

# 検証サービス／「さつき」施設サービス

産業技術総合研究所(以下、産総研)関西センターの協力により、形式手法による検証サービス、連携検証施設「さつき」の利用サービスをご提供します。短期間のプロジェクトでも手軽にご利用できます。

## 検証サービス

検証サービスは、要求仕様や設計仕様、ソースコード、ヒアリング等を元に、モデル検査など形式手法に基づく自動検査を、産総研で実施するサービスです。主な検査内容は下記のとおりです。

- 原因不明のバグの解析
- 仕様書・設計書の検証
- ソースコードの検証
- テストパターンの自動生成

## ▶ サービスのポイント

### 形式手法による検証

- ・検証対象を厳密に、網羅的に評価するので、微妙なタイミングのずれ等に起因する不具合や発生頻度の低いバグも発見が可能
- ・品質向上と不具合解析の両面でのアプローチが可能
- ・不具合の発見と原因解析が同時に完了

### 産総研の高い技術力・先進の施設

- ・共同研究等で開発の上流工程から下流工程までの様々な段階を対象にモデル検査を実施し多くのノウハウを蓄えているので、状態爆発を抑制するようにモデル作成を工夫して検証できる
- ・大容量メモリ高速演算クラスターと大規模演算クラスターを利用して、従来不可能であった大規模なモデル検査やSAT(satisfiability)手法による検証が可能

### 機構独自のサービススキーム

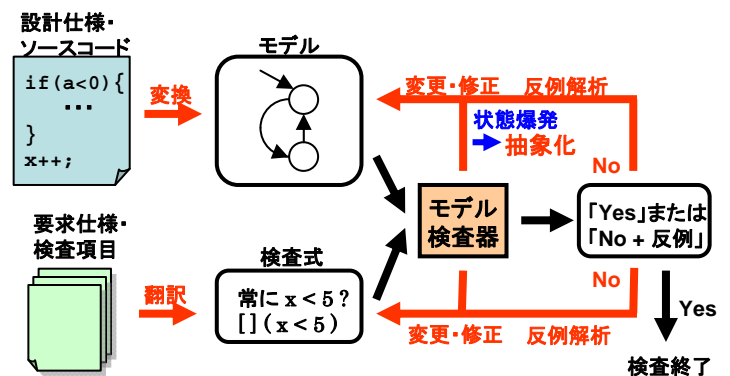
- ・産総研と機構との共同研究を活用しており、短期間のプロジェクトでも手軽に利用できる

## ▶ 検証方法

### ● 大規模モデル検査

モデル検査は詳細設計などを計算機上で記述し、その振る舞いを網羅的に自動検査する形式手法の一つです。モデル検査を用いた検査の流れを、右図に示します。

黒い矢印・文字は、特に人手を介さない処理、赤い矢印・文字は専門の技術者によって行われる処理を表しています。モデル検査を利用していると、状態爆発は簡単に起こってしまうので、抽象化などにより問題の本質を保ったままモデルを単純化する必要があります。このため、検査ができる適切なモデルを作成するためには、多くのノウハウ・時間を必要とすることがあります。



モデル検査の流れ

## ● 大規模充足可能性判定

充足可能性判定機(SATソルバー)は、制約条件を与えると、それらの制約条件をすべて満たす解があるかどうかを判定して、そのような解があれば出力します。

## ● 大規模シミュレーションによる検証

車載システム、家電ネットワーク、制御システムなど、組込みシステムを要素とする大規模ネットワークのシミュレーションのうえで、モデル指向試験を行うことができます。

## 「さつき」施設サービス

「さつき」を利用することで、従来は不可能であったような大規模なソフトウェアテスト等も可能となります。また、機構サービスでは短期間の利用も可能となり、セットアップ料金も免除されます。



グループ	CPU		メモリー	台数
	クロック	コア数		
X	3.0GHz	16	256GB	28
Y	2.9GHz	64	1TB	3
総数		480	10TB	31

大容量メモリー  
クラスター  
(Fat Node Cluster)

SAT ソルバー	
minisat2	sat4j
pmsat	
モデル検査	
NuSMV	divine
spin	prism
ブルーファシスタント	
agda	
数理的仕様記述	
vdmtool	

大規模演算  
クラスター  
(Thin Node Cluster)

グループ	CPU		メモリー	台数
	クロック	コア数		
A	3.3GHz	2	8GB	112
B	3.0GHz	8	24GB	16
C	3.0GHz	8	48GB	16
総数		480	2TB	144

インストール済み  
形式手法ツール

## ご利用の手順

### 1. 機構へのご利用のお申し込み

検証対象の確認／ヒヤリングを行い、費用見積もり  
(必要があれば機構とNDA締結)

### 2. 機構と個別利用契約を締結、費用支払い

検証作業(必要に応じて会員の支援を要請)  
作業結果報告書等の作成

### 3. 検証作業結果、作成したモデル、検査式等の成果物の受領、さつき利用料

## 費用

機構を利用することで小プロジェクトから安価にご利用いただけます。モデル検査の適否など、個々のケースによって大きく異なりますので、まずはお気軽にご相談ください。施設利用の手順、料金につきましても、お気軽にお問合せ下さい。