2014年度ソフトウェア工学分野の先導的研究支援事業

保守プロセスにおけるモデル検査技術の開発現場への適用に関する研究

芝浦工業大学
SIT総合研究所
システム理工学部電子情報システム学科
松浦佐江子

Agenda

- 研究概要（内容、目標、課題等）
- 研究成果
- 成果の活用見込み
- 研究成果の発表、投稿、引用等

研究概要

2012年度ソフトウェア工学分野の先導的研究支援事業
要件定義プロセスと保守プロセスにおける
モデル検査技術の開発現場への適用に関する研究

目標

- リリース判断やマイグレーション時にシステムが「仕様」を満たしているかの確認作業を高効率・高品質で実施したい。
- 形式手法のスペシャリストでなくても、モデル検査の恩恵を受けられる。

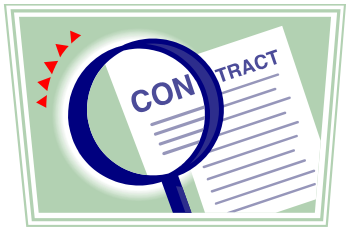
⇒　モデル検査を用いたソースコード検証

課題

- 「仕様」は定義されているのか？
- どのような「仕様」が検証できるのか？

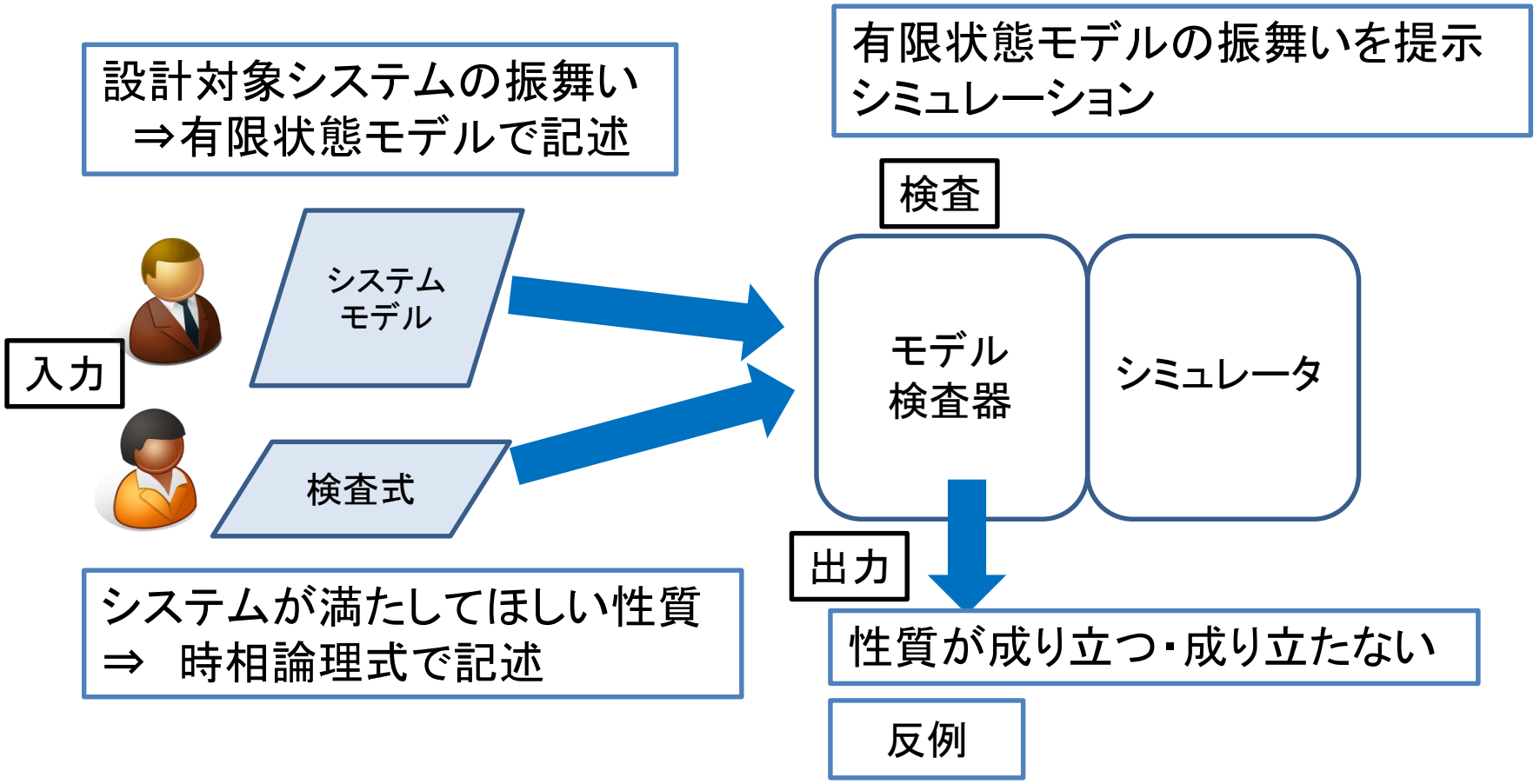
モデル検査

- 有限の状態空間（定義）を網羅的に調べて、与えられた性質が成り立つか否かを調べる。
- 成り立たない場合には、その理由となる反例を具体的に提示する。
- 反例を解析すると、不具合の原因を探ることができる。
- 上記の特徴を知っていれば、その仕組みを詳しく知らなくても、ブラックボックス化して使用できる。



