様 式 Ｃ－７－１

平成２１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 ２０ 年 度 ～ 平 成 ２２ 年 度

5. 課 題 番 号 | 2 | 0 | 5 | 0 | 0 | 0 | 3 | 4 |

6. 研 究 課 題 名　言語組込みアクセス制御の高信頼化に関する研究

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
	ﾌﾘｶﾞﾅ		
	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

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。

「言語組込みアクセス制御」と呼ばれる機構に着目し，ソフトウェアがセキュリティ要求仕様を満たして動作することを保証するため自動生成技術について以下の研究を行った．

1． アクセス制御モデルとしてHistory-based Access Control（実行履歴に基づくアクセス制御）を仮定し，情報流の概念を用いて仕様記述言語を定義した．さて，情報流に基づくセキュリティ基準として非干渉性(noninterference)が知られている．しかし，非干渉性は一般の再帰プログラムに対しては決定不能である．そこでまず，再帰プログラムPとセキュリティ仕様Sに対し，Sにおける機密度を型とみなすことでSの下でのPの型安全性を定義した．そして，PがSの下で型安全ならば，PはSに対して非干渉性を満たすこと（型安全性は非干渉性の十分条件であること）を証明した．

2． 自動生成問題を「再帰プログラムPとセキュリティ仕様Sが与えられたとき，PがSの下で型安全となるようPにアクセス検査文を挿入する問題」と定義し，自動生成問題がco-NP困難であることを証明した．

3． プッシュダウンシステム(PDS)のモデル検査法を利用して自動生成問題を解くアルゴリズムを提案した．PDSは再帰プログラム型の簡潔な計算モデルである．提案手法ではまず，与えられたプログラムPにおいて変数値をその機密度（型）に抽象化することによりPをPDS Mに変換する．Mに対してモデル検査を実行し，もし型安全性に反する実行列が発見されれば，その実行列が強制終了されるようMにアクセス検査文を挿入する．

4． 提案手法に基づいて自動生成システムを実装し，いくつかの例題に対して実験を行った結果，実用的な時間で自動生成が行えることを実証した．

10. キーワード

(1)	アクセス制御	(2)	情報流解析	(3)	セキュリティ
(4)	実行履歴	(5)	スタック検査	(6)	自動生成
(7)	静的解析	(8)			

（裏面に続く）

11.研究発表（平成２１年度の研究成果）

〔雑誌論文〕　計（1）件　　うち査読付論文　計（1）件

著者名	論文標題			
Yoshiaki Takata and Hiroyuki Seki	Comparison of the Expressive Power of Language-based Access Control Models			
雑誌名	査読の有無	巻	発行年	最初と最後の頁
IEICE Transactions on Information and Systems	有	E92-D(5)	2009	1033-1036

著者名	論文標題			
雑誌名	査読の有無	巻	発行年	最初と最後の頁

著者名	論文標題			
雑誌名	査読の有無	巻	発行年	最初と最後の頁

〔学会発表〕計（6）件　　うち招待講演　計（6）件

発表者名	発表標題	
関浩之	Synthesis and Verification of History-based Access Control	
学会等名	発表年月日	発表場所
The 2009 SJTU-JAIST Joint Workshop on Formal Methods	2009年6月17日	中華人民共和国上海市

発表者名	発表標題	
関浩之	アクセス制御 －言語ベースセキュリティをめざして－	
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7回 ディペンダブルシステムワークショップ	2009年7月15日	北海道亀田郡七飯町

発表者名	発表標題	
高田喜朗，森田剛正，関浩之	情報流仕様に基づくアクセス権検査文自動挿入法	
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7回 ディペンダブルシステムワークショップ	2009年7月15日	北海道亀田郡七飯町

発表者名	発表標題	
森田剛正，高田喜朗，関浩之	情報流仕様に基づくアクセス制御文の自動生成	
学会等名	発表年月日	発表場所
電子情報通信学会ソフトウェアサイエンス研究会	2009年8月7日	北海道北見市

発表者名	発表標題	
関浩之	ソフトウェアの静的解析と動的検査 － 言語ベースセキュリティを例にして －	
学会等名	発表年月日	発表場所
情報処理学会 組込みシステムシンポジウム2009	2009年10月21日	東京都渋谷区

発　表　者　名	発　　表　　標　　題		
高田喜朗，関浩之，森田剛正	情報流仕様に基づくアクセス権検査文自動挿入法		
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12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		2010年3月4日	香川県仲多度郡琴平町

〔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。
