社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

GearsOS の Hoare triple をベースにした検証手法

外間　政尊†　　河野　真治††

† 琉球大学大学院理工学研究科情報工学専攻
†† 琉球大学工学部情報工学科
E-mail: †{,}@cr.ie.u-ryukyu.ac.jp

あらまし　あらまし
キーワード　プログラミング言語, 検証

Masataka HOKAMA† and Shinji KONO††

† Interdisciplinary Information Engineering, Graduate Sc k533 hool of Engineering and Science, University of the Ryukyus.
†† Information Engineering, University of the Ryukyus.
E-mail: †{,}@cr.ie.u-ryukyu.ac.jp

1. ま え が き

Gears OS は継続を主とするプログラミング言語 CbC で記述されている。OS やアプリケーションの信頼性を上げるには仕様を満たしていることを確認する必要がある。現在 GearsOS の仕様の確認には定理証明系である Agda を用いている。CbC では関数呼び出しを用いず goto 文により遷移する。これは Agda 上では継続渡しの記述を用いた関数として記述する。また、継続にはある関数を実行するための事前条件や事後条件などをもたせることが可能である。Hoare triple では事前条件が成り立っているときにある関数を実行して、それが停止する際に事後条件を満たすことを確認する。これは継続を用いた Agda 上では事前条件を継続で関数に渡し、関数からさらに継続した先で事後条件が成り立つという形で記述できる。本発表では GearsOS の仕様確認に Hoare triple をベースとした証明を導入し、今まで行っていた証明との比較を行う。

2. GearsOS

GearsOS について

3. CodeGear と DataGear

CodeGear と DataGear について

4. Agda と GearsOS

Agda と GearsOS

文　　献

[1] 外間政尊, 河野真治, GearsOS の Agda による記述と検証, システムソフトウェアとオペレーティング・システム研究会, 2018.