様 式 Ｃ－７－１

平成２２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	セキ 関 ヒロユキ 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

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. 昨年度までに，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．また，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．前年度までの理論的検討に引き続き，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）の証明を完成させた．
2. 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昨年度提案したが，今年度はそのアルゴリズムを改良した．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．
3. 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．具体的に，「互いにセキュリティレベルの異なるk個の入力変数から一つを非決定的に選択して内部変数にその値を代入し，次に，互いにセキュリティレベルの異なるk個の出力変数のいずれか一つにその内部変数の値を書き出す」というプログラムをベンチマークとして実験を行った結果，k=200でも20秒以内で自動生成が可能であることを実証した．

10. キーワード

(1)	アクセス制御	(2)	情報流解	(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２２年度の研究成果）

〔雑誌論文〕　計（　0　）件　　うち査読付論文　計（　0　）件

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（　4　）件　　うち招待講演　計（　1　）件

発　表　者　名	発　　表　　標　　題		
Yoshiaki Takata, Hiroyuki Seki	Automatic generation of history-based access control from information flow specification		
学　会　等　名		発表年月日	発　表　場　所
8th International Symposium on Automated Technology for Verification and Analysis		2010年9月23日	Singapore

発　表　者　名	発　　表　　標　　題		
Hiroyuki Seki	Automatic insertion of access checks into recursive programs		
学　会　等　名		発表年月日	発　表　場　所
3rd SJTU-JAIST Workshop on Formal Method		2010年6月4日	金沢市

発　表　者　名	発　　表　　標　　題		
Kenji Hashimoto, Hiroyuki Seki	Tree language theoretic approach to security verification for XML databases		
学　会　等　名		発表年月日	発　表　場　所
3rd Japan-Vietnam Workshop on Software Engineering 2010		2010年12月9日	Hanoi, Vietnam

発　表　者　名	発　　表　　標　　題		
関　浩之	システム設計・検証の数理		
学　会　等　名		発表年月日	発　表　場　所
2011年電子情報通信学会総合大会		2011年3月14日	東京都市大学で開催予定が中止となり、DVD の配布をもって、すでに公表されているので、大会での発表は成立とみなす。

〔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。
