# 形式仕様記述（基礎・VDM 編）

平成２４年度シラバス

２０１２年1月13日

国立情報学研究所

トップエスイープロジェクト

代表者　本位田　真一

## 1. 講義名

形式仕様記述（基礎・VDM 編）

## 2. 担当者

石川　冬樹

## 3. 本講義の目的

本講義では，形式仕様記述と総称される手法の基本的な考え方について学びます．形式仕様記述においては，ソフトウェア開発の上流成果物，特に機能仕様の，形式仕様言語を用いたモデル化・記述と，それに基づいた分析・検証を行います．形式仕様言語とは，（プログラミング言語のように）厳密な文法・意味論を持つ言語であり，「何をするシステムを作るのか」を抽象的に記述するのに適したものです．言い換えると，「計算機上でどう作るか・どう動かすか)」を捨象した形で記述するのに適したものです．

形式仕様記述言語の効果としては第一に，厳密な記述を行う過程において，思い込みや誤解の原因となる曖昧さを排除することができます．第二に，厳密な記述を行うことにより，特にツールを用いての科学的・系統的な検証の可能性が大きく広がります．

本講義ではまず，代表的な手法の一つである VDM の学習を通し，形式仕様記述の基本的な考え方を学びます．VDM は，言語構文やその典型的な活用方法などにおいて，現状の一般的な開発者にとって馴染みやすい，ライトウェイトな手法となっています．このため本講義では VDM を形式仕様記述の活用への第一歩として学びます．

ここで，単に VDM に関する知識を得るだけでなく，実際のモデル化・記述や分析・検証の体験を通して，形式仕様記述や VDM における利点と限界，適用の際の留意点や課題などを実感，理解，議論することを目指します．

加えて本講義では，VDM を用いた体験を踏まえて比較を行うことにより，自然言語や図表による記述，他の形式手法・ツールのアプローチなども俯瞰的に議論します．これにより，VDM という一つの道具にとらわれず，仕様のあり方や記述・検証に関する原則を理解し，課題に応じた様々なアプローチを議論するための素養を身につけることを目指します．

## 4. 本講義のオリジナリティ

特定の手法に関する知識・スキルの習得に限らず，以下に取り組む点が特長である．
実在する先端的な標準仕様を題材としたグループ演習をはじめとして，現実に必要となるモデル化や検証の方針に関する検討，議論を行い，実際の適用の際に必要になる検討事項を実感し，意見を交え議論し，自身で実践する．

VDM に関する実際の体験を得た上で，様々な手法・ツール（B，Event-B，Alloy など）について俯瞰的に比較，議論することにより，形式仕様記述における共通の原則と異なるアプローチについて理解を深める．

## 5. 本講義で扱う難しさ

仕様をはじめとした開発上流の成果物における品質（特に信頼性）を確保することは非常に重要です．そのためには系統的に，成果物に対する信頼性の基準を設け，その基準を満たしているかどうかを検証する方法・過程を定めることが必要となります．しかし厳密な文法・意味論がない言語（日本語や多くの図表）を用いた場合，基準に対する明確な定義と効率的な検証，双方において多くの困難がつきまといます．本講義ではそれらに対し，形式言語を軸とした解決の考え方について扱います．

ここで情報システムは，非常に多様な側面を持ちます．本講義ではその中で，情報の管理という最も重要な側面を主に扱います．すなわち，まず情報の構造やその保持・操作について，システムが達成すべきことを明確に定義することを考えます．その上で，処理の結果が意図通りの情報になるか，不整合のある情報になっていないか，といったことを検証することを考えます．

## 6. 本講義で取得する技術

本講義では、モデル規範型形式仕様言語による，ソフトウェアの機能仕様の記述における原則を学びます．すなわち，不変条件や事前・事後条件を正しさの基準として系統的に定めることや，それらを通して「システムが何をするか（What)」を，「どう作るか・どう動かすか（How)」を捨象して厳密に定義することに関し，必要な考え方を身につけます．