モデル検査ツール

- モデル検査アルゴリズムに基づいたソフトウェア開発ツール
- 設計段階で利用

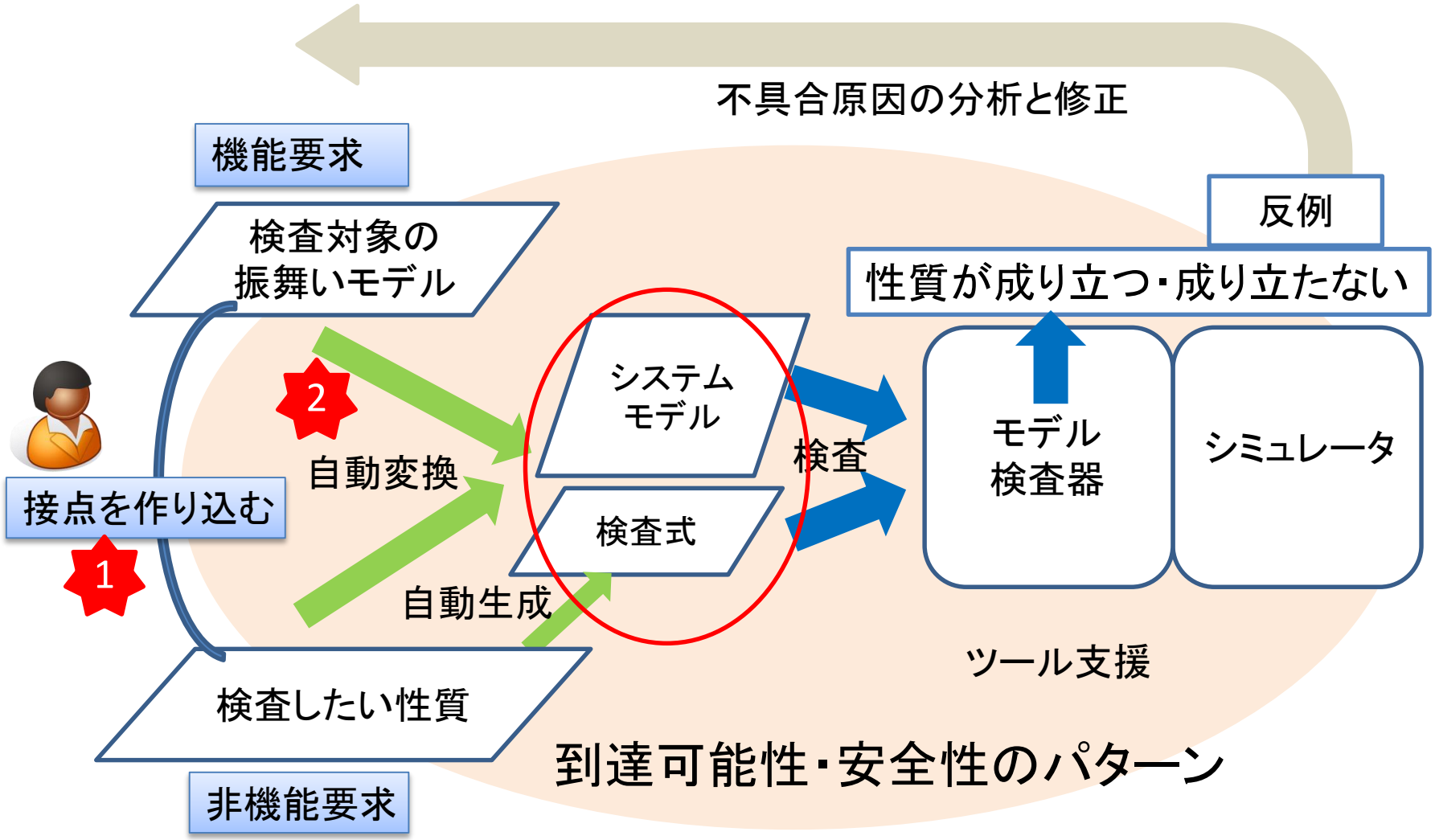


検証できる性質

- 活性 （liveness）
  - システムがある条件下で、将来いつか必ずある特定の状況が起こる。
- 到達可能性 （reachability）
  - システムが、初期状態から、ある特定の状態へ到達する可能性がある。
- 安全性 （safety）
  - システムが、ある条件のもとで、ある正当でない状況に陥ることが決して起こらない。
- 公平性 （fairness）
  - システムが、ある条件のもとである特定の状況が無限回起こる。

システムへの要件
　　システムの振舞いにより実現すべき機能要件
　　振舞いや状態に対する制約や条件を表す非機能要件
機能要件　⇔　活性
非機能要件　⇔　到達可能性・安全性・公平性

