様　式　Ｃ－７－１

平成１７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１６年度　～　平成１７年度

5. 課題番号　1 6 5 0 0 0 1 9

6. 研究課題名　アクティブソフトウェアの設計検証手法に関する研究

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）実行履歴に基づくアクセス制御系の検証法：昨年度我々が提案した実行履歴に基づくアクセス制御系のモデルHBAC(History-Based Access Control)に対し，本年度は検証器の実装を行った．検証器は，与えられたHBACプログラムの実行系列を生成する文脈自由文法(CFG) Gを構成し，Gの生成する言語L(G)が検証性質を表す正則言語L(R)に包含されるかどうかを判定する．単純な実装ではGのサイズがアクセス権の種類に対して指数的となり実用的でない．そこで，(a) Gの開始記号から生成規則によって到達可能な非終端記号のみを幅優先探索で構成する，(b) Gの各非終端記号Aには，Aの表す実行区間の先頭と末尾においてプログラムのもつアクセス権集合が埋め込まれているが，実行区間末尾におけるアクセス権集合を先行計算（部分計算）することにより，構成すべき非終端記号の個数を減らす，という２種の最適化を実装した．これにより，オンラインバンキングシステムをモデル化したHBACプログラムにおいて，アクセス権の総数が24のとき，最適化(a)のみでは検証に約71秒要したのに対して，(a)(b)を共に行うことにより0.24秒に短縮できた．

（２）XMLアクセス制御における静的解析法：昨年度に引き続き，XMLデータベースにおける要素レベルアクセス制御について木オートマトン理論を用いて考察した．本年度は我々の問合せモデルがNevenのquery automatonより真に表現能力が大きいことを示した．また，スキーマ変換Φとその入力/出力スキーマにおけるアクセス制御ポリシーPin, Poutが与えられたとき，「Pinによって保護されるデータは，Φによる変換後もPoutによって保護されること」を検証する問題が判定可能であることを示した．

（３）内部状態を考慮した信用管理システム：PKI(公開鍵基盤)ディジタル証明書の認証に基づく信用管理システムにおいて，システムの内部状態を考慮した形式モデルならびにそのモデル検査法を提案した．さらに，モデル検査器SPINとPrologを組み合わせた検証法とPrologのみを用いた検証法を実装し，後者の方が検証効率が良いことを実証した．

※　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) アクティブソフトウェア
(4) アクセス制御	(5) 静的解析	(6) 実行履歴
(7) 形式言語	(8) セキュリティポリシー	

(裏面に続く)

11.研究発表(平成17年度の研究成果)

〔雑誌論文〕　計（6）件

著者名	論文標題			
Isao Yagi, et al.	A Static Analysis using Tree Automata for XML Access Control			
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		SS2005-18	2005	1-6

著者名	論文標題			
Hisashi Mouri, et al.	A Formal Model for Stateful Trust Management Systems			
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		SS2005-20	2005	13-18

著者名	論文標題			
Isao Yagi, et al.	A Static Analysis using Tree Automata for XML Access Control			
雑誌名		巻・号	発行年	ページ
3rd Int'l Symp. on Automated Technology for Verification and Analysis, Lecture Notes in Computer Science		3707	2005	234-247

著者名	論文標題			
Hisashi Mouri, et al.	A Formal Model for Stateful Trust Management Systems			
雑誌名		巻・号	発行年	ページ
IASTED International Conference on Software Engineering and Applications		467-030	2005	87-92

著者名	論文標題			
王静, 他	実行履歴に基づくアクセス制御付き再帰プログラムのモデル検査			
雑誌名		巻・号	発行年	ページ
日本ソフトウェア科学会第8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			2006	183

著者名	出版社		
Isao Yagi, et al.	A Static Analysis using Tree Automata for XML Access Control		
書名		発行年	総ページ数
コンピュータソフトウェア		2006	印刷中

〔図　書〕　計（0）件

著者名	論文標題			
雑誌名		巻・号	発行年	ページ

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