ラーセン教授を迎えて

ー【SEC特別セミナー】形式手法の98導入事例の調査・分析から見る高信頼性ソフトウェア開発の現状（2012年10月23日開催）よりー

SEC 調査役
新谷 勝利

1 はじめに

SEC では、開発の上流工程からの品質作り込みという課題に取り組んでいるが、上流品質技術部会の人材育成ワーキンググループ（WG）では形式手法の導入教材の検討・作成を行い、その成果を公開している。その人材育成 WG の準備会において、海外での動向について広く紹介していこうということを相談し、国際的な形式手法活用調査を実施しているデンマーク・オーフス大学のラーセン教授を招聘し講演していただく計画を立てた。

ラーセン教授はヨーロッパのみならず、日本を含む多くの国で形式手法の実践を支援しており、その活躍はデンマーク国内にとどまらず、EU 域内、日本を含むアジア諸国、ロシア、全米と広範囲に及んでいる。

多忙なラーセン教授の日程調整は、以前から VDM 及びそのツールの日本への導入で教授と協力関係にあった佐原委員にフォローをお願いした。その後、パリでの形式手法会議にて、荒木主査及び佐原委員とラーセン教授との間で、どのような講演内容が日本での形式手法の啓発に有効かを相談していただいた。詳細な内容と流れ、及び具体的な時期などについては新谷が担当し、何回かやりとりをした後、講演内容を以下のように決めた。

「社会の隅々までソフトウェア及びそれを中心とするシステムが構築されている現在、それらの構築を担当する私たちは、プロフェッショナルとして如何なる知見を持つのが望ましいのか。銀の弾丸は無いとされながらも、一つの可能性としての形式手法についての展開、実践、今後についての講演を行う、1 日の SEC 特別セミナーを実施する。このセミナーは一方通行の講演をするだけではなく、参加者との積極的な質疑応答も可能とするようにしたい。」

当日の資料は SEC ホームページからダウンロード可能となっている（http://sec.ipa.go.jp/seminar/2012/20121023.html）。

以降で、講演資料を引用しながら、ラーセン教授のメッセージを再現することとする。

図 1　ラーセン教授（デンマーク・オーフス大学）

2 セッション 1：形式手法の概要

今回の SEC 特別セミナーに参加していただきたい受講者のプロファイルを次のように設定した。

「実務者が大部分であり、必ずしもいままで形式手法について詳しく学習・調査した経験は無い。しかしながら、形式手法を机上の話ではなく実践するとどうなるか、どのように導入出来るのかを理解したいとの思いを持っている。」

SEC 人材育成 WG では、形式手法入門の教材を開発し、パイロット研修コースの実施を通じてその改良を進めてきた。この WG のテーマは、どうすれば形式手法へのある意味「食わず嫌い」を払拭出来るかということであった。この経験も踏まえて、ラーセン教授による最初のプレゼンテーションにあたっては、SEC 人材育成 WG の荒木主査及び WG の各委員から日本での導入にかかわる経験など追加のコメントをしていただいた。

「数学が形式手法の基礎となっている」ため、近寄り難いとい

う傾向があることが実際のようである。そこで、ラーセン教授には、形式手法は数学を基礎にしているが、多くの人が考えるように難しいものではない、という話から始めていただいた。

ただ「数学」というだけで苦手意識を持ってしまう人に対しては、複雑な記号や数式の意味を説明するのではなく、どのようにしたら数学が本質的に持っている抽象化能力を活用してもらえるであろうか。例えば、「ある対象の要素が集まって構成されている」と見えれば「集合論を活用すればよい」ということである。このときに高校で学習する集合論の基本的知識で十分ということである。また、対象を何らかの表現で説明するときに、厳密さの観点では「段階」があることに言及していただいた。なぜなら「形式手法を導入するということは、数学が基礎であるから証明をしなければ使ったことにならない」という誤解があるからである。そうではなく、まずは「背景となる数学の考え方で記述してみる」というのを“レベル 1”とし、次に「ツールの支援で抽象化記述が可能な言語、例えば VDM を使用する」ことを“レベル 2”とする。このアプローチは、実際に世界の多くの形式手法の導入例で実践されている。