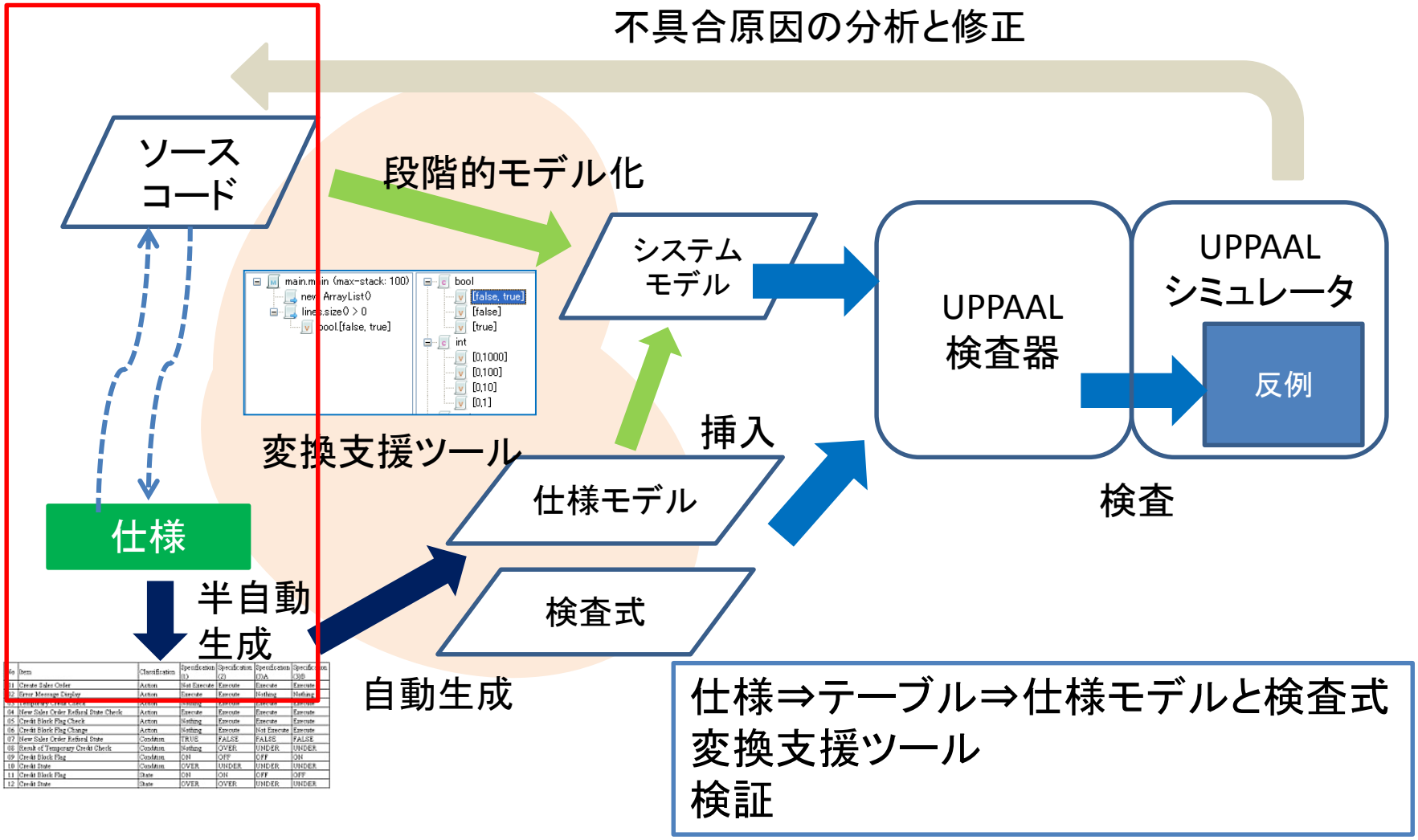
アプローチ


不具合原因の分析と修正
機能要求
検査対象の
振舞いモデル
反例
性質が成り立つ・成り立たない
システム
モデル
検査
モデル
検査器
シミュレータ
2
自動変換
接点を作り込む
1
検査式
自動生成
ツール支援
検査したい性質
非機能要求
到達可能性・安全性のパターン

