修士 (工学) 学位論文
Master's Thesis of Engineering

GearsOS のメタ計算

2021 年 3 月
March 2021

清水 隆博
Takahiro Shimizu

琉球大学
大学院理工学研究科
情報工学専攻

Information Engineering Course
Graduate School of Engineering and Science
University of the Ryukyus

指導教員：教授 和田 知久
Supervisor: Prof. Tomohisa Wada

本論文は、修士 (工学) の学位論文として適切であると認める。

論　文　審　査　会

印

(主　査)　　和田 知久

印

(副　査)　　山田 孝治

印

(副　査)　　當間 愛晃

印

(副　査)　　河野 真治

要旨

アプリケーションの信頼性を保証するには、土台となる OS の信頼性は高く保証されていなければならない。信頼性を保証する方法としてテストコードを使う手法が広く使われている。OS のソースコードは巨大であり、並列処理など実際に動かさないと発見できないバグが存在する。OS の機能をテストですべて検証するのは不可能である。

テストに頼らず定理証明やモデル検査などの形式手法を使用して、OS の信頼性を保証したい。証明を利用して信頼性を保証する定理証明は、 Agda や Coq などの定理証明支援系を利用することになる。支援系を利用する場合、各支援系で OS を実装しなければならない。証明そのものは可能であるが、 支援系で証明されたソースコードがそのまま OS として動作する訳ではない。証明されたコードと、実際に動作する OS を記述する C 言語などのプログラミング言語の間にはギャップが存在し、 C での実装時に入ってしまうバグを取り除くことはできない。このためには定理証明されたコードを等価な C 言語などに変換する処理系が必要となる。

信頼性を保証するほかの方法として、プログラムの可能な実行をすべて数え上げて仕様を満たしているかを確認するモデル検査がある。モデル検査は実際に動作しているプログラムに対して実行することが可能である。

Abstract

hogefuga

研究関連業績

- Takahiro SHIMIZU. How to build traditional Perl interpreters. PerlCon2019 , Aug, 2019
- 継続を基本としたOS Gears OS 清水 隆博, 河野真治 第61回プログラミング・シンポジウム, Jan, 2020
- Perl6のサーバを使った実行 福田 光希, 清水 隆博, 河野真治 第61回プログラミング・シンポジウム, Jan, 2020
- xv6の構成要素の継続の分析 清水 隆博, 河野 真治 (琉球大学), 情報処理学会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 (OS), May, 2020

目 次

図 目 次

表 目 次

ソースコード目次

第1章　OSとアプリケーションの信頼性

コンピューター上では様々なアプリケーションが常時動作している。動作しているアプリケーションは信頼性が保証されていてほしい。信頼性の保証には、 実行してほしい一連の挙動をまとめた仕様と、 それを満たしているかどうかの確認である検証が必要となる。アプリケーション開発では検証に関数や一連の動作をテストを行う方法や、デバッグを通して信頼性を保証する手法が広く使われている。

実際にアプリケーションを動作させる OS は、アプリケーションよりさらに高い信頼性が保証される必要がある。OS は CPU やメモリなどの資源管理と、 ユーザーにシステムコールなどの API を提供することで抽象化を行っている。OS の信頼性の保証もテストコードを用いて証明することも可能ではあるが、 アプリケーションと比較すると OS のコード量、 処理の量は膨大である。また OS は CPU 制御やメモリ制御、 並列・並行処理などを多用する。テストコードを用いて処理を検証する場合、テストコードとして特定の状況を作成する必要がある。実際に OS が動作する中でバグやエラーを発生する条件を、並列処理の状況などを踏まえてテストコードで表現するのは困難である。非決定的な処理を持つ OS の信頼性を保証するには、 テストコード以外の手法を用いる必要がある。

テストコード以外の方法として、 形式手法的と呼ばれるアプローチがある。形式手法の具体的な検証方法の中で、 証明を用いる方法 [1][2][3] とモデル検査を用いる方法がある。証明を用いる方法では Agda[4] や Coq[5] などの定理証明支援系を利用し、 数式的にアルゴリズムを記述する。Curry-Howard 同型対応則により、型と論理式の命題が対応する。この型を導出するプログラムと実際の証明が対応する。証明には特定の型を入力として受け取り、証明したい型を生成する関数を作成する。整合性の確認は、記述した関数を元に定理証明支援系が検証する。証明を使う手法の場合、 実際の証明を行うのは定理証明支援系であるため、 定理証明支援系が理解できるプログラムで実装する必要がある。Agda や Coq の場合は Agda、 Cow 自身のプログラムで記述する必要がある。しかし Agda で証明ができても Agda のコードを直接 OS のソースコードとしてコンパイルすることはできない。Agda 側で C のソースコードを吐き出せれば可能ではあるが、 現状は検証したコードと実際に動作するコードは分離されている。検証されたアルゴリズムをもとに C で実装することは可能であるが、 この場合移植時にバグが入る可能性がある。検証ができているソースコードそのものを使って OS を動作させたい。

他の形式手法にモデル検査がある。モデル検査はプログラムの可能な実行をすべて数

え上げて要求している使用を満たしているかどうかを調べる手法である。例えば Java のソースコードに対してモデル検査をする JavaPathFinder などがある。モデル検査を利用する場合は、実際に動作するコード上で検証を行うことが出来る。OS のソースコードそのものをモデル検査すると、実際に検証された OS が動作可能となる。しかし OS の処理は膨大である。すべての存在可能な状態を数え上げるモデル検査では状態爆発が問題となる。状態を有限に制限したり抽象化を行う必要がある。

OS のシステムコールは、ユーザーから API 経由で呼び出され、 いくつかの処理を行う。その処理に着目すると OS は様々な状態を遷移して処理を行っていると考えることができる。OS を巨大な状態遷移マシンと考えると、 OS の処理の特定の状態の遷移まで範囲を絞ることができる。範囲が限られているため、有限時間でモデル検査などで検証することが可能である。この為には OS の処理を証明しやすくする表現で実装する必要がある。[6] 証明しやすい表現の例として、 状態遷移ベースでの実装がある。

証明を行う対象の計算は、 その意味が大きく別けられる。OS やプログラムの動作においては本来したい計算がまず存在する。これはプログラマが通常プログラミングするものである。これら本来行いたい処理のほかに、 CPU、メモリ、スレッドなどの資源管理なども必要となる。前者の計算をノーマルレベルの計算と呼び、後者をメタレベルの計算と呼ぶ。OS はメタ計算を担当していると言える。ユーザーレベルから見ると、データの読み込みなどは資源へのアクセスが必要であるため、システムコールを呼ぶ必要がある。システムコールを呼び出すと OS が管理する資源に対して何らかの副作用が発生するメタ計算と言える。副作用は関数型プログラムの見方からするとモナドと言え、 モナドもメタ計算ととらえることができる。OS 上で動くプログラムは CPU により並行実行される。この際の他のプロセスとの干渉もメタレベルの処理である。実装のソースコードはノーマルレベルであり検証用のソースコードはメタ計算だと考えると、OS そのものが検証を行ない、システム全体の信頼を高める機能を持つべきだと考える。ノーマルレベルの計算を確実に行う為には、メタレベルの計算が重要となる。

プログラムの整合性の検証はメタレベルの計算で行いたい。ユーザーが実装したノーマルレベルの計算に対応するメタレベルの計算を、自由にメタレベルの計算で証明したい。またメタレベルで検証ががすでにされたプログラムがあった場合、都度実行ユーザーの環境で検証が行われるとパフォーマンスに問題が発生する。この場合はメタレベルの計算を検証をするもの、しないものと切り替えられる柔軟な API が必要となる。メタレベルの計算をノーマルレベルの計算と同等にプログラミングできると、動作するコードに対して様々なアプローチが掛けられる。この為にはノーマルレベル、メタレベル共にプログラミングできる言語と環境が必要となる。

プログラムのノーマルレベルの計算とメタレベルの計算を一貫して行う言語として、Continuation Based C(CbC) を用いる。CbC は基本 `goto` 文で `CodeGaar` というコードの単位を遷移する言語である。通常の関数呼び出しと異なり、スタックあるいは環境と呼ば

れる隠れた状態を持たない。このため、計算のための情報は CodeGear の入力にすべてそろっている。そのうちのいくつかはメタ計算、つまり、OS が管理する資源であり、その他はアプリケーションを実行するためのデータ (DataGear) である。メタ計算とノーマルレベルの区別は入力のどこを扱うかの差に帰着される。CbC は C と互換性のある C の下位言語である。CbC は GCC[7][8] あるいは LLVM[9][10] 上で実装されていて、通常の C のアプリケーションやシステムプログラムをそのまま包含できる。C のコンパイルシステムを使える為に、 CbC のプログラムをコンパイルすることで動作可能なバイナリに変換が可能である。また CbC の基本文法は簡潔であるため、 Agda などの定理証明支援系 [11] との相互変換や、 CbC 自体でのモデル検査が可能であると考えられる。

第2章　Continuation Based C

Continuation Based C(CbC) とは C 言語の下位言語であり、 関数呼び出しではなく継続を導入したプログラミング言語である。CbC では通常の関数呼び出しの他に、 関数呼び出し時のスタックの操作を行わず、次のコードブロックに `jmp` 命令で移動する継続が導入されている。この継続は Scheme の call/cc などの環境を持つ継続とは異なり、 スタックを持たず環境を保存しない継続である為に軽量である事から軽量継続と呼べる。また CbC ではこの軽量継続を用いて `for` 文などのループの代わりに再起呼び出しを行う。これは関数型プログラミングでの Tail call スタイルでプログラミングすることに相当する。Agda よる関数型の CbC の記述も用意されている。実際の OS やアプリケーションを記述する場合には、GCC 及び LLVM/clang 上の CbC 実装を用いる。

