2016 年度「形式手法と仕様記述」 実施報告

Report on “Formal Methods and Specification Description” FY2016

主査　　：栗田　太郎（ソニー株式会社）
副主査　：石川　冬樹（国立情報学研究所）
研究員　：酒井　雄太（キヤノンアイテック株式会社）
　　宮本　陽子（株式会社メタテクノ）

研究概要
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]．

今年度の参加者は VDM の学習経験および，各自の課題意識が明確にあったため，夏以降は各自による（１）の取り組みに集中的に取り組んだ．

4.　各取り組みの概要

以下では 2016 年度に行った 2 つの取り組みの概要について紹介する.

4.1　さまざまな視点に合わせた仕様書の作成・維持の支援手法（酒井）

読み手に応じて様々な抽象度・視点の仕様記述を準備するために工数がかかるという問題,また複数の記述に対する維持が難しく不整合が生じやすいという問題に対処するため,VDM を中心とした一つの仕様記述から，読み手のさまざまな視点に合わせた仕様記述を生成する手法に取り組んだ．この取り組みについては別途報告書にまとめているのでそちらをご参照いただきたい[Sakai16].

4.2　文章作成用フレームワークの開発と導入（宮本）

(1.1) 背景

ソフトウェア開発においては，仕様書や設計書などの文書を作成する機会が多く,その質の良し悪しが,開発スケジュールに影響することもある.そのため,私の組織においては,文章作成能力（以下,文章力とする.）の向上が重要な課題となっている.

これまで私の組織では，文章力向上の取り組みとして，2～4 年目程度の若手社員を対象とした文章の基礎を教える集合研修と，開発現場での OJT を実施してきた．しかし，これらの取り組みだけでは，期待通りに文章力が伸びず，若手社員の文章には下記の課題がある.

【若手社員の文章に関する課題】

① 文章を通して誰に何を伝えたいのか，意図をつかみにくい文章がある.

② 思いつくままに書いた文章が多く，論理的なつながりがわかりにくい.

(1.2) 研究テーマ

前述の課題①は，まず「文章の目的」と「読み手」を想定することが文章作成の基本であるが，定着していないことが問題であると考えた．そのため，定着を促す仕組みを検討することにした．課題②は，下図 1 に示す文章作成に必要な能力のうち,「論理構成力」が育成できていないことが問題であると考え，本研究のテーマを下記とした.

