「実用化を目指した組込みシステム用ディペンダブル・オペレーティングシステム」
平成 18 年度採択研究代表者

平成 20 年度
実績報告

前田　俊行

東京大学　大学院情報理工学系研究科　助教

ディペンダブルシステムソフトウェア構築技術に関する研究

1. 研究実施の概要

計算機（携帯電話、PDA、PC 等)、そして計算機を相互に接続するネットワークは、既に広く一般に普及し、もはや生活に欠かすことのできない社会基盤となった。このため、これらの計算機上で動作するソフトウェアの安全性・信頼性を確保することが非常に重要な課題である、ということが既に広く認識されている。

しかしながら、計算機システムで最も基礎的で重要なソフトウェアであるシステムソフトウェア（オペレーティングシステムなど）は、依然として 30 年以上前に考案された C 言語や、アセンブリ言語等の安全でない言語を用いて構築されており、その安全性・信頼性には大きな疑いがあると言わざるを得ない。また現実に多くの問題、例えばシステムの異常停止、情報漏洩等の問題が発生している。

これに対し本研究では、近年目覚しい発展を遂げた静的プログラム解析技術（プログラムを数学的理論に基づいて解析することで、プログラムを実行することなく、その性質を知る技術)、特に型理論とモデル検査理論に基づいた、システムソフトウェアの構築・検証技術を実現することで、システムソフトウェアの高信頼化に寄与することを目指す。より具体的には、(1) システムソフトウェアを記述可能な型付きアセンブリ言語の設計・実装 (2) C 言語から型付きアセンブリ言語への変換器の設計・実装 (3) モデル検査技法に基づくシステムソフトウェアの解析、の 3 つについて研究を行う。

本年度は、前年度のまでの理論設計や試験実装にもとづき、本研究領域全体で設計・実装中のディペンダビリティ支援のための OS 機構（P-Bus・P-Component）の検査・検証を目標として、システムソフトウェアを記述可能な型付きアセンブリ言語のプロトタイプ実装や、C 言語から型付きアセンブリ言語への変換器のプロトタイプ実装、また C 言語プログラムを対象としたモデル検査器のプロトタイプ実装を進めた。また、実装を進める中で新たに生じた課題について、更なる理論設計の検討も行った。次年度は、本年度行ったプロトタイプ実装の完成度を上げて、P-Component の検査を行うことを目指す。また検証の結果を本研究領域内の他のチームにフィードバックしたり、検証手法の効果や限界を他のチームと共有したりすることにより、プログラム実行前の検証手法とプログラム実行

時の動的検査手法を効果的に組み合わせたディペンダビリティ支援のための新しい枠組みの検討を目指す。

2. 研究実施内容（文中にある参照番号は 4.(1)に対応する）

(1) システムソフトウェアを記述可能な型付きアセンブリ言語の設計・実装

本年度は前年度より引き続き、システムソフトウェアを記述可能な型付きアセンブリ言語の実装を進めた。具体的には、前年度までに行った、型付きアセンブリ言語を異なる CPU アーキテクチャへ移植することを容易とするための手法検討に基づき、本研究領域全体で設計・実装中であるディペンダビリティ支援のための OS 機構（P-Bus・P-Component）を記述することを目標としてプロトタイプ実装を行った。加えて、前年度までに行ったハードウェア割込みやマルチコア・SMP に対応した型付きアセンブリ言語の設計を更に進め、実際に簡単な試験実装も行った。

また、従来よりも柔軟なメモリ管理の記述を可能とするために、参照カウント方式のメモリ管理に対応した型付きアセンブリ言語の設計を行った。従来の型付きアセンブリ言語では、ガーベジコレクション等の外部のメモリ管理機構に依存するか、もしくはポインタ（メモリ参照）のエイリアス（複数のポインタが同一のアドレスを指すこと）に制限を課す必要があったため、参照カウント方式のようなメモリ管理機構を型付きアセンブリ言語で記述することは困難であった。これに対し、実際のメモリ中の（あるアドレスを指す）ポインタの数と、参照カウント値としてメモリ中に保存されている値との誤差を型システムで追跡することによって、参照カウント方式のメモリ管理を型付きアセンブリ言語で記述できることを示した。

また、副作用のない高階関数と副作用のある計算とを含むプログラムの正当性を検証するための型システムの一つであるホーア型理論に対して、従来の手法ではプログラム内で更新されるロケーションの数が静的に決まっている必要があり、ロケーション（メモリアドレス）の数が動的に変化する場合を扱うことができなかったのに対し、ロケーションの扱い方を変更し、配列などのように更新されるロケーションの数が動的に決まるデータ構造に対応できるように拡張した型システムの設計を行った。

(2) C 言語から型付きアセンブリ言語への変換器の設計・実装

本年度は、昨年度より引き続き C 言語から型付きアセンブリ言語への変換のための理論の設計と、実際に C 言語で記述されたシステムソフトウェアを変換するための変換器のプロトタイプ実装を行った。具体的には、P-Bus・P-Component の一部分を実際に型付きアセンブリ言語に変換可能なプロトタイプ実装を行った。ただし、GCC（システムソフトウェア開発で広く用いられている C 言語コンパイラ）のインラインアセンブリ機能等は実装されていないため、現状ではソースコードを修正する等の対応が必要である。

(3) モデル検査技法に基づくシステムソフトウェアの解析

本年度は、昨年度より引き続き C 言語で記述されたプログラムの安全性を検証するためのモデル検査理論の構築と、それに基づいたモデル検査器のプロトタイプ実装を進めた。具体的には、検査するプログラムの仕様を記述するための仕様記述言語を定義し、これを解釈してプログラム

中に注釈として挿入する仕様記述変換器と、挿入された検査条件が満たされているかを検査するモデル検査器のプロトタイプ実装を進めた。このプロトタイプ実装は未完成であるが、P-Bus・P-Component の一部分に対して、実際に簡単な検査を試行することができた。

また、C 言語のメモリ安全性を保証する手法の一つとして、依存型システムを導入して配列の境界検査などを行う手法があるが、この依存型の推論を、モデル検査器を用いて行なう方法を考案した。具体的には、与えられた C 言語プログラムに対してモデル検査を行い、配列の境界違反を生じうる実行パスを得て、このパスを解析してプログラム中の変数が満たすべき性質を依存型として抽出し、これを元のプログラムに型注釈として挿入する。また、この手法を既存のモデル検査器を用いて実装し実験を行った。

また、モデル検査器を並列化し、大規模計算機上で実行するための予備実験として既存のモデル検査器を改造して並列化し実際に大規模計算機上で動作を確認した。

3. 研究実施体制

(1)東京大学グループ

①研究分担グループ長:前田　俊行(東京大学、助教)

②研究項目

(1)システムソフトウェアを記述可能な型付きアセンブリ言語の設計・実装

(2)C 言語から型付きアセンブリ言語への変換器の設計・実装

(3)モデル検査技法に基づくシステムソフトウェアの解析

4. 研究成果の発表等

(1) 論文発表 (原著論文)

1. Toshiyuki Maeda and Akinori Yonezawa, “Writing an OS Kernel in a Strictly and Statically Typed Language”, Lecture Notes in Computer Science 5458, pp. 181-197, 2009. In press.

(2) 特許出願

平成 20 年度 国内特許出願件数：0 件 (CREST 研究期間累積件数：0 件)