本講義では，一手法として VDM を取り上げ，上で述べた記述の考え方について具体的に学びます．加えて検証に関し，最も採り入れやすい方法として，仕様の解釈実行を用いたテストの方法について学びます．ただし VDM 以外の手法についても触れ，定理証明や（有界）モデル検査，モデル発見，段階的詳細化といった一般的な概念についても学びます．

## 7. 前提知識

本講義の受講生は，下記の基礎知識を有していることが望まれます．

- ソフトウェア工学に関する基礎知識．特に，開発プロセス，上流工程やその成果物（要求仕様や機能仕様，設計など）の役割，オブジェクト指向．
- プログラミング言語に関する基礎知識．
- 集合論，命題論理，一階述語論理に関する基礎知識（「基礎理論」講義の一部)．

## 8. 講義計画

（実際の講義時間の配置などにより多少変更することがあります）

第１回　イントロダクション

- 形式手法・形式仕様記述の考え方
- VDM の概要と位置づけ
- 本講義の狙い・内容

第２～３回　VDM 基礎

- 抽象的な仕様記述のための基本的な概念，構文
- ツールの基本的な利用方法

第４～５回　VDM による仕様記述演習

- 様々な記述の要素・構文

第６～７回　VDM 中規模例題

- 様々なモデル化方針
- 仕様記述における考え方

第８～９回　VDM の活用

- 言語・ツールの発展事項
- 現状の利点と限界

第１０～１１回　VDM グループ演習

- グループ演習・発表

第１２～１４回　形式手法と仕様・設計記述における様々なアプローチ

- 記述のアプローチ（自然言語，図表，他の形式言語など）
- 分析・検証のアプローチ（証明，モデル検査，モデル発見，段階的詳細化など）

第１５回　まとめ・今後に向けた議論

- 事例・動向紹介

他の手法・他の技術・他の講義との関連

- 直接的・間接的な活用に向けて

## 9. 教育効果

講義を受講することにより，形式仕様記述の手法・ツールを利用するための基本ノウハウ，およびその裏にある仕様や設計において誤解や誤りをなくすための原則，基本ノウハウを習得できます．これらのノウハウを各開発プロジェクトの特性に合わせて適用することにより，開発の信頼性・効率を高めることができます．

## 10. 使用ツール

本講義では，以下のツールを利用します.

- VDMTools（VDM-SL Toolbox，VDM++ Toolbox）
- Overture IDE

## 11. 実験及び演習

主に VDM を用いて下記に関する演習を行います.

- 仕様記述の明確化・構造化
- 抽象的なデータ構造・操作の，厳密な定義
- 不変条件，事前条件・事後条件の定義，記述
- 実際の仕様記述におけるモデル化・検証方針の議論，決定

## 12. 評価

3 回のレポート課題を通して評価します.

## 13. 教科書

資料を配付する

## 14. 参考書

- VDM++による形式仕様記述
  石川 冬樹，荒木 啓二郎（監修），近代科学社，2011
- VDM++によるオブジェクト指向システムの高品質設計と検証
  J. Fitzgerald ら，酒匂 寛（翻訳），翔泳社，2010
- ソフトウェア開発のモデル化技法
  荒木 啓二郎ら（翻訳），岩波書店，2003
- プログラム仕様記述論
  荒木 啓二郎，張 漢明，オーム社，2002
- 形式手法活用ガイド，
  Dependable Software Forum， http://www.nttdata.co.jp/dsf/ ， 2011
- フォーマルメソッド導入ガイダンス
  三菱総合研究所， http://formal.mri.co.jp/ ， 2011
- 「形式手法適用調査」報告書
  情報処理推進機構 ソフトウェア・エンジニアリング・センター（IPA-SEC），
  http://sec.ipa.go.jp/reports/20100729.html ， 2010

他の手法・アプローチ，応用事例，ソフトウェア工学の原則などについては，その他の書籍，報告書，論文も適宜引用します.