2012年度ソフトウェア工学分野の先導的研究支援事業

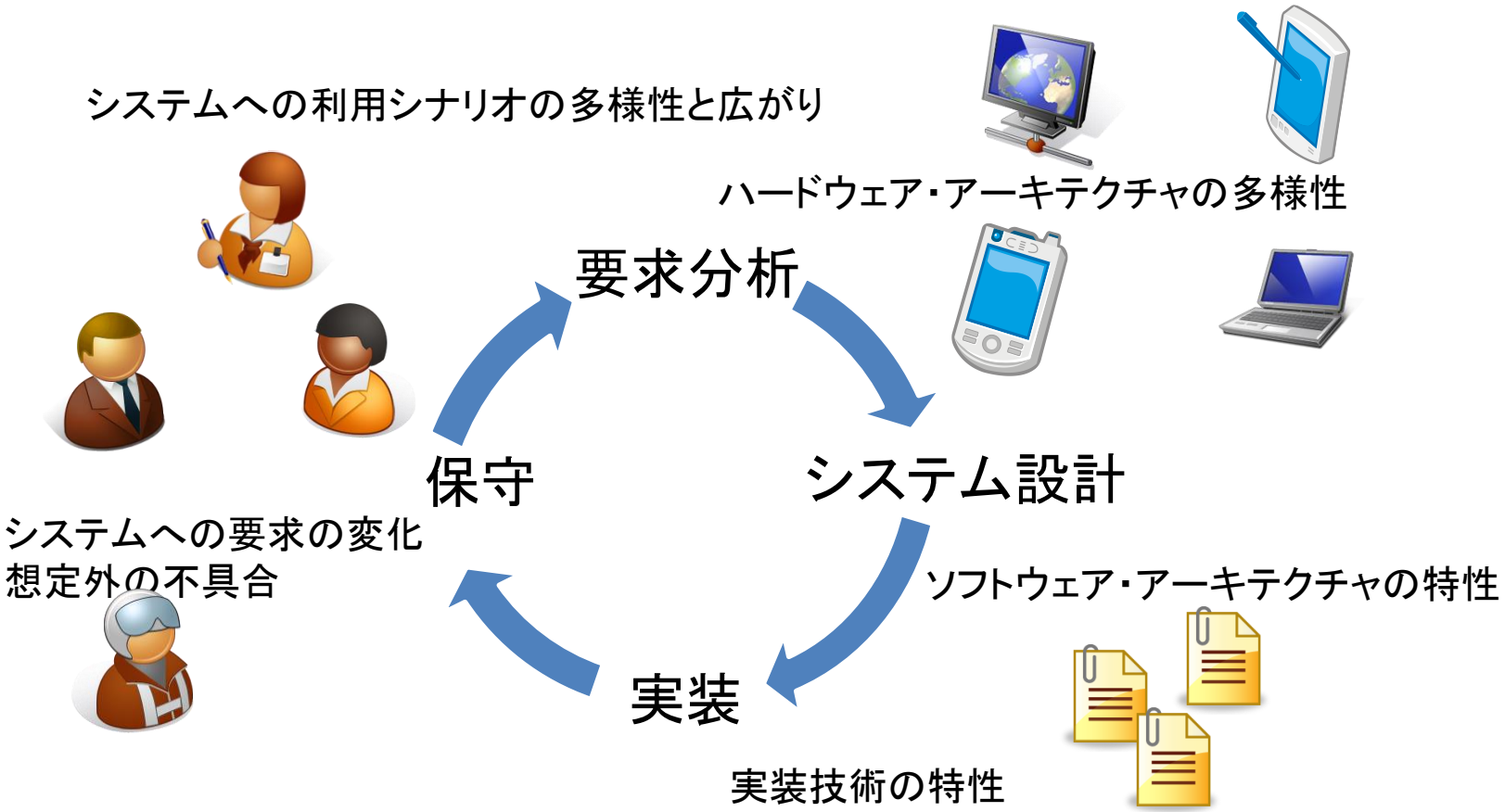
要件定義プロセスと保守プロセスにおける モデル検査技術の開発現場への適用に関する研究

芝浦工業大学
SIT総合研究所ソフトウェア開発技術教育研究センター
松浦佐江子

Agenda

- 研究背景
- アプローチ
- 研究課題と中間目標
- 課題に対する成果
  - UML2UPPAAL
    - 要求分析モデルと業務セオリーの定義
    - 検査プロセス
    - 検証事例
  - Source2UPPAAL
    - 検査プロセス
    - 検証事例
- 問題点と今後の課題

研究の背景



開発のプロセスが変わる　定義と検証のサイクル
要件定義プロセス：定義した要件を早期に様々な観点で検証
保守プロセス：不具合現象の原因の特定や仕様との齟齬を発見

アプローチ

モデル検査技術

– モデル検査技術はテストでは実現できない網羅的検査に特徴がある

– システム構築の上流工程において、その仕様の妥当性を検証するための形式検証技術

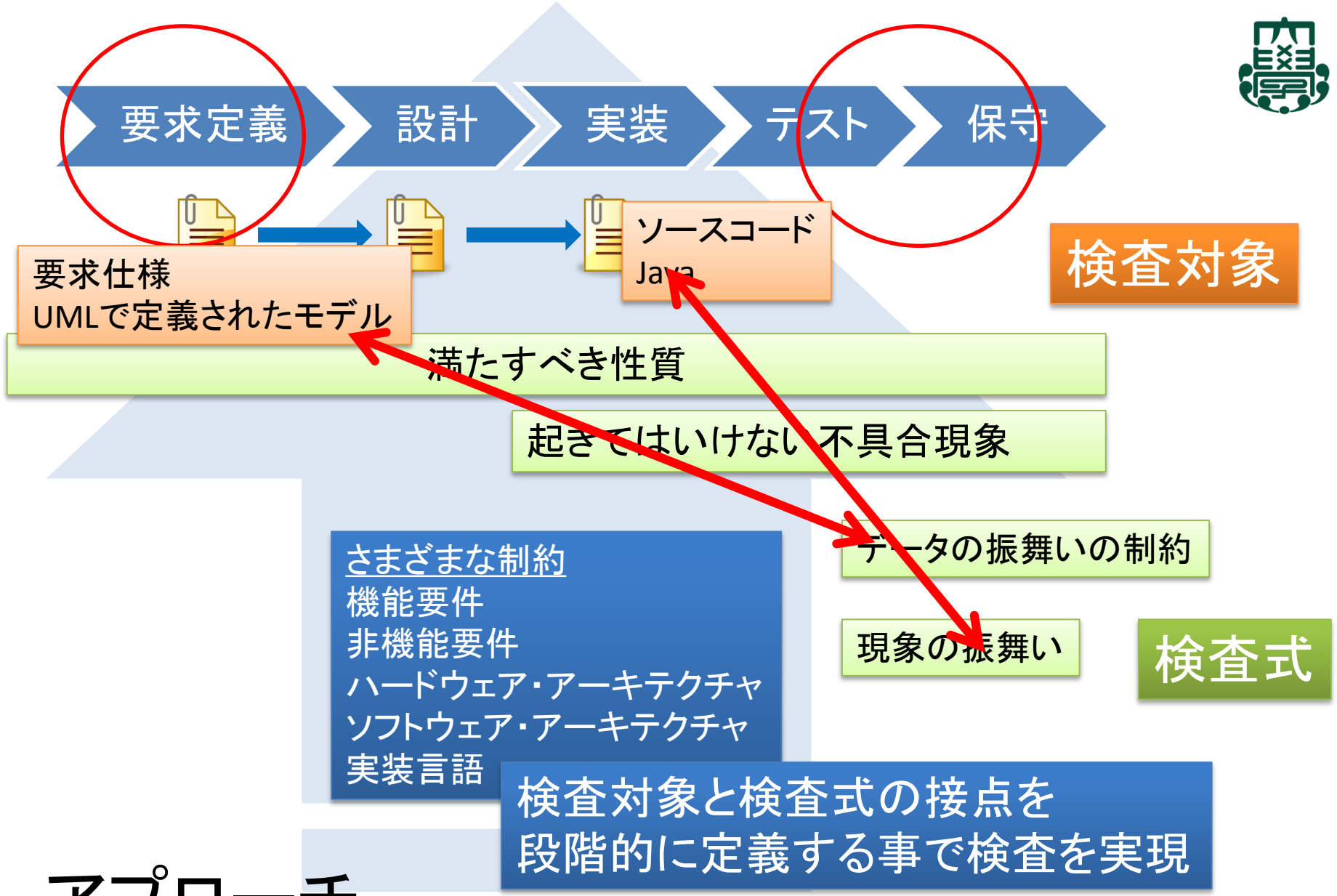
- 開発現場で用いるための課題へのアプローチ
  - 開発現場での適用シナリオを想定する
    - 3つのシナリオ
  - それぞれの場面で検査対象システムのモデルとその検証したい性質の検査式を現場の開発者が容易かつ適切に定義できる方法と支援ツール
    - **検査対象**: 要求仕様　ソースコード　⇒　システムの振舞いモデル
    - **検査式**: データの振舞い　現象の振舞い　⇒　特定対象の振舞いモデル
    - 統一感のある**支援**

