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（フェリカネットワークス株式会社）
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にはまだその実際は馴染みがない．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，形式手法における原則を実感した．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，様々な手法の学習や活用模索を行った．

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]．なお，VDM

およびその他の手法について，8 月に追加のセミナーも 2 回行った．

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つつ，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，各自で対象とする手法・ツールを定め学習や取り組みを行った．

各自の取り組み概要を下記に示す．（1）の詳細については演習コースⅡの論文をご参照いただきたい．

（1）に関する取り組み

- テスト駆動開発の考え方を応用し，高い確信度を保ちつつ仕様記述を進め，また事後条件などの検証を系統的に行う手法を提案した．（伊藤）

（2）に関する取り組み

- 典型的な Web アプリケーション仕様書に関し，IPA による機能要件の合意形成ガイドで「コツ」として述べられている要点も踏まえた，VDM++言語での記述構造を検討した．

  IPA による形式手法適用手順を参考に、Web アプリケーションの画面機能仕様書に記述されている内容を構造,機能,振る舞いに分け、VDM++言語で記述した(図 1).そのうえで、機能要件の合意形成ガイドの「コツ」から，仕様記述において注意すべき事柄を抽出し比較を行った．

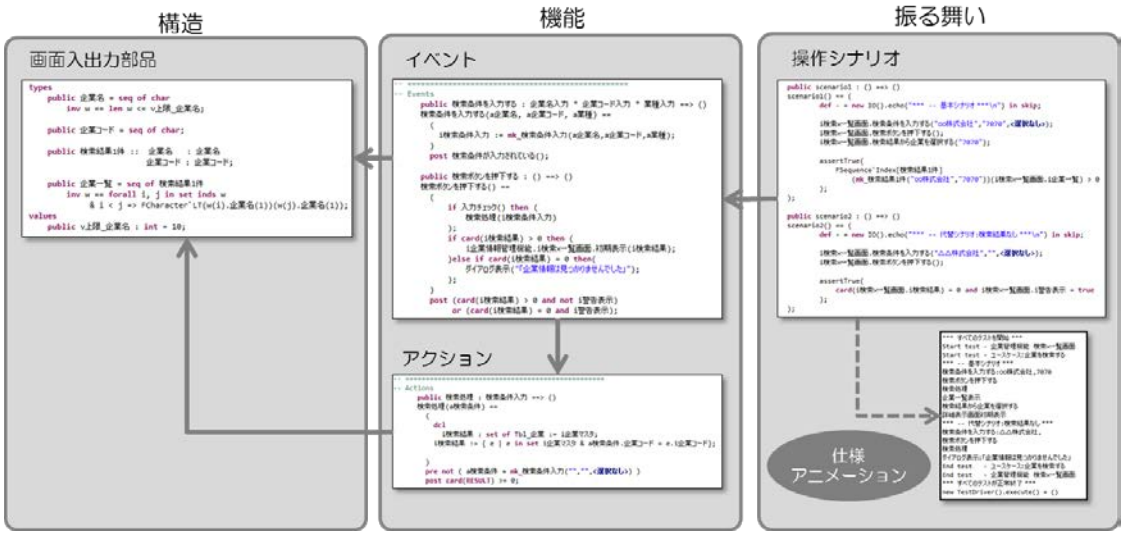

図 1 画面機能仕様書の VDM++言語での記述構造

比較を行った結果,特に以下のような点について効果を実感することができた．

- VDM++で記述するためにモデルを考える過程で,共通化すべき項目(入出力項目やフォーム)の洗い出しが促進される．
- 名詞や述語を厳密に定義するため，勝手熟語や略語を排除しやすい.また,ガイドに記載されている用語の表記の統一だけでなく，用語自体の定義により本質的な理解を促す．

今回は簡単なサンプルへの適用であったため,比較的短時間で記述することができたが,実際の業務において集合論と述語論理を用いて仕様をコンパクトに記述するのは,まとまった学習機会,経験が必要であると感じた.しかし,うまく表現することができれば,似通った入出力項目や用語・ルールが多く存在するようなエンタープライズ系 Web アプリケーション仕様書への適用に,効果が期待できると考えられる．（圓通）

- 組織・チーム・プロジェクトなど，複数レベルごとに定義された開発プロセス定義

に対し，レベル間の整合性検証の意義やその方法について検討した．
レベル間の整合性検証への形式手法適用については，上位プロセスの遵守を証明するために有効であると推測される．また，プロセスの記述・検証に適した手法については，検査ツールの検査能力の高さから Alloy を第一候補に検討を進めたが，より適切な手法の調査については今後の課題としたい．（亀田）

- 自社における工場生産設備の制御仕様書の改善を目指し，日本語，状態遷移表，VDM++など複数の仕様記述方式の比較や，VDM++による仕様記述の試行に取り組んだ．
  仕様記述の比較結果は下表となり、自社の問題を改善できる可能があるため、今後、実際に VDM++を制御仕様の一部へ適用して効果を判断したい．（降旗）

仕様記述	理解の容易度	厳密な表現	全体イメージがつかみやすい	状態組合せの検討	モデルの動作検討	記述の規則検査
日本語	○	×	×	×	×	×
ステートマシン図	△	×	○	△	×	×
状態遷移表	△	×	×	○	×	×
VDM＋＋	×	○	×	×	○	○

- 仕様書を記述する際には，用語・文・文章・段落・文書・構成といった，いくつかの枠組みを考える必要がある．その中から，本年度は「用語」と文章の中の基本の単位である「文」の厳密な定義について考えるため，ビジネス文書などの形式記述を行うための OMG（Object Management Group）による標準 SBVR（Semantics of Business Vocabulary and Business Rules）を素材として活用することを検討した．
  SBVR には，自然言語(英語)上でビジネスルールに用いる語を構造化して定義する方法や，「ファクトタイプ」と呼ぶ名詞と動詞から成り立つ文の関連・表現法が，論理学用語と合わせてまとめられている．これまで，仕様書の記述があいまいな場合，どのように詳細化していくかという点について，知見を得られていなかったが，SBVR のビジネスルールの作り方を活用することで，仕様文の詳細化につながるということがわかった．さらに，SBVR の構造化された用語定義の例は，日本語で仕様書の用語集を作成する際にも参考になると思われる．しかし，SBVR のような構造化用語定義ができるようになるまでには，根本的な意味を抽出して表現するための高度な言語力，抽象化と概念化の能力が求められるうえ，仕様書で用いる語は数も多く，個人の努力だけでは困難であると思われる．そのため，SBVR を日本語でわかりやすく紹介するなど，組織的に取り組むための基盤づくりが必要であると感じた．（宮本）

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.com/jp/ja/dsf/index.html

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