研究テーマ「文章の目的と読み手の想定を促す仕組みの開発，および，思考の整理と論理構成の検討を促すためのフレームワークの導入」

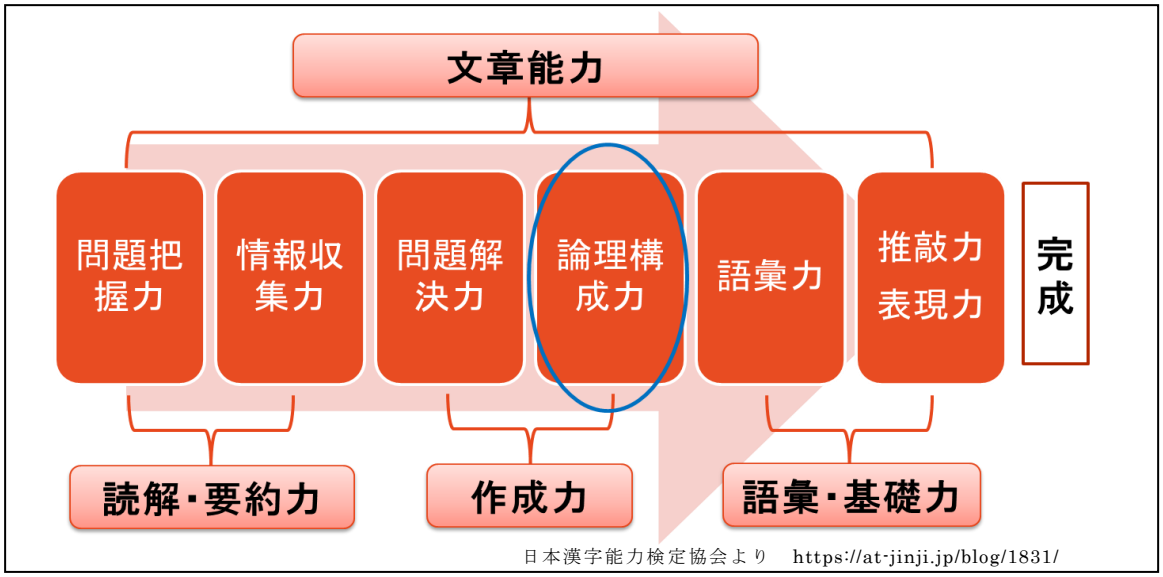

図 1：文章作成に必要な能力（文章能力）と本研究での主眼

(1.3) 研究方法

研究の方法は，次の手順で行った．

１）文章作成時に用いるフレームワークとして「文章の設計図」[Umejima15]の導入を検討した．「文章の設計図」はそのままの形式で導入してもよいが，目的と読み手の検討を促すために一部を改良した．改良後のフレームワークを下図 2 に示す．