例えば、日本における本格的な形式手法導入の例としてしばしば引用されるフェリカネットワークス株式会社においても、信頼性を確保することを意図した部分（モジュール）での信頼性獲得のために十分な成果を出している。私たちは自然言語で表現された仕様書を、コンピュータで実行出来るように C 言語を用いて翻訳し、HOW の記述をしている。このときに留意しなければならないのは、翻訳前の仕様書があいまいであったら、どんなにうまく翻訳をしても良い結果にはならないことである。形式手法導入のレベル 1 及びレベル 2 は、対象に数学の力を活用して抽象化、あるいはモデル化して、WHAT の仕様記述をすることである。形式手法をこの段階で導入することのメリットの一つは、仕様記述言語を利用出来ることであり、WHAT の段階で、従来だと HOW の段階でなければチェック出来なかったことをチェック出来ることである。HOW あるいは実装の段階の前に挙動をチェックすることは、ソフトウェアのような論理対象ではなく、物理対象ではモデル化してその挙動を解析することで実施されている。例えば、航空機の操縦ではシミュレータを作り、空中での挙動を論理的に表現して抽象化している。形式手法をソフトウェア開発に適用するということは、実装の前の段階で、対象に数学の力を活用し、抽象化あるいはモデル化して、シミュレーションするということに他ならない。

3 セッション２：形式手法の導入事例の分析

形式手法には多くの提案がなされているが、実践という観点では、ツールによる支援の豊富さもあり VDM[※1] が代表的なものとなっている。この 2 番目のセッションではまず、1994 年の ConForm プロジェクトから 2007 年の FelicaMobileChip プロジェクト（現在、三代目として進行中）までの 7 つの VDM プロジェクトが説明された。次いで、交通システムへ展開されている形式手法の例として B メソッドが示された。

(1) セッション2の概要

セッション 2 のハイライトは、2009 年に実施された 60 以上のプロジェクト調査からの報告と、2012 年に報告書としてまとめられた Deploy[※2] という EU の 4 年にわたるプロジェクトからの報告である。当報告書は、98 のプロジェクトが同じ様式で整理してまとめられている。

① 2009 年の調査報告

以下の項目がサマリーとしてまとめられている。

- 形式手法導入の将来は明るい。活用状況は報告されており、素晴らしい成功例が出ている
- 形式手法導入例の殆どが軽量の形式手法[※3]
- 形式手法導入にあたり、ツールが極めて重要な位置を占めているが使用容易性にまだ問題がある
- 形式手法導入の決定の助けになる証拠は不十分である
- 形式手法導入の理由はリスク回避のためである
- 形式手法が継続したプロジェクトに活用されたというデータは不十分である
- 形式手法導入に関わるスキルと心理的障壁は依然として高い
- 形式手法導入に対しては、訓練と教育が依然として必須である

② 2012 年の調査報告

以下の項目が定量的にまとめられている。

- 分野別：交通機関に関するものが 30 以上。金融関係が 10 以上。防衛、消費者用電気製品及びテレコムがそれぞれ約 10
- 適用タイプ:実時間システムが 30 以上。分散システムが 25 弱。大量にデータを扱うもの、制御、並列処理、及びハードウェアが 15 程度
- 適用技術内容：仕様記述及びモデリングに 80 以上。形式記述の実行に 50 以上。インスペクションに 40 弱。モデルチェッキングに 30 以上
- 事前経験：51% が以前の経験が大。37% が以前の経験が少。18% が未経験。これは、2009 年調査報告からは明らかな変化で、複数回の経験があることを明確に示している。これは結果として新しい訓練・教育を必要としない
- 品質：88% が改善。12% が以前と変わらず
- 経費：33% が改善。59% が以前と変わらず。8% が以前より悪い
- 期間：25% が改善。55% が以前と変わらず。20% が以前より悪い
- 抽象化に対して効果的：実際に形式手法を導入しないとしても、形式手法の考え方を取り入れるだけでも開発の助けになっている

・テストの自動化に効果的：数千の異なるパラメータを構成してソフトウェアが出来ており、テストケースをすべて手で書くのは不可能
・形式手法を導入したプロジェクトの 80% がツールは十分揃っているとし、7% がそう思っていない
・プロジェクトの 73%が形式手法を積極的に再使用するとし、２%が再利用しない

