2011年度　第 6 回特別講義　レポート

日時	2011 年 11 月 18 日（金）　10:00～12:00
会場	(財)日本科学技術連盟・東高円寺ビル　2 階講堂
テーマ	「形式手法って何？　～その特質と効用について～」
講師名・所属	荒木　啓二郎氏　（九州大学大学院システム情報科学研究院）
司会	栗田　太郎氏（フェリカネットワークス(株)）
アジェンダ	・ 形式手法の歴史 ・ 形式手法の特質 ・ 実践のポイントと適用事例
アブストラクト	形式手法（フォーマルメソッド）に対する認識を周りに聞いてみると、「新しいソフトウェアの開発技術らしい」、「難しい数学を使うらしい」など多くの誤解が見受けられる。今回はそれらの誤解を解いて、形式手法の出自や役割、国内外での適用事例、現場で実践する際のコツなどを紹介していく。（書記の小田部が記す）

＜講義の要約＞

◆形式手法の歴史

ヨーロッパでプログラムの正しさを検証しようと言う話が 1960 年代からあり、1970 年代には検証理論に関する研究に発展し、様々な形式仕様記述言語や方法論、ツールが開発されていった。そして、形式手法における記述方法は、何時誰が見ても一意に記述内容を解釈出来るよう厳密に記述しようとする過程で、自然と数理論理学に基づくものとなっていった。

現在では 30 年以上の歴史と 100 種類以上の手法があり、分析や設計、検証など、様々な分野に適用されている。またソフトウェアの高信頼化に伴い形式手法の必要性は増し、ISO や IEC などの国際標準規格で形式手法が推奨され始めているので、国際的な活動をする際にも必要になって来ている。

◆形式手法に関する社会通念（スライドからの引用）

[J.A.Hall:Seven Myths of Formal Methods, IEEE Software, Vol.7, No.5, pp.11-19, 1990]

以下の誤解が世間でよく言われている。

・ソフトウェアが完全であることを保証できる

・須くプログラムの正しさを証明するためのものである

・セーフティクリティカルシステムにのみ有効である

・高度に訓練された数学者を必要とする

・開発コストを増加させる

・ユーザに受け入れられない
・現実の大規模ソフトウェアには使われない

◆形式手法に関する事実（スライドからの引用）
[J.A.Hall:Seven Myths of Formal Methods, IEEE Software, Vol.7, No.5, pp.11-19, 1990]
実際は以下の効果を期待できる。
・開発初期段階での誤りの発見に有効である
・開発対象のシステム自体を深く考えさせることに寄与する
・いかなる応用分野にも有効である
・数学を基礎とはしているものの、プログラムよりは理解しやすい
・開発コストを減少させる
・顧客が購入しようとしているものの理解を助ける
・産業界における実用プロジェクトに用いられて成功している

◆難しい数学が必要か？
形式手法のベースとなる知識には、基礎的な集合論、論理学、帰納法等である。これは基本情報技術者試験のレベル2のシラバスに載っている程度の知識なので、受講している皆さんの多くは問題なく形式手法を習得出来るだろう。

◆形式的（数理的）モデルの構成手順
要求定義書を読み、潜在的なデータ型と機能を抽出する。名詞に着目するとデータ型、動詞に着目すると機能が抽出できる。抽出したデータ型の詳細は未定のままでも抽象化モデルでは様々なことを記述できる。例えば名前や生年月日のデータ型が開発のある時点で決まっていない、または決められなかったとしても、その時に定めている範囲でデータを定義可能であり、データ同士の対応関係の記述が行える。その後必要になったときに具体化を行えばよい。
重要なのは、データ型の構成だけを考えるのではなく、システムをシステムたらしめるデータの制約条件を見つけて明記することである。記述上の注意点は、何をするのか（What）を記述することで、どう解を得るか（How）は記述しない。