2.1　CodeGear

CbC では関数の代わりに CodeGear という単位でプログラミングを行う。CodeGear は通常の C の関数宣言の返り値の型の代わりに `__code` で宣言を行う。各 CodeGear は DataGear と呼ばれるデータの単位で入力を受け取り、 その結果を別の DataGear に書き込む。入力の DataGear を InputDataGear と呼び、 出力の DataGear を OutputDataGear と呼ぶ。CodeGear がアクセスできる DataGear は、 InputDataGear と OutputDataGear に限定される。

CodeGear は関数呼び出し時のスタックを持たない為、一度ある CodeGear に遷移してしまうと元の処理に戻ってくることができない。しかし CodeGear を呼び出す直前のスタックは保存される。部分的に CbC を適用する場合は CodeGear を呼び出す `void` 型などの関数を経由することで呼び出しが可能となる。

この他に CbC から C へ復帰する為の API として、 環境付き goto という機能がある。これは呼び出し元の関数を次の CodeGear の継続対象として設定するものである。これは GCC では内部コードを生成を行う。LLVM/clang では `setjmp` と `longjmp` を使い実装している。したがってプログラマから見ると、通常の C の関数呼び出しの返り値を CodeGear から取得する事が可能となる。

2.2 DataGear と MetaDataGear

DataGear は CbC でのデータの単位である。基本は C 言語の構造体そのものであるが、DataGear の場合はデータに付随するメタ情報も取り扱う。これはデータ自身がどういう型を持っているかなどの情報である。ほかに計算を実行する CPU、 GPU の情報や、 計算に必要なすべての DataGear の管理などの実行環境のメタデータも DataGear の形で表現される。このメタデータを扱う DataGear を MetaDataGear と呼ぶ。

2.3 CbC を使ったシステムコールディスパッチの例題

CbC を用いて MIT が開発した教育用の OS である xv6[12] の書き換えを行った。CbC を利用したシステムコールのディスパッチ部分をソースコード 2.1 に示す。この例題では特定のシステムコールの場合、 CbC で実装された処理に `goto` 文をつかって継続する。例題では CodeGear へのアドレスが配列 `cbccodes` に格納されている。引数として渡している `cbc_ret` は、 システムコールの返り値の数値をレジスタに代入する CodeGear である。実際に `cbc_ret` に継続が行われるのは、 `read` などのシステムコールの一連の処理の継続が終わったタイミングである。

ソースコード 2.1: CbC を利用したシステムコールのディスパッチ

```
1 void syscall(void)
2 {
3     int num;
4     int ret;
5
6     if((num >= NELEM(syscalls)) && (num <= NELEM(cbccodes)) && cbccodes[
    num]) {
7         proc->cbc_arg.cbc_console_arg.num = num;
8         goto (cbccodes[num])(cbc_ret);
9     }
```

軽量継続を持つ CbC を利用して、 証明可能な OS を実装したい。その為には証明に使用される定理証明支援系や、モデル検査機での表現に適した状態遷移単位での記述が求められる。CbC で使用する CodeGear は、 状態遷移モデルにおける状態そのものとして捉えることが可能である。CodeGear を元にプログラミングをするにつれて、 CodeGear の入出力の Data も重要であることが解ってきた。CodeGear とその入出力である DataGear を基本とした OS として、 GearsOS の設計を行っている。[13] 現在の GearsOS は並列フレームワークとして実装されており、 実用的な OS のプロトタイプ実装として既存の OS 上への実装を目指している。

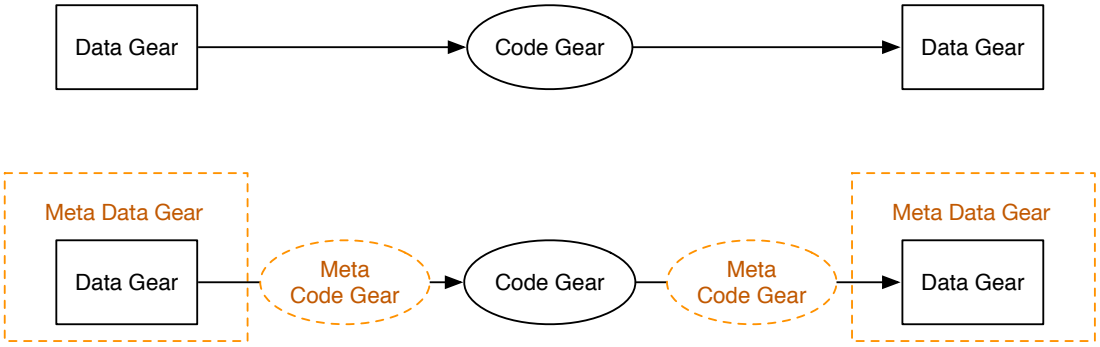

図 2.1: CodeGear と MetaCodeGear

2.4 メタ計算

プログラミング言語からメタ計算を取り扱う場合、 言語の特性に応じて様々な手法が使われてきた。関数型プログラミングの見方では、 メタ計算はモナドの形で表現されていた。[14] OS の研究ではメタ計算の記述に型付きアセンブラを用いることもある。[15]

CbC でのメタ計算は CodeGear、 DataGear の単位がそのまま使用できる。メタ計算で使われるこれらの単位はそれぞれ、 MetaCodeGear、 MetaDataGear と呼ばれる。

2.5 MetaCodeGear

GearsOS では、CodeGear と DataGear を元にプログラミングを行う。遷移する各 CodeGear の実行に必要なデータの整合性の確認などのメタ計算は、 MetaCodeGear と呼ばれる各 CodeGear ごと実装された CodeGear で計算を行う。この MetaCodeGear の中で参照される DataGear を MetaDataGear と呼ぶ。また、 対象の CodeGear の直前で実行される MetaCodeGear を StubCodeGear と呼ぶ。MetaCodeGear や MetaDataGear は、プログラマが直接実装することはなく、 現在は Perl スクリプトによって GearsOS のビルド時に生成される。CodeGear から別の CodeGear に遷移する際の DataGear などの関係性を、図 2.1 に示す。

通常のコード中では入力の DataGear を受け取り CodeGear を実行、 結果を DataGear に書き込んだ上で別の CodeGear に継続する様に見える。この流れを図 2.1 の上段に示す。しかし実際は CodeGear の実行の前後に実行される MetaCodeGear や入出力の DataGear を MetaDataGear から取り出すなどのメタ計算が加わる。これは図 2.1 の下段に対応する。

2.6 MetaDataGear

第3章　GearsOS

GearsOS とは Continuation Based C を用いて実装している OS プロジェクトである。CodeGear と DataGear を基本単位として実行する。GearsOS は OS として実行する側面と、 CbC のシンタックスを拡張した言語フレームワークとしての側面がある。

3.1　GearsOSのビルドシステム

GearsOS ではビルドツールに CMake を利用している。ビルドフローを図 3.1 に示す。CMake は automake などの Make ファイルを作成するツールに相当するものである。GearsOS でプログラミングする際は、ビルドしたいプロジェクトを CMakeLists.txt に記述する。CMake は自身がコンパイルをすることはなく、ビルドツールである make や ninja-build に処理を移譲している。CMake は make や ninja-build が実行可能な Makefile、 build.ninja の生成までを担当する。

GearsOS のビルドでは直接 CbC コンパイラがソースコードをコンパイルすることはなく、 間に Perl スクリプトが 2 種類実行される。Perl スクリプトはビルド対象の GearsOS で拡張された CbC ファイルを、純粋な CbC ファイルに変換する。ほかに GearsOS で動作する例題ごとに必要な初期化関数なども生成する。Perl スクリプトで変換された CbC ファイルなどをもとに CbC コンパイラがコンパイルを行う。ビルドの処理は自動化されており、 CMake 経由で make や ninja コマンドを用いてビルドする。

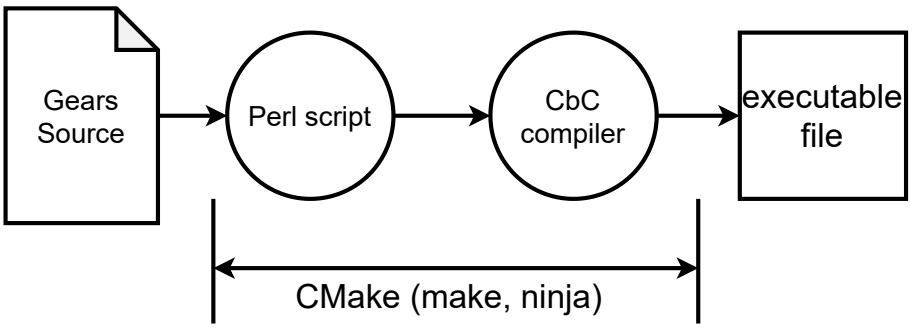

図 3.1: GearsOS のビルドフロー

3.2　pmake

GearsOS をビルドする場合は、x86 アーキテクチャのマシンからビルドするのが殆どである。この場合ビルドしたバイナリは x86 向けのバイナリとなる。これはビルドをするホストマシンに導入されている CbC コンパイラが x86 アーキテクチャ向けにビルドされたものである為である。

CbC コンパイラは GCC と llvm/clang 上に構築した 2 種類が主力な処理系である。LVM/-clang の場合は LLVM 側でターゲットアーキテクチャを選択することが可能である。GCC の場合は最初から j ターゲットアーキテクチャを指定してコンパイラをビルドする必要がある。

