

# 大規模検証のための 検査モデルの構築方法の提案

中川 雄一郎  
Yuichiro NAKAGAWA

## 背景・課題

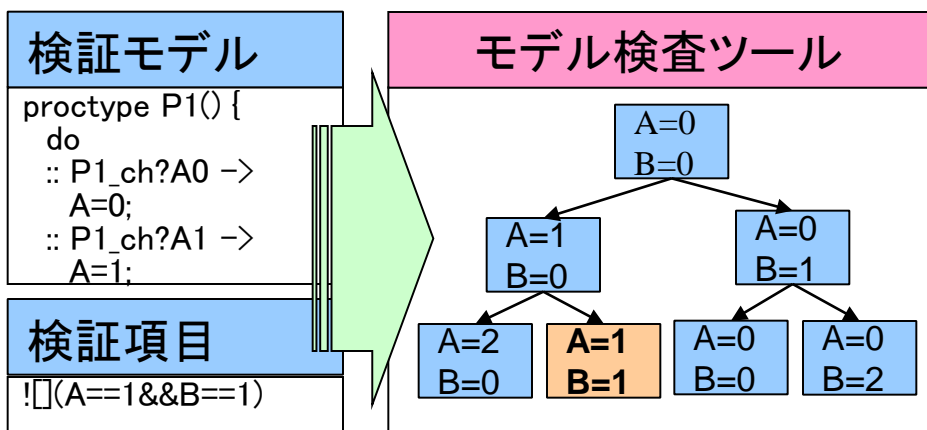
ソフトウェア開発の大規模・複雑化に伴い、その検証が困難になってきている。そのような中、ソフトウェアのモデルを網羅的、自動的に検証を行うモデル検査が注目されている。一方でモデル検査には『①仕様・設計のモデル化が困難』『②全ての状態を網羅するため状態爆発が起こる』という問題がある。

## 分散向けモデル検査方法の提案

本報告では、『①既存の検証モデルの活用』を用いた『②分散環境でのモデル検査』によりモデル検査の適用範囲の拡大を目指す。既存のモデル検査ツールSPIN (Promela)用の検証モデルから、分散環境向けモデル検査ツールDiVinE (DVE)への検証モデルの変換方法の提案を行う。

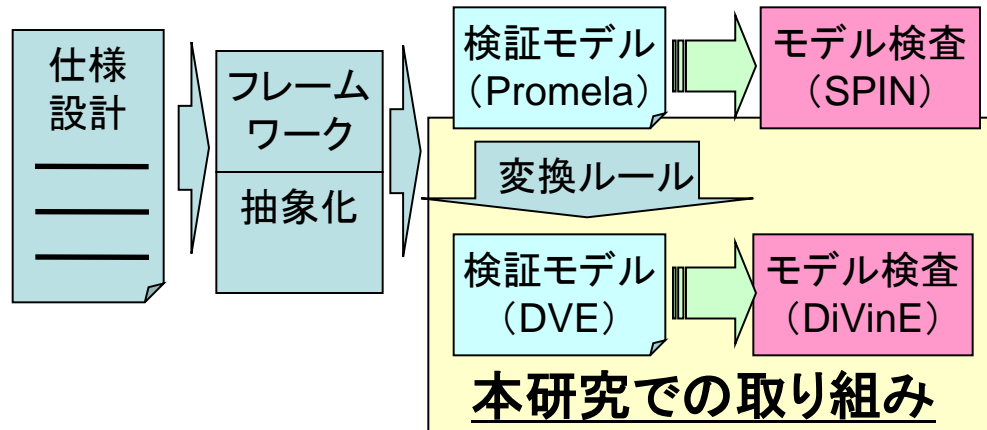
## 1. モデル検査とは

・検証モデルが検証項目を満たすか、否かを取り得る全状態に対して網羅検査



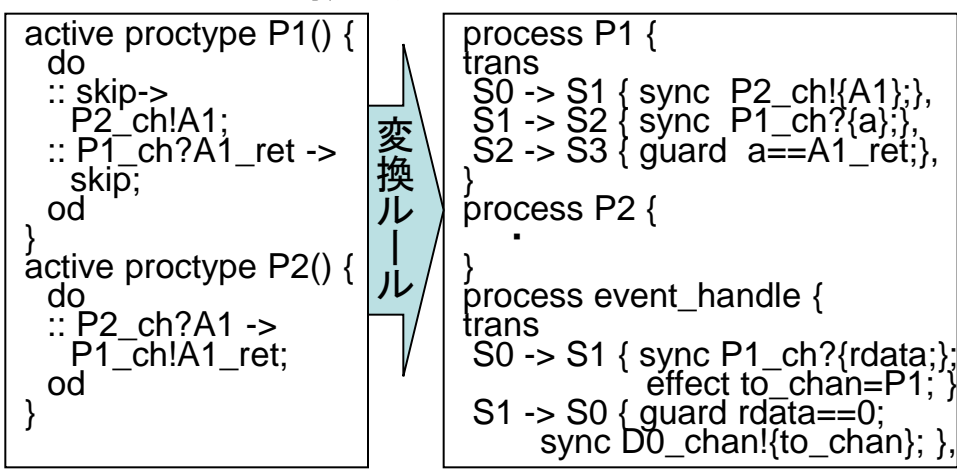
## 2. モデル検査適用プロセス

・既存の検証モデルに変換ルールを適用し、分散環境向け検証モデルを生成



## 3. モデル変換ルール

並列計算に向けたモデルに変換  
 1.モデリング方針を変更(機器→データ)  
 2.使用する言語の記述制約を吸収  
 -メッセージの擬似選択受信機能追加  
 -メッセージ振り分けイベントハンドラ生成



## 4. 結論・今後の課題

### 結論

・変換ルールを用いることで容易にSPIN (Promela)からDVEへの検証モデルの変換を可能とした  
 ・サンプルケースを用いて、クラウド環境にてモデル検査を実施。仮想マシン16台使用し、モデル検査が実施可能であることを確認

### 今後の課題

・規模の大きなソフトウェアに対する分散環境でのモデル検査の実現  
 ・分散環境での効率的なデバッグ手法の検討