研究成果

- セキュリティ要件の定義
- セキュリティ要件の検証
  - ソースコードからの情報の取得
  - 変換支援ツールを用いた検証

ソースコード検証



2014年度ソフトウェア工学分野の先導的研究支援事業

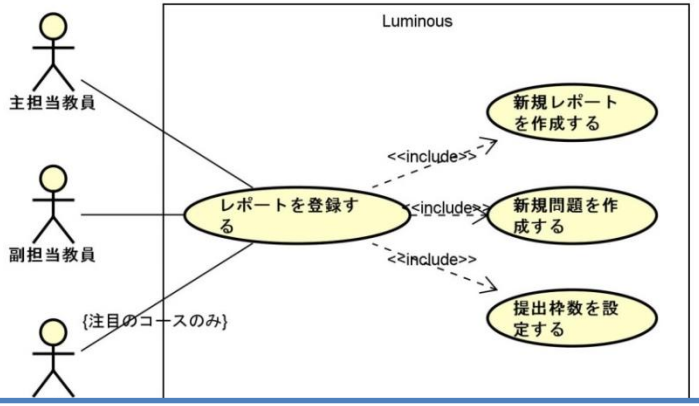
セキュリティ要件の定義

仕様の定義

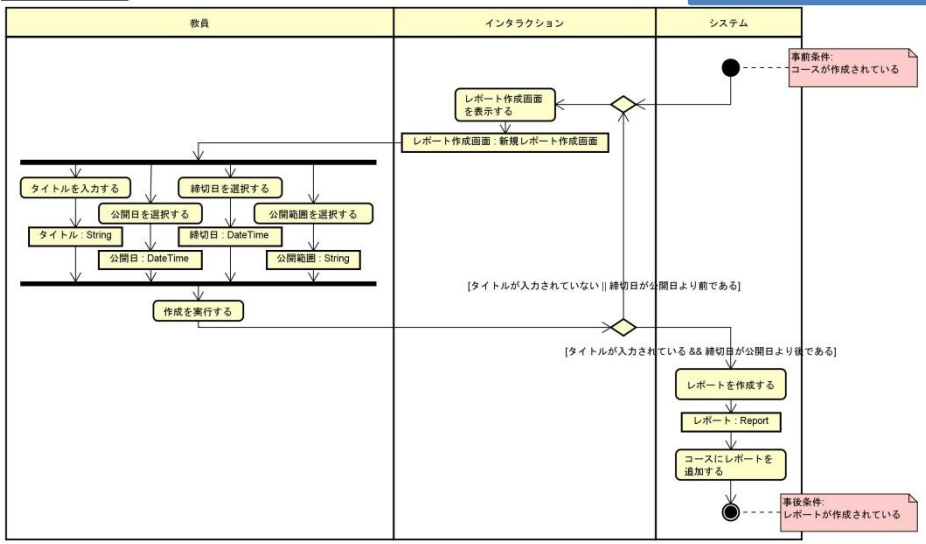
セキュリティ機能方針表の定義

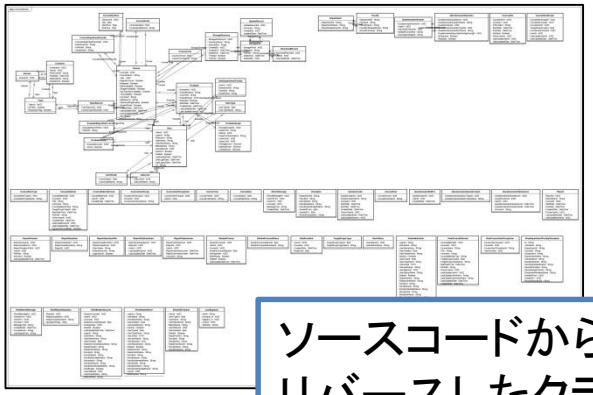
仕様の定義

学習支援システム　LUMINOUS



LUMINOUSのユースケース定義
- メニュー構成から実際に操作して手順を記述する

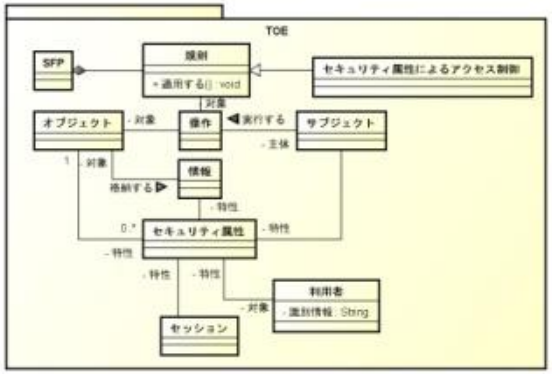




ソースコードから
リバースしたクラス図により
オブジェクトノードを記述する

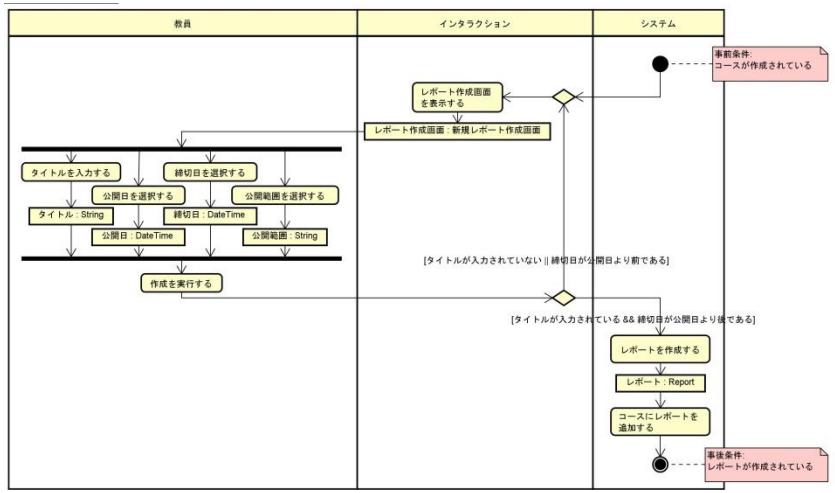
セキュリティ要件の定義

情報セキュリティの国際評価基準
（ISO/IEC15408）である
Common Criteria（CC)



CCの用語の意味

機能要件のアクター・データ・アクションと規則を結び付ける



セキュリティ機能方針（SFP)

