演習コースⅡ 形式手法と仕様記述

「形式手法と仕様記述」 実施報告

Report on “Formal Methods and Specification Description”

主査　　：栗田　太郎（株式会社フェリカネットワークス）
副主査　：石川　冬樹（国立情報学研究所）

報告概要
仕様をはじめとした開発上流の成果物における品質確保のため，国内産業界でも，形式手法への注目が高まっている．しかし一般の開発者がその実際を把握する機会はあまりない．加えて，技術を学ぶことができたとしても，プロジェクトの性質など状況に応じた適切な活用方法を定めることは難しい．本演習コースにおいては，参加者はまず，形式手法の一つ VDM の学習を通して，形式手法における原則を実感した．参加者はその上で，各自の要望，悩み，興味に応じ，学んだ手法の活用のための研究提案や，用途の異なる手法の学習と活用模索を行った．

Abstract For quality assurance of early deliverables in development, especially specifications, formal methods have recently attracted attentions of the Japanese industry. However, they are still “unknown” for most ordinary developers. Moreover, even if technology is obtained, difficulties lie in deciding proper usages according to contexts such as project characteristics. In this exercise course, participants first studied VDM, one of formal methods, to catch principles in formal methods. Each of the participants then worked for research proposals to leverage the methods, or studied specific methods and their applications, according to their requirements, concerns and interests.

1. 仕様記述における様々な問題

開発上流工程の成果物における品質確保は，効果の大きさ，効率の高さの双方の観点から非常に重要とされる．逆に，上流工程に起因する不具合が，発見，解消されないまま後の工程に引き継がれると，その修正コストは上流での修正コストの何十倍にもなる[Feiler09]．特に仕様は,「何を作ろうとしているのか（何を作ったのか)」を記述，維持するものであり，複数の組織・チーム・人をまたがって設計・実装，テスト，運用・保守等の拠り所となるものである．このため，仕様の品質確保は非常に重要なのである．

一方，仕様の記述においては，様々な種類の難しさが混在し，それらに起因する多種多様な問題が生じる．その代表的な例として，下記が挙げられる．

【厳密さ・可読性に関する問題】　発注者や設計・実装担当者，将来の仕様担当者など，想定する読み手が，容易に理解し，また一意に解釈できるように，指針を定めて記述や確認を行っていない．このため，誤解が発生し手戻りの原因となり，後の保守や派生開発も非常に困難になる．

【整合性・正当性に関する問題】　並行動作するオブジェクトの状態遷移や，データの読み書きなどによるモジュール間の依存関係が非常に複雑であるが，それらが整理，検証されていない．このため，特定のケースでのみ影響が現れる不具合が残る．一方，実装後のプログラム・システムは，様々な側面を含み，実行環境や状態が複雑すぎて，再現や理解，修正ができない．

【合目的性・必要十分性に関する問題】 仕様全体やその中の各項目が定める「ゴール」と，その上位の「ゴール」(正当性や妥当性の基準）が結びついておらず，仕様が必要であり十分であることが検証されていない．このため，仕様項目の漏れが発生しやすくなるとともに，後に適切な変更内容を定めることが難しくなる．

設計や実装，テスト，ソフトウェア保守・進化（派生開発）などにおけるトラブルの根幹には，仕様に関するこういった問題があることが多い．

2. 形式手法

仕様に関する問題の解決には様々なアプローチがあるが，国内産業界では近年「形式手法」が注目されている（詳細は，[MRI11, DSF11, IPA10] などにまとめられている）．
それでは，「形式手法とはどういうものなのか」という問いを投げかけると，人によって次のように様々な答えが返ってくるだろう．

- 数理論理学に基づいた手法のことである．
- プログラミング言語のように，文法や意味論が定まった言語で記述するので，記述の表す内容・意味が一意に定まり，定義の不整合や不足もツールで確認することができる．
- テストとは異なり，バグがないことを証明できる．
- スレッドの切り替えのタイミングや通信の成否などにより分岐する，大量で複雑な状態遷移の可能性を，網羅的に自動検査してくれる（モデル検査）．
- 様々な例を自動生成したり，シミュレーションしたりして，ユーザや開発者の確信度を高めたり，漏れに対する気づきを促したり，テストケースを生成したりすることができる（モデル発見，仕様アニメーション）．
- 原子力や航空などのミッションクリティカルな領域において，コストをかけて高信頼性を確保するためのアプローチである．
- 様々な領域において，品質確保のためにかけるコストを上流に移すこと（フロントローディング）により，手戻りによるコスト増大を防止し，全体のコストを下げたり，実装・テスト段階に負荷が集中することを避けたりするためのアプローチである．

