トップエスイー修了制作

状態遷移表のモデル検証自動化ツールの開発

（株）東芝　ソフトウェア技術センター　　高田　沙都子　　satoko.takada@toshiba.co.jp

開発における問題点

近年、高まりをみせているソフトウェア品質の向上への施策としてモデル検証が着目されている。しかし、独自の記述言語や時相論理といった専門的知識が必要な点や人手によりモデルを作成することで検証結果を得るまでに時間を要する、といった点がモデル検査を開発現場へ導入、展開する際の足かせとなっている。

モデル検証自動化ツールの開発

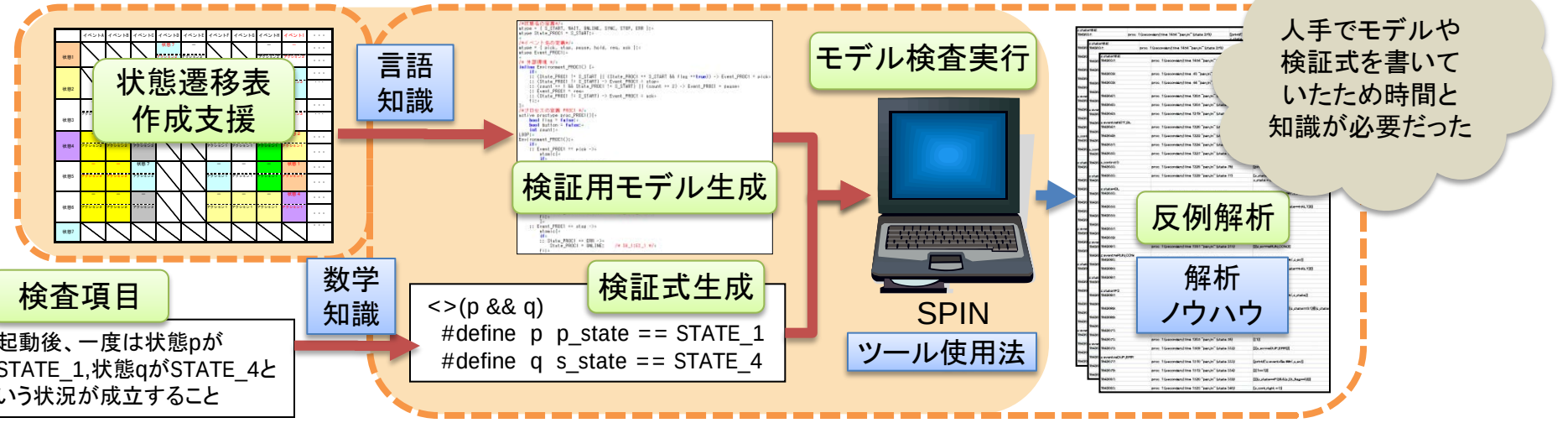
状態遷移表から検証用モデルを生成し、モデル検査を実行する作業を自動化し、更に時相論理の知識が必要とされる検査式作成を支援する機能を加えたツールを開発した。これにより、モデル検査経験のない開発者でもモデル検査適用への敷居を感じることなく取り組むことができるようになった。

モデル検証の流れと開発ツールの概要

ツールによって作業の一部を支援・自動化する

開発目標範囲　今回開発した個所

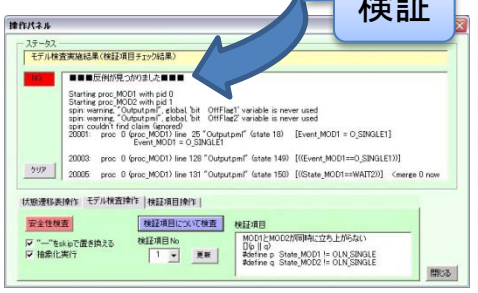
ツールによって自動化された個所



開発ツールの特徴

パネル操作で検証式や検証用モデルを生成後、検証を実行

検証



これまで…
モデルや検証式の記述方法、ツールの使い方を習得した上でモデル検査を実行

状態遷移表と変数定義を入力すればパネル上でモデル検査が可能

ツール適用の効果

実際の事例を適用

- 二重化構成による冗長性を持たせたシステム
  - 規模状態遷移表：約300セル（状態×イベント）
  - Promela行数：約500行

検査結果獲得までの時間が短縮された

開発ツール未適用	開発ツール適用
約30日	**約1日**

  - ツールの使用方法や言語習得が不要
  - モデルが自動生成されるのでケアレスミスの混入がない

専門的知識を意識せずに検証が可能

  - 簡単なGUI操作で結果を取得できる

モデル検証経験のない開発者でも取り組みが容易になった