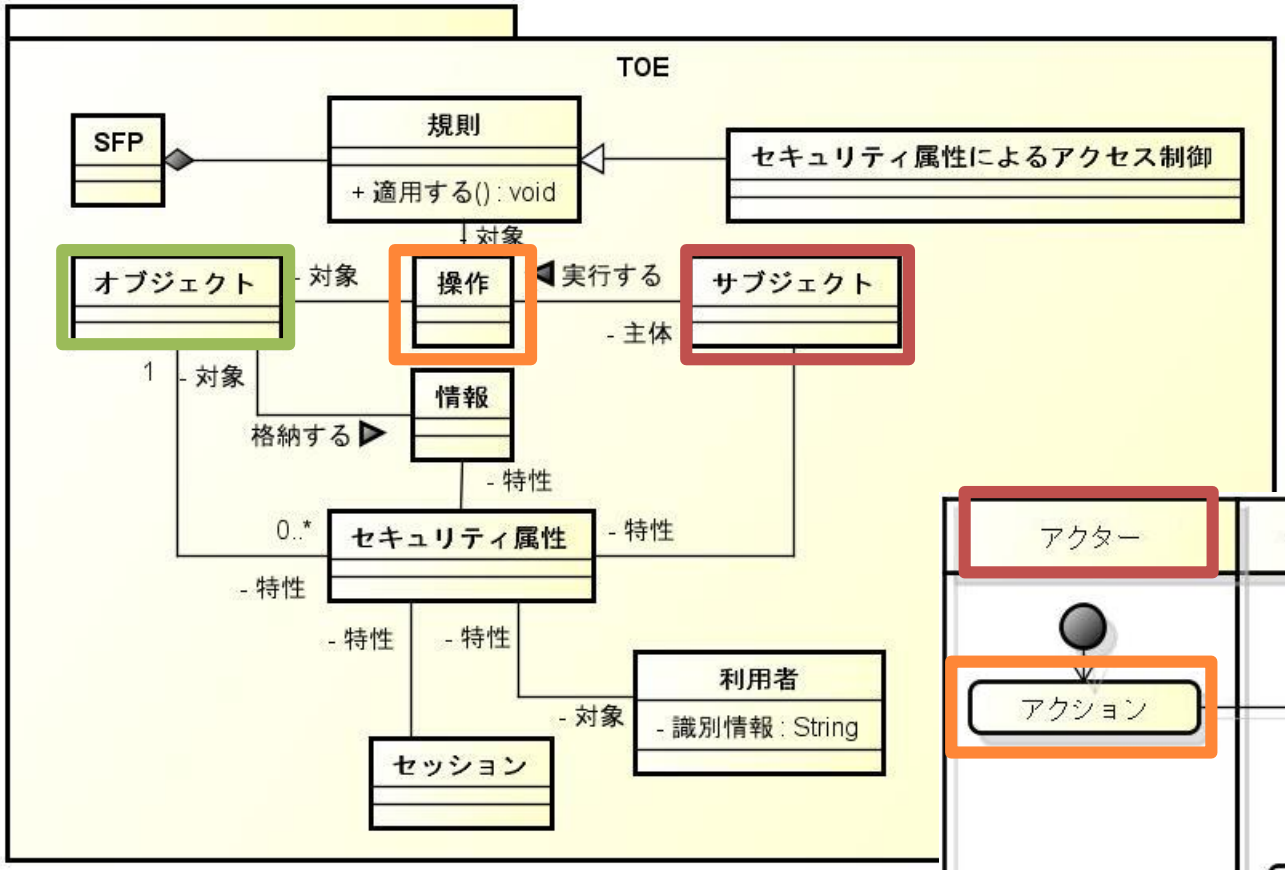
セキュリティ属性

サブジェクト		オブジェクト		操作		ルール		
アクター	セキュリティ属性	クラス	セキュリティ属性	ユースケース	アクション	FDP_ACF.1	FMT_MSA.3	FMT_MSA.1
学生	役割(学籍番号)	…						
		話題	公開非公開	質問を投稿する	話題を生成する		ルールB1	
		日時		質問を投稿する	現在日時を取得する			
		投稿者	役割	話題を選択する(学生)	現在の利用者を取得する			
				質問を投稿する	投稿者を取得する			
		投稿内容		話題を閲覧する(学生)	投稿内容を取得する			
		添付ファイル	公開非公開	話題を閲覧する(学生)	添付ファイルをダウンロードする	ルールA		
				質問を投稿する	添付ファイルを生成する		ルールB2	
教員	役割(教員)	…						
		話題	公開非公開	質問に回答する	（質問番号により選択された話題を取得する			
				質問に回答する	回答を追加して話題を更新する			
					話題の公開非公開を公開に変更する			ルールC1
					話題の公開非公開を非公開に変更する			ルールD1
		日時		質問に回答する	現在日時を取得する			
		投稿者	役割	話題を選択する(教員)	現在の利用者を取得する			
				質問に回答する	投稿者を取得する			
		投稿内容		話題を閲覧する(教員)	投稿内容を取得する			
		添付ファイル	公開非公開	話題を閲覧する(教員)	添付ファイルをダウンロードする			
				質問に回答する	添付ファイルを生成する		ルールB3	
					添付ファイルの公開非公開を公開に変更する			ルールC1
					添付ファイルの公開非公開を非公開に変更する			ルールD1