時にマシンスペックの問題などから、別のアーキテクチャ向けのバイナリを生成したいケースがある。教育用マイコンボードである Raspberry Pi[16] は ARM アーキテクチャが搭載されている。Raspberry Pi 上で GearsOS のビルドをする場合、ARM 用にビルドされた CbC コンパイラが必要となる。Raspberry Pi 自体は非力なマシンであるため、GearsOS のビルドはもとより CbC コンパイラの構築を Raspberry Pi 上でするのは困難である。マシンスペックが高めの x86 マシンから ARM 用のバイナリをビルドして、 Raspberry Pi に転送し実行したい。ホストマシンのアーキテクチャ以外のアーキテクチャ向けにコンパイルすることをクロスコンパイルと呼ぶ。

GearsOS はビルドツールに CMake を利用しているので、 CMake でクロスコンパイル出来るように工夫をする必要がある。ビルドに使用するコンパイラやリンカは CMake が自動探索し、決定した上で Makefile や build.ninja ファイルを生成する。しかし CMake は今ビルドしようとしている対象が、自分が動作しているアーキテクチャかそうでないか、クロスコンパイラとして使えるかなどはチェックしない。つまり CMake が自動でクロスコンパイル対応の GCC コンパイラを探すことはない。その為そのままビルドすると x86 用のバイナリが生成されてしまう。

CMake を利用してクロスコンパイルする場合、CMake の実行時に引数でクロスコンパイラを明示的に指定する必要がある。この場合 x86 のマシンから ARM のバイナリを出力する必要があり、 コンパイラやリンカーなどを ARM のクロスコンパイル対応のものに指定する必要がある。また、 xv6 の場合はリンク時に特定のリンカスクリプトを使う必要がある。これらのリンカスクリプトも CMake 側に、 CMake が提供しているリンカ用の特殊変数を使って自分で組み立てて渡す必要がある。このような CMake の処理を手打ちで行うことは難しいので、 `pmake.pl` を作成した。`pmake.pl` の処理の概要を図 3.2 に示す。`pmake.pl` は Perl スクリプトで、 シェルコマンドを内部で実行しクロスコンパイル用のオプションを組み立てる。`pmake.pl` を経由して CMake を実行すると、 make コマンドに対応する Makefile、 ninja-build に対応する build.ninja が生成される。以降は cmake ではなく make などのビルドツールがビルドを行う。

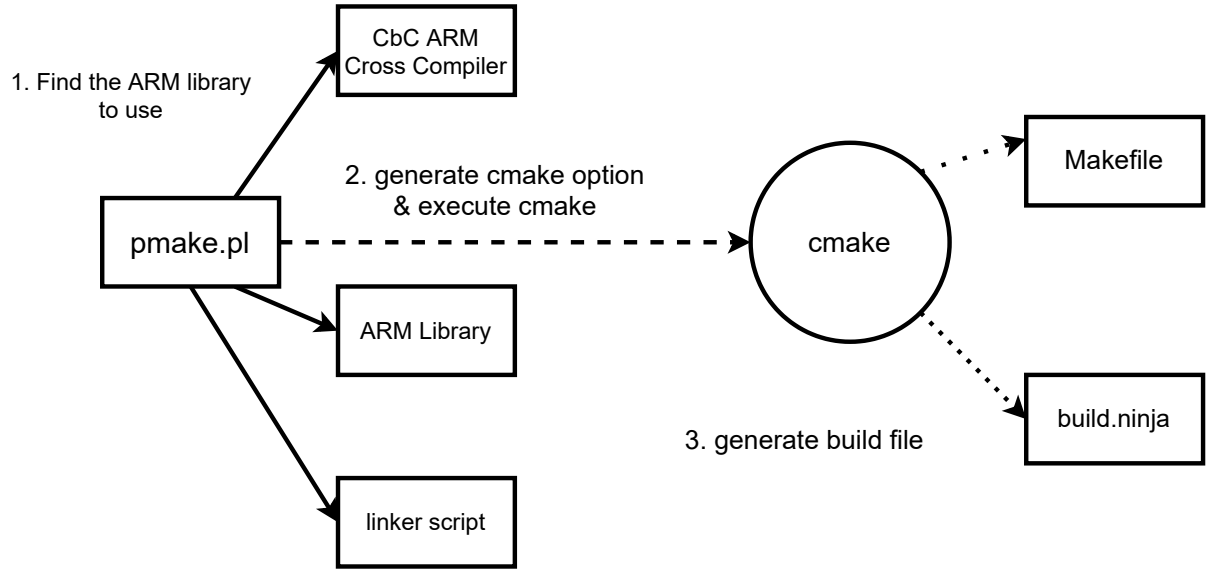

図 3.2: pmake.pl の処理フロー

3.3　Interface の取り扱い方法の検討

GearsOS の Interface はモジュール化の仕組みと goto 文での引数の一時保管場所としての機能を持っている。Interface の Implement のヘッダーファイルを実装したことで、GearsOS 上で Interface を実装する際に新たな方法での実装を検討した。Implement の CodeGear は今までは Interface で定義した CodeGear と 1 対 1 対応していた。Implement の CodeGear から goto する先は、入力として与えられた CodeGear か、Implement 内で独自に定義した CodeGear に goto するケースとなっていた。後者の独自に定義した CodeGear に goto するケースも、 実装の CbC ファイルの中に記述されている CodeGear に遷移していた。

GearsOS を用いて xv6 OS を再実装した際に、 実装側の CodeGear を細かく別けて記述した。細分化によって 1 つの CbC ファイルあたりの CodeGear の記述量が増えてしまうという問題が発生した。見通しをよくする為に、 Interface で定義した CodeGear と直接対応する CodeGear の実装と、 それらから goto する CodeGear で実装ファイルを分離することを試みた。

第4章　トランスコンパイラによるメタ計算

GearsOS は CbC で実装を行う。CbC は C 言語よりアセンブラに近い言語であるため、すべてを純粋な CbC で記述しようとすると記述量が膨大になってしまう。またノーマルレベルの計算とメタレベルの計算を、全てプログラマが記述する必要が発生してしまう。メタ計算では値の取り出しなどを行うが、 これはノーマルレベルの CodeGear の API が決まれば一意に決定される。したがってノーマルレベルのみ記述すれば、 機械的にメタ部分の処理は概ね生成可能となる。また、メタレベルのみ切り替えたいなどの状況が存在する。ノーマルレベル、メタレベル共に同じコードの場合は記述の変更量が膨大であるが、メタレベルの作成を分離するとこの問題は解消される。

GearsOS ではメタレベルの処理の作成に Perl スクリプトを用いており、ノーマルレベルで記述された CbC から、メタ部分を含む CbC へと変換する。変換前の CbC を GearsCbC と呼ぶ。

4.1　トランスコンパイラ

プログラミング言語から実行可能ファイルやアセンブラを生成する処理系のことを、一般的にコンパイラと呼ぶ。特定のプログラミング言語から別のプログラミング言語に変換するコンパイラのことを、 トランスコンパイラと呼ぶ。トランスコンパイラとしては JavaScript を古い規格の JavaScript に変換する Babel[17] がある。

またトランスコンパイラは、変換先の言語を拡張した言語の実装としても使われる。JavaScript に強い型制約をつけた拡張言語である TypeScript は、 TypeScript から純粋な JavaScript に変換を行うトランスコンパイラである。すべての TypeScript のコードは JavaScript にコンパイル可能である。JavaScript に静的型の機能を取り込みたい場合に使われる言語であり、 JavaScript の上位の言語と言える。

GearsOS は CbC を拡張した言語となっている。ただしこの拡張自体は CbC コンパイラである gcc、 llvm/clang には搭載されていない。その為 GearsOS の拡張部分を、等価な純粋な CbC の記述に変換する必要がある。現在の GearsOS では、 CMake によるコン

パイル時に Perl で記述された generate_stub.pl と generate_context.pl の 2 種類のスクリプトで変換される。

- generate_stub.pl
  - 各 CbC ファイルごとに呼び出されるスクリプト
  - 対応するメタ計算を導入した CbC ファイル (拡張子は c) に変換する
    - 図 4.1 に処理の概要を示す
- generate_context.pl
  - 生成した CbC ファイルを解析し、使われている CodeGear を確定する
  - context.h を読み込み、使われている DataGear を確定する
  - Context 関係の初期化ルーチンや CodeGear、 DataGear の番号である enum を生成する
    - 図 4.2 に処理の概要を示す

これらの Perl スクリプトはプログラマが自分で動かすことはない。Perl スクリプトの実行手順は CMakeLists.txt に記述しており、 make や ninja-build でのビルド時に呼び出される。(ソースコード 4.1)

ソースコード 4.1: CMakeList.txt 内での Perl の実行部分

```
1  macro( GearsCommand )
2      set( _OPTIONS_ARGS )
3      set( _ONE_VALUE_ARGS TARGET )
4      set( _MULTI_VALUE_ARGS SOURCES )
5      cmake_parse_arguments( _Gears "${_OPTIONS_ARGS}" "${_ONE_VALUE_ARGS}"
       "${_MULTI_VALUE_ARGS}" ${ARGN} )
6
7      set (_Gears_CSOURCES)
8      foreach(i ${_Gears_SOURCES})
9          if (${i} MATCHES "\\.cbc")
10             string(REGEX REPLACE "(.*).cbc" "c/\\1.c" j ${i})
11             add_custom_command (
12                 OUTPUT    ${j}
13                 DEPENDS   ${i}
14                 COMMAND  "perl" "generate_stub.pl" "-o" ${j} ${i}
15             )
16         elseif (${i} MATCHES "\\.cu")
17             string(REGEX REPLACE "(.*).cu" "c/\\1.ptx" j ${i})
18             add_custom_command (
19                 OUTPUT    ${j}
20                 DEPENDS   ${i}
21                 COMMAND  nvcc ${NVCCFLAG} -c -ptx -o ${j} ${i}
```

```
22              )
23          else()
24              set(j ${i})
25          endif()
26          list(APPEND _Gears_CSOURCES ${j})
27      endforeach(i)
```