解決しなければならない問題

モデル検査を行うには式の定義要素は検査対象の定義要素を
用いて定義しなければならない

ソースコード
全ての要件が定義されている
しかし、表現は多様
性質はわかっていても
コード上の定義要素を使って検査式を
定義するのは大変

要求仕様
UMLでユースケースの手順とデータは定義
しかし、自然言語記述の曖昧性が残る
要求を分析している段階で厳密に書き始めることは難しい
定義要素を使って検査式をいきなり定義するのは大変


要求定義
設計
実装
テスト
保守
要求仕様
UMLで定義されたモデル
ソースコード
Java
検査対象
満たすべき性質
起きてはいけない不具合現象
さまざまな制約
機能要件
非機能要件
ハードウェア・アーキテクチャ
ソフトウェア・アーキテクチャ
実装言語
データの振舞いの制約
現象の振舞い
検査式
検査対象と検査式の接点を
段階的に定義する事で検査を実現

アプローチ

課題と中間目標と解決策

目標:
開発現場でモデル検査による検査を一般的な開発者が有効利用可能な場面を想定
検査方法とその支援ツールを研究開発

要件定義プロセスにおける要件定義の不整合の早期発見

UML2UPPAAL

モデル駆動要求分析手法で定義したUML要求分析モデルからUPPAALモデルを生成する方法の確立
データのライフサイクルおよび属性の制約に基づく業務セオリーの策定

運用時の想定外の使用による不具合の特定

業務セオリー

ソースコードからその制御フローを表すUPPAALモデルを生成する方法の確立
不具合現象や業務システムに必須の業務セオリーの策定

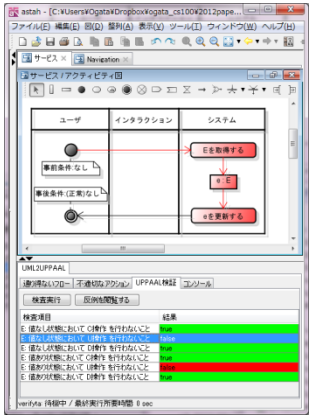
満たすべき性質
不具合現象

Source2UPPAAL

マイグレーションによるシステムの再構築時のシステムの仕様の保証

システムのマイグレーション事例の分析による業務セオリーの策定

要件定義プロセスにおける要件定義の不整合の早期発見
達成できたこと

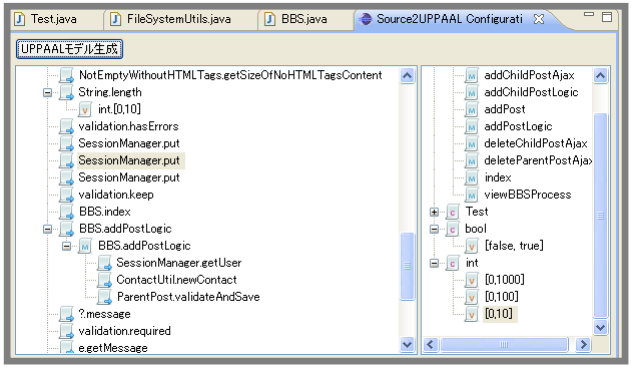


- 検査方式
  - 要求分析モデルに対して、業務セオリーを検査したい対象データのステートマシン図で定義
  - UPPAALモデルとその検査式を自動生成
- 検査できた性質
  - 到達可能性
  - システムの永続化データに対して定義した基本的な性質であるCRUDの振舞いとシステムの全サービスを定義した振舞いモデル間に矛盾が発生しない。
  - セキュリティ属性が定義されたデータのセキュリティ属性に関する基本的な性質に対して、システムのあるサービスがその属性に関する適切な振舞いを満たしている。

※「適切な」の意味は、セキュリティ評価標準規格であるコモンクライテリアによって定義

運用時の想定外の使用による不具合の特定
達成できたこと

- 検査方式
  - アプリケーションコードに依存しない不具合現象をモデル化
  - 開発者が、関連するソースコードのメソッドを段階的に、非決定性をもつ値を設定しながら、検査
  - これらの作業をツールで支援



- 検査できた性質
  - 到達可能性：制御により期待される結果が得られない場合に、すべての制御フローが全て通りえる状態であるかを検査する。検査式は、生成されたロケーションへの到達の検査であり、自動的に生成できる。
  - 観測できる状態として「停止しない」ことを検査する。無限ループのモデルを制御の条件式に対して設定することで、無限ループの発生を検査する。検査式は無限ループ状態のロケーションへの到達の検査であり、自動で生成できる。

マイグレーションによるシステムの再構築時のシステムの仕様の保証
達成できたこと

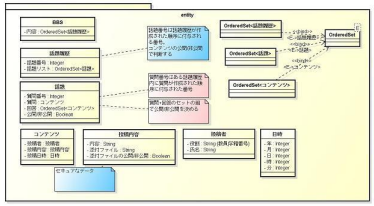
- 検査方式
  - 仕様を理解している技術者が、あるデータの識別したい状態とそれらの間の遷移によって、そのデータの満たすべき性質を定義する
- 検査できる性質
  - その振舞いが、ソースコードのどの要素に対応づくかを特定できた場合に、検査を行うことが可能