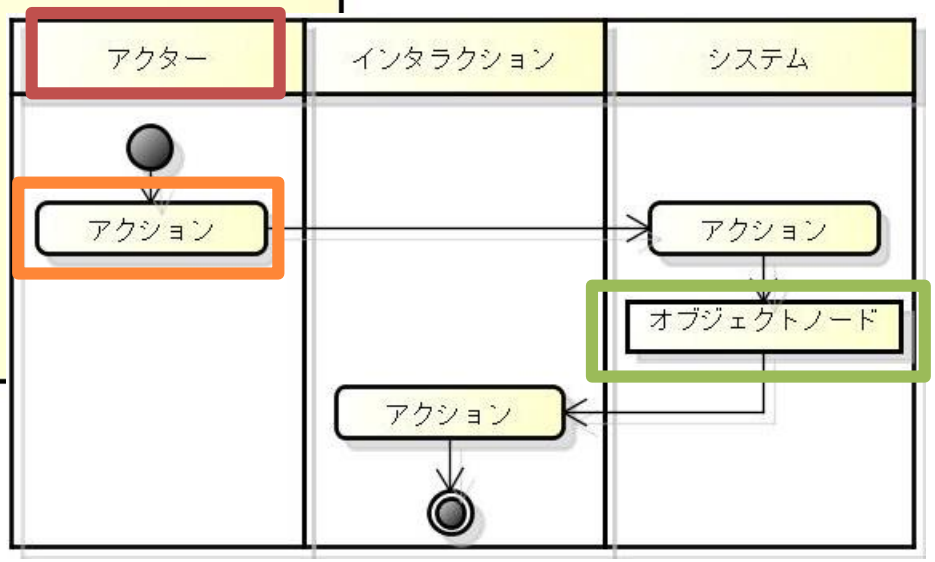
規則

ルールA	アクション開始時，公開非公開=公開	|投稿者.役割=学生.役割である。
ルールB	表示されている話題は公開非公開=公開	|話題.投稿者.役割=学生.役割である。
ルールC	アクション後，公開非公開=非公開になっている。
ルールD	アクション後，公開非公開=公開	|非公開になっている。
ルールE	アクション開始時,公開非公開=非公開&&アクション終了時，公開非公開=公開である。
ルールF	アクション開始時,公開非公開=公開&&アクション終了時，公開非公開=非公開である。
ルールG	表示されている投稿者は学生.役割=投稿者.役割である。

セキュリティ要件の定義



SFPのクラス図



セキュリティ機能方針表の定義

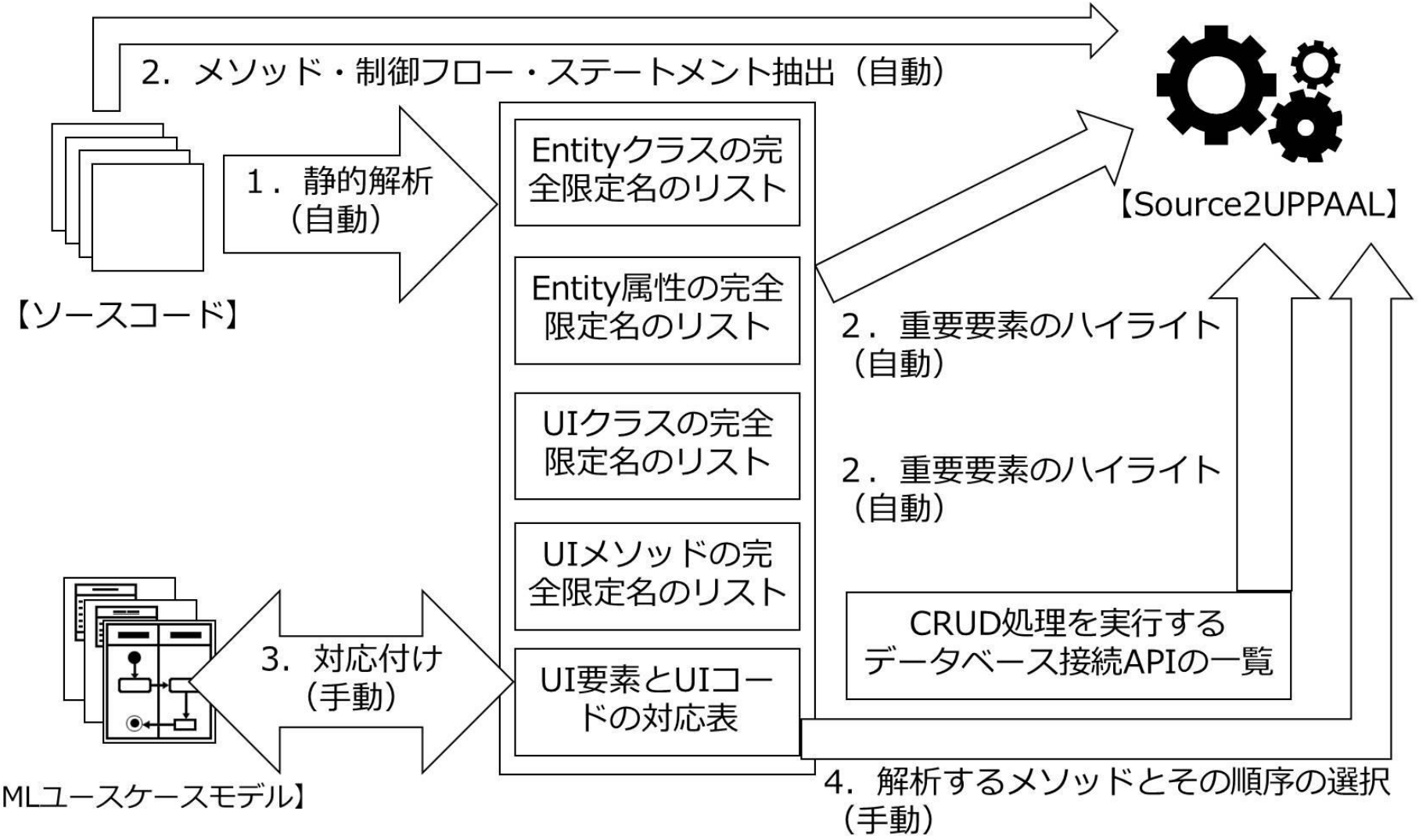
サブジェクト		オブジェクト		操作		ルール		
アクタ	セキュリティ属性	クラス	セキュリティ属性	ユースケース	アクション	FDP_ACF.1	FMT_MSA.3	FMT_MSA.1
学生	役割(学籍番号)	・・・						
		話題	公開非公開	質問を投稿する	話題を生成する		ルールB1	
		日時		質問を投稿する	現在日時を取得する			
		投稿者	役割	質問を投稿する	投稿者を取得する			
		投稿内容		話題を閲覧する(学生)	投稿内容を取得する			
		添付ファイル	公開非公開	話題を閲覧する(学生)	添付ファイルをダウンロードする	ルールA		
				質問を投稿する	添付ファイルを生成する		ルールB2	
教員	役割(教員)	・・・						
		話題	公開非公開	質問に回答する	<質問番号>により選択された話題を取得する			
				質問に回答する	回答を追加して話題を更新する			
					話題の公開非公開を公開に変更する			ルールC1
					話題の公開非公開を非公開に変更する			ルールD1
		日時		質問に回答する	現在日時を取得する			
		投稿者	役割	質問に回答する	投稿者を取得する			
		投稿内容		話題を閲覧する(教員)	投稿内容を取得する			
		添付ファイル	公開非公開	話題を閲覧する(教員)	添付ファイルをダウンロードする			
				質問に回答する	添付ファイルを生成する		ルールB3	
					添付ファイルの公開非公開を公開に変更する			ルールC2
					添付ファイルの公開非公開を非公開に変更する			ルールD2