これらの答えそれぞれは，正しいとも言えるし間違っているとも言える．というのも，形式手法という言葉は総称にすぎないからである．具体的な手法やツールは多種多様である（VDM, B, Event-B, Alloy, SPIN, UPPAAL など）．さらに，それらの手法・ツールを直接利用しなくとも，その裏にある原則，考え方を，日本語仕様の記述規約や DSL (Domain Specific Language) の文法，レビュー方法やレビュー基準などに埋め込むことにより，手軽に活用できることも多い．

結局のところ，個々の手法，ツール，その裏側にある原則，考え方に対し，それが対象とする問題と効果，限界を十分に理解，実感した上で，組織やプロジェクト，開発対象の性質に応じた活用方法を定める必要がある．加えて，形式手法の利用によってある問題に対処できそうだとしても，学習，移行や運用の課題もあれば，他にも考えなければならない問題が多々あるため，総合的な施策の整理，構築が求められる．

3. 演習コースⅡにおける取り組み

本演習コースでは，前述の背景を踏まえ，下記 2 つの観点からの取り組みを行う場を参加者全員で作り上げることを目指している．

（1） 形式手法の考え方も踏まえての，仕様記述における問題解決の模索と議論
（2） 特定の手法・ツールの学習と活用に向けた検討

まず準備段階として，5～6 月においては，最も手軽な手法として国内での知名度が高い VDM を中心として講義，演習を行った． VDM は，構造化プログラミングやオブジェクト指向に基づいてのモデリングや，解釈実行を通したテストなど，一般の開発者にとって馴染

みのある記述・検証方法を用いる手法である．また日本語でのツール利用や情報取得が行いやすく，国内における適用事例もよく知られている［VDMTools，Kurita10］．

このように，VDM を一例として形式手法全体に関する理解と実感を得た上で，7 月の合宿以降は，各参加者の要望，興味，悩みに応じてグループ分けと取り組みテーマの決定を行い，実際の取り組みを行った．上記（１）については，研究の取り組みとして，課題を分析し，達成目標とアプローチを定め取り組んだ．（２）については，それぞれのグループで対象とする手法・ツールを定め学習した．ただし，学習の後半においては，自身の問題意識に対応した活用のための検討を行い，理解を深めるように心がけた．

グループごとの取り組み概要を下記に示す．詳細については演習コースⅡの論文，報告書をご参照いただきたい．

（１）に関する取り組み

- 自然言語による仕様に対する構造化により，合目的性などを向上しようとする USDM と，VDM を効果的に併用する仕様記述手法を検討し，提案した．

（２）に関する取り組み

- 網羅的な状態探索に基づく検証を行うモデル検査ツール SPIN や SMV について学習した．また，半日など短期間でその位置づけなどを学ぶための教育コースを構築した．
- 時間制約の検証も扱うことができる実時間モデル検査ツール UPPAAL について学習した．また，勘違いや理解不足が起こりやすい，時相論理による検証項目の記述に対し，多数の基本的な記述例を用意し，学習や活用において参照できるようにした．
- 仕様に対して，それを満たすデータや実行列などの例を網羅的に生成することができる手法 Alloy について学習した．また，テストケースの生成ロジックに対する挙動確認を試行し，その活用可能性について検討した．

4. まとめと展望

ここまで述べたように，形式手法と一口に言っても多種多様な側面を扱っている．また仕様記述から，システム分析における妥当性確認，設計の検証，テストとの連動など，様々な活用の可能性がある．限られた時間において，様々な可能性を模索したり，特定のアプローチをしっかり使いこなせるようになったりすることは難しい．しかし本コースでの経験を基に，参加者が継続的に適応，進化を続けていって欲しい．

コース自身のあり方としては，「各参加者が成長した」ということだけでなく，取り組みにおける成果物を積み重ね，コース全体として成長し成果物を出していくことが重要と考えられる．いずれにしても，主査，副主査も含めメンバ全員でアプローチを議論し，楽しく進めていきたい．

（文責：石川 冬樹）

参考文献

[Feiler09] Peter H. Feiler et al (2009). System Architecture Virtual Integration: An Industrial Case Study. Technical Report CMU/SEI-2009-TR-017, Carnegie Mellon University

[MRI11] 三菱総合研究所・経済産業省 (2011). フォーマルメソッド導入ガイダンス. http://formal.mri.co.jp/

[DSF11] Dependable Software Forum (2011). 形式手法活用ガイドなど. http://www.nttdata.co.jp/dsf/

[IPA10] IPA (2010). 形式手法適用調査 . http://sec.ipa.go.jp/reports/20100729.html

[VDMTools] SCSK 株式会社. VDM information web site. http://www.vdmtools.jp/

[Kurita10] 栗田 太郎 (2010). モバイル FeliCa のソフトウェア開発における品質確保のための構造と実践　抽象度の制御やコミュニケーションの活性化に向けて. 情報処理学会デジタルプラクティス Vol.1 No.3