概要

近年あらゆるものがデジタル化されている。さらに技術革新が加速し、AIやIoTなどの新しい技術が登場しシステムの重要性はますます高まっている。こうした中で継続的にシステムがアップデートを繰り返しながら進化していく為、システムが安全に稼働する事はとても重要である。その為の一つの手法としてモデル検査がある。このモデル検査を正しく扱えるように本課題研究報告書では、いくつかの事例を用いて形式仕様の作成とモデル検査についてまとめる。すでに知られている事例を題材にするが、あえて誤りを注入したものを取り扱い理解を深めた。調査研究を進める中で遭遇した課題（状態爆発)、現象（状態が無限に作り出される現象）についても報告書でまとめ、対策を施しながらまとめている。

本課題研究報告書は7章から構成される。第1章では本課題研究報告書の背景、目的を述べて続く章の構成に関してまとめている。第2章では状態機械を定義して不可分な命令であるtest&setを利用した相互排除プロトコルを用いてどのように状態を表現するかについて述べ、Maudeでの記述方法、Searchコマンドによるモデル検査方法についてまとめた。第3章では不可分な待ち行列を利用した相互排除プロトコルであるQLockを用いて形式仕様の作成、Maudeでの記述、モデル検査についてまとめた。Qlockでは相互排除性を満たさないQlockを扱いながら違いについてもまとめた。第4章では敵味方を識別する為のプロトコルであるIdentity-Friend-or-Foe認証プロトコル (IFF) を用いて形式仕様の作成、Maudeでの記述、モデル検査についてまとめた。ここでは本学の大容量メモリ計算機であるLarge Memory PC Cluster (LMPCC) を活用したモデル検査の実施や状態爆発の課題に直面しながら改善した内容をまとめている。第5章と6章では公開鍵暗号を用いた相互認証プロトコルのNeedham-Schroeder公開鍵認証プロトコル (NSPK)、NSPKの改良版であるNeedham‐Schroeder‐Lowe公開鍵認証プロトコル (NSLPK) を用いて前の章で得られた知見をもとに形式仕様の作成、Maudeでの記述、モデル検査についてまとめた。第7章では課題研究報告書を通して得られた知見をまとめると共に近い将来直面する課題と対策を考察し、言及する。