フレッシャーズのために

ライン・トレース・カーで学ぶ組み込みシステム開発の基礎知識

佐藤 洋介

＜執筆協力＞
山郷 成仁

第5回　システム・アーキテクチャ記述のその先にあるもの（最終回）

第1回から第3回までは，ライン・トレース・カーを題材に，単一製品のシステム開発に関する技術を紹介しました．第4回では，複数製品を仕様上どのように扱うかを焦点に差分開発技術を紹介しました．最終回の今回は，仕様検証をテーマにします．（筆者）

1．仕様検証の考え方

システムの品質は主にシステム設計工程で作り込まれます．設計時に混入する不具合の多くは，解釈のミスや分割・詳細化前の情報が引き継がれないなどの漏れ・抜けが原因です．混入してしまった不具合は，検査工程で検出して除去し，不具合の流出を防ぎます（**図1**）．

しかし，検査工程で不具合が発見されるとその影響はほかのサブシステムまで及び，修復するのに莫大な工数が必要となることも多々あります．このような状況を防ぐためにも，不具合を混入させない品質の作り込みが特に重要となります．

そのためには，要求を段階的に分割・詳細化し，システム仕様書を書き上げる技術が必要です．そして，その仕様書を検証する必要があります．第1回（本誌2009年8月号，pp.130-142）ではシステム仕様書を書き上げる技術を解説したので，最終回の今回は仕様を検証する技術を解説します．

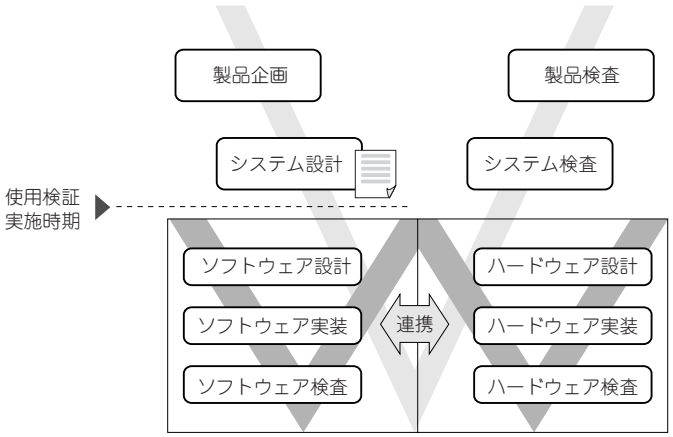

図1　仕様検証実施時期

● 代表的な仕様検証技術

代表的な仕様検証技術として，以下が挙げられます．

- シミュレーション…仕様の振る舞いを確認する
- 形式手法　　…仕様の論理的な正しさを検証する
- モデル・レビュー…あらかじめ設定したレビュー観点に基づき，検証する

組み込みシステム開発の中でも，特に制御系や状態遷移系についてのシミュレーション技術は，Simulink や ZIPC に代表されるシミュレーション・ツールが普及しつつあり，解説書や実施例が豊富に入手できます．今回は，解説や実施例が少ない，形式手法とモデル・レビューについて詳しく解説します．

2．形式手法による仕様検証

● 形式手法とは数学的な手法

形式手法とはフォーマル・メソッド（Fomal Method）の訳で，仕様を「正確に記述し，正確に検証する」技法を指すもので，形式的手法ともいわれます．日本語で形式的というと，建前やうわべだけという印象を思い浮かべる方もいるかもしれませんが，もともとは数学的に正確，厳密なという意味の formal（形式的）からきています．数学に裏付けされた技法なので詳細まで理解することは本当に難しいのですが，技術者として使う側の視点から見ると，「形式手法の目的や考え方」というエッセンスを学ぶことは設計の上で非常に役立ちます．本稿では数学的な詳細に深く立ち入らず，これらを学ぶことに注力します．

● 仕様は日本語より UML より数式で書いた方が正確

さて形式手法の定義は上に書いたとおりですが，何だか