審 査 の 結 果 の 要 旨

氏　　名　　前田　俊行

情報科学における基礎理論の一つである型理論を基にした実用的プログラミング言語（例えばJavaやC#など）が台頭してきている。厳密に型付けされた言語の長所の一つは、それらの言語で記述されたプログラムが、実行時に不正なメモリ操作やコード実行をしないということが、型検査によって保証できる点である。このような長所を基に、例えば、Java言語は、WEBアプリケーション、ビジネスアプリケーションなど幅広いアプリケーションで利用されている。

これら型理論の成果が未だに有効に応用されていないソフトウェアとしてオペレーティングシステム(OS)がある。従来の OS は C 言語やアセンブリ言語などの厳密に型付けされていない言語、もしくは全く型付けされていない言語で記述されてきた。このため、OS の安全性を保証・検証することは著しく困難であった。

本論文では、OS 記述の中で特に重要なメモリ管理機構およびスレッド管理機構を記述可能とするために、新しい型システムを提案し、それに基づいた型言語TALKを提案している。さらに、OSのプロトタイプ実装を通して本論文で提案している型システムおよび言語の有効性を立証している。本論文で保証される安全性は、メモリ安全性(プログラムが不正なメモリアクセスをしないこと)と制御フロー安全性(プログラムが不正にコードを実行しないこと)である。

本論文で提案している型システムでは、型理論分野に対して4つの新しい提案がある。1つは、新しい型として、可変長配列型(実行時まで長さが分からない配列)を導入している。これにより、メモリそのものを表現できるようになった。2つめは、整数変数の値を型システムで扱えるように整数制約型を導入している点である。これによりメモリをアクセスする時の範囲検査を型システム上で扱えるようになった。後の2つは、エイリアス型および配列の分割・結合操作である。OSではメモリ領域を動的に分割あるいは結合し、複数の型として扱う。これを扱えるように、エイリアス型を導入し、型システムによる明示的なエイリアス追跡機能を実現した。配列の分割・結合操作により配列領域の分割を型システムで表現できるようにした。

さらに、システムソフトウェア分野に対する貢献としては、従来不可能とされていたOS記述における静的メモリ安全性および制御フロー安全性検査を型理論に基づくアセンブリ言語で実現できることを示したことである。

このように型理論分野に対して新しい型システムを提案し、型言語TALKを設計実装し、さらに、システムソフトウェア分野に対しても型理論に基づく言語を用いてOSを記述することにより安全性検査が静的に行なえることを示し、当該分野に顕著なる貢献を行った。

よって本論文は博士（情報理工学）の学位請求論文として合格と認められる。