新連載

形式手法による組み込みソフトウェア開発

第1回 カップラーメン・タイマの要求分析

藤倉 俊幸

形式手法を使用した組み込みソフトウェア開発をテーマとして連載をすることになりました．難しいといわれる形式手法ですが，開発事例を使いながら説明していきます．

（筆者）

1．形式手法とは

● 人間の手によるテストの限界

組み込みソフトウェアは，規模が大きくなり処理も複雑化しています．また，対応すべきハードウェアも多様化しています．しかし，開発現場は人海戦術で自然言語とプログラミング言語を駆使して開発し，時々UML（Unified Modeling Language）などで絵を描いてみる，といった本質的には10年前とほとんど変化しない状態が続いています．

必要なのは，考えることを支援してくれる助っ人です．人間は必ず間違いを犯します．なのに，組み込みソフトウェアで実現したいことに矛盾がないことを確認するには，現状では人間によるレビューしかありません．実現方法が正しいのか確認するのも人間によるレビューです．結局，人間によるレビュー以外に検証するすべがないまま，コーディングを行い，実際に動作させてテストします．

しかし，組み込みソフトウェアのテストで実際に動作させてテストできる範囲は，時間的にも技術的にも限界があります．強運の持ち主でない限りやってられないのが組み込みソフトウェア開発です．最近は，組み込みソフトウェア開発も複数の人がかかわっています．モジュールごとに人が異なるだけでなく．要求をまとめる人，設計をする人，実装する人，テストする人が別であることも多くなってきました．自然言語とプログラミング言語しか武器がない現状では，コーディングしない人は何をすればよいのでしょうか．作文が仕事なのでしょうか．ポンチ絵を描くことが仕事なのでしょうか．

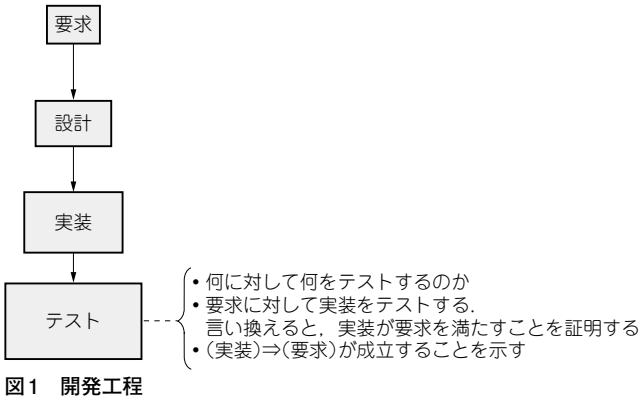

図1　開発工程

● コンピュータによる検証を可能にする＝形式手法

形式手法とは，上流成果物として動くモデルを導入し，人間によるレビュー以外にコンピュータによる検証を可能にする手法です．あるときは網羅的な検証を，それが無理なときは部分的な検証を実現してくれます．本連載では，従来手法と形式手法を使って同じ開発課題を扱っていきます．形式手法を使わない場合と比較することで，形式手法の特徴を理解できるでしょう．個々の手法やツールの特徴ではなく，ものの見方としての形式手法を理解してもらいたいと思います．ものの見方やアプローチの仕方が最も役に立ちます．個々のツールや手法は今後もどんどん進化していきますが，形式的あるいは数理的なものの見方は変わりません．

2．組み込みソフトウェアの開発工程

● 開発工程の分割

一般的な組み込みソフトウェアの開発工程は，**図1**のように要求，設計，実装，テストに分割されます．要求工程では何を作るか明確にして，設計工程ではそれをソフトウェアでどのように実現するか決めて，実装でコーディングや

KEYWORD——形式手法，開発工程，要求工程，検証