様式 C-19

科学研究費補助金研究成果報告書

平成 21 年 6 月 10 日現在

研究種目：若手研究(B)
研究期間：2007～2008
課題番号：19700026
研究課題名（和文）　ＸＭＬデータベースのための木オートマトンを用いた効率的アクセス制御法
研究課題名（英文）　A tree automata-based efficient access control method for XML databases
研究代表者　　高田　喜朗 (TAKATA YOSHIAKI)
高知工科大学・工学部・講師
研究者番号　　60294279

研究成果の概要：
XMLデータベースのためのアクセス制御の効率化を目標に，木オートマトン理論に基づく静的解析法の研究を行った．本研究の基本アイデアは，アクセス制御ポリシーおよび問い合わせをそれぞれ木オートマトンでモデル化し，問い合わせがアクセス制御ポリシーに違反するかどうか判定する問題を木オートマトンの言語の包含性判定に帰着して解くことである．AND意味論とOR意味論という二つの意味論を定義し，AND意味論では多項式時間で解析可能であるのに対しOR意味論では決定性指数時間完全であることなどを明らかにした．

交付額

（金額単位：円）

	直接経費	間接経費	合　計
2007 年度	2,000,000	0	2,000,000
2008 年度	1,100,000	330,000	1,430,000
年度			
年度			
年度			
総　計	3,100,000	330,000	3,430,000

研究分野：総合領域
科研費の分科・細目：情報学・ソフトウェア
キーワード：XML データベース，アクセス制御，木オートマトン，静的解析

１．研究開始当初の背景

各種データや文書の記述言語としての XML (eXtensible Markup Language)の有用性が広く認識されるにつれ，XML をデータモデル（スキーマ）として用いる XML データベースの研究・開発が盛んに行われるようになっていた．木構造データモデルである XML は従来主流だった関係データモデルと本質的に異なるため，専用の問合せ言語，問合せ最適化法，アクセス制御ポリシー記述言語などが各種研究・提案されてきた．

アクセス制御はデータベースの最も基本的なセキュリティ機能であり，「どの利用者にどのデータへのアクセスを許すか」という規則（アクセス制御ポリシ）に従って，許可されていないアクセスを遮断する．

XML 用アクセス制御ポリシー記述言語として 2000 年前後にいくつかの代表的提案がなされ，その後標準化団体により XACML が制定された．XACML の表現能力に関する研究はその後も行われていたが，効率的なアクセス制

御法の研究は少なかった．実際に運用されるデータベースは通常非常に大きくなるため，データベースサイズが大きくなっても計算量が増加しないような，工夫されたアクセス制御法が強く望まれる．

Murata ら(2003)は，静的解析に基づく XML アクセス制御法を初めて提案した．これは，データベース本体を参照することなく問合せとアクセス制御ポリシーの照合によってポリシー違反を検出するものであり，計算量がデータベースサイズに依存しないという優れた特徴をもつ．しかし彼らの方法は，木構造中の根からの経路のみに着目した近似手法であるため，子孫や兄弟の構造を参照するような木構造独特のポリシーを表現できないという問題があった．

２．研究の目的

Murata らの方法は系列に関する有限オートマトンを用いたものであるが，系列有限オートマトンの拡張として木オートマトンがあり，XML 用のスキーマ記述言語や問合せ言語のモデルとして利用されていた．

そこで，木オートマトンに基づく静的解析法を開発することで木構造独特のポリシーを正確に扱えるようになると考え，静的解析法の提案および試作システムによる実証を目指した．

まず，代表的な XML 用要素指定言語（現実に広く用いられている XPath や Neven らの 2DQA）と申請者らの木オートマトンに基づくモデルとの関係を解明し，実用的な表現能力を保ちつつ静的解析の計算量が大きくならないようなクラスの提案を行う．そして，提案法を実装したプロトタイプを作成し，ベンチマークデータ集合などを使った評価実験によって有効性を確認する．