形式手法では仕様記述段階での検証が可能になることで、従来はプログラムを動作させて初めて明らかになる不具合の除去が可能になり、手戻りを減らすことが出来る。また厳密に書かれた成果物を読み取ることで記述対象への理解と技術の習得が促進され、知識の共有と継承へとつながっていく。

◆実践のポイント
管理職の意識が重要である。最初は進捗していないように見えても我慢する。また形式手法への関心や期待が推進力となり、担当ドメインエキスパートの意欲へ影響する。
形式手法の厳密な記述と議論に対し最初は戸惑うが、理解が進むにつれ新鮮な感動へと変わってくる。形式仕様記述言語は読むのは難しくないが、書くには言語仕様や記述対象への理

解、抽象化の能力、モデル化やイディオムの知識や経験が必要になる。また、慣れてきた段階で、チームビルディングなど維持継続の努力と支援が重要である。

日本語の教材も出そろってきたので是非学んでいって欲しい。また普段から相談相手がいることも重要である。社外のコミュニティなども活用して欲しい。

◆形式手法の十戒（スライドからの引用）

[J.P.Bowen & M.G.Hinchey: Ten Commandments of Formal Methods, IEEE Computer, Vol.28, No.4, pp.56-63, 1995.]

含蓄のある言葉なので覚えておいて欲しい。

・汝、適切な表記法を選ぶべし
・汝、形式化を行うべし、されど過ぐること勿れ
・汝、コスト予測をすべし
・汝、形式手法の師匠を身近に持つべし
・汝、従来の開発法を棄つること勿れ
・汝、十分に文書化すべし
・汝、自らの品質標準を危うくすること勿れ
・汝、独善となるなかれ
・汝、テストすべし、またテストすべし、さらにテストすべし
・汝、再利用すべし

◆検証例：単純な通信プロセス

例えばプロセス A と B が並行動作するシステムにおいて、A と B の 2 つのプロセス間でのメッセージのやりとりで問題が起こらないかについて形式手法を用いて検証することができる。「到達可能木」と呼ばれるモデルを用いると取り得る状態を網羅的に確認することが出来ので、そこからデッドロックの有無や通信チャンネルが溢れないか、また通信チャンネルにメッセージが残り続けないか等を証明することが出来る。

◆適用事例：モバイル FeliCa IC チップ

モバイル FeliCa の開発プロセスでは、仕様の記述と検証に形式手法を適用した。
VDM（形式手法の一つ）での仕様記述が約 10 万行、外部仕様書 677 ページ分とプロトコルマニュアル 383 ページ分、C/C++言語換算で約 11 万行分を記述した。成果としては、2010 年 9 月の時点で不具合件数が「ゼロ」である。

◆講義に対する質問

Q：「要求定義書を読む」とあるが、資料の内容が抽象化可能なレベルに達していない場合はどうすれば良いのか？
A：要求仕様書と数理モデルを行き来してみる。そうすると曖昧な点や不明な点が出てきて、資料の内容そのものが改善される。また私のように開発対象に対する素人が訊いた方が質問しや

すい場合もある。質問から今まで暗黙知や常識として捉えていたものが実はそうではなかったことが分かる事も大事である。また質問に対して「勉強不足」などと言わない／言われないルール作りも大事である。

Q：十戒の「テストすべし」は、必要なテストをするべしと言うことか？
A：形式手法はツール等の使用により、検証（Verification）が容易になる手法であるが、その一方で妥当性（Validation）の確認は苦手で従来通りのテストが必要になる。形式手法で何が出来るか知ることが重要である。

＜講義の感想＞
恥ずかしながら、私自身、講義を聴くまで形式手法が自分の仕事に利用できるとは考えていなかった。「形式手法で記述し直すことで、対象への理解がより深まる」「誰が何時読んでも内容が一意に伝わるように記述できる」点は、上手く使えばドメインの知識を整理した上で、距離が離れた相手同士でも誤解無くコミュニケーションがとれる可能性があり魅力を感じた。