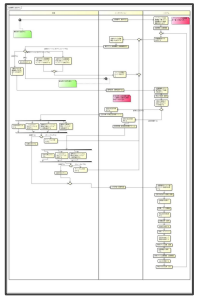
要求分析モデルと業務セオリーの定義
検査プロセス
検証実験

UML2UPPAAL

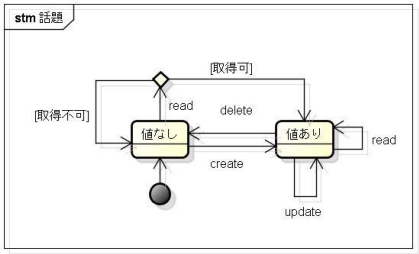
要求分析モデルと業務セオリーの定義

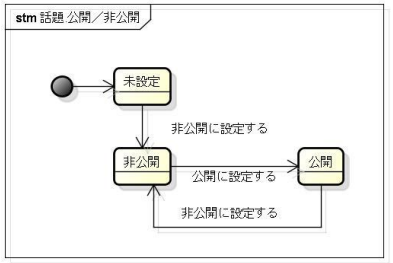
- 要求分析モデル定義プロセス
  - ユースケースを抽出
  - UMLのアクティビティ図とクラス図によりユースケースを定義
  - ユースケースの関係を定義
  - オブジェクトノードをグルーピング



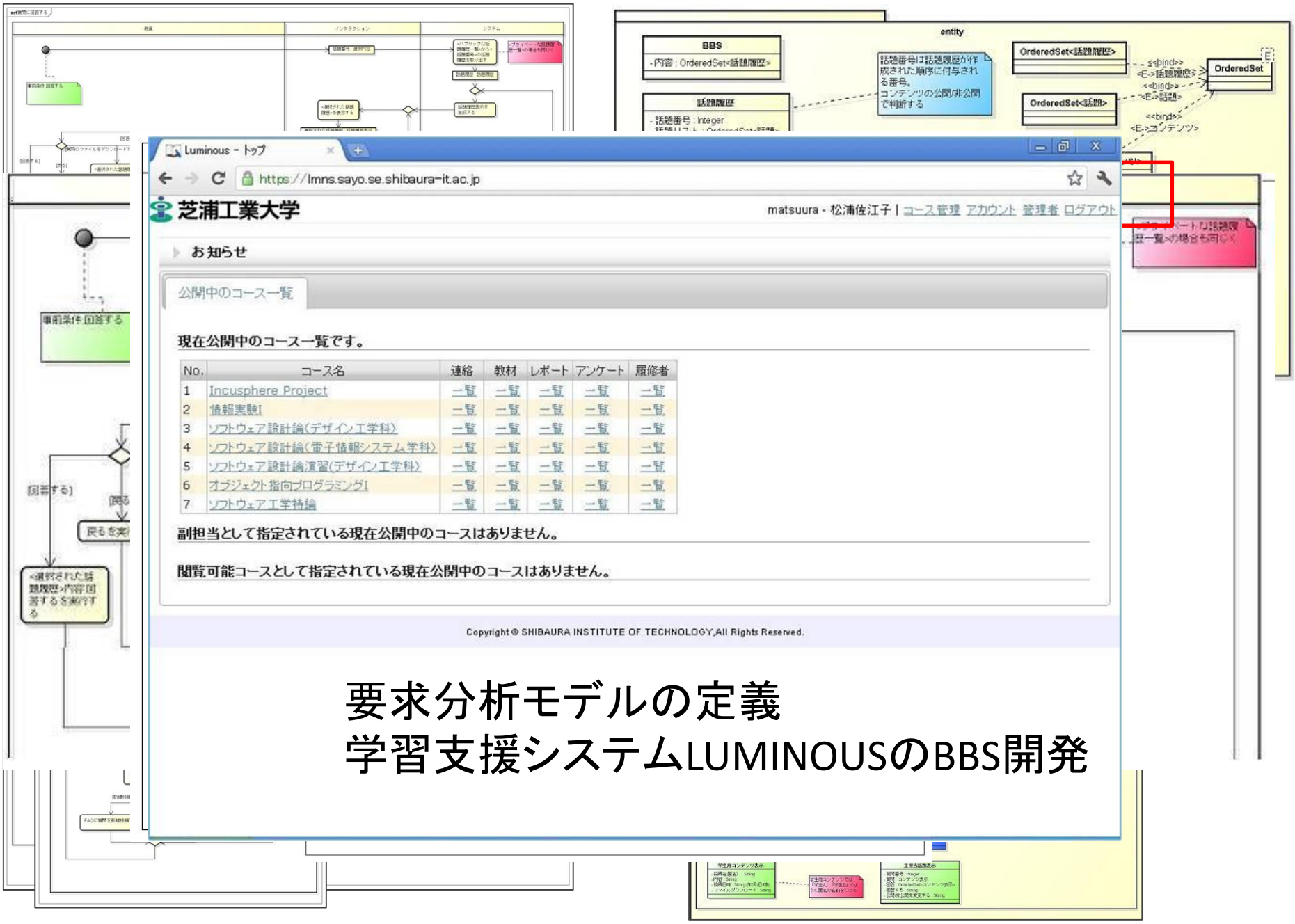


- 業務セオリー
  - ユースケースに登場したクラスの識別したい状態を抽出
    - 値をもつ・もたない
    - 属性Xが＊＊
    - その遷移イベントを定義