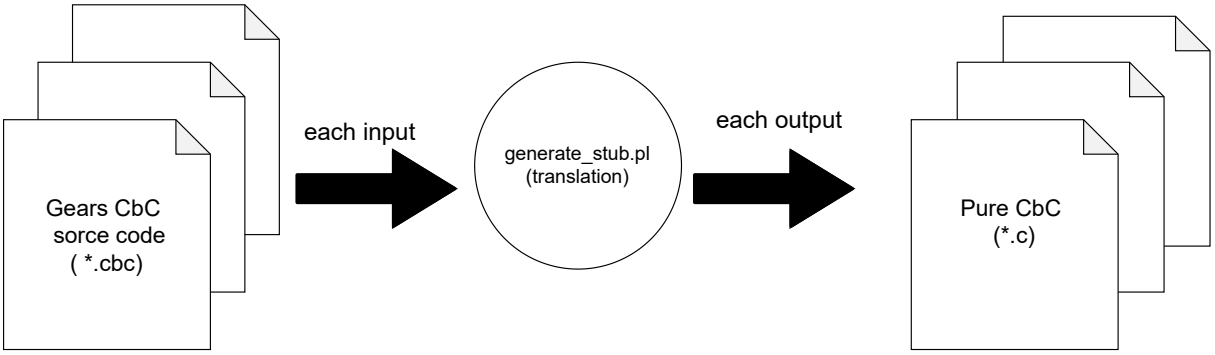

図 4.1: generate_sub.pl を使ったトランスコンパイル

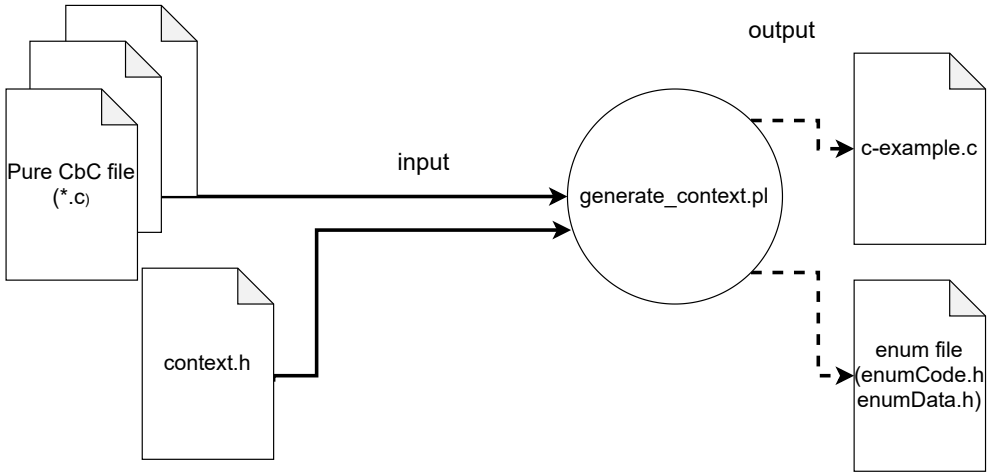

図 4.2: generate_context.pl を使ったファイル生成

4.2　GearsCbC の Interface の実装時の問題

Interface とそれを実装する Impl の型が決定すると、最低限満たすべき CodeGear の API は一意に決定する。ここで満たすべき CodeGear は、Interface で定義した CodeGear と、

Impl 側で定義した private な CodeGear となる。例えば Stack Interface の実装を考えると、各 Impl で pop, push, shift, isEmpty などを実装する必要がある。

従来はプログラマが手作業でヘッダーファイルの定義を参照しながら .cbc ファイルを作成していた。手作業での実装のため、 コンパイル時に次のような問題点が多発した。

- CodeGear の入力のフォーマットの不一致
- Interface の実装の CodeGear の命名規則の不一致
- 実装を忘れている CodeGear の発生

特に GearsOS の場合は Perl スクリプトによって純粋な CbC に一度変換されてからコンパイルが行われる。実装の状況とトランスコンパイラの組み合わせによっては、 CbC コンパイラレベルでコンパイルエラーを発生させないケースがある。この場合は実際に動作させながら、gdb, lldb などの C デバッガを用いてデバッグをする必要がある。また CbC コンパイラレベルで検知できても、すでに変換されたコード側でエラーが出てしまうので、トランスコンパイラの挙動をトレースしながらデバッグをする必要がある。Interface の実装が不十分であることのエラーは、 GearsOS レベル、最低でも CbC コンパイラのレベルで完全に検知したい。

4.3　Interfaceを満たすコード生成の他言語の対応状況

Interface を機能として所持している言語の場合、Interface を完全に見たいしているかどうかはコンパイルレベルか実行時レベルで検知される。例えば Java の場合は Interface を満たしていない場合はコンパイルエラーになる。

Interface の API を完全に実装するのを促す仕組みとして、Interface の定義からエディタやツールが満たすべき関数と引数の組を自動生成するツールがある。

Java では様々な手法でこのツールを実装している。Microsoft が提唱している IDE とプログラミング言語のコンパイラをつなぐプロトコルに Language Server がある。Language Server はコーディング中のソースコードをコンパイラ自身でパースし、 型推論やエラーの内容などを IDE 側に通知するプロトコルである。主要な Java の Language Server の実装である eclipse.jdt.ls[18] では、 LanguageServer の機能として未実装のメソッドを検知する機能が実装されている。[19] この機能を応用して vscode 上から未実装のメソッドを特定し、 雛形を生成する機能がある。他にも IntelliJ IDE などの商用 IDE では、 IDE が独自に未実装のメソッドを検知、雛形を生成する機能を実装している。

golang の場合は主に josharian/impl[20] が使われている。これはインストールすると impl コマンドが使用可能になり、 実装したい Interface の型と、 Interface を実装する

Impl の型 (レシーバ) を与えることで雛形が生成される。主要なエディタである vscode の golang の公式パッケージである `vscode-go`[21] でも導入されており、 vscode から呼び出すことが可能である。vscode 以外にも vim などのエディタから呼び出すことや、 シェル上で呼び出して標準出力の結果を利用することが可能である。

4.4　GearsOS での Interface を満たす CbC の雛形生成

GearsOS でも同様の Interface の定義から実装する CodeGear の雛形を生成したい。LanguageServer の導入も考えられるが、 今回の場合は C 言語の LanguageServer を CbC 用にまず改良し、 さらに GearsOS 用に書き換える必要がある。現状の GearsOS が持つシンタックスは CbC のシンタックスを拡張しているものではあるが、これは CbC コンパイラ側には組み込まれていない。LanguageServer を GearsOS に対応する場合、CbC コンパイラ側に GearsOS の拡張シンタックスを導入する必要がある。CbC コンパイラ側への機能の実装は、 比較的難易度が高いと考えらる。CbC コンパイラ側に手をつけず、 Interface の入出力の検査は既存の GearsOS のビルドシステム上に組み込みたい。

対して golang の `impl` コマンドのように、 シェルから呼び出し標準出力に結果を書き込む形式も考えられる。この場合は実装が比較的容易かつ、 コマンドを呼び出して標準出力の結果を使えるシェルやエディタなどの各プラットフォームで使用可能となる。先行事例を参考に、コマンドを実行して雛形ファイルを生成するコマンド `impl2cbc.pl` を GearsOS に導入した。`impl2cbc.pl` の処理の概要を図 4.3 に示す。

4.4.1　雛形生成の手法

Interface では入力の引数が Impl と揃っている必要があるが、 第一引数は実装自身のインスタンスがくる制約となっている。実装自身の型は、Interface 定義時には不定である。その為、 GearsOS では Interface の API の宣言時にデフォルト型変数 `Impl` を実装の型として利用する。デフォルト型 `Impl` を各実装の型に置換することで自動生成が可能となる。

実装すべき CodeGear は Interface と Impl 側の型を見れば定義されている。`__code` で宣言されているものを逐次生成すればよいが、 継続として呼び出される CodeGear は具体的な実装を持たない。GearsOS で使われている Interface には概ね次の継続である `next` が登録されている。`next` そのものは Interface を呼び出す際に、入力として与える。その為各 Interface に入力として与えられた `next` を保存する場所は存在するが、 next そのものの独自実装は各 Interface は所持しない。したがってこれを Interface の実装側で明示的に実装することはできない。雛形生成の際に、入力として与えられる CodeGear を生成してしまうと、プログラマに混乱をもたらしてしまう。

入力として与えられている CodeGear は、Interface に定義されている CodeGear の引数として表現されている。コードに示す例では、whenEmpty は入力して与えられている CodeGear である。雛形を生成する場合は、入力として与えられた CodeGear を除外して出力を行う。順序は Interface をまず出力した後に、 Impl 側を出力する。

4.4.2　コンストラクタの自動生成

雛形生成では他にコンストラクタの生成も行う。GearsOS の Interface のコンストラクタは、 メモリの確保及び各変数の初期化を行う。メモリ上に確保するのは主に Interface と Impl のそれぞれが基本となっている。Interface によっては別の DataGear を内包しているものがある。その場合は別の DataGear の初期化もコンストラクタ内で行う必要があるが、 自動生成コマンドではそこまでの解析は行わない。

コンストラクタのメンバ変数はデフォルトでは変数は 0、ポインタの場合は NULL で初期化するように生成する。このスクリプトで生成されたコンストラクタを使う場合、CbC ファイルから該当する部分を削除すると、generate_stub.pl 内でも自動的に生成される。自動生成機能を作成すると 1CbC ファイルあたりの記述量が減る利点がある。

