新・組み込みソフトへの数理的アプローチ
～形式仕様記述をどのように使うか～

第14回

形式仕様記述は役に立つのか
―― 形式手法導入でバグはどれくらい減らせたのか

藤倉 俊幸

1 早い段階でバグを取り除く

本連載では，プログラム仕様を正確に記述すること，そして検証を行うための技術を扱っている．この技術を使うと開発の初期の段階でバグを取り除くことが可能になる．形式手法は，数学や論理学を使うので慣れるまでは大変だが，この壁を乗り越えれば効率的にバグを減らすことができると信じている．…が，使う人が何時までたっても増えてこない．確かに早い段階でバグを取り除くことはできるが，手間が増えるだけでバグが減らなかったという開発シミュレーションの報告が参考文献(1)にある．どんな報告か読んでみよう．

その報告では，形式仕様記述ツールのVDM(The Vienna Development Method)を使って効果を定量的に調べる実験を行っている．実験といっても，あくまでも思考実験であり実際に何かを開発したわけではないらしい．でも，その割にはリアルだ．ソフトウェア開発というのは人に強く依存する．開発者が変われば状況も変わるので比較できないし，同じ開発者による実験でも1回目と2回目では学習してしまうので比較できない．だから思考実験によって調べるしかないのかもしれない．

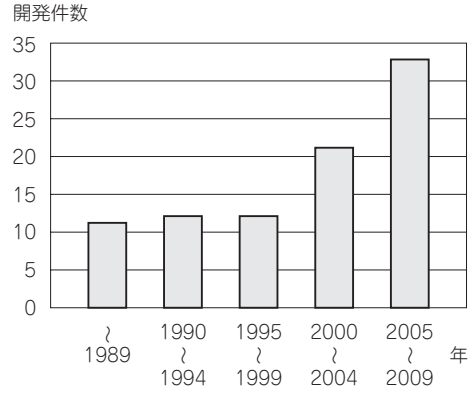

図1
形式手法関連プロジェクト[3]

2 VDMの特徴

● 海外では多く使われているVDMだが…

報告で使用しているVDMとは，形式手法を使って要求を厳密に記述して設計品質を向上させるためのツールであり，形式仕様記述の老舗で，形式手法の事例では必ず出てくる．この連載でこだわっている命題論理ではなく，やや難易度の高い述語論理をベースにしている．VDMは2005年から日本のCSKシステムズが所有していて，研究会[2]などを立ち上げて普及に努めている．ISOにもなっているフリーのツールだが日本では使う人が少ない．しかし，世界に目を向ければ20年も前からコンスタントに使われている有名なツールだ[3]．

最近IPA(独立行政法人 情報処理推進機構)から発表された参考文献(3)に掲載されている形式手法関連プロジェクト数の推移を**図1**に示す．多いとはいえないが2000年ぐらいから機能安全などの規制が入る関係で増えてきている．この中の11.8%がVDMを使用している．それなのに日本では皆無といってよい状態になっていて，CSKもなかなかビジネスにならず持て余し気味と聞いている．その謎が明らかになるかもしれない．

実験は形式手法を使わなければならなくなった学生を想定して行われている．したがって，初心者が段階的にVDMを利用していく設定になっている．導入のステップは**表1**のようになっている．VDMにはVDM++とVDM-SLの2種類がある．今回使用しているのはVDM-SLである．