

平成30年度 情報工学コース卒業研究報告要旨

高田 研究室	氏 名	山 内 克 哉
卒業研究題目	mruby on EV3RT+TECS の VM のメモリ保護の実現	
<p>近年、情報社会が進むにつれて組込みシステムが広く使用されるようになってきた。組込みシステムとはある機能を実現するために機器に組み込まれるコンピュータシステムのことである。情報社会の発展に向けて、製造業のデジタル化・コンピュータ化を目指す Industry 4.0 が 2011 年にドイツで発表され、日本でも IoT や AI を活用した問題解決をコンセプトとした Society 5.0 が提唱された。こうしたシステムを使用した製品の普及により競争が激化し、競争力を保つためにシステムの要求が増大している。その結果システム自体には高い性能が求められるようになり、システムの複雑化が発生している。組込みシステムに適したコンポーネントシステムである TECS では、ソフトウェアの部品化や組込み向けスクリプト言語の mruby を利用することで複雑化に対応し、これらの実行方法としてプログラムを動作させるための仮想マシン (VM) も使用されるようになってきた。</p> <p>システムが普及するにつれて大切になってくるのが、信頼性の保証である。これらのシステムを実行する環境は、利用者によってさまざまである。どの環境でも安全に使用することができ、製品が正常に動作することを保証しなければならない。さらに多種多様なデータをあつかうシステムでは、情報の流出や漏洩があってはならない。そのため高い信頼性を保つには、VM も含めて部品化した環境でのシステムの保護をする必要がある。</p> <p>そこで本研究では、mruby の VM からのアクセスをメモリ保護機能によって制限する手法について検討する。システム全体を管理するホスト側に対して、VM は利用者を想定してユーザ側から動かすものとする。指定したユーザから実行可能な機能の定義、および他のユーザからのアクセスを拒否する設計をすることで、信頼性を満たすシステムを実現する。</p> <p>本論文ではまず、研究を進めるうえで必要となる TECS について紹介している。本研究では TECS の技術であるコンポーネント記述とリージョン記述を利用して VM のメモリ保護の環境を整えている。コンポーネント記述ではインスタンス化されたコンポーネントであるセルの属性とセル間の結合を記述し、リージョン記述ではセルの保護境界を定義してアクセス制御を行う。以上の記述を用いて、VM の保護を実現するための設計方法や手順について述べている。設計ではタスクやメモリ領域の配置を決定し、VM を配置する領域に対して許可されたすべての API を呼び出せるような環境を作成する。そして動作確認としてサンプルプログラムを実行することで、設計したセル配置で動作が正常にできるかの確認を行う。ここまでの設計は VM が一つだけの場合に限定して実装したため、VM の数を増やして異なる保護環境から実行することで、正しくメモリ保護ができているのかも確認する。最後に今回の設計を見直し、保護機能についての考察を行っている。</p> <p>本研究では、設計を加えることで指定したユーザからすべての API が実行できるという最低限の目標は達成した。複数の VM で実行した結果、異なる保護環境で定義されるタスクとメモリ領域ではタスクのアクセスができず、不正なアクセスを拒否する機能も確認した。以上の結果から、本研究の目的であるシステムの信頼性・安全性の保障は満たしていると考えられる。しかし VM からのアクセスを制限するという最低限の機能は実現できたとはいえ、システムとしての精度や性能を上げるための課題も依然として多く残されている。例として、VM 間の共有メモリの動作方法や複数の VM でのタスク切り替えなどがあげられる。これらの課題についても今後の設計の参考となるように、一つずつ取り上げて実装方法を提案した。</p>		