明示的にコンストラクタが書かれていた場合は、Perl スクリプト内での自動生成は実行しないように実装した。これはオブジェクト指向言語のオーバーライドに相当する機能と言える。現状の GearsOS で使われているコンストラクタは、 基本は struct Context*型の変数のみを引数で要求している。しかしオブジェクトを識別するために ID を実装側に埋め込みたい場合など、 コンストラクタ経由で値を代入したいケースが存在する。この場合はコンストラクタの引数を増やす必要や、 受け取った値をインスタンスのメンバに書き込む必要がある。具体的にどの値を書き込めば良いのかまでは Perl スクリプトでは判定することができない。このような細かな調整をする場合は、 generate_stub.pl 側での自動生成はせずに、 雛形生成されたコンストラクタを変更すれば良い。あくまで雛形生成スクリプトはプログラマ支援であるため、 いくつかの手動での実装は許容している。

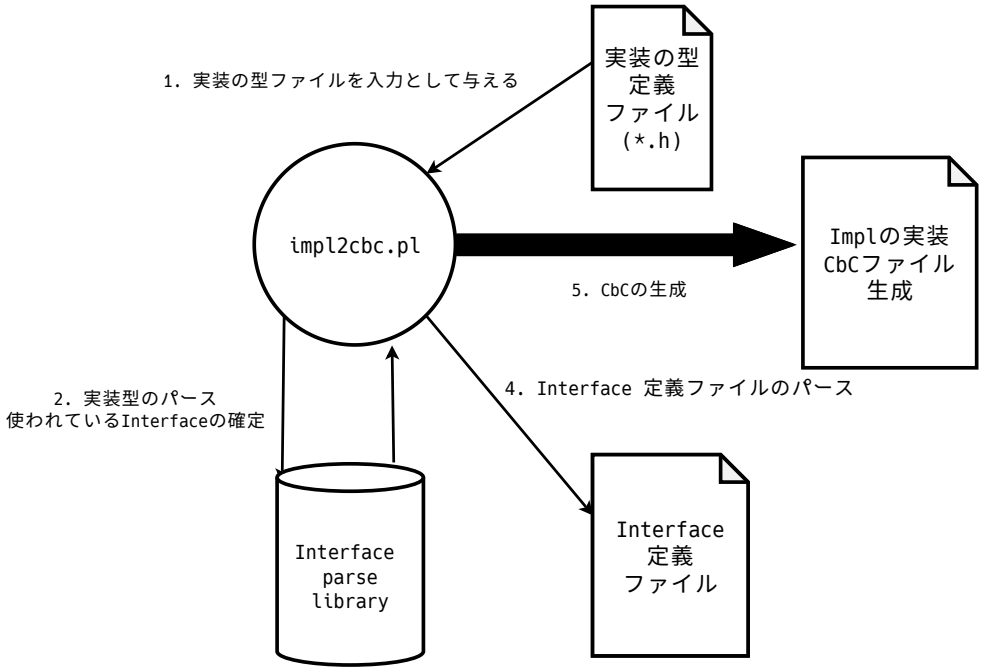

図 4.3: impl2cbc の処理の流れ

第5章　GearsOSのInterfaceの改良

5.1　GearsOSのInterfaceの構文の改良

GearsOS の Interface では、 従来は DataGear と CodeGear を分離して記述していた。CodeGear の入出力を DataGear として列挙する必要があった。CodeGear の入出力として__code() の間に記述した DataGear の一覧と、Interface 上部で記述した DataGear の集合が一致している必要がある。ソースコード 5.1 は Stack の Interface の例である。

ソースコード 5.1: 従来の Stack Interface

```
1  typedef struct Stack<Type, Impl>{
2          union Data* stack;
3          union Data* data;
4          union Data* data1;
5          /* Type* stack; */
6          /* Type* data; */
7          /* Type* data1; */
8          __code whenEmpty(...);
9          __code clear(Impl* stack,__code next(...));
10         __code push(Impl* stack,Type* data, __code next(...));
11         __code pop(Impl* stack, __code next(Type* data, ...));
12         __code pop2(Impl* stack, __code next(Type* data, Type* data1,
       ...));
13         __code isEmpty(Impl* stack, __code next(...), __code whenEmpty
       (...));
14         __code get(Impl* stack, __code next(Type* data, ...));
15         __code get2(Impl* stack, __code next(Type* data, Type* data1,
       ...));
16         __code next(...);
17 } Stack;
```

従来の分離している記法の場合、 この DataGear の宣言が一致していないケースが多々発生した。また Interface の入力としての DataGear ではなく、 フィールド変数として DataGear を使うようなプログラミングスタイルを取ってしまうケースも見られた。GearsOS では、 DataGear やフィールド変数をオブジェクトに格納したい場合、Interface 側ではなく Impl 側に変数を保存する必要がある。Interface 側に記述してしまう原因は複数考えられる。GearsOS のプログラミングスタイルに慣れていないことも考えられるが、構文によるところも考えられる。CodeGear と DataGear は Interface の場合は密接な関係

性にあるが、分離して記述してしまうと「DataGear の集合」と「CodeGear の集合」を別個で捉えてしまう。あくまで Interface で定義する CodeGear と DataGear は Interface の API である。これをユーザーに強く意識させる必要がある。

golang にも Interface の機能が実装されている。golang の場合は Interface は関数の宣言部分のみを記述するルールになっている。変数名は含まれていても含まなくても問題ない。

ソースコード 5.2: golang の interface 宣言

```
type geometry interface {
    area() float64
    perim() float64
}
```

GearsOS の Interface は入力と出力の API を定義するものであるので、golang の Interface のように、関数の API を並べて記述するほうが簡潔であると考えた。改良した Interface の構文で Stack を定義したものをソースコード 5.3 に示す。

ソースコード 5.3: 変更後の Stack Interface

```
typedef struct Stack<>{
        __code clear(Impl* stack,__code next(...));
        __code push(Impl* stack,union Data* data, __code next(...));
        __code pop(Impl* stack, __code next(union Data* data, ...));
        __code pop2(Impl* stack, __code next(union Data* data, union Data
   * data1, ...));
        __code isEmpty(Impl* stack, __code next(...), __code whenEmpty
   (...));
        __code get(Impl* stack, __code next(union Data* data, ...));
        __code get2(Impl* stack, __code next(union Data* data, union Data
   * data1, ...));
        __code next(...);
        __code whenEmpty(...);
} Stack;
```

従来の Interface では<Type, Impl>という記述があった。これはジェネリクスの機能を意識して導入された構文である。Impl キーワードは実装自身の型を示す型変換として使われていた。しかし基本 Interface の定義を行う際に GearsOS のシステム上、CodeGear の第一引数は Impl 型のポインタが来る。これはオブジェクト指向言語で言う self に相当するものであり、 自分自身のインスタンスを示すポインタである。Impl キーワードは共通して使用されるために、 宣言部分からは取り外し、デフォルトの型キーワードとして定義した。Type キーワードは型変数としての利用を意識して導入されていたが、現在までの GearsOS の例題では導入されていなかった。ジェネリクスとしての型変数の利用の場合は T などの 1 文字変数がよく使われる。変更後の構文ではのちのジェネリクス導入のことを踏まえて、Type キーワードは削除した。

構文を変更するには、 GearsOS のビルドシステム上で Interface を利用している箇所を修正する必要がある。Interface は generate_stub.pl で読み込まれ、 CodeGear と入出力の DataGear の数え上げが行われる。この処理は Interface のパースに相当するものである。当然ではあるが、パース対象の Interface の構文は、変更前の構文にしか対応していない。

5.2　Implement の型定義ファイルの導入

Interface を使う言語では、 Interface が決まるとこれを実装するクラスや型が生まれる。GearsOS も Interface に対応する実装が存在する。例えば Stack Interface の実装は SingleLinkedStack であり、 Queue の実装は SingleLinkedQueue や SynchronizedQueue が存在する。

この SynchronizedQueue は GearsOS では DataGear として扱われる。この DataGear の定義は、 Interface の定義のように型定義ファイルが存在するわけではなかった。従来は context.h の DataGear の宣言部分に、構造体の形式で表現したものを手で記述していた。(ソースコード 5.4)

ソースコード 5.4: cotnext.h に直接書かれた型定義

```
union Data {
   /* 略 */
    // Queue Interface
    struct Queue {
        union Data* queue;
        union Data* data;
        enum Code whenEmpty;
        enum Code clear;
        enum Code put;
        enum Code take;
        enum Code isEmpty;
        enum Code next;
    } Queue;
    struct SingleLinkedQueue {
        struct Element* top;
        struct Element* last;
    } SingleLinkedQueue;
    struct SynchronizedQueue {
        struct Element* top;
        struct Element* last;
        struct Atomic* atomic;
    } SynchronizedQueue;
   /* 略 */
};
```

CbC ファイルからは context.h をインクルードすることで問題なく型を使うことが可能であるが、型定義ファイルの存在の有無が Interface と実装で異なってしまっていた。Perl のトランスコンパイラである generate_stub.pl は Interface の型定義ファイルをパースして

いた。Implement の型も同様に定義ファイルを作製すれば、generate_stub.pl で型定義を用いた様々な処理が可能となり、ビルドシステムが柔軟な挙動が可能となる。また型定義は一貫して*.h に記述すれば良くなるため、 プログラマの見通しも良くなる。本研究では新たに Implement の型定義ファイルを考案する。

GearsOS ではすでに Interface の型定義ファイルを持っている。Implement の型定義ファイルも、 Interface の型定義ファイルと似たシンタックスにしたい。Implement の型定義ファイルで持たなければいけないのは、 どの Interface を実装しているかの情報である。この情報は他言語では Interface の実装を持つ型の宣言時に記述するケースと、型名の記述はせずに言語システムが実装しているかどうかを確認するケースが存在する。Java では `implements` キーワードを用いてどの Interface を実装しているかを記述する。[22] ソースコード 5.5 では、`Pig` クラスは `Animal` Interface を実装している。