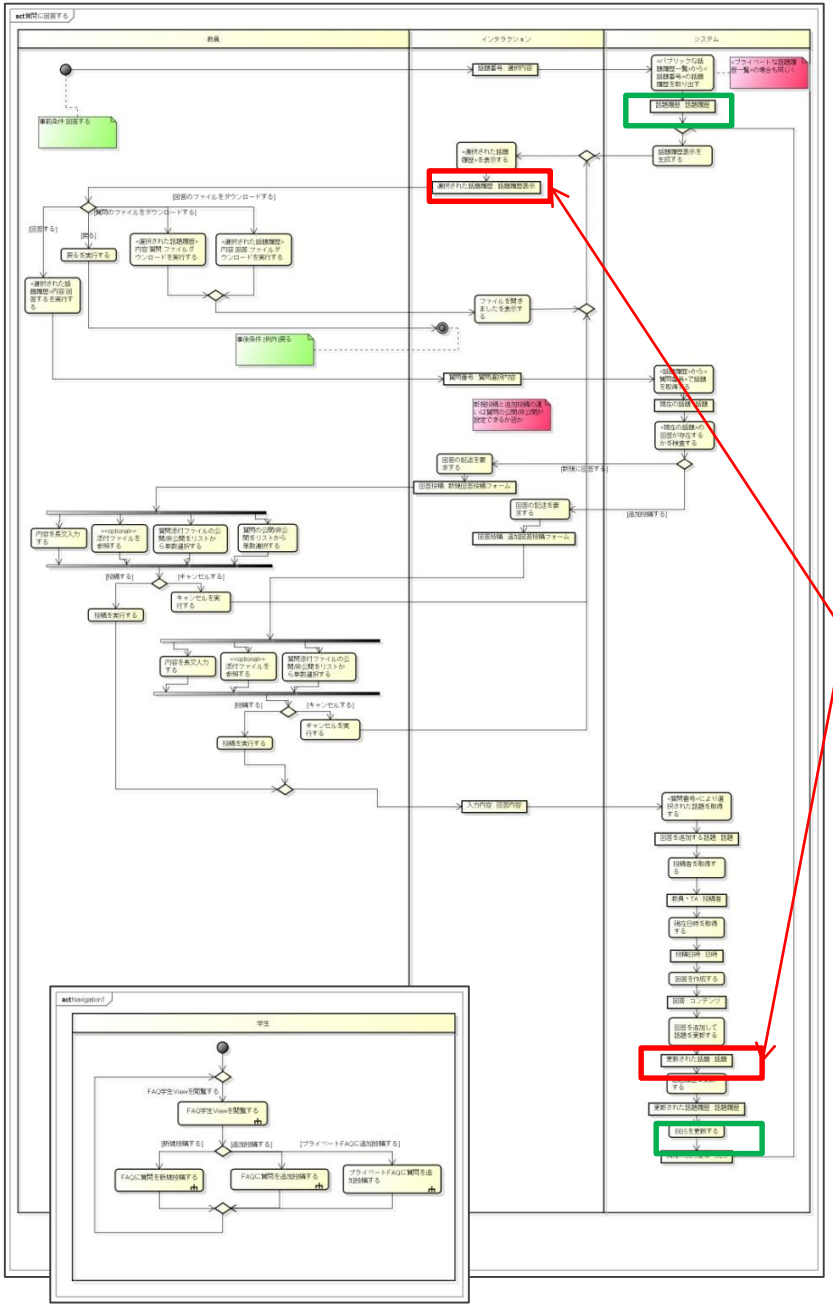


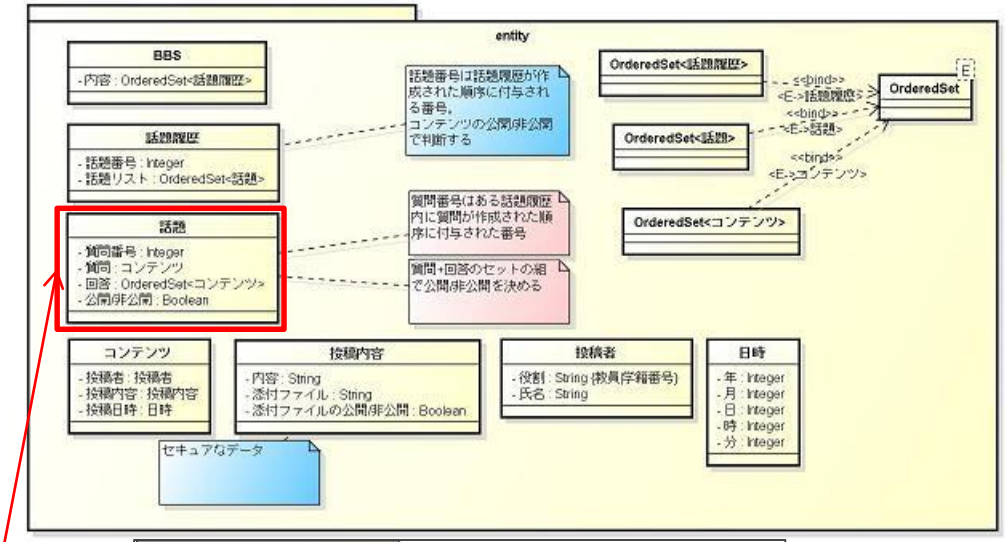


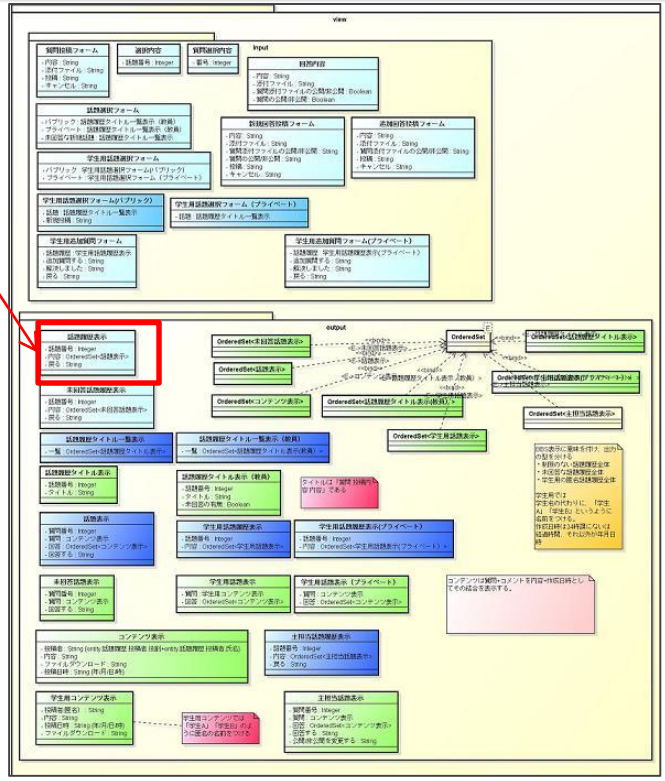
- 要求分析モデルと業務セオリーの接点を整理
  - アクティビティ図のアクションと遷移イベントを対応させる
  - アクティビティ図の遷移条件をオブジェクトノードの状態で定義



要求分析モデルの定義
学習支援システムLUMINOUSのBBS開発




entity
BBS
- 内容 : OrderedSet<話題履歴>
話題履歴
- 話題番号 : Integer
- 話題リスト : OrderedSet<話題>
話題
- 質問番号 : Integer
- 質問 : コンテンツ
- 回答 : OrderedSet<コンテンツ>
- 公開/非公開 : Boolean
話題番号は話題履歴が作成された順序に付与される番号。
コンテンツの公開/非公開で判断する
質問番号(はある話題履歴内に質問が作成された順序に付与された番号
質問+回答のセットの組で公開/非公開を決める
OrderedSet<話題履歴>
OrderedSet<話題>
OrderedSet<コンテンツ>
OrderedSet
コンテンツ
- 投稿者 : 投稿者
- 投稿内容 : 投稿内容
- 投稿日時 : 日時
投稿内容
- 内容 : String
- 添付ファイル : String
- 添付ファイルの公開/非公開 : Boolean
投稿者
- 役割 : String (教員/学籍番号)
- 氏名 : String
日時
- 年 : Integer
- 月 : Integer
- 日 : Integer
- 時 : Integer
- 分 : Integer
セキュアなデータ

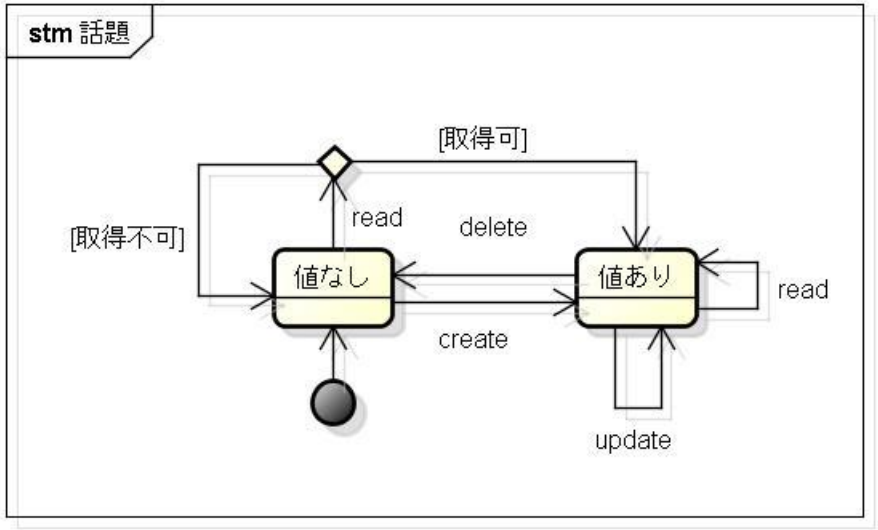

view
input
output

事例開発

① 大学院授業課題：大学生協教科書販売システム
② 授業で用いるグループワーク支援システムGWSS
③ 大学で運用しているLMS　LUMINOUSの拡張機能(BBS)
④ 研究室内図書管理システム (2009年度版）
⑤ 研究室内図書管理システム (2011年度版）

