ソフトウェア工学 118－25
（1998．3．11）

パネル

精密ソフトウェア工学のすすめ

司会：大槻 繁（日立）
パネリスト：玉井哲雄（東大），大蒔和仁（電総研），金藤栄孝（日立）

ソフトウェアクリーンルーム手法を始めとする形式的アプローチ，計算の論理，正しい仕様・プログラム等を話題としてとりあげ，ソフトウェア工学の罪・罠・心・夢などについて語り合う．「精密ソフトウェア工学 (Precision Software Engineering)」という新しいパラダイムは，このパネルの一つのメッセージとして位置付けられている．

1．クリーンルーム手法ワーキンググループの活動

「クリーンルーム手法ワーキンググループ」は，ソフトウェア工学研究会のもとに 1996 年 10 月に設立され，同手法をとりまく様々な側面について議論・検討を重ねて来た．

クリーンルーム手法は，1980 年代初頭に Harlan D. Mills の着想に基づいて米国ＩＢＭで開発された複合技術である．理論面での証明・検証技術，品質保証面での統計的品質管理技術，組織面でのチーム技術，さらには，開発パラダイム面でのインクリメンタルモデルなどの技術から構成されている．実際のクリーンルーム手法の適用に当っては，各組織やプロジェクトの文化的な側面や種々の制約から，その一部を導入したり，変形・適合化している．

ソフトウェア工学に関する技術というのは，そのアイディアの提唱から実際に使われるまでには，実用化・適合化に関する活動を数多く伴うものであり．ワーキンググループでは，クリーンルーム手法やこれに関連した技術の実務への適用へ向けた意見交換・技術交流・評価等を行って来た．

ワーキンググループは，下記の方々に参加いただいた．

主査：佐伯元司／東京工業大学，
幹事：大槻　繁，金藤栄孝／日立製作所，西橋幹俊／日本アイ・ビー・エム，
メンバ：秋長弘人／日科技連出版社，網本正直／NEC テレコムシステム，
石橋良造／日本ヒューレット・パッカード，上原　修／NEC，金地克之／東芝，
河野善弥／埼玉大学，染谷　誠／日本ユニシス，友納正裕，中島　震／NEC，
中島　毅／三菱電機，橋口一生／CSK，早川　明／富士通プログラム技研，
古川善吾／九州大学，鶴見佳彦／三菱電機，本吉由紀夫／日立電子サービス，
谷津弘一／日本ユニシス

「精密ソフトウェア工学」は，ワーキンググループの活動を通して筆者等がつかみとったクリーンルーム手法の「こころ」を，ソフトウェア工学の分野で，より広く，より深く効率的に探求して行くために提唱したいと考えているパラダイムである．

「精密ソフトウェア工学」という言葉は金藤栄孝氏による命名であり，その基本的な着想や枠組みについては，1997 年 11 月のワーキンググループの会合にて提唱された．

2. 科学と工学：理論と実践

ソフトウェア工学という分野は，大変間口が広く，さまざまな関連分野から構成されおり，また，複数の分野を統合するところにこそソフトウェア工学の本領があるといっても過言ではない．ソフトウェアに関する開発技術，あるいは，メタ技術は全てソフトウェア工学という名のもとに含めることができる．組織や人間を扱うこと，宗教色の強い技法や手順を扱うこと，精神活動や躾を扱うことも可能である．

一方，学問としての知識の蓄積という視点では，工学には科学を対峙させる必要がある．単に，役に立つ技術の体系として工学を捉えるのならば，極言すれば，ソフトウェア工学では「管理」と「標準化」だけでもよいことになってしまう．工学を学問としての普遍的な知識として権威付けているのは，その裏付けとなる理論があるからである．化学工学には化学が，機械工学には静力学が，電子工学には電子物理学が基礎付けの学問として存立している．ソフトウェア工学の基礎付けはソフトウェア科学という名前で呼ばれることになるが，これは，論理学や数学に近い．この対峙のさせ方は，C.A.R.Hoare が述べている次の考え方に代表されている．

(1) 計算機 ＝ 数学機械
計算機の動作のあらゆる局面は，数学的な厳密さで定義することができる．その詳細は，純粋な論理法則と数学的な確実さで，定義から演繹することができる．

(2) プログラム ＝ 数学的表現
プログラムは， 厳密に，かつ，すべての細部にわたる詳細さで計算機の動作を記述する．

(3) プログラミング言語 ＝ 数学的理論体系
プログラミング言語は，プログラマが仕様を満たすプログラムを開発し，そのことを証明するのに役立つ概念，記法，定義，公理，定理等を含んでいる．

(4) プログラミング ＝ 数学的活動
プログラミングを行なうためには，数学的な理解，計算，証明等の方法を適用することが要求される．

精密ソフトウェア工学では，この「数学的な考え方」を徹底させ，ソフトウェア開発の全ての過程に対し計算の論理や数学的な活動を適用する．逆に，「数学的な考え方」でないものは基礎付けとして使用しない．