ルールA	アクション開始時，添付ファイル.公開／非公開==公開 ‖ 投稿者.役割==学生.役割
ルールB1	アクション終了時，話題.公開／非公開==非公開
ルールB2	アクション終了時，添付ファイル.公開／非公開==非公開
ルールB3	アクション終了時，（話題.公開／非公開==公開ならば添付ファイル.公開／非公開==公開 ‖ 添付ファイル.公開／非公開==非公開） &&（話題.公開／非公開==非公開ならば添付ファイル.公開／非公開==非公開）
ルールC1	アクション開始時に話題.公開／非公開==非公開ならば，アクション終了時に話題.公開／非公開==公開
ルールC2	アクション開始時に添付ファイル.公開／非公開== 非公開ならば，アクション終了時に添付ファイル.公開／非公開== 公開
ルールD1	アクション開始時に話題.公開／非公開== 公開ならば，アクション終了時に話題.公開／非公開==非公開
ルールD2	アクション開始時に添付ファイル.公開／非公開== 公開ならば，アクション終了時に添付ファイル.公開／非公開==非公開

セキュリティ要件の検証

ソースコードからの情報の取得

ソースコードからの情報の取得



検査シナリオ

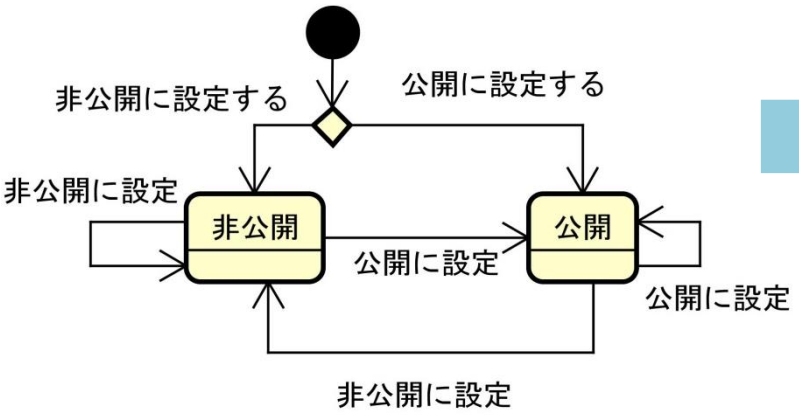
サブジェクト		オブジェクト		操作		ルール		
アクタ	セキュリティ属性	クラス	セキュリティ属性	ユースケース	アクション	FDP_ACF.1	FMT_MSA.3	FMT_MSA.1
学生	役割(学籍番号)	話題	公開／非公開	質問を投稿する	話題を生成する		ルールB1	
教員	役割	話題	公開／非公開	質問に回答する	話題の公開／非公開を非公開に変更する			ルールD1