モデル名	①	②	③	④	⑤
クラス数	110	162	58	33	45
属性数	387	157	112	91	125
ユースケース数	11	13	9	6	7
アクション数	390	315	183	119	138
サイクロマチック数の平均	22.9	28.2	14.9	15	12.3
フローとアクション数の平均	106.5	85.7	56.1	64.3	58
要素数の平均	65.5	60.5	39.5	43.5	39.57

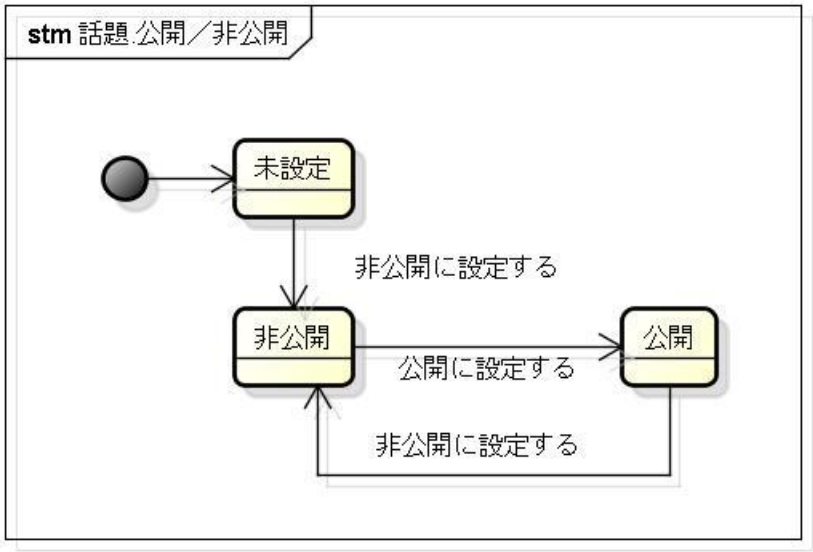
業務セオリーの定義

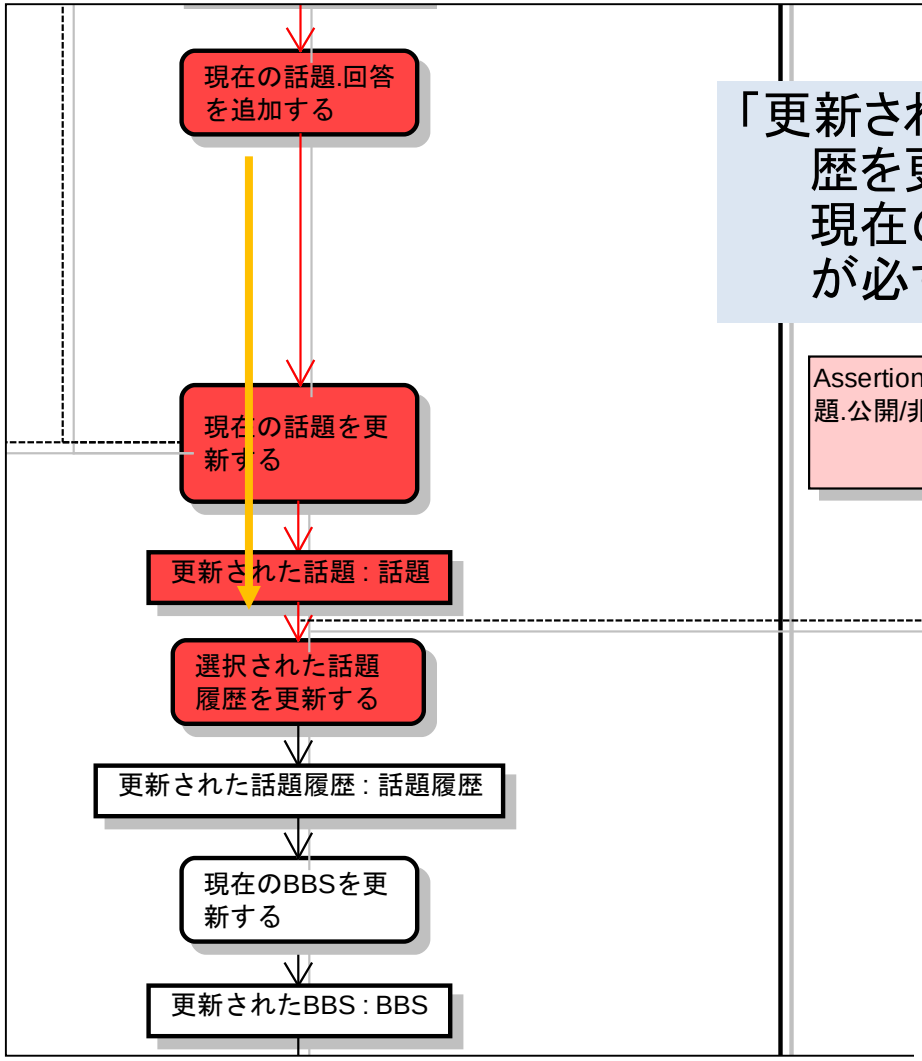


クラス「話題」の業務セオリー
取得できないこともある
まだ値がない状態で更新はできない！

対象システムでは常に値があるクラスなら
「値あり」の状態だけが許容される

話題の属性である公開/非公開の業務セオリー
