

【講座シリーズ担当】

・・・1・・・

[講座シリーズリーダー]

来間 啓伸

国立情報学研究所 特任教授 / 日立製作所

研究分野：形式手法, コンピュータ・セキュリティ

・・・2・・・

桑野 文洋

国立情報学研究所 特任准教授 / 三菱総合研究所

研究分野：形式手法, ソフトウェア工学教育

・・・3・・・

田辺 良則

国立情報学研究所 特任准教授

研究分野：ソフトウェア検証, モデル検査, 様相論理, 形式検証技術

・・・4・・・

石川 冬樹

国立情報学研究所 助教

研究分野：形式手法, サービスコンピューティング

## 【本講座コースの基本思想・特徴】

本講座シリーズでは、ソフトウェアの仕様をどのように記述するか、仕様の正しさをどのように検証するかについて、形式仕様記述言語を使って学習します。形式仕様記述言語の意味規則は、数学的基盤のもとに厳密に規定されています。このことから、人間にとって仕様をあいまい性なく解釈できるだけでなく、計算機にとっても仕様を正確に解釈することができ、仕様の整合性の機械的なチェックが可能になります。その一方、ソフトウェアの仕様を最初から厳密に記述することは困難ですし、仕様は最終的にプログラムとして実現されなければ意味がありません。ソフトウェア工学的な観点からの仕様記述とプログラム構成の過程は、形式仕様記述においても重要な要素です。

本講座シリーズは、基礎編、応用編、セキュリティ編の3つの講座から構成されています。基礎編と応用編では形式仕様記述の基本テクニック、特にデータの制約をどう表現し検証するか、について学びます。セキュリティ編では、形式仕様記述の適用例としてセキュア・システム開発での使い方について学びます。なお、形式仕様記述言語にはそれぞれ特徴があり、ソフトウェア開発での使い方が異なります。そこで、各講座では複数の形式仕様記述言語を使い、異なる仕様記述／検証スタイルを示します。

基礎編では、仕様記述についてBメソッドとVDM-SLを使って学びます。Bメソッドは、集合記法と一階の述語論理に基づく仕様記述言語と、仕様の整合性を論理的に検証する方法を与えます。講義では、集合記法による仕様の表現と仕様の整合性の検証の、基本的な考え方を学びます。VDM-SLは実行可能な仕様を記述することが可能であり、仕様の正しさを実行によって確認することができます。講義では、実行可能な仕様を作成した後に仕様にデータを与え、直接実行して振舞いを検証します。

応用編では、仕様からプログラムへの段階的詳細化技術についてBメソッドを使って学び、テストング技術を用いた仕様検証方法についてVDM++を使って学びます。段階的詳細化技術は、抽象的な仕様からプログラムに近い具体的な仕様へ、正しさを確認しながら変形する技術です。講義では、詳細化の正しさを検証するための、基本的な考え方を学びます。VDM++はオブジェクト指向設計のモデル化を行うようVDM-SLを拡張したものであり、近年でも言語、支援ツールともに様々な拡張が行われています。講義では、テストングフレームワークの利用や外部ツールとの連携等、VDM++を実際に活用していく過程について学び議論していきます。

セキュリティ編では、セキュリティポリシーの記述と整合性検証を題材に、段階的詳細化、定理証明、モデル検査の3つの検証技術を適用します。ポリシー記述には、Event-B、Z記法、Promelaを使いますので、モデル検査講座シリーズと形式仕様記述講座シリーズの検証技術の集大成とも位置付けることができます。

いずれの講座でも、開発支援ツールを利用した仕様記述と検証の実習を行います。ツールは、仕様記述／構文チェック／型チェックだけでなく仕様の直接実行あるいは証明も支援しますので、形式仕様記述言語を使ったソフトウェア開発過程を実践的に学ぶことができます。

このように、本講座シリーズでは正確な仕様記述や仕様の整合性の検証方法さらにはプログラムの導出過程について、厳密な理論に基づいて学習します。本講座シリーズの目的は、信頼性の高いソフトウェアを開発できる技術者を育成することにあります。

### 【該当講座】

- ・ 形式仕様記述（基礎編） [ 石川 冬樹 ・ 来間 啓伸 ]
- ・ 形式仕様記述（応用編） [ 石川 冬樹 ・ 来間 啓伸 ]
- ・ 形式仕様記述（セキュリティ編） [ 来間 啓伸 ・ 田辺 良則 ・ 桑野 文洋 ]

## 【演習のひとつま】

アドホックネットワークはメッセージ中継機能を持つ端末から構成される「一時的な」ネットワークであり、各端末が協調してメッセージを伝達することで、直接通信できない端末間でもメッセージ送受信を行うことができる。ここで、適切なメッセージ転送を行うためには、各々の端末が直接通信できる周囲の端末から情報を得て、ネットワーク内の端末の通信関係を計算する必要がある。この手順はルーティングプロトコルによって定められているが、それが正しいことを確認しなさい。すなわち、ルーティングプロトコルにしたがって各端末が処理を進めれば、各端末の局所的な通信関係の情報が他の端末に伝播され、最終的にはネットワーク内の全ての端末が全ての通信関係の情報を持つことを確認しなさい。ここで、通信関係は十分長い時間変化しないものとするが、その他に必要な前提があれば明らかにしなさい。