ルールB1	ユースケース終了時に話題.公開／非公開==非公開
ルールD1	ユースケース終了時にアクションを実行したら話題.公開／非公開==非公開

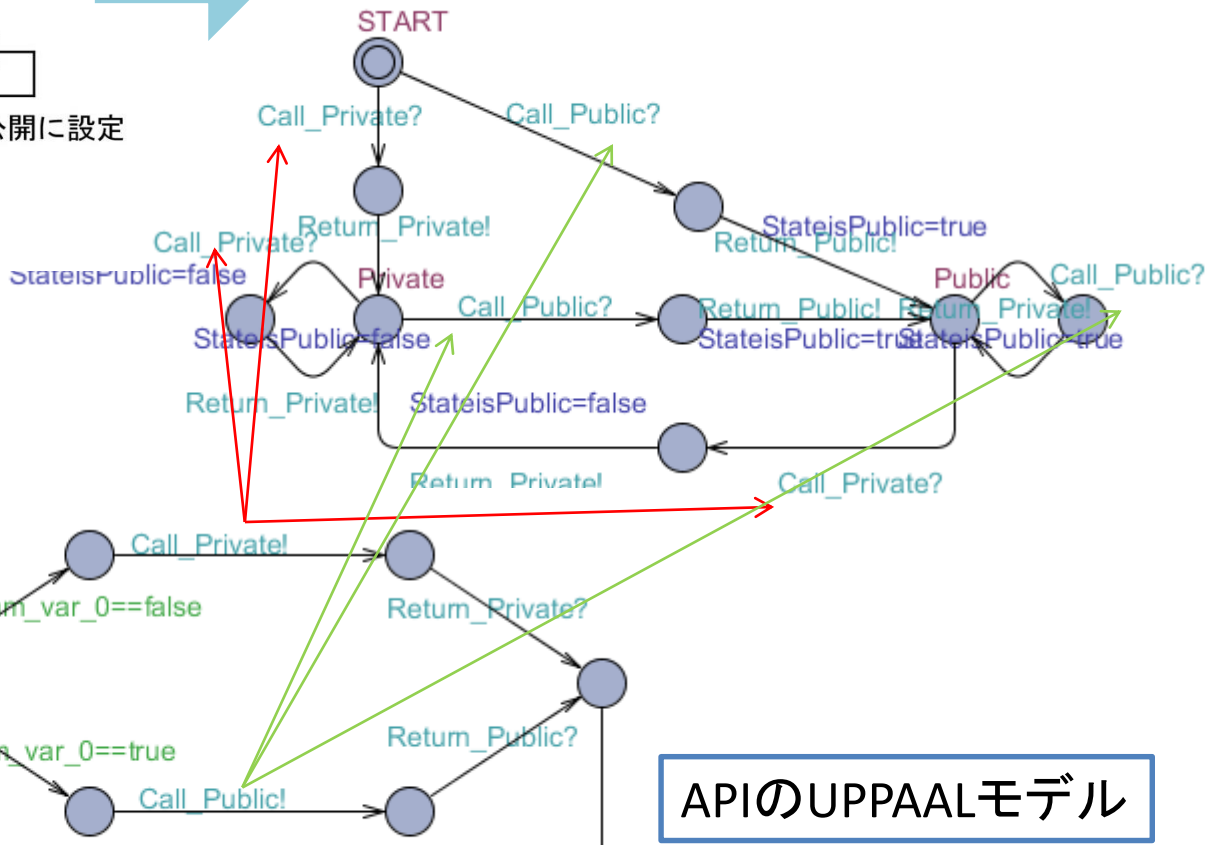
学生が質問を投稿する(ここでは非公開)
教員が質問に回答する(非公開に設定する||公開に設定する)
回答終了時に、非公開に設定していれば、話題は非公開

02	教員が質問に回答する	回答処理終了時に非公開指定で公開になることはない	A[] not (SYSTEM_SIT_Luminous_Web_course_detail_bbs_newtopicanswer_buttonCreate_Click(0,0).END && SaveChanges_param_var_0==false && SYSTEM_State_Private_Public.Public)

話題のセキュリティ属性の満たすべき状態遷移



変換されたUPPAALモデル



APIのUPPAALモデル

成果の活用見込み

- 検証
  - 個々の機能と密接な関係にあるシステムの持つ資産に対する脅威に関するセキュリティ要件の検証
  - 機能要件に対するデータの不変条件の検証
- 仕様の定義
  - ドキュメントのないシステムの仕様の再定義
  - ソースコードからの情報取得

研究成果の発表、投稿

- 松浦, 小形, 青木, 谷沢, 西村, 要件定義プロセスと保守プロセスにおけるモデル検査技術の開発現場への適用，SEC journal No.37, 第10巻，第2号, 2014, pp.8-15.（査読有）
- Saeko Matsuura, Yoshitaka Aoki and Shinpei Ogata, Practical Behavioral Inconsistency Detection between Source Code and Specification using Model Checking, ISSRE2014, pp.124-125, 2014.（査読有）
- Yoshitaka Aoki and Saeko Matsuura, Verifying Security Requirements using Model Checking Technique for UML-Based Requirements Specification, Proc. of 1st International Workshop on Requirements Engineering and Testing, pp.18-25, 2014.（査読有）
- 小形，青木，谷沢，松浦，ユースケースモデルに基づくソースコード検証のためのリバースエンジニアリング手法の検討－ASP.NETアプリケーションを事例として－，信学技報, vol. 114, no. 420, KBSE2014-42, pp. 19-24, 2015.
- 青木，松浦，反例からの検査式自動生成による不具合原因特定支援，信学技報, vol. 114, no. 128, KBSE2014-19, pp. 87-92, 2014.
- 青木，松浦，モデル検査における反例解析容易化支援，信学技報, vol. 113, no. 475, KBSE2013-79, pp. 1-6,2014
- SIT　産官学連携研究交流会　ポスター展示　3月発表予定