生成時は未設定
初期値は非公開
設定することで公開⇔非公開を遷移する

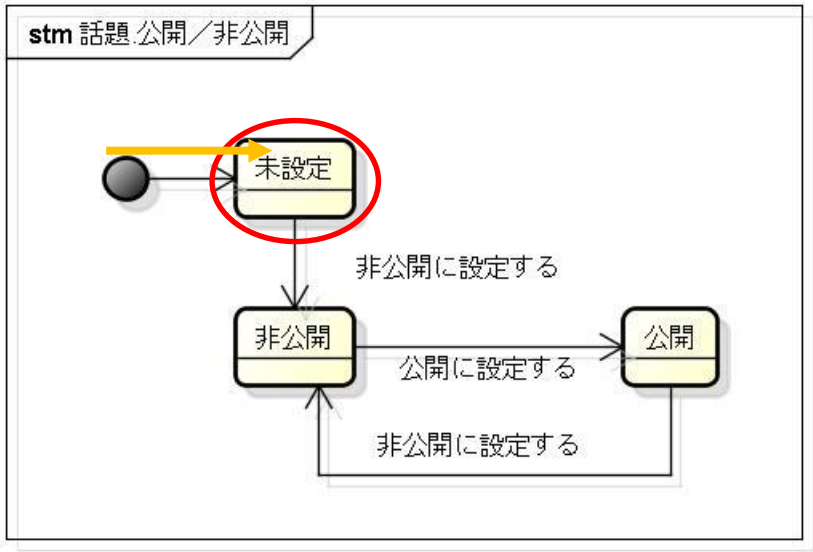




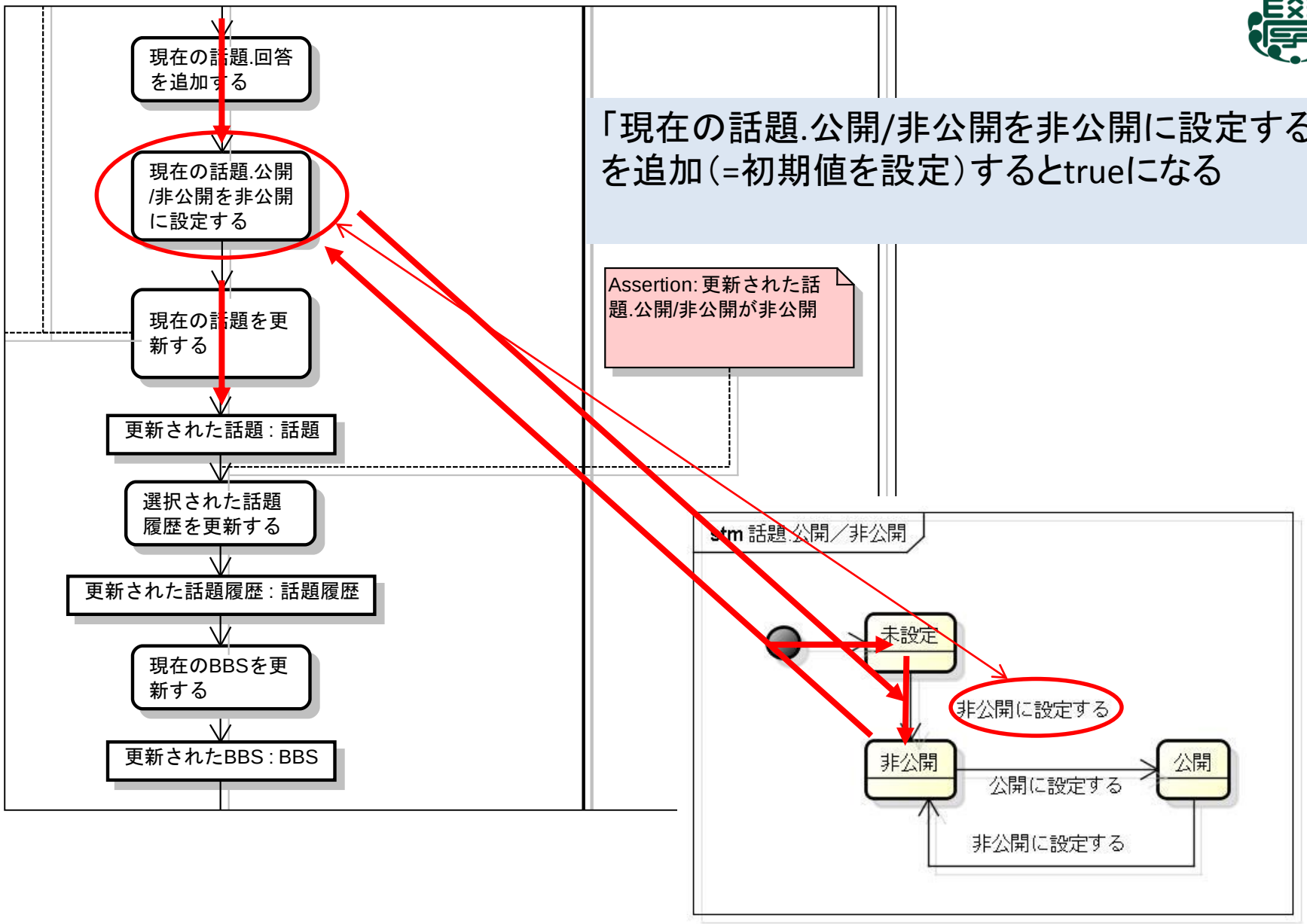
「更新された話題 から 選択された話題履歴を更新する において 更新された話題, 現在の話題:話題[instance=5]が非公開が必ず成功すること」がfalse

Assertion: 更新された話題.公開/非公開が非公開

「話題」の属性「公開／非公開」が満たすべき性質

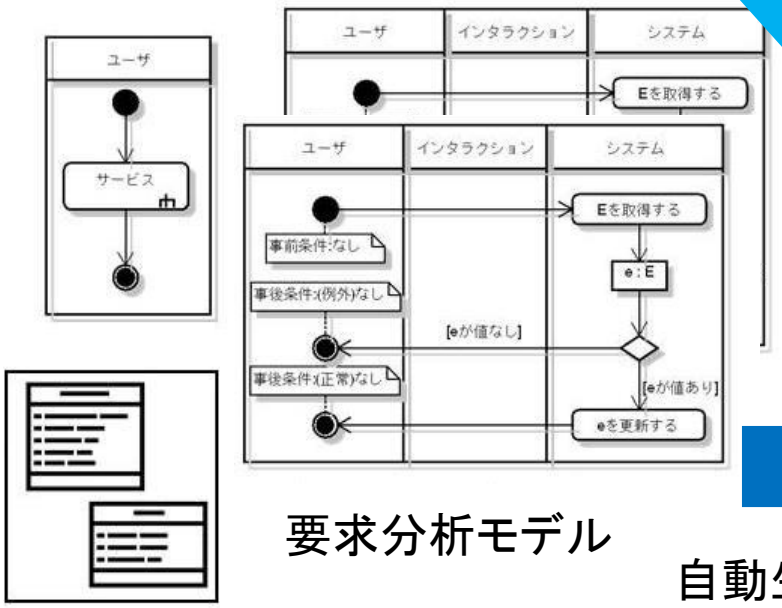


「質問に回答する」というユースケース



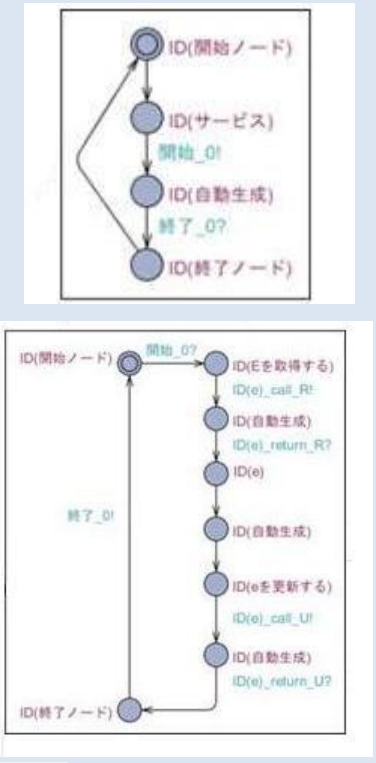
「現在の話題.公開/非公開を非公開に設定する」を追加(=初期値を設定)するとtrueになる

