様　式　Ｃ－７－１

平成２３年度科学研究費助成事業（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(B)　　4．補助事業期間　平成２３年度～平成２６年度

5．課題番号　2 3 3 0 0 0 0 8

6．研究課題　形式言語理論に基づく静的解析法とその安全性検査への応用

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	セキ　ヒロユキ 関　浩之	情報科学研究科	教授

8．研究分担者

研究者番号	研究分担者名	所属研究機関名・部局名	職名
40362024	オガワ　ミズヒト 小川　瑞史	北陸先端科学技術大学院大学・情報科学研究科	教授
70263431	カジ　ユウイチ 楫　勇一	情報科学研究科	准教授
90548447	ハシモト　ケンジ 橋本　健二	情報科学研究科	助教

9．研究実績の概要

今年度は主に木言語理論を用いた安全性検証法について次の成果を挙げた。データベース内に格納されている機密度の高い情報の漏えいを防止するため、問合せを許可問合せと禁止問合せに分類するというアクセス制御がよく用いられる。しかし、許可問合せの結果を巧みに組合せることで禁止問合せの結果（もしくはその候補）を得られることがある。このような操作を推論攻撃という。データベースtに対する問合せQの結果をQ(t)とかく。Dデータベースt、許可問合せQS、禁止問合せQUが与えられたとき、問合せ結果QS(t)、およびQS，QUのコード、tの従うスキーマを用いても、QU(t)の候補値をk個未満に絞れないとき、tはQS,QUについてk-安全であるという。同様に、候補値を有限個に絞れないとき、tはQS,QUについて∞-安全であるという。データベーススキーマDS，許可問合せQS，禁止問合せQUが与えられたとき、DSに従うすべてのインスタンスtに対して、tがQS,QUについてk-安全（もしくは、∞-安全）であるとき、スキーマDSは、QS,QUに対してk-安全（もしくは、∞-安全）であるという。本研究では、XMLデータベースを形式化するため、DSが木オートマトン、QS，QUが決定性線形トップダウン木変換器で与えられると仮定し、スキーマDSのk-安全性は判定不能であること、および、∞-安全性は判定可能であることを示した。

次に、アクセス制御法について以下の成果を挙げた。ロールに基づくアクセス制御(RBAC)では個人とロール間の関係は単一組織内で閉じており多組織間で共有することができない。そこで本研究では、異なる組織のロール間関係だけを定義し、個人がどのロールをもつかを階層的IDベース暗号で認証できる仕組み導入することにより、個人が所属する組織のロールを用いて他組織でアクセス制御を行う機構を提案した。

10.キーワード

(1) ソフトウェア検証	(2) 形式言語理論	(3) モデル検査	(4)
(5)	(6)	(7)	(8)

11.現在までの達成度

（区分）（2）おおむね順調に進展している。

（理由）

木言語を用いたセキュリティ検証法に関する研究は予定通りに進展した。また、類似の手法により、XMLデータベースの文書変換に対する情報保存性に関する研究に着手している。文書データベースを長期使用する場合、中途で文書構造を変更したいという要求がしばしば起こる。しかし、不用意な文書構造の変換により、変更前に抽出可能であった情報が変更後は抽出不可能になる場合がある。このような不都合が起こらないとき、文書変換は情報保存性をもつという。与えられたデータベーススキーマDSと文書変換Tに対し、Tが情報保存性をもつかどうかを判定する問題を検討するのがここでの目的である。そのためには、情報保存性を形式的に定義する必要がある。そこで本研究では、DSとTに加え、DSに従うデータベースインスタンスtに対する問合せQが与えられるとし、変換前のインスタンスに対するQの結果と同一の結果を返す変換後インスタンスへの問合せQ’が存在するとき、すなわち、「DSに従う任意のインスタンスtに対し、Q’(T(t))=Q(t)」を満たすQ’ が存在するとき、TはDSのもとでQに対して情報保存性をもつと定義する。DSは推論攻撃の場合と同様に木オートマトンで与えるとし、TとQを現実的に意味のあるいくつかのモデルで形式化し、情報保存性が判定可能かどうかを検討している。情報保存性に関する成果は平成２４年度後半より学会等で発表予定であり、また同年度分の科研報告書に記載する予定である。

12.今後の研究の推進方策

（今後の推進方策）

（１）推論攻撃問題については、問合せのクラスの決定性と線形性は保持しつつ、ボトムアップ型や、先読み付きトップダウン型に変更、拡張したときの判定可能性について考察する。さらに、判定可能である場合の計算量の上界及び下界を解析する。
（２）情報保存性については、文書変換および問合せのクラスの設定について種々のバリエーションを検討する。我々は主にXMLデータベースに興味をもっており、XML文書は木構造で表現されるので、文書変換のクラスとしては木変換器の適切な部分クラスを設定する。問合せのクラスについては結果が再びXML文書となる場合、および、結果が数値等の値または値の集合となる場合の両方を想定し、前者については木変換器、後者については木オートマトンのrun（状態の木頂点への割当て）に基づく問合せモデルを用いる。
（３）セキュリティ安全性やプライバシー保全の量的尺度として、量的情報流、k-匿名性、差分プライバシー等の概念が最近提案されている。これらの概念を扱えるような静的解析の手法も種々提案されているが、主にその定義から、情報理論的もしくは統計的アプローチが主流である。しかし、データを外部に出力もしくは漏洩する実体はプログラムである。そこで今後の研究では、プログラムの振舞いを、上記の概念を組み込んだ形で形式言語理論を用いて適切にモデル化し、より現実的な解析手法を提案することを目指す。

13.研究発表（平成23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

掲載論文のDOI（デジタルオブジェクト識別子）

〔学会発表〕 計(4)件　うち招待講演 計(1)件

発表者名	発表標題
Chittaphone Phonharath, Kenji Hashimoto and Hiroyuki Seki	Static Analysis for k-secrecy against Inference Attacks

学会等名	発表年月日	発表場所
Korea-Japan Joint Workshop on Software Science and Engineering	2011年06月30日	高麗大学, 韓国

発表者名	発表標題
Hiroyuki Seki	Multiple Context-Free Grammars: Basic Properties and Complexity

学会等名	発表年月日	発表場所
the Second Workshop on Multiple Context-Free Grammars and Related Formalisms (MCFG+2)（招待講演）	2011年09月09日	奈良県文化会館

発表者名	発表標題
Ramon Mejia, Yuichi Kaji and Hiroyuki Seki	Trans-Organizational Role-Based Access Control

学会等名	発表年月日	発表場所
ACM Computer and Communications Security (ACM CCS) 2011	2011年10月19日	Chicago, USA

発 表 者 名	発 表 標 題
Chittaphone Phonharath, Kenji Hashimoto and Hiroyuki Seki	Verification of the Security against Inference Attacks on XML Databases

学 会 等 名	発表年月日	発 表 場 所
1st International Workshop on Trends in Tree Automata and Tree T2ransducers (TTATT 2012)	2012年06月02日	名古屋大学

〔図書〕 計(0)件

著 者 名	出 版 社

書 名	発行年	総ページ数

14.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 出願年月日	国内･外国の別

15.備考