仕様記述からプログラム・コードの自動生成，実機による実行まで

FM3マイコン基板で学ぶ Bメソッドによる形式手法

新連載

第1回 Bメソッドの開発手順とモールス信号点滅プログラムの実行

Web

和田 学，水口 大知

これまでの組み込み開発では仕様を文章で記述し，それを参照しながらプログラムを作成していた．しかしこの手法は複雑・大規模化する昨今では限界に達しつつある．そこで仕様を仕様記述言語で記述し，正しさを証明しながらプログラムを作成する形式手法が必要になってくる．

本連載では，Bメソッドと呼ばれる形式手法の一つについて，フリーのツールを使い，仕様の記述からプログラム・コードの自動生成，FM3マイコン基板での実行を行いながら学んでいく．（編集部）

ここ数年，雑誌や技術者向けのポータル・サイトなどで頻繁に形式手法が紹介されています．組み込みソフトウェアは大規模化・複雑化の一途にある一方で，より高い信頼性と説明責任が求められるようになってきています．しかし従来の人手によるレビューやテストによる検証では，漏れや手戻りが発生し，十分な品質を得るために多大なコストがかかっています．こうした状況に対する解決策の一つとして，形式手法が注目されています．

● Bメソッドとは

Bメソッドはソフトウェア開発のための形式手法の一つで，証明によって正しさを検証した仕様から，仕様を正しく満たすプログラム・コードを得るための方法論です．そして実用性に優れた支援ツールを活用しながら仕様や実装のレビューを行うことで，検証漏れや手戻りを防ぐことができる開発手法です．こうしたことからBメソッドは研究用途のみならず，安全関連システムなどの製品開発への適用が世界中で広がっています．

この連載ではツールの利用方法も含めたBメソッドの実践方法を紹介していきます．付属基板上で動作するプログラムの作成を通して，Bメソッドの世界を体感してもらいたいと考えています．

第1回目の今回は，形式手法の現状について触れた上で，Bメソッドによるソフトウェア開発の全体像を説明します．形式的な仕様記述からプログラムに至るまでの流れを，ツールを使いながら追いかけてみましょう．

1 組み込みソフトウェア開発と形式手法

● 身近になった形式手法――FeliCa，Microsoftも採用

形式手法は1960年代から研究されていましたが，ツールの使い勝手やパソコンの性能が向上したことにより，現在は手軽に使えるようになりました．実開発での利用が広

連載は6回シリーズの予定です．
第1回：Bメソッドの開発手順
第2回：Bの仕様記述（抽象機械）
第3回：証明（自動証明，対話証明）
第4回：Bの詳細化と実装表現
第5回：より実践的な設計
（構造化，実行環境）
第6回：Bの関連ツール
（EventB，ProB検証など）

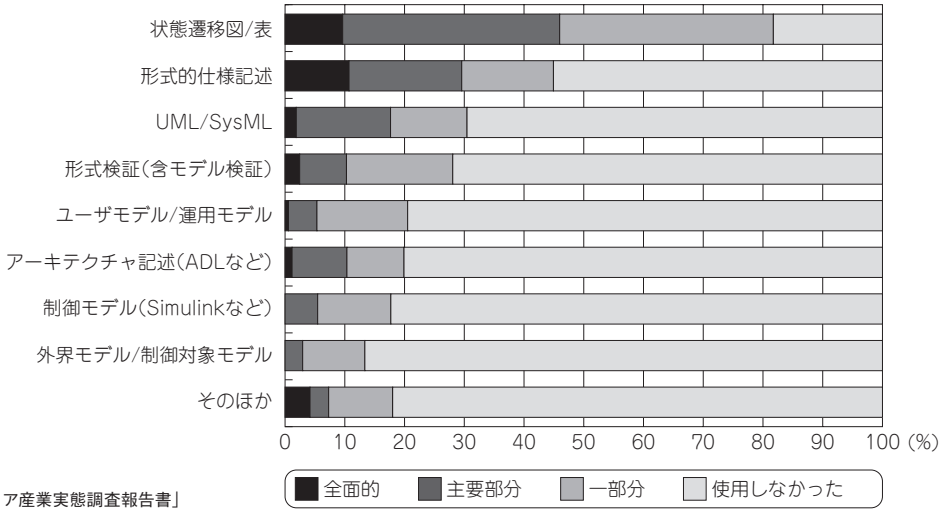

図1
プロジェクトで利用した手法・技法
出典：経済産業省「2010年 組込みソフトウェア産業実態調査報告書」

KEYWORD――形式手法，Bメソッド，Atelier B