フィードバック　モデルの修正

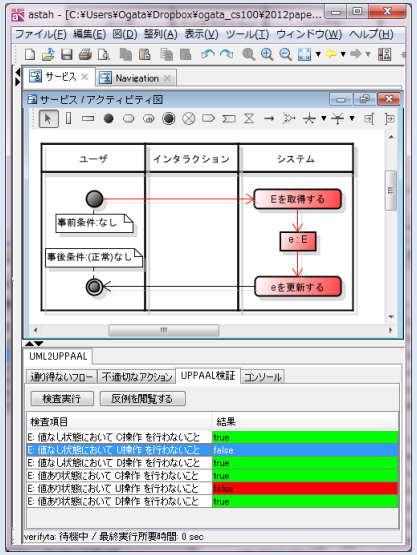


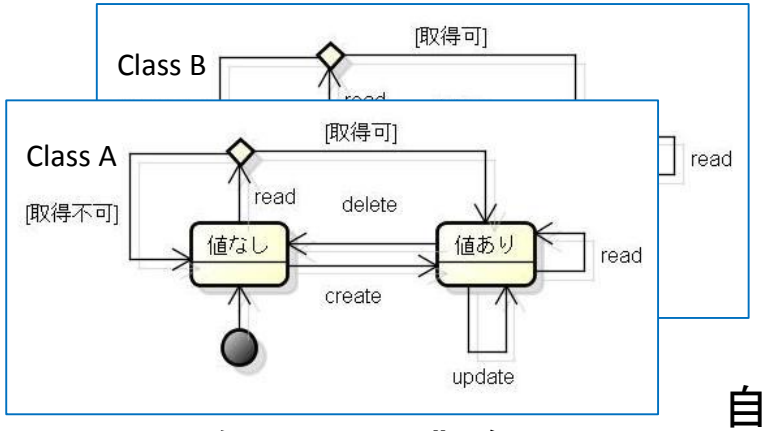
要求分析モデル

自動生成



検査式の実行
反例の表示

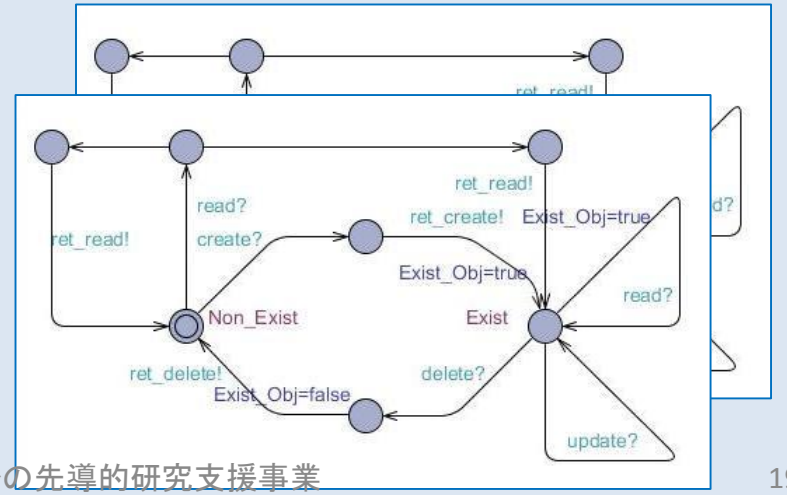




クラス毎のCRUD業務セオリー

自動生成

検査式A　検査式B



実験結果の分析

名称	説明	発見数
分岐判定記述漏れ	業務セオリー上でReadの値あり／なしを非決定に決定する分岐が存在する場合に、それに対応したReadの値あり／なし分岐を記述していない問題	10
分岐判定記述漏れによって発見されたモデルの問題	値あり／なしによる分岐判定を考慮しない事によって生じた、値なし状態でのUpdate／Deleteに関する問題	2
値ありフローの中でのオブジェクトのCreate問題	Createは値なし状態において作成させるべきで有り、値あり状態でのCreateでは、サービス期間中にオブジェクトを作成されない問題	1

名称	説明	発見数
クラス間の関連・属性が解釈されない問題	クラス間の関連と属性を対象とする解釈機構が存在しない為、その意図を正しくモデルに反映できない問題	4
値なしが取り得ないRead	Readの結果が必ず値ありになる場合に対する問題。業務セオリーの定義はエンティティ単位にしか行えないが、オブジェクト単位に定義したい場合がある。	7

その他、定義ミス、定義漏れ等　合計83個の発見

UML2UPPAAL検査事例

システムの永続化データに対して定義した基本的な性質であるCRUDの振舞いとシステムの全サービスを定義した振舞いモデル間に矛盾が発生しない。

① 大学院授業課題：大学生協教科書販売システム
② 授業で用いるグループワーク支援システムGWSS
③ 大学で運用しているLMS LUMINOUSの拡張機能(BBS)
④ 研究室内図書管理システム (2009年度版）
⑤ 研究室内図書管理システム (2011年度版）

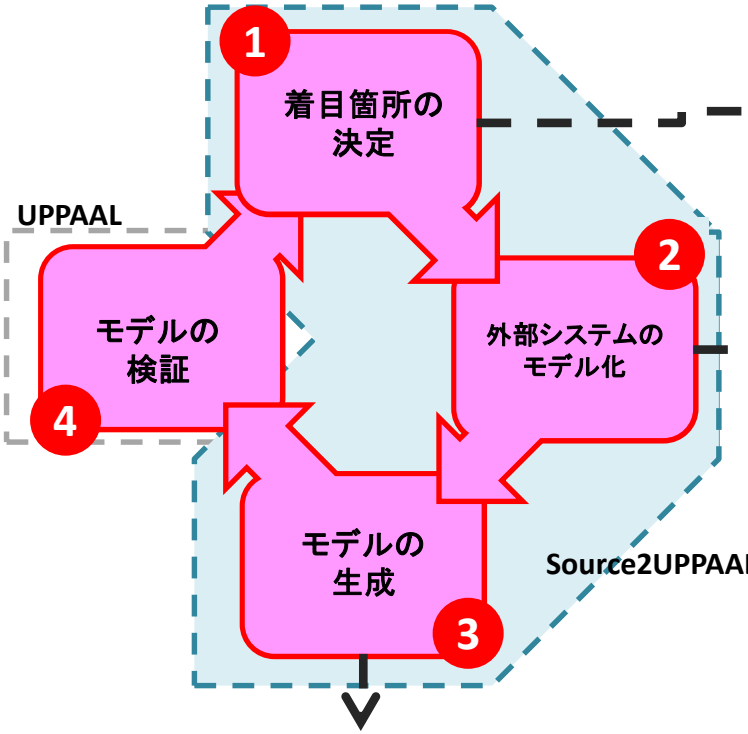
セキュリティ属性が定義されたデータのセキュリティ属性に関する基本的な性質に対して、システムのあるサービスがその属性に関する適切な振舞いを満たしている。

