006年12月22日(11:10〜12:10).

[3] 住井 英二郎. ２時間で真似(まね)ぶ関数型言語のコンパイラ（招待講演）. 日本ソフトウェア科学会 プログラミング論研究会 第４回プログラミングおよびプログラミング言語サマースクール, 東京大学本郷キャンパス, 2006年9月12日(13:45-15:45).

〔その他〕
ホームページ等
http://www.kb.ecei.tohoku.ac.jp/~sumii/

６．研究組織
(1)研究代表者
住井　英二郎（SUMII EIJIRO）
東北大学・大学院情報科学研究科・准教授
研究者番号：００３３３５５０
(2)研究分担者
（　　）
研究者番号：
(3)連携研究者
（　　）
研究者番号：