(2) 2012 年調査報告の分析によるラーセン教授の推奨事項

・「産」は新しい解決策によってシステム全体に対応する製品を早くマーケットに出さなければいけない。一方、「学」は研究及び論文になる問題に偏っているため、システム全体への適用というより小さな差分アプローチが主体であり、それではマーケットに対応出来ない。このような違いを認識した上で両者を結び付ける橋渡しの役割が必要になる。この役割を果たす支援者あるいは組織があってこそ「産学協働」は成立する
・形式手法導入の経験が無い場合、小プロジェクトで試行し成功するアプローチが適切。開発環境を最初から大きく変革しない
・形式手法で全体を記述することはせず従来型開発との並行利用をすることが重要
・B メソッドを交通機関に採用した方法、ロックウェル・コリンズ社がツールチェーンで実施した方法では、長期間のコミットメントが必要
・形式手法に知見が無い場合、まずは教育から始める
・形式手法の適用先として、クリティカルなシステムなどの従来手法では適切に問題解決出来ない分野がある
・形式手法は、どんな問題にも対応出来る万能薬とは考えない
・形式手法導入にあたっては、良い指導者を周りに持つ

4 セッション３：これからのソフトウェア開発と形式手法

今後形式手法の導入を進める分野は、従来手法では不十分で問題がある、と考えられる分野であり、それは計算（Computation）、通信（Communication）及び制御（Control）の 3 分野をカバーする Cyber-Physical Systems と考えられる。この予測から、ラーセン教授が関係するプロジェクトのみでも約 10 億円のファンドを EU から得て計画が進行中であることに留意する必要がある。日本においてもシステムを構成するソフトウェアが社会のインフラの基盤となっているという状況はますます拡大するであろう。Cyber-Physical Systems というものの具体化も進むであろう。既存システムの単なる追加拡張というものではなく、全体的なシステムとしてアーキテクチャ上の統一性が維持され、システムとしての安心・安全は担保されていなければならない。このために、前節でラーセン教授が指摘されているように、「産学協働」が必須であり、それを推進するために「官」の支援も必要になってくる。EU における Cyber-Physical Systems への取り組みは、以下の要素をもって「産官学」で推進されていることに留意する必要があるであろう。

・組込みシステムにおけるシミュレーション機能を取り込んだ DESTECS※4
・システム・オブ・システムズ（SoS、Systems of Systems）への統合ツール環境としての COMPASS※5

これからのシステムは規模も大きく、複数のシステムが相互に関係する SoS に向かうであろうし、SoS では 3 つの C（Computation, Communication, Control）を要素として持つ Cyber-Physical Systems になるであろう。これらは規模も大きく複雑で、相互に関係するが故に、従来の開発手法のみでは必要とされる高信頼性を担保するのは困難であろう。形式手法は万能薬ではないが、極めて重要な手法であることは明らかであると考えている。

5 おわりに

VDM が開発されたのは、1960 年代から 70 年代にかけてであり、決して新しいものではない。またその導入は、遅々としたものではあるが徐々に実績が出てきている。その習得のための教育に企業が投資することは十分に意味があることであると考えている。今後のシステム開発で想定しなければならない事項は、更に大きく複雑なものとなり、それに備える上でも形式手法の学習及び小さなプロジェクトでの形式手法の適用が有効であると考えられる。今回のラーセン教授のセミナーは、それらを教示していただいたものであり心より感謝申し上げる次第である。また、このセミナーの質疑応答において積極的に関与していただいた荒木主査を始め委員の皆様方にも感謝申し上げる。

脚注

※1 VDM：Vienna Development Method, オーストリアのウィーン（Vienna）になる IBM の研究所で 1960 年代から 70 年代にかけて開発された形式手法。その仕様記述言語である VDM-SL は 1996 年に ISO/IEC 13817 として ISO 化。
※2 Deploy：EU における形式手法の実践プロジェクトで、成果が Industrial deployment of system engineering methods providing high dependability and productivity, A. Romanovsky, M. Thomas（Eds）, Springer. November 2012. にて発表予定。
※3 軽量の形式手法：「2. ステップ 1：形式手法概要」に説明されている厳密さのレベル 1 に相当する仕様記述がされている状況を軽量と称している。
※4 DESTECS：Design Support and Tooling for Embedded Control Software というコンソーシアムで、詳しくは、http://www.destecs.org/ 参照
※5 COMPASS：Comprehensive Modelling for Advanced Systems of Systems というコンソーシアムで、詳しくは、http://www.compass-research.eu/index.html 参照