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

第4回（最終回） 仕様記述の証明を繰り返し，実装表現に変換していく

北川 さやか，竹内 舞

今回は，抽象的な仕様記述に基づき，仕様を満たす実装を作成する過程について説明します．例題として，連載第2回で作成した自動販売機の仕様記述（抽象機械）から，実装表現（インプリメンテーション）を作成します．さらに，実装表現が仕様を満たしていることも検証します．（筆者）

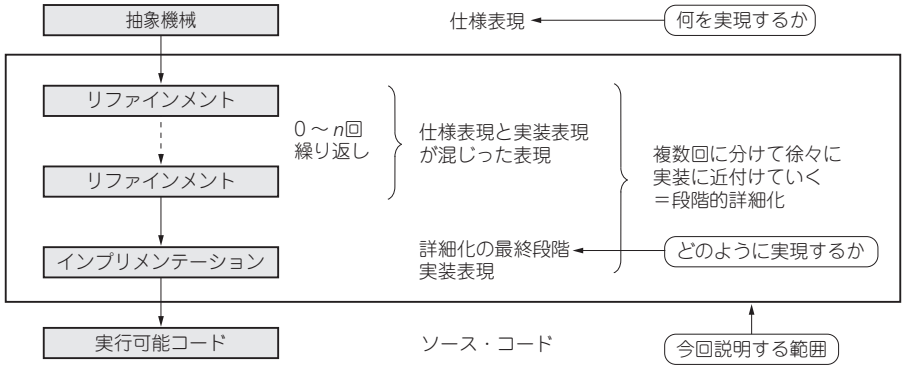

図1　Bメソッドで仕様から実装可能なコードを作るまでの流れ

1 仕様の詳細化と検証

● 仕様と実装を明確に区別する

Bメソッドでは，仕様と実装を明確に区別して記述します．

仕様＝「何を実現するか（What）」

実装＝「どのように実現するか（How）」

を表します．

仕様と実装を表現するためのコンポーネントも分かれています．仕様を表現するためのコンポーネント（抽象機械）と実装を表現するためのコンポーネント（インプリメンテーション，実装という意味）があり，抽象機械からインプリメンテーションを得る作業を詳細化といいます．詳細化では，途中に仕様表現と実装表現が入り混じったコンポーネント（リファインメント，改善という意味）を段階的に作成することもできます（**図1**）．

そして，各段階の詳細化が正しく行われていること（詳細化の正当性）を証明により確認することで，仕様から実装にするときのミスを防ぐことができます．

Bメソッドにおける詳細化の作業では，「データの詳細化」と「非決定性の除去」の二つを主に行います．以降にそれぞれについて説明します．

■ 実装コンポーネントを作成する詳細化

● ①データの詳細化：例えば金額を硬貨の枚数で表現する

上位（詳細化前）のコンポーネントでは，データの表現を，詳細設計の方針や実装手段などにとらわれずに抽象的な形で記述することが可能です．下位（詳細化後）のコンポーネントでは，上位の抽象的なデータ表現をより具象的な表現に置き換えていき，最終的にはC言語などに変換可能な実装表現のみの記述とします．これをデータの詳細化と呼びます．

今回の自動販売機の仕様と実装を考える例題（**図2**）の場合，抽象機械では売上金額を自然数の値`MoneyStock`として保持していますが，詳細化の後では硬貨の種類別の枚数としてより具象的に管理しています．詳細化前後の変数の間に成り立つべき対応関係は，下位コンポーネント側の不