様 式 Ｃ－７－１

平成１９年度科学研究費補助金実績報告書（研究実績報告書）

1. 機 関 番 号 14603　2. 研究機関名 奈良先端科学技術大学院大学

3. 研 究 種 目 名 基盤研究（C）　4. 研究期間 平 成 １８ 年 度 ～ 平 成１９ 年 度

5. 課 題 番 号 18500023

6. 研 究 課 題 名 無限状態モデル検査を用いた高信頼性ソフトウェアの自動検証に関する研究

7. 研 究 代 表 者

研 究 者 番 号	研 究 代 表 者 名	所 属 部 局 名	職 名
80196948	ﾌﾘｶﾞﾅ セキ, ヒロユキ 関, 浩之	情報科学研究科	教授

8.研究分担者(所属研究機関名については、研究代表者の所属研究機関と異なる場合のみ記入すること。)

研 究 者 番 号	研 究 分 担 者 名	所属研究機関名・部局名	職 名
60294279	ﾌﾘｶﾞﾅ タカタ,ヨシアキ 高田, 喜朗	高知工科大学・工学部	講師
	ﾌﾘｶﾞﾅ		
	ﾌﾘｶﾞﾅ		
	ﾌﾘｶﾞﾅ		
	ﾌﾘｶﾞﾅ		

9. 研究実績の概要(国立情報学研究所でﾃﾞｰﾀﾍﾞｰｽ化するため、600 字～800 字で記入。図､ｸﾞﾗﾌ等は記載しないこと。)

（下欄には、当該年度に実施した研究の成果について、その具体的内容、意義、重要性等を、交付申請書に記載した「研究の目的」､「研究実施計画」に照らし、600 字～800 字で、できるだけ分かりやすく記述すること。また、国立情報学研究所でﾃﾞｰﾀﾍﾞｰｽ化するため、図、ｸﾞﾗﾌ等は記載しないこと。）

(1) 情報フロー解析

(a) HBAC 情報フロー解析:昨年度､実行履歴に基づくアクセス制御付プログラム HBAC (History-Based Access Control) に対するモデル検査器を実装し、その有効性を実証した。今年度はこのモデル検査法を応用した情報フロー解析を開発した。情報フロー解析を行うことにより、「望ましくない情報漏えいが生じない」という意味でアクセス制御が意図通りに機能しているかどうかを確認できる。従来の情報フロー解析法では主にメソッドの入出力間の情報フロー関係を解析していた。これに対して我々は、モデル検査法を応用することにより、一般の実行系列上に拡張された情報フロー解析を行う手法を提案することができた。

(b) 最近、自己合成法と呼ばれる情報フロー解析法が提案されている。これは解析精度が従来の型推論に基づく解析法より精度がよいという特長をもつ。本研究では、自己合成法を一般の再帰プログラムに適用できるように拡張した。

(2) 実行履歴に基づくアクセス制御モデルの表現能力の比較：Schneider のセキュリティオートマトン、Fong の狭履歴オートマトン、スタック検査、HBAC をアクセス制御機構にもつプログラムの表現能力を比較した。

(3) その他：上記(1)の言語理論ベースの手法を用いて、以下のような研究成果を挙げた。

(a) 等式系と書換え系を内部に演繹系としてもつ木オートマトンの諸性質を明らかにし、XML 文書処理への応用についても考察した。

(b) 公開木戦略(DTS)とよばれる信用交渉戦略が知られている。文脈自由文法(CFG)によるモデル化を用いて DTS の計算量を明らかにし、妥当な前提条件のもとで効率良く動作する DTS 実行アルゴリズムを示した。

(c) CFG の構文解析法を応用し、相互作用をもつ RNA の２次構造予測法を提案した。

10. キーワード

(1)	形式的検証	(2)	モデル検査	(3)	静的解析
(4)	形式言語	(5)	アクセス制御	(6)	セキュリティ
(7)	実行履歴	(8)	ソフトウェア学		

（裏面に続く）

11.研究発表（平成１９年度の研究成果）

〔**雑誌論文**〕　計（４）件

著　者　名	論　文　標　題			
Hitoshi Ohsaki and Hiroyuki Seki	Languages Modulo Normalization			
雑　誌　名	査読の有無	巻	発 行 年	最初と最後の頁
Lecture Notes in Artificial Intelligence (FroCos07)	有	4720	2007	221-236

著　者　名	論　文　標　題			
Yoshiaki Takata and Hiroyuki Seki	Computational Complexity of the Disclosure Tree Strategy in Trust Negotiation			
雑　誌　名	査読の有無	巻	発 行 年	最初と最後の頁
2007 International Conference on Next Era Information Networking (NEINE07)	有		2007	323-328

著　者　名	論　文　標　題			
Yuki Kato, Tatsuya Akutsu and Hiroyuki Seki	A Grammatical Approach to RNA-RNA Interaction Prediction			
雑　誌　名	査読の有無	巻	発 行 年	最初と最後の頁
2007 International Symposium on Computational Models for Life Sciences (CMLS'07)	有		2007	197-206

著　者　名	論　文　標　題			
高田喜朗，王静，関浩之	実行履歴に基づくアクセス制御の形式モデルと検証			
雑　誌　名	査読の有無	巻	発 行 年	最初と最後の頁
電子情報通信学会論文誌 D	有	J91-D(4)	2008	847-858

〔**学会発表**〕計（３）件

発　表　者　名	発　表　標　題	
高田喜朗，関浩之	モデル検査によるHBACプログラムの情報流解析	
学　会　等　名	発表年月日	発　表　場　所
日本ソフトウェア科学会第5回ディペンダブルシステムワークショップ	2007年7月	函館

発　表　者　名	発　表　標　題	
Hiroyuki Seki and Yoshiaki Takata	Comparison of the Expressive Power of Language-based Access Control Models	
学　会　等　名	発表年月日	発　表　場　所
日本ソフトウェア科学会第5回ディペンダブルシステムワークショップ	2007年7月	函館

発　表　者　名	発　表　標　題	
伊藤信裕，関浩之	自己合成法を利用した再帰プログラムの情報流解析について	
学　会　等　名	発表年月日	発　表　場　所
電子情報通信学会技術研究報告SS2007-62	2008年3月	長崎

〔**図　書**〕　計（０）件

著　者　名	出　版　社	
書　名	発 行 年	総ページ数

12. 研究成果による産業財産権の出願・取得状況

〔**出　願**〕　　計（０）件

産業財産権の名称	発明者	権利者	産業財産権の種類、番号	出願年月日	国内・外国の別

〔取　得〕　　計（0）件

産業財産権の名称	発明者	権利者	産業財産権の種類、番号	取得年月日	国内・外国の別

13. 備考

※　研究者又は所属研究機関が作成した研究内容又は研究成果に関するｗｅｂページがある場合は、ＵＲＬを記載すること。
