段階的詳細化手法に基づく鉄道信号へのフォーマルメソッド適用法

寺田夏樹

鉄道信号のソフトウェアの品質向上のための手法としてフォーマルメソッド（Formal Methods：形式的手法）と呼ばれる手法がある。これはソフトウェアの仕様をコンピュータに分かる形で数学的論理的に記述し，それをコンピュータ等を使用して分析して仕様の段階で問題点を十分に洗い出すことで最終的な製品の品質を高めることを目指している。

大規模なシステムや複雑なシステムに対してフォーマルメソッドを適用する際，一気に仕様を記述するのではなく，段階的に仕様の記述を詳細にしていく段階的詳細化手法が有効である。さらに各詳細化段階での整合性の証明により，仕様を忠実に実行するプログラムを生成することができる。本報告ではブレーキ曲線の計算プログラムに本手法を適用し，証明と段階的詳細化が有効であることを確認した。また，実際のシステムに適用しやすい段階的詳細化手法についても提案する。

（鉄道総研報告，2007年11月）