様　式　Ｃ－７－１

平成１８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　1 4 6 0 3　　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　1 8 5 0 0 0 2 3

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
8 0 1 9 6 9 4 8	フリガナ　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
6 0 2 9 4 2 7 9	フリガナ　タカタ，ヨシアキ 高田，喜朗	情報科学研究科	助手
	フリガナ		
	フリガナ		
	フリガナ		
	フリガナ		

9. 研究実績の概要(国立情報学研究所でデータベース化するため、600字～800字で記入。図、グラフ等は記載しないこと。)

(1) 再帰的プログラムのモデル検査に関する研究.

(a) 我々が以前より取り組んでいる，実行履歴に基づくアクセス制御付きプログラム（HBAC プログラム）の安全性検証法において，種々の最適化を行うことにより，高速な検証が可能であることを実証した．我々のモデル検査アルゴリズムでは，検証対象のプログラムに対するモデル検査問題を，文脈自由文法(CFG)の空判定問題に帰着しており，一般にアクセス権の個数に対して指数的な検証時間を要する．そこで，CFG を構成する際，useless な規則（開始記号から到達しないか，または，終端記号列を一つも生成しない規則）の構成を防ぐ最適化法を提案した．Chinese-Wall ポリシとオンラインバンキングシステムの２つの例題について最適化の効果を実測した結果，どちらの検証例においても，最適化を行わない場合，アクセス権の数が５個程度までしか検証できなかったのに対し，最適化を行うことにより，前者の例ではアクセス権の数が 80 個のとき約 64 秒，後者の例では 60 個のとき約 0.01 秒で検証を行えた．

(b) プログラムの実行による情報流出を解析する手法として情報フロー解析が有効である．本研究では，HBAC プログラムに対し，モデル検査に基づく新しい情報フロー解析法を提案した．提案手法を用いることにより，プログラムの実行完了時に出力の機密度（security class, SC）がどのようになるかだけでなく，「SC が τ であるような値を引数として関数 f が呼び出されたならば，いつか SC が τ’ である値を引数として関数 g が呼び出される」のような，実行系列上に拡張された情報フローに関する性質を調べることができる．

(2) 実行履歴に基づくアスペクト折込み機能の形式モデル：Aspect-J 等で採用されている PA (pointcut and advice) の形式モデル A-LTS を提案した．A-LTS と既存の計算モデルの表現能力を比較した結果，A-LTS の受理言語，決定性文脈自由言語，線形文脈自由言語のクラスはすべて互いに他を含まないことを証明した．その系として，A-LTS にはプッシュダウンシステムのモデル検査法が適用可能であることがわかった．

※　成果の公表を見合わせる必要がある場合は、その理由及び差し控え期間等を記入した調書(A4判縦長横書1枚)を添付すること。

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) XML
(7) セキュリティ	(8) 実行履歴	

（裏面に続く）

11. 研究発表(平成18年度の研究成果)

〔雑誌論文〕　計（５）件

著者名	論文標題			
Jing Wang, Yoshiaki Takata and Hiroyuki Seki	HBAC: A Model for History-based Access Control and Its Model Checking			
雑誌名		巻・号	発行年	ページ
11th European Symposium On Research In Computer Security, Lecture Notes in Computer Science		4189	2006	263-278

著者名	論文標題			
王, 伊藤, 高田, 関	実行履歴に基づくアクセス制御付きプログラムのモデル検査法による情報フロー解析			
雑誌名		巻・号	発行年	ページ
電子情報通信学会技術研究報告		SS2006-72	2007	7-12

著者名	論文標題			
王, 高田, 関	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			
雑誌名		巻・号	発行年	ページ
日本ソフトウェア科学会第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論文集			2007	90

著者名	論文標題			
王, 伊藤, 高田, 関	HBACプログラムのモデル検査の情報フロー解析への応用			
雑誌名		巻・号	発行年	ページ
電子情報通信学会2007年総合大会		D-3-1	2007	(CD-ROM)

著者名	論文標題			
Isao Yagi, Yoshiaki Takata and Hiroyuki Seki	A Labeled Transition Model A-LTS for Histroy-based Aspect Weaving and Its Expressive Power			
雑誌名		巻・号	発行年	ページ
IEICE Transactions on Information and Systems		E90-D(5)	2007	印刷中

著者名	論文標題			
雑誌名		巻・号	発行年	ページ

〔図　書〕　計（０）件

著者名	出版社		
書名		発行年	総ページ数

12. 研究成果による工業所有権の出願・取得状況

計（０）件

工業所有権の名称	発明者	権利者	工業所有権の種類、番号	出願年月日	取得年月日