ソースコード 5.5: Java の Implement キーワード

```
1  // interface
2  interface Animal {
3    public void animalSound(); // interface method (does not have a body)
4    public void sleep(); // interface method (does not have a body)
5  }
6
7  // Pig "implements" the Animal interface
8  class Pig implements Animal {
9    public void animalSound() {
10     // The body of animalSound() is provided here
11     System.out.println("The pig says: wee wee");
12   }
13   public void sleep() {
14     // The body of sleep() is provided here
15     System.out.println("Zzz");
16   }
17 }
```

golang では Interface の実装は特にキーワードを指定せずに、 その Interface で定義しているメソッドを、Implement に相当する構造体がすべて実装しているかどうかでチェックされる。これは golang はクラスを持たず、構造体を使って Interface の実装を行う為に、構造体の定義にどの Interface の実装であるかの情報をシンタックス上書けない為である。GearsOS では型定義ファイルを持つことができるために、 golang のような実行時チェックは行わず、 Java に近い形で表現したい。

導入した型定義で SynchronizedQueue を定義したものをソースコード 5.6 に示す。大まかな定義方法は Interface 定義のものと同様である。違いとして `impl` キーワードを導入した。これは Java の `implements` に相当する機能であり、 実装した Interface の名前を記述する。現状の GearsOS では Impl が持てる Interface は 1 つのみであるため、`impl` の後ろにはただ 1 つの型が書かれる。型定義の中では独自に定義した CodeGear を書いてもいい。これは Java のプライベートメソッドに相当するものである。特にプライベートメソッド

がない場合は、 実装側で所持したい変数定義を記述する。SynchronizedQueue の例では top などが実装側で所持している変数である。

ソースコード 5.6: SynchronizedQueue の定義ファイル

```
1 typedef struct SynchronizedQueue <> impl Queue {
2   struct Element* top;
3   struct Element* last;
4   struct Atomic* atomic;
5 } SynchronizedQueue;
```

従来 context.h に直接記述していたすべての DataGear の定義は、 スクリプトで機械的に Interface および Implement の型定義ファイルに変換している。

5.3 Implement の型をいれたことによる間違った Gears プログラミング

Implement の型を導入したが、 GearsOS のプログラミングをするにつれていくつかの間違ったパターンがあることがわかった。自動生成される StubCodeGear は、 goto meta から遷移するのが前提であるため、引数を Context から取り出す必要がある。Context から取り出す場合は、 実装している Interface に対応している置き場所からデータを取り出す。この置き場所は data 配列であり、 配列の添え字は enum Data と対応している。また各 CodeGear から goto する際に、 遷移先の Interface に値を書き込みに行く。

Interface で定義した CodeGear と対応している Implement の CodeGear の場合はこのデータの取り出し方で問題はない。しかし Implement の CodeGear から内部で goto する CodeGear の場合は事情が異なる。内部で goto する CodeGear は、Java などのプライベートメソッドのように使うことを想定している。この CodeGear のことを private CodeGear と呼ぶ。privateCodeGear に goto する場合、 goto 元の CodeGear からは goto meta 経由で遷移する。goto meta が発行されると Stub Code Gear に遷移するが、現在のシステムでは Interface から値をとってくることになってしまう。

5.4 context.h の自動生成

GearsOS の Context の定義は context.h にある。Context は GearsOS の計算で使用されるすべての CodeGear、DataGear の情報を持っている。context.h では DataGear に対応する union Data 型の定義も行っている。Data 型は C の共用体であり、 Data を構成する要素として各 DataGear がある。各 DataGear は構造体の形で表現されている。各 DataGear 自体の定義も context.h の union Data の定義の中で行われている。

DataGear の定義は Interface ファイルで行っていた。Interface ファイルは GearsOS 用に拡張されたシンタックスのヘッダファイルを使っており、 直接 CbC からロードすることができない。その為従来はプログラマが静的に Interface ファイルを CbC の文脈に変換し、 context.h に構造体に変換したものを書いていた。この手法では手書きでの構築のために自由度は高かったが、 GearsOS の例題によっては使わない DataGear も、 context.h から削除しない限り context に含んでしまう問題があった。さらに Interface ファイルで定義した型を context.h に転記し、それをもとに Impl の型を考えて CbC ファイルを作製する必要があった。これらをすべてユーザーが行うと、ファイルごとに微妙な差異が発生したりとかなり煩雑な実装を要求されてしまう。DataGear の定義は Interface ファイルを作製した段階で決まり、 使用している DataGear、CodeGear はコンパイル時に確定するはずである。使用している各 Gear がコンパイル時に確定するならば、 コンパイルの直前に実行される Perl トランスコンパイラでも Gear の確定ができるはずである。ここから context.h をコンパイルタイミングで Perl スクリプト経由で生成する手法を考案した。

5.4.1　context.h の作製フロー

GearsCbC からメタ計算を含む CbC ファイルに変換する generate_stub.pl は各 CbC ファイルを 1 つ 1 つ呼び出していた。context.h を生成しようとする場合、 プロジェクトで利用する全 CbC ファイルを扱う必要がある。

Context の初期化ルーチンを作製する generate_context.pl は、その特性上すべての CbC ファイルをロードしていた。したがって context.h を作製する場合はこのスクリプトで行うのが良い。

Perl のモジュールとして `Gears::Template::Context` を作製した。xv6 プロジェクトの場合は一部ヘッダファイルに含める情報が異なる。

派生モジュールとして `Gears::Template::Context::XV6` も実装している。これらのテンプレートモジュールは generate_context.pl の実行時のオプションで選択可能とした

5.5　メタ計算部分の入れ替え

GearsOS では次の CodeGear に移行する前の MetaCodeGear として、 デフォルトでは `__code meta` が使われている。`__code meta` は context に含まれている CodeGear の関数ポインタを、 enum からディスパッチして次の Stub CodeGear に継続するものである。

例えばモデル検査を GearsOS で実行する場合、 通常の Stub CodeGear のほかに状態の保存などを行う必要がある。この状態の保存に関する一連の処理は明らかにメタ計算であるので、 ノーマルレベルの CodeGear ではない箇所で行いたい。ノーマルレベル以外の CodeGear で実行する場合は、 通常のコード生成だと StubCodeGear の中で行うことにな

る。StubCodeGear は自動生成されてしまうため、 値の取り出し以外のことを行う場合は自分で実装する必要がある。しかしモデル検査に関する処理は様々な CodeGear の後に行う必要があるため、 すべての CodeGear の Stub を静的に実装するのは煩雑である。

ノーマルレベルの CodeGear の処理の後に、StubCodeGear 以外の Meta Code Gear を実行したい。Stub Code Gear に直ちに遷移してしまう `__code meta` 以外の Meta CodeGear に、 特定の CodeGear の計算が終わったら遷移したい。このためには、特定の CodeGear の遷移先の MetaCodeGear をユーザーが定義できる API が必要となる。この API を実装すると、ユーザーが柔軟にメタ計算を選択することが可能となる。

GearsOS のビルドシステムの API として `meta.pm` を作製した。これは Perl のモジュールファイルとして実装した。meta.pm は Perl で実装された GearsOS のトランスコンパイラである generate_stub.pl から呼び出される。meta.pm の中のサブルーチンである `replaceMeta` に変更対象の CodeGear と変更先の MetaCodeGear への goto を記述する。ユーザーは meta.pm の Perl ファイルを API として GearsOS のトランスコンパイラにアクセスすることが可能となる。

具体的な使用例をコード 5.7 に示す。meta.pm はサブルーチン `replaceMeta` が返すリストの中に、特定のパターンで配列を設定する。各配列の 0 番目には、goto meta を置換したい CodeGear の名前を示す Perl 正規表現リテラルを入れる。コード 5.7 の例では、`PhilsImpl` が名前に含まれる CodeGear を指定している。すべての CodeGear の goto の先を切り替える場合は `qr/.*/` などの正規表現を指定する。

ソースコード 5.7: meta.pm

```
1  package meta;
2  use strict;
3  use warnings;
4
5  sub replaceMeta {
6    return (
7      [qr/PhilsImpl/ => \&generateMcMeta],
8    );
9  }
10
11 sub generateMcMeta {
12   my ($context, $next) = @_;
13   return "goto mcMeta($context, $next);";
14 }
15
16 1;
```

generate_stub.pl は Gears CbC ファイルの変換時に、 CbC ファイルがあるディレクトリに meta.pm があるかを確認する。meta.pm がある場合はモジュールロードを行う。meta.pm がない場合は meta Code Gear に goto するものをデフォルト設定として使う。各 Gode Gear が `goto` 文を呼び出したタイミングで replaceMeta を呼び出し、 ルールにしたがって goto 文を書き換える。変換する CodeGear がルールになかった場合は、 デフォル

ト設定が呼び出される。

5.6　別Interfaceからの書き出しを取得する必要があるCodeGear

従来の MetaCodeGear の生成では、 別の Interface からの入力を受け取る CodeGear の Stub の生成に問題があった。具体的なこの問題が発生する例題をソースコード 5.8 に示す。

ソースコード 5.8: 別 Interface からの書き出しを取得する CodeGear の例

```
1  #interface "String.h"
2  #interface "Stack.h"
3
4  #impl "StackTest.h" for "StackTestImpl3.h"
5
6  /* 略 */
7
8  __code pop2Test(struct StackTestImpl3* stackTest, struct Stack* stack,
       __code next(...)) {
9      goto stack->pop2(pop2Test1);
10 }
11
12
13 __code pop2Test1(struct StackTestImpl3* stackTest, union Data* data,
       union Data* data1, struct Stack* stack, __code next(...)) {
14     String* str = (String*)data;
15     String* str2 = (String*)data1;
16
17     printf("%d\n", str->size);
18     printf("%d\n", str2->size);
19     goto next(...);
20 }
```

