氏　名（本籍）	Pablo Lamilla Alvarez（スペイン）
学位の種類	博士（工学）
学位記番号	甲第２５６号
学位授与年月日	平成２６年３月２０日
学位授与の要件	学位規則第４条第１項
研究科・専攻名	工学研究科・基盤工学専攻
学位論文題目	Verification Model and Approximation-Based Implementation of Information-Based Access Control 情報ベースアクセス制御の検証用モデルと近似による実装
論文審査	（主査）高知工科大学　准教授　高田　喜朗 高知工科大学　教授　坂本　明雄 高知工科大学　准教授　松崎　公紀 高知工科大学　教授　岩田　誠 高知工科大学　教授　横山　和俊

審 査 結 果 の 要 旨

１.論文の評価

通信を介してソフトウェアを入手することが日常的になった現在，悪意のあるソフトウェアから実行端末上の情報や装置を守ることは重要な課題である．本論文は，Java 等のプログラム言語実行環境に組み込まれているアクセス制御機能の拡張として，Pistoia らによって近年提案された情報ベースアクセス制御(IBAC)に関して，モデル検査法による形式的検証に適したモデル化法を提案している．また，IBAC の前身である履歴ベースアクセス制御(HBAC)に近似的に変換することによる実装法を提案している．

IBAC は，信頼できないソフトウェア部品が，組み込みライブラリを介して重要な資源にアクセスすることをできるだけ過不足なく禁止することを目的とした機構である．しかし，アクセス制御実行文の配置や設定に誤りがあると，意図した通りの安全性が得られなくなってしまう．本研究は，そのような誤りがないか数理的な方法で厳密に検証する方法を提案するものであり， IBAC の数理的検証を初めて議論したものである．

IBAC は，関数呼び出し及び復帰を基準としてアクセス権を管理し，また変数内のデータのアクセス権を扱うという性質がある．その挙動を表現でき，かつモデル検査問題が決定可能となるような数理モデルを選択する必要があるが，本研究では拡張重み付きプッシュダウンシステム(extended weighted pushdown system; EWPDS)を採用することでこの課題を解決している．本論文では，この EWPDS によるモデル化の健全性を証明するとともに，モデル検査ツールの試作を行い，アクセス権の数が 20 程度の規模のプログラムであれば現実的な時間で検証可能であることを実験的に明らかにしている．

本論文の後半では，IBAC の近似的実装法を提案している．IBAC の公知の実装はまだないが，これを直接実装するのではなく，前身である HBAC への近似によって模倣実行するという独創的な方法を提案している．これは，IBAC の実装を新たに構築する必要をなくすという利点があるのと同時に，HBAC と IBAC の理論的な差を検討する第一歩という意義があり，今後の発展につながる研究と言える．

２.審査の経過と結果

（１）平成２６年１月１５日　博士後期課程委員会で学位論文の受理を決定し、5 名がその審査委員として指名された。

（２）平成２６年２月１２日　公開論文審査発表会及び最終試験を実施した。

（３）平成２６年２月１９日　博士後期課程委員会で学位授与を可とし、教育研究審議会で承認された。