２）改良後のフレームワークを集合研修で若手社員 11 名に伝え，研修後のアンケートにより，改良後のフレームワークを使用した感想や意見を集めた．

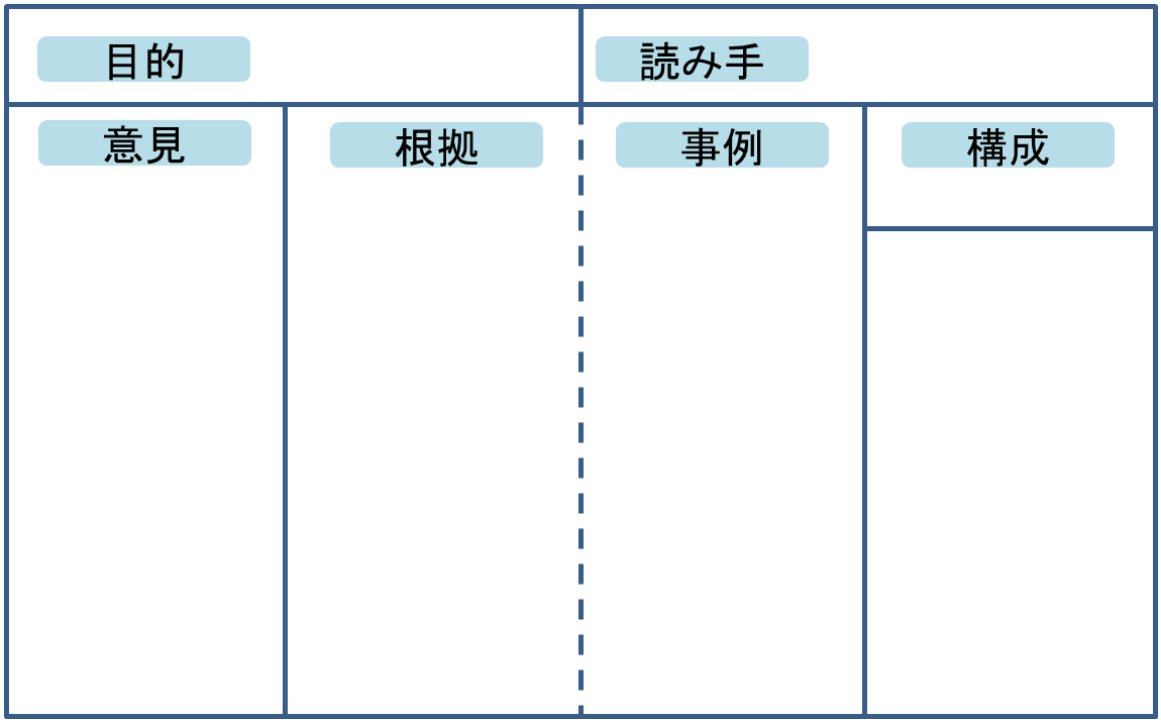

図 2：改良後のフレームワーク「文章の設計図」

(1.4) 研究結果

研修後のアンケートを分析した結果，改良後のフレームワークを用いた研修は，11 名の参加者全員から有用であるとの回答を得た．有用性を質問した回答結果を下記に示す．

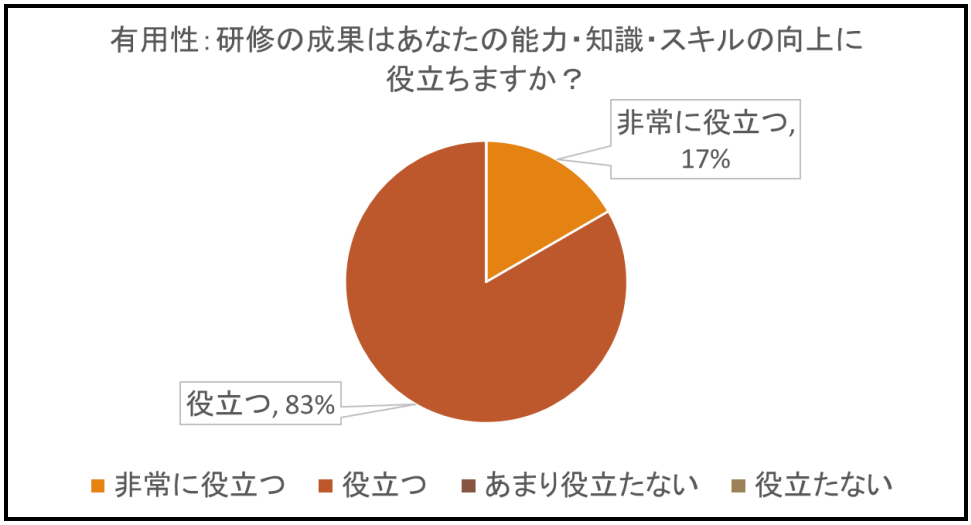

図 3：フレームワークを用いた研修の有用性（研修後アンケートより）

また，改良後のフレームワークを使用した感想から，主な意見を抜粋し下記に示す．

【受講者アンケートの感想より】

- 設計図という形式が視覚的にわかりやすいと思った．また，その設計図の説明がわかりやすかった．自分で設計図を作る点も良かった．
- 小論文の構成だけでなく，業務のドキュメント作成でも活かせそうだと思った．
- このような文章の設計を考えたことがなかったので，参考にしたい．
- メール作成や設計書作成などの際に活用できると思う．
- 数分で設計図を記載するのが難しかった．
- 研修中にもう少し実践する時間があるとよかった．

(1.5) 研究テーマに対する考察

研究テーマ「文章の目的と読み手の想定を促す仕組みの開発，および，思考の整理と論理構成の検討を促すためのフレームワークの導入」のうち,「文章の目的と読み手の想定を促す仕組みの開発」に対しては，フレームワークに文章の目的と読み手を記載するという 1 段階を追加することで大きな負荷を与えずに実践できた．文章の目的と読み手は，文章作成時の基本として重要な点であるものの，文章を書くことに夢中になるあまり，忘れてしまうこともありうる．フレームワークに明記しておくことにより，文章作成に夢中になっても，立ち返って考えなおすことができるとわかった．

研究テーマのうち,「思考の整理と論理構成の検討を促すためのフレームワークの導入」に対しては，集合研修で文章の設計図という考え方と仕組みを紹介し，実践することで，思考の整理や論理構成の重要性と難しさを実感してもらえた．

また，集合研修では小論文を作成するという前提のみでフレームワークを利用していたが，参加者から業務のドキュメントやメール作成などにも活かせそうだという感想を多く得た．文章作成時にはフレームワークを使うことを習慣にしてほしいと願っていたため，よい兆候だと思われる．

(1.6) 今後に向けて

今回の研究では，文章作成時のフレームワークの開発と導入にとどまっているので，導入したことにより，どのような効果が得られたかについて，さらに研究を続けたい．

また，文章作成能力のうち，論理構成力以外の力を伸ばす方法についても研究したいと考えている．

5. 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．

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らびに参考資料
http://www.ipa.go.jp/sec/softwareengineering/reports/20120928.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
[Sakai16] 酒井 雄太 (2016). さまざまな視点に合わせた仕様書の作成・維持の支援手法. 日本科学技術連盟 第32年度ソフトウェア品質管理研究会 演習コースⅡ
[Umejima15] 梅嶋 真樹他 (2015). 論理コミュニケーション〔第2版〕. 慶應義塾大学出版会株式会社