この例では pop2TestCode Gear から stack->pop2 を呼び出し、 継続として pop2Test1 を渡している。pop2Test 自体は StackTest Interface であり、 stack->pop2 の stack は Stack Interface である。例題では Stack Interface の実装は SingleLinkedStack である。SingleLinkedStack の pop2 の実装をソースコード 5.9 に示す。

ソースコード 5.9: SingleLinkedStack の pop2

```
1  __code pop2SingleLinkedStack(struct SingleLinkedStack* stack, __code next
       (union Data* data, union Data* data1, ...)) {
2      if (stack->top) {
3          data = stack->top->data;
4          stack->top = stack->top->next;
5      } else {
6          data = NULL;
7      }
8      if (stack->top) {
9          data1 = stack->top->data;
10         stack->top = stack->top->next;
```

```
11      } else {
12          data1 = NULL;
13      }
14      goto next(data, data1, ...);
15  }
```

pop2 はスタックから値を 2 つ取得する API である。pop2 の継続は next であり、 継続先に data と data1 を渡している。data、 data1 は引数で受けている union Data*型の変数であり、 それぞれ stack の中の値のポインタを代入している。この操作で stack から値を 2 つ取得している。

このコードを generate_stub.pl 経由でメタ計算を含むコードに変換する。変換した先のコードを 5.10 に示す。

ソースコード 5.10: SingleLinkedStack の pop2 のメタ計算

```
1   __code pop2SingleLinkedStack(struct Context *context,struct
        SingleLinkedStack* stack, enum Code next,union Data **O_data,union
        Data **O_data1) {
2     Data* data  __attribute__((unused))  = *O_data;
3     Data* data1  __attribute__((unused))  = *O_data1;
4       if (stack->top) {
5           data = stack->top->data;
6           stack->top = stack->top->next;
7       } else {
8           data = NULL;
9       }
10      if (stack->top) {
11          data1 = stack->top->data;
12          stack->top = stack->top->next;
13      } else {
14          data1 = NULL;
15      }
16    *O_data = data;
17    *O_data1 =  data1;
18      goto meta(context, next);
19  }
20
21
22  __code pop2SingleLinkedStack_stub(struct Context* context) {
23    SingleLinkedStack* stack = (SingleLinkedStack*)GearImpl(context, Stack,
        stack);
24    enum Code next = Gearef(context, Stack)->next;
25    Data** O_data = &Gearef(context, Stack)->data;
26    Data** O_data1 = &Gearef(context, Stack)->data1;
27    goto pop2SingleLinkedStack(context, stack, next, O_data, O_data1);
28  }
```

実際は next は goto meta に変換されてしまう。data、data1 は goto meta の前にポインタ変数 O_data が指す値にそれぞれ書き込まれる。O_data は pop2 の Stub CodeGear である pop2SingleLinkedStack_stub で作製している。つまり O_data は context 中に含まれ

ている Stack Interface のデータ保管場所にある変数 data のアドレスである。pop2 の API を呼び出すと、 Stack Interface 中の data に Stack に保存されていたデータのアドレスが書き込まれる。

当初 Perl スクリプトが生成した pop2Test1 の stub CodeGear はソースコード 5.11 のものである。CodeGear 間で処理されるデータの流れの概要図を図 5.1 に示す。

ソースコード 5.11: 生成された Stub

```
1 __code pop2Test1StackTestImpl3_stub(struct Context* context) {
2   StackTestImpl3* stackTest = (StackTestImpl3*)GearImpl(context,
      StackTest, stackTest);
3   Data* data = Gearef(context, StackTest)->data;
4   Data* data1 = Gearef(context, StackTest)->data1;
5   Stack* stack = Gearef(context, StackTest)->stack;
6   enum Code next = Gearef(context, StackTest)->next;
7   goto pop2Test1StackTestImpl3(context, stackTest, data, data1, stack,
      next);
8 }
```

__code pop2Test で遷移する先の CodeGear は StackInterface であり、 呼び出している API は pop2 である。pop2 で取り出したデータは、 上記で確認した通り Context 中の Stack Interface のデータ格納場所に書き込まれる。しかしソースコード 5.11 の例では Gearef(context, StackTest) で Context 中の StackTest Interface の data の置き場所から値を取得している。これは Interface の Impl の CodeGear は、Interface から値を取得するという GearsOS のルールの為である。現状では pop2 でせっかく取り出した値を StubCodeGear で取得できない。

ここで必要となってくるのは、 実装している Interface 以外の呼び出し元の Interface からの値の取得である。今回の例では StackTest Interface ではなく Stack Interface から data、 data1 を取得したい。どの Interface から呼び出されているかは、 コンパイルタイムには確定できるので Perl のトランスコンパイラで Stub Code を生成したい。

別 Interface から値を取得するには別の出力がある CodeGear の継続で渡された CodeGear をまず確定させる。今回の例では pop2Test1 が該当する。この CodeGear の入力の値と、出力がある CodeGear の出力を見比べ、出力をマッピングすれば良い。Stack Interface の pop2 は data と data1 に値を書き込む。pop2Test1 の引数は data, data1, stack であるので、前 2 つに pop2 の出力を代入したい。

Context から値を取り出すのはメタ計算である Stub CodeGear で行われる。別 Interface から値を取り出そうとする場合、 すでに Perl トランスコンパイラが生成している Stub を書き換えてしまう方法も取れる。しかし StubCodeGear そのものを、 別 Interface から値を取り出すように書き換えてはいけない。これは別 Interface の継続として渡されるケースと、 次の goto 先として遷移するケースがあるためである。前者のみの場合は書き換えで問題ないが、 後者のケースで書き換えを行ってしまうと Stub で値を取り出す先が異

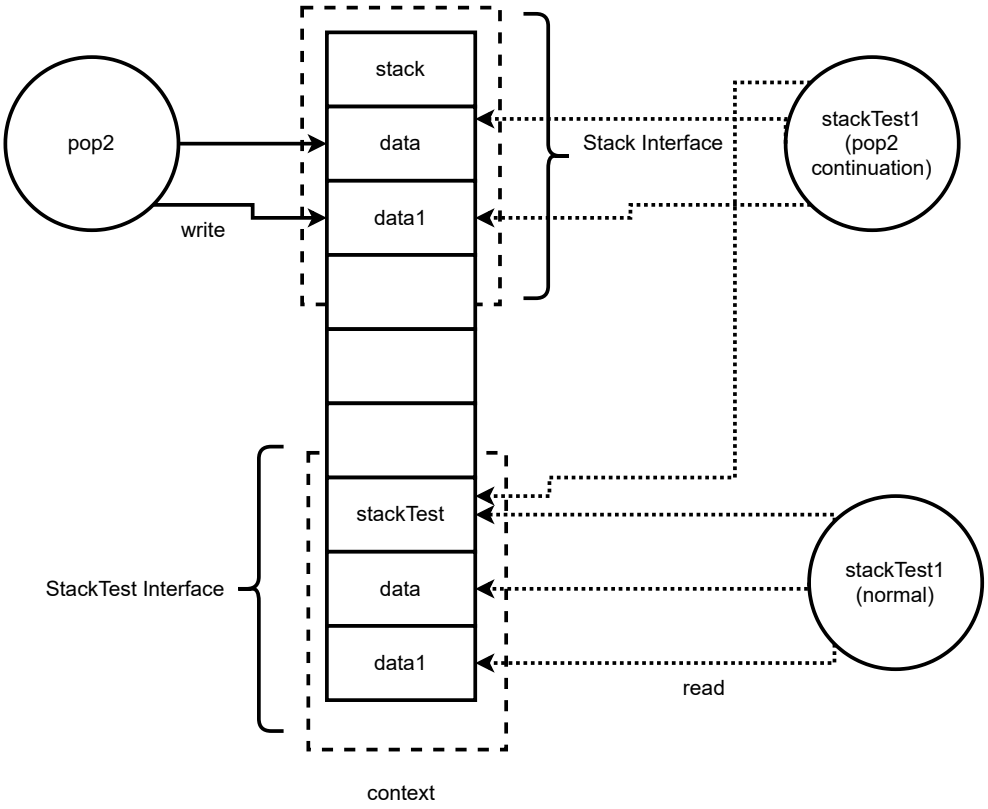

図 5.1: stackTest1 の stub の概要

なってしまう。どのような呼び出し方をしても対応できるようにするには、 Stub を別に別ける必要がある。

GearsOS では継続として渡す場合や、 次の goto 文で遷移する先の CodeGear はノーマルレベルでは enum の番号として表現されていた。enum が降られる CodeGear は、厳密には CodeGear そのものではなく Stub CodeGear に対して降られる。StubCodeGear を実装した分だけ enum の番号が降られるため、 `goto meta` で遷移する際に enum の番号さえ合わせれば独自定義の Stub に継続させることが可能である。別 Interface から値を取り出したいケースの場合、 取り出してくる先の Interface と呼び出し元の CodeGear が確定したタイミングで別の StubCodeGear を生成する。呼び出し元の CodeGear が継続として渡す StubCodeGear の enum を、独自定義した enum に差し替えることでこの問題は解決する。この機能を Perl のトランスコンパイラである `generate_stub.pl` に導入した。

5.7　別 Interface からの書き出しを取得する Stub の生成

別 Interface からの書き出しを取得する場合、 generate_stub.pl では次の点をサポートする機能をいれれば実現可能である。

- goto 先の CodeGear が出力を持つ Interface でかつ継続で渡している CodeGear が別 Interface の場合の検知
  - この場合は goto している箇所で渡している継続の enum を、新たに作製した stub の enum に差し替える
- 継続で実行された場合に別に Interface から値をとってこないといけない CodeGear 自身
  - Stub を別の Interface から値をとる実装のものを別に作製する

