論文内容の要旨

博士論文題目　Security Verification of Programs with Stack Inspection
(スタック検査機能を持つプログラムに対するセキュリティ検証)

氏名　新田 直也

論文内容の要旨

近年コンピュータネットワーク環境の急速な発展に伴い, 適切なアクセス制御法の確立が, ますます必要となってきている. Java development kit 1.2 は, プログラム実行時に制御スタックを検査することでアクセス制御を行うプログラム環境である. Jensen らは, このようなスタック検査機能を持つプログラム P および時相論理式を用いて記述された検証条件 ψ を与えたときに, P の到達可能な状態全てが ψ を満たすかどうかを決定する問題として検証問題を定義し, 相互再帰を含まないプログラムのクラスに対して検証問題が決定可能となることを示した.

本論文では, 時相論理式よりも真に表現能力の大きい正規言語を用いて検証問題を定義する. そして, プログラムの実行系列の集合がインデックス言語となることを示し, その系としてプログラムが相互再帰を含む場合も含めて検証問題が一般に決定可能となることを示す.

また検証問題の計算複雑さについて解析を行ない, 一般に検証問題が計算量的に手におえない問題のクラスに属することを示す.

現実的な計算時間で検証問題を解くには, 問題のクラスを制限する必要がある. そこで, Java development kit 1.2 のスタック検査機構をモデル化したプログラムからなる部分クラスを考え, そのクラスに対して検証問題をプログラムサイズの線形時間で解く効率のよい検証アルゴリズムを提案する. さらに, 同アルゴリズムを実装した検証システムについて実験を行ない, その結果を基に本検証法の実用性について議論する.

氏　名	新田　直也

（論文審査結果の要旨）

近年の計算機ネットワークの急速な発展に伴い，ネットワークからダウンロードしたJavaアプレットなどのプログラムを，ユーザの計算機上で実行するということが日常的に行なわれている．このような状況の下で，悪意あるプログラムからユーザ資源を保護するための動的アクセス制御法の一つとして，Java Development Kit 1.2 (JDK1.2)のcheckPermissionに代表されるスタック検査が注目されている．アクセス制御のため，あらかじめいくつかのアクセス権が用意され，各メソッドごとに，いくつかのアクセス権が割当てられる．プログラム実行時にメソッドが呼出されると，実行管理スタックに，呼出されたメソッドが用いるフレームという記憶域がプッシュされる．checkPermission(p) (p はアクセス権)が実行されると，現在のスタックの内容が走査され，スタック内のフレームに対応するメソッド，すなわち呼出し中のメソッドのすべてが，アクセス権 p をもつかどうかが検査される．もしこの条件が成り立てば実行は継続され，そうでければアクセス権違反により実行は中断される．プログラムの規模が大きくなるに従って，スタック検査文を適切な箇所に過不足なく配置するのは困難な作業となる．

そこで本論文では，スタック検査を含むプログラム P と検証条件 F が与えられたとき，「P の任意の実行状態において F が成り立つかどうか」を判定する検証問題について考察し，以下のような結果を得ている．

1. Jensenらが1999年に提案したモデルを拡張し，プログラムをフローグラフでモデル化し，検証条件を正規言語で記述することにより，検証問題を定義している．

2. プログラムのトレース集合がインデクス言語になることを証明し，その系として，検証問題が決定可能であることを示している．

3. 検証問題の計算量の下界について考察している．例えば，スタック検査文が決定性有限オートマトン，検証条件が決定性または非決定性有限オートマトンで与えられたとき，検証問題が決定性多項式指数時間完全になることを示している．

4. JDK1.2のcheckPermissionをモデル化したプログラムの部分クラスを定義し，そのクラスに対する検証を，プログラム記述長の多項式時間で行なうアルゴリズムを提案し，試作システムによる評価も行なっている．

この種の自動検証にはモデル検査法が用いられることが多いが，モデル検査法は原理的に有限状態遷移系にしか適用できない．本論文の第一の貢献は，形式言語理論の手法を用いることにより，単純なモデル検査法の適用が困難なプログラムのクラスに対して自動検証が可能であることを示した点にある．また，厳密な正当性の議論が難しいとされてきた動的アクセス制御法に対して，具体的な検証手法を示した点も評価に値する．

これらの結果は，ソフトウェアの検証法，特にセキュリティ安全性検証法に対して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．