静的解析の限界として，モデルでは表現できない機能を近似表現して解析した場合，「ポリシに違反するともしないとも言えない」という結果になることがある．このような場合には，問合せを実際にデータベースに適用しながらポリシに違反しないか調べる動的解析を行うことになるが，静的解析時に得られた情報を使って動的解析の効率を改善できる可能性がある．この点についても考察し，有用な手法の開発を目指す．

３．研究の方法

(1) 既存モデルと木オートマトンに基づくモデルとの関係の解明：
XPath や 2DQA などの代表的要素指定言語と提案モデルとの表現能力の比較，および効率的な相互変換法の開発を行う．特に，実用上有用な機能と静的解析問題が多項式時間可解となる条件との関係について考察し，実用性と効率を両立させるモデルの提案を目指す．

(2) アクセス制御法のプロトタイプ作成と評価実験：
(1)の検討結果に基づき，提案モデルのいくつかの部分クラスに対して静的解析法を実装し，評価実験のためのプロトタイプを作成する．XMark などのベンチマークテスト集合を利用して，実装した解析法の性能を評価する．プロトタイプの作成にあたっては，教育的効果も狙い，大学院生の補助を得て行う．

(3) 最適化法の検討：
(1)では静的解析法の最悪時計算量について検討するが，不要となる計算をなるべく省くことで，最悪時の計算量は大きくとも多くの場合には効率よく解けるという可能性がある．実用上，このような最適化法の検討は基本解法の開発と同じくらい重要である．そこで，(2)の結果に基づいて本問題に対する最適化法を検討し，実装・再実験する．

(4) 実際的なアクセス制御モジュールの設計及び実装：
Xindice などのオープンソースの XML データベースシステムを用いて，そのアクセス制御モジュールとして提案法を実装することを検討する．そして，作成したモジュールを組み込んだデータベースを研究室内にて稼働させ，運用実験を行う．

申請者らの研究グループでは，奈良先端科学技術大学院大学・大阪大学・産業技術総合研究所等の XML および木構造データの研究に従事する研究者と，小規模な研究交流会を定期的に実施して密な情報交換・意見交換を行っている．本研究においても，XML 研究の最新動向を知り，また提案法自体や研究アプローチに関する適切なコメントを得る機会として，この研究交流会を活用する．

４．研究成果

(1) 木オートマトンに基づくアクセス制御ポリシーと問い合わせのモデルを提案し，アクセス制御のための静的解析の枠組みを提案した（図1）．アクセス制御ポリシーは本来，XMLデータベースのインスタンスを表す木が与えられたときに，各頂点

にアクセス許可または禁止のラベルを割り当てる規則のことである．本モデルではこれを，各頂点に＋または-をラベル付けした木を受理する木オートマトンとしてモデル化する（図2）．問い合わせについては，アクセスする頂点・しない頂点をそれぞれ＋および-のラベルで表すことで，同様に木オートマトンでモデル化する．同じデータベースインスタンスに対して複数の＋-割り当てを行うアクセス制御ポリシーが与えられたときの解釈として，AND意味論とOR意味論という二つの意味論を提案した．

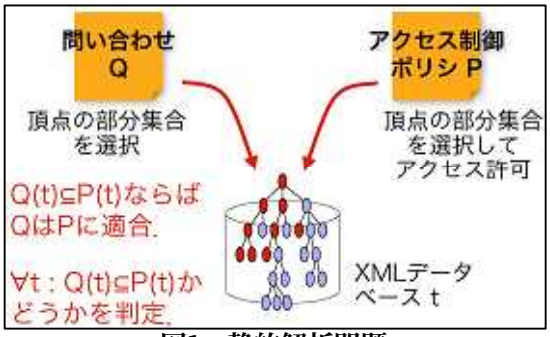

図1　静的解析問題

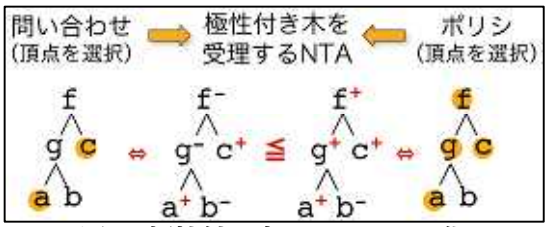

図2　極性付き木によるモデル化

(2) OR意味論の方がAND意味論より表現能力が高いことを示した．

(3) 静的解析の計算複雑さについて考察し，AND意味論では多項式時間で解析可能であるのに対しOR意味論では決定性指数時間完全であることを示した．また，OR意味論が等価なAND意味論のアクセス制御ポリシーを持つかどうか判定する問題も決定性指数時間完全であることを示した．