`generate_stub.pl` 内では変換対象の CbC のソースコードを 2 度読み込む。最初の読み込み時に継続の状況を確認し、 2 度目の読み込み時に状況を踏まえてコードを生成すれば良い。初回の読み込み時に Interface 経由の `goto` 文があった場合に、別 Interface からの出力があるかなどの情報を確認したい。

5.7.1　初回 CbC ファイル読み込み時の処理

Interface 経由での goto 文は `goto interface->method()` の形式で呼び出される。ソースコード 5.12 はこの形式で来ていた行を読み込んだタイミングで実行される処理である。

ソースコード 5.12: goto 時に使用する interface の解析

```
1  } elsif (/^(.*)goto (\w+)\-\>(\w+)\((.*)\);/) {
2    debug_print("getDataGear",__LINE__, $_) if $opt_debug;
3    # handling goto statement
4    # determine the interface you are using, and in the case of a goto
     CodeGear with output, create a special stub flag
5    my $prev = $1;
6    my $instance = $2;
7    my $method = $3;
8    my $tmpArgs = $4;
9    my $typeName = $codeGearInfo->{$currentCodeGear}->{arg}->{$instance};
10   my $nextOutPutArgs = findExistsOutputDataGear($typeName, $method);
11   my $outputStubElem = { modifyEnumCode => $currentCodeGear,
     createStubName => $tmpArgs };
12
13   if ($nextOutPutArgs) {
14     my $tmpArgHash = {};
15     for my $vname (@$nextOutPutArgs) {
```

```
16          $tmpArgHash->{$vname} = $typeName;
17        }
18
19        $outputStubElem->{args} = $tmpArgHash;
20
21        #We're assuming that $tmpArgs only contains the name of the next
      CodeGear.
22        #Eventually we need to parse the contents of the argument. (eg.
      @parsedArgs)
23        my @parsedArgs = split /,/ , $tmpArgs; #
24
25        $generateHaveOutputStub->{counter}->{$tmpArgs}++;
26        $outputStubElem->{counter} = $generateHaveOutputStub->{counter}->{
      $tmpArgs};
27        $generateHaveOutputStub->{list}->{$currentCodeGear} =
      $outputStubElem;
28      }
```

1 行目の正規表現は Interface 経由での goto 文の正規表現パターンである。変数$instance は Interface のインスタンスである。正規表現パターンでは interface->method の->の前に来ている変数名に紐づけられる。変数$method は goto 先の Interface の API である。正規表現パターンでは interface->method の->の後に来ている API 名である。ソースコード 5.8 の pop2Test では、 stack->pop2 の呼び出しをしているため、 stack がインスタンスであり、 pop2 が API である。現在解析している goto 文が含まれている CodeGear の名前は、変数$currentCodeGear で別途保存している。連想配列である$codeGearInfo の中には、 各 CodeGear で使われている変数と変数の型などの情報が格納されている。ソースコード 5.12 の 9 行目では、 $codeGearInfo 経由で Interface のインスタンスから、具体的にどの型が呼ばれているかを取得する。pop2Test では、 インスタンス stack に対応する型名は Stack と解析される。

ソースコード 5.12 の 10 行目で実行されている findExistsOutputDataGear は generate_stub.pl 内の関数である。これは Interface の名前とメソッド名を与えると、 Interface の定義ファイルのパース結果から出力の有無を確認する動きをする。出力がある場合は出力している変数名の一覧を返す。ソースコード 5.8 の例では pop2 は data と data1 を出力している為、 これらがリストとして関数から返される。出力がない場合は偽値を返すために 13 行目からの if 文から先は動かない。出力があった場合は generate_stub.pl の内部変数に出力する変数名と、 Interface の名前の登録を行う。生成する Stub は命名規則が、__code CodeGearStub_1 のように末尾に_に続けて数値をいれる。この数値は変換した回数となるため、 この回数の計算を行う。

27 行目で$generateHaveOutputStub の list 要素に現在の CodeGear の名前と、 出力に関する情報を代入している。現在の CodeGear の名前を保存しているのは、この後のコード生成部分で enum の番号を切り替える必要があるためである。ソースコード 5.8 の例では pop2Test が使う enum を書き換える必要がある為、 ここの$currentCodeGear は

pop2Test となる。ここで作製した$outputStubElem は、返還後の CbC コードを生成しているフェーズで呼びされる。

5.7.2　enum の差し替え処理

ソースコード 5.13 の箇所は遷移先の enum を Perl スクリプトで生成し、 GearsOS が実行中に enum を context に書き込むコードを生成するフェーズである。

ソースコード 5.13: Gearef のコード生成部分

```
1 if ($outputStubElem && !$stub{$outputStubElem->{createStubName}."_stub
    "}->{static}) {
2   my $pick_next = "$outputStubElem->{createStubName}_$outputStubElem->{
    counter}";
3   $return_line .= "${indent}Gearef(${context_name}, $ntype)->$pName =
    C_$pick_next;\n";
4   $i++;
5   next;
6 }
```

if 文で条件判定をしているが、前者は出力があるケースかどうかのチェックである。続く条件式は GearsOS のビルドルールとして静的に書いた stub の場合は変更を加えない為に、静的に書いているかどうかの確認をしている。変数$pick_next で継続先の CodeGear の名前を作製している。CodeGear の名前は一度目の解析で確認した継続先に_とカウント数をつけている。ここで作製した CodeGear の名前を、3 行目で context に書き込む CbC コードとして生成している。

実際に生成された例題をソースコード 5.14 に示す。

ソースコード 5.14: enum の番号が差し替えられた CodeGear

```
1 __code pop2TestStackTestImpl3(struct Context *context,struct
    StackTestImpl3* stackTest, struct Stack* stack, enum Code next) {
2     Gearef(context, Stack)->stack = (union Data*) stack;
3     Gearef(context, Stack)->next = C_pop2Test1StackTestImpl3_1;
4     goto meta(context, stack->pop2);
5 }
```

第6章　まとめ

6.1　総括

6.2　今後の課題

6.2.1　hogehoge

謝辞

ホゲ様，フガ様ありがとうございます

参考文献

[1] Gerwin Klein, Kevin Elphinstone, Gernot Heiser, June Andronick, David Cock, Philip Derrin, Dhammika Elkaduwe, Kai Engelhardt, Rafal Kolanski, Michael Norrish, Thomas Sewell, Harvey Tuch, and Simon Winwood. sel4: Formal verification of an os kernel, 2009.

[2] Helgi Sigurbjarnarson, James Bornholt, Emina Torlak, and Xi Wang. Push-button verification of file systems via crash refinement. pp. 1–16, 2016.

[3] Haogang Chen, Daniel Ziegler, Tej Chajed, Adam Chlipala, M. Frans Kaashoek, and Nickolai Zeldovich. Using crash hoare logic for certifying the fscq file system. pp. 18–37, 2015.

[4] Ulf Norell. Dependently typed programming in agda. pp. 1–2, 2009.

[5] the coq proof assistant. *https://coq.inria.fr/*.

[6] Luke Nelson, Helgi Sigurbjarnarson, Kaiyuan Zhang, Dylan Johnson, James Bornholt, Emina Torlak, and Xi Wang. Hyperkernel: Push-button verification of an os kernel. *Proceedings of the 26th Symposium on Operating Systems Principles*, 2017.

[7] GNU Compiler Collection (GCC) Internals. *http://gcc.gnu.org/onlinedocs/gccint/*.

[8] 大城信康, 河野真治. Continuationbasedc の gcc4.6 上の実装について. 第 53 回プログラミング・シンポジウム予稿集, Vol. 2012, pp. 69–78, jan 2012.

[9] Chris Lattner and Vikram Adve. LLVM: A Compilation Framework for Lifelong Program Analysis & Transformation. In *Proceedings of the 2004 International Symposium on Code Generation and Optimization (CGO'04)*, Palo Alto, California, Mar 2004.

[10] Kaito TOKKMORI and Shinji KONO. Implementing continuation based language in llvm and clang. *LOLA 2015*, July 2015.

[11] 外間政尊, 河野真治. Gearsos の hoare logic をベースにした検証手法. ソフトウェアサイエンス研究会, Jan 2019.

[12] Russ Cox, Frans Kaashoek, Robert Morris. xv6 a simple, unix-like teaching operating system. https://pdos.csail.mit.edu/6.828/2018/xv6/book-rev11.pdf.

[13] 河野真治, 伊波立樹, 東恩納琢偉. Code gear、data gear に基づく os のプロトタイプ. 情報処理学会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 (OS), May 2016.

[14] Eugenio Moggi. Notions of computation and monads, July 1991.

[15] Jean Yang and Chris Hawblitzel. Safe to the last instruction: Automated verification of a type-safe operating system, 2010.

[16] Raspberry Pi. https://www.raspberrypi.org.

[17] Babel. https://babeljs.io/.

[18] Eclipse jdt language server. https://github.com/eclipse/eclipse.jdt.ls.

[19] yaohaizh. Add unimplemented methods code action.

[20] josharian/impl. https://github.com/josharian/impl.

[21] golang. golang/vscode-go.

[22] Java implements keyword. https://www.w3schools.com/java/ref_keyword_implements.asp.

[23] Zhiyi Wang. xv6-rpi. https://code.google.com/archive/p/xv6-rpi/, 2013.

[24] 坂本昂弘, 桃原優, 河野真治. 継続を用いた x.v6 kernel の書き換え. 情報処理学会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 (OS), No. 4, may 2019.

[25] J. Lions. *Lions' Commentary on UNIX 6th Edition with Source Code*. Computer classics revisited. Peer-to-Peer Communications, 1996.

付 録A　研究会業績

A-1　研究会発表資料