ソフトウェア開発の全ての過程に対して適用するということは，C.A.R.Hoare の立場よ

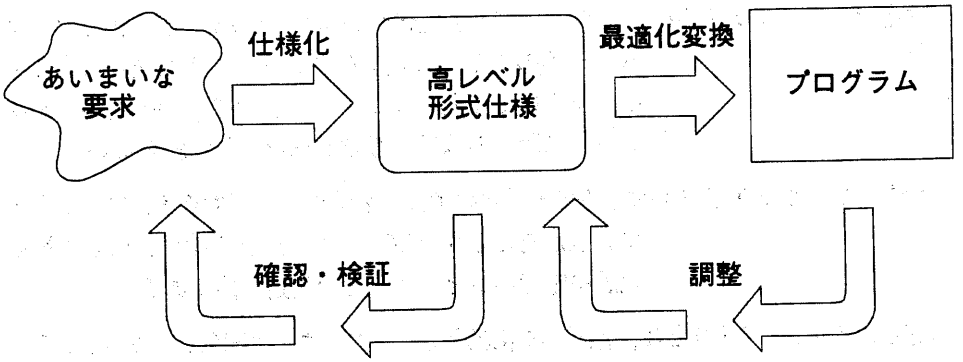
り強いことを意味している．すなわち，問題の定式化，仕様の構築，設計，プログミング，保守に至るまで広範囲に渡って技術構築を試みる必要がある．M.A.Jackson の「問題フレーム」の考え方も，数学の問題の発見や解法に関する「数学的な考え方」を，要求定義や仕様化の領域に援用しようという試みとして位置付けることができる．

クリーンルーム手法は，純粋な精密ソフトウェア工学的手法ではないが，このアプローチの有効性を示唆している．この手法の本質的な技術は検証技術であり，その基礎付けはダイクストラ検証や関数等価性の理論に負っている．開発レビューや検証レビューといったチームで行われる活動も，数学的な思考を助長することに主眼があり，それがゆえに，この手法が工業技術として成功していると言える．

自動車や航空機の場合と同様に，ソフトウェアの開発においても，単一の工学分野のみで済むということはない．組織工学，人間工学，管理工学等，さまざまな技術が必要であろう．しかし，精密ソフトウェア工学は，ソフトウェア開発において，前提となる第一の技術体系でなくてはならない．

3. ソフトウェア工学の課題

1980 年代初頭のソフトウェアのライフサイクルに関する論争があり，従来のウォータフォール型のライフサイクルモデルの欠点が浮き彫りにされ，厳密な仕様化の過程を含む「自動プログラミング」のパラダイムの有用性が説かれた．



しかしながら，このような形式仕様を核としたパラダイム提唱という結論に 15 年以上前に至ったにもかかわらず，依然として形式仕様記述の事例が，小さなものに限られているし，本格的に日常的に実務で使われているということもないようである．間違いなくプログラムそのものは，（実行可能な）形式記述である．上記のパラダイムは，問題を上流に先送りしたに過ぎないし，要求抽出に関して形式仕様を得る属人性を排除した有効な技法が確立しているとも言えない．すなわち，所望のプログラムを得るのにハッカーに頼らなくてはならないのと同様に，要求抽出に形式仕様の達人が必要なのである．

ソフトウェア工学に関する本質的な問題提起は，F. P. Brooks, Jr. の「人月の神話」で述べられているように，規模や複雑さといった本質的問題にある．これを管理技術によって解決するという途もあるが，それだけでは，単に躾や教えの世界にとどまってしまうことになる．

クリーンルーム手法では，少なくともプログラミングの工程に対して，属人性を排除した数学的活動に基づく方法を提示している．精密ソフトウェア工学では，ソフトウェア開発の本質的な困難に対しても，数学的活動によってこれを解決する途を探ることを要請する．非常に複雑で抽象的な概念構造体に対しても，計算の論理に基づく厳密な分析や意思決定を行えるようにするということである．これをあえて，プロタイピングやインクリメンタル開発プロセス，あるいは，優秀な人材だけに頼ることなく達成できるようにしなくてはならない．

4. 精密ソフトウェア工学とは

ソフトウェア工学の罪：ソフトウェア工学が，製品としてのソフトウェアの責任の拠り所になっていないのではないだろうか？過去 30 年間のソフトウェア工学の歩みは正しかったのだろうか？

ソフトウェア工学の罠：ソフトウェア工学は，正しい高級化，高抽象化を達成して来たのだろうか？あるいは，どんなに高級化，高抽象化を図っても，複雑さは解消されないのではないだろうか？

精密ソフトウェア工学の心：拠り所を計算の論理以外に求めない．小規模なプログラムは無論のこと，大規模なソフトウェア開発においても，そのあらゆる工程でソフトウェアそのものの問題に集中し，原理的に計算の論理と数学的思考にしか頼らない．

精密ソフトウェア工学の夢：誰でも「銀の弾丸」を撃つことができる．ソフトウェアに欠陥があるとすれば，それが計算の論理に反した誤った意思決定であるということが判定可能である．

精密ソフトウェア工学とは，数学的な活動としてソフトウェア開発プロセスをとらえ，その知識を属人性を排除した技術として構築する学問である．

本資料は，パネル討論：「精密ソフトウェア工学のすすめ」を進行するにあたり，司会者の立場として，議論のきっかけを与えるために執筆したものである．

大槻　繁