(4) オートマトン理論に基づくアクセス制御機構の解析に関連して，Abadiらが提案した履歴に基づくアクセス制御機構(HBAC)のモデル化について研究を行い，HBACプログラムの検証問題が一般には決定性指数時間完全であることを示した．また，検証法の計算量を低減するための最適化法を提案した（図3）．

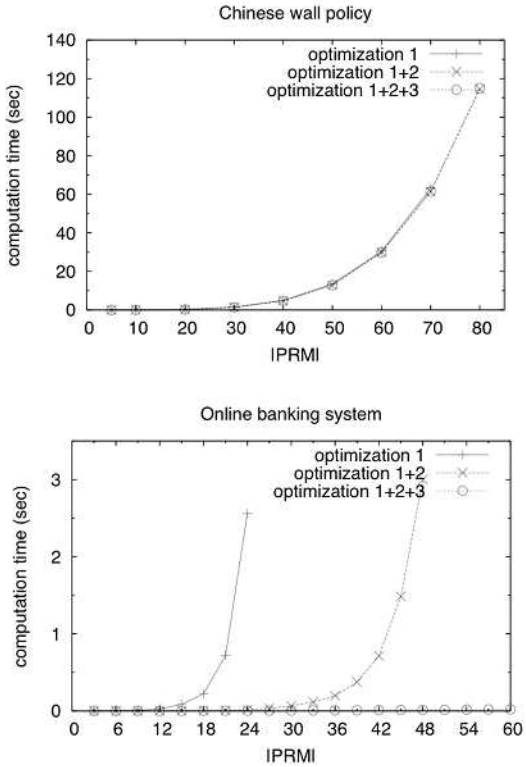

図3　最適化法の効果

(5) HBACと既存のアクセス制御モデルとの表現能力の比較を行った．その結果，HBAC，正規スタック検査，有限セキュリティオートマトンの表現能力は互いに比較不能であることを示すとともに，HBACに小さい拡張を行うことで正規スタック検査より真に表現能力が高くなることを示した（図4）．

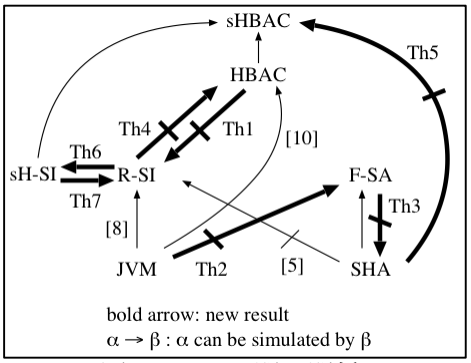

図 4　モデル間の関係

5．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　1　件）

(1) Yoshiaki Takata and Hiroyuki Seki. Comparison of the Expressive Power of Language-based Access Control Models, IEICE Transactions on Information and Systems, Vol.E92-D, 1033-1036, 2009

〔学会発表〕（計　2　件）

(1) 高田喜朗, モデル検査による HBAC プログラムの情報流解析, 日本ソフトウェア科学会第 5 回ディペンダブルシステムワークショップ, 2007 年 7 月 2 日, 函館.

(2) 高田喜朗, 情報流仕様からの言語組み込みアクセス制御文の自動挿入, 日本ソフトウェア科学会第 6 回ディペンダブルシステムワークショップ, 2008 年 7 月 4 日, 函館.

６．研究組織

(1)研究代表者

高田　喜朗（TAKATA YOSHIAKI）
高知工科大学・工学部・講師
研究者番号　60294279

(2)研究分担者

(3)連携研究者