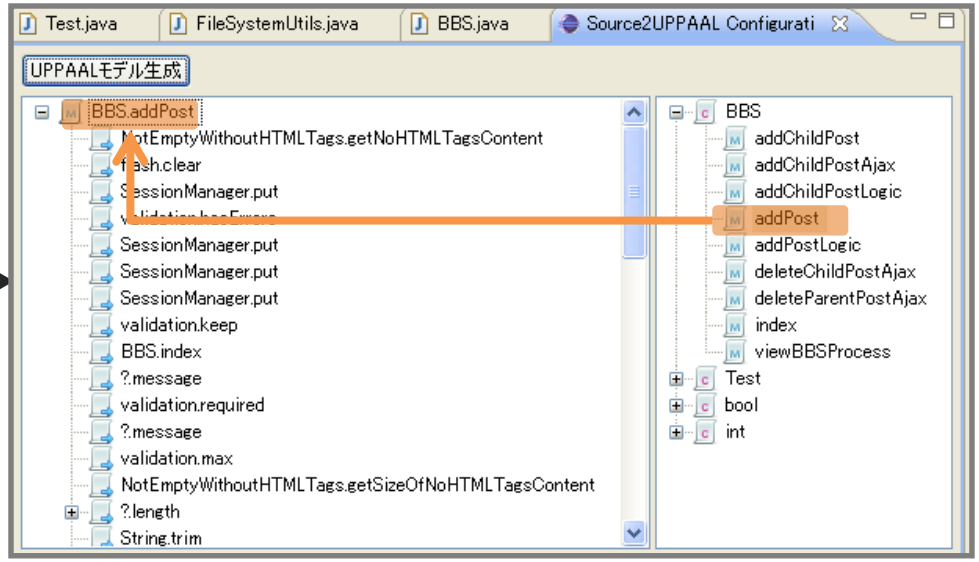
- 大学で運用しているLMS LUMINOUSの拡張機能(BBS)のアクセス制御方針に関わる検査

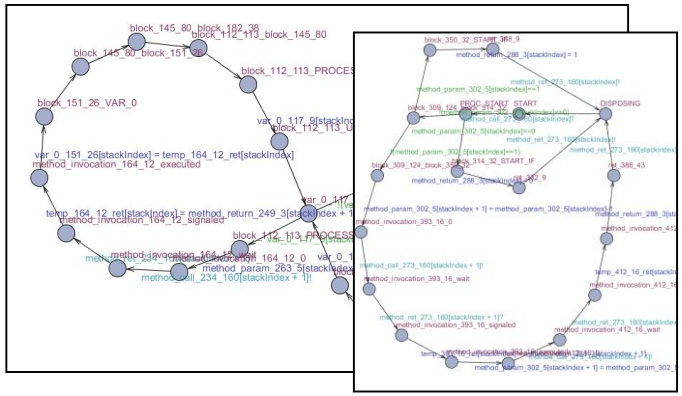
検査概要

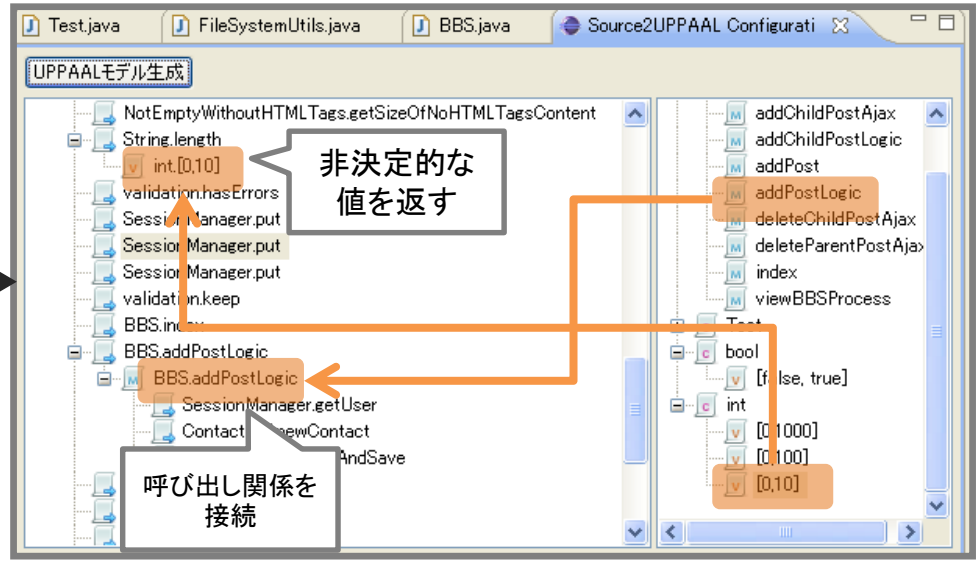
事例開発

Source2UPPAAL


1
着目箇所の
決定
UPPAAL
2
外部システムの
モデル化
モデルの
検証
4
モデルの
生成
3
Source2UPPAAL


Test.java
FileSystemUtils.java
BBS.java
Source2UPPAAL Configurati
UPPAALモデル生成
BBS.addPost
NotEmptyWithoutHTMLTags.getNoHTMLTagsContent
Flash.clear
SessionManager.put
SessionManager.put
SessionManager.put
SessionManager.put
validation.keep
BBS.index
?.message
validation.required
?.message
validation.max
NotEmptyWithoutHTMLTags.getSizeOfNoHTMLTagsContent
?.length
String.trim
BBS
addChildPost
addChildPostAjax
addChildPostLogic
addPost
addPostLogic
deleteChildPostAjax
deleteParentPostAjax
index
viewBBSProcess
Test
bool
int




Test.java
FileSystemUtils.java
BBS.java
Source2UPPAAL Configurati
UPPAALモデル生成
NotEmptyWithoutHTMLTags.getSizeOfNoHTMLTagsContent
String.length
int.[0,10]
validation.hasErrors
SessionManager.put
SessionManager.put
SessionManager.put
validation.keep
BBS.addPostLogic
BBS.addPostLogic
SessionManager.getUser
非決定的な
値を返す
呼び出し関係を
接続
addChildPostAjax
addChildPostLogic
addPost
addPostLogic
deleteChildPostAjax
deleteParentPostAjax
index
viewBBSProcess
bool
int
[0,1000]
[0,100]
[0,10]

Source2UPPAAL検査事例

到達可能性：制御により期待される結果が得られない場合に、すべての制御フローが全て通りえる状態であるかを検査する。検査式は、生成されたロケーションへの到達の検査であり、自動的に生成できる。

- ETロボコンプログラムへの適用
  - ドリフトターンと呼ばれるレース開始後に決定されるペットボトルの位置によって、ターンエリアの旋回ルートを変更するという難所の走行プログラムにおける不具合
  - 現象：走行アクションの基点となるペットボトルの検出ができない

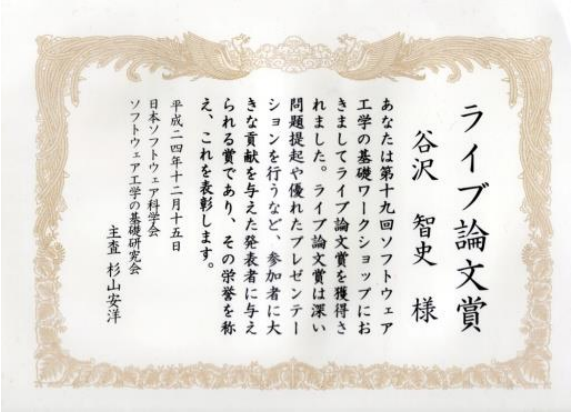
観測できる状態として「停止しない」ことを、無限ループのモデルを制御の条件式に対して設定することで、無限ループの発生を検査する。検査式は無限ループ状態のロケーションへの到達の検査であり、自動で生