論 文 内 容 の 要 旨

博士論文題目

Formal Models for XML Access Control and Aspect-Oriented Programs beyond Regular Languages

（XML アクセス制御とアスペクト指向プログラムに対する正規言語を超える表現能力をもった形式モデルの提案）

氏　名　八木 勲

（論文内容の要旨）

近年、情報技術の著しい発展に伴い、大規模な情報システムが構築されるようになった。このようなシステムは、高度な機能を持つ反面、動作が複雑になるため、システム開発者の予期しない振る舞いを行うことがある。この問題を解決する方法の１つとして、システムの形式モデル化がある。システムを簡潔な形式モデルで表すことで、複雑な動作を把握しやすくなり、システムの形式検証にも利用することができる。本論文では、XML データベースのアクセス制御、および、アスペクト指向プログラム（AOP）の実行制御の形式モデル化が試みられている。これらの技術は、研究者、開発者の双方から注目されている分野であるが、そのモデルは未だ確立されていない。本研究では、簡潔で、かつ、様々な性質が知られている形式言語理論に基づいて、これらの技術がモデル化されている。

第２章では、XML データベースのアクセス制御に対する形式モデルが提案され、アクセス制御の静的解析問題について考察されている。静的解析問題とは、アクセス制御ポリシ（以下、ポリシと呼ぶ）と問い合わせが与えられたとき、ポリシによってアクセスが禁止された要素または属性へのアクセスが発生しないかどうかを、問い合わせ実行前に調べることをいう。既存研究では、ポリシおよび問い合わせを木中のパスの正規集合でモデル化しているが、この方法では正確に表現できないポリシが存在する。本論文では、ポリシおよび問い合わせは木オートマトンでモデル化され、ポリシに２つの意味論（AND 意味論、OR 意味論）が与えられている。そして静的解析問題の時間計算量が、AND 意味論の下では 2 乗オーダであり、OR 意味論の下では決定性指数時間完全であることが示されている。また、提案された問い合わせモデルの表現能力が、Neven らの query automaton より真に大きいことが示されている。さらに、XML データベースのスキーマ

変換におけるポリシの整合性問題について議論されており、この問題が決定可能であることが示されている。

第3章では、ラベル付き遷移システムに基づいた、アスペクト指向プログラムのモデル A-LTS が提案されている。A-LTS は、既存モデルでは考慮されていないアドバイスの再帰性を特に考慮している。そして、A-LTS の表現能力が有限状態機械の表現能力より真に大きく、プッシュダウンオートマトン（PDA）の表現能力より真に小さいことが示されている。さらに、PDA（および、文脈自由文法）のサブクラスである、決定性 PDA と線形文法との表現能力の比較も行われている。最後に、よく知られた AOP 言語である AspectJ のポイントカットと A-LTS の関係が議論されており、それらが A-LTS によって表現可能であることが示されている。

氏　名	八木　勲

（論文審査結果の要旨）

形式言語理論は、プログラミング言語のコンパイラをはじめ情報科学の諸分野で応用されている重要な基礎理論の一つである。特に正規言語は有限状態遷移系と対応する言語クラスであり、また、集合演算（和、積、補集合）に関する閉包性、空集合判定問題などの重要な問題の判定可能性などの望ましい性質をもつため、従来からシステムのモデル化に広く用いられてきた。

近年の情報科学の発展に伴い、新しいプログラミングパラダイム、データ交換と蓄積のための汎用形式とそれらデータのセキュリティ保全などについて、有用な技術が提案されている。しかし、正規言語はこれらの新技術をモデル化するには表現能力が不足している。従って、正規言語のもつ望ましい性質を保存しつつ、現実のシステムをできる限り正確に表現できる形式モデルが望まれる。本論文では具体的に、XML アクセス制御とアスペクト指向プログラムの二つに着目し、前者については正規木言語（木オートマトン）、後者については複数の有限状態遷移系からなる並行系を用いてモデル化を行っている。

本論文前半では、構造化文書形式の暗黙的標準として広く利用されている XML データベースにおけるアクセス制御の静的解析問題、および関連するいくつかの問題を取り上げている。ここでの静的解析問題とは、アクセス制御ポリシと問合せが与えられたとき、問合せの実行中に、ポリシで禁止されたデータへのアクセスが起こらないかどうかを判定する問題である。静的解析の結果を利用して問合せ実行時の効率を向上することができる。本論文では木オートマトンによりポリシと問合せをモデル化することにより、村田らによる正規言語を用いた従来法と比較して、より精密な解析が行えることを示している。特にポリシの意味論として AND 意味論と OR 意味論の二つが提案され、これら二つの意味論について静的解析問題の計算量が精緻に考察されている。

本論文後半では、オブジェクト指向を補間するパラダイムとして提案されているアスペクト指向を取り上げ、アスペクト指向プログラム（AOP）の形式モデル化を試みている。具体的に AOP の要素である基プログラム、アドバイス、およびポイントカットのそれぞれを有限状態系として簡潔に定義し、系全体をこれら有限状態系からなる並行系（A-LTS と呼ぶ）として定義している。A-LTS は、既存の研究では考慮されていなかったアドバイスの再帰性を一般的に表現できるモデルとなっている。また、A-LTS の表現能力が正規言語より真に大きくプッシュダウンオートマトンより真に小さいこと等を示しており、言語理論的観点からも A-LTS は興味深いモデルである。

以上の通り、本論文で提案する手法と得られた結果は、形式言語理論に基づく形式的技法、とりわけ XML アクセス制御とアスペクト指向プログラムの静的解析技術に重要な知見を与えており、博士（工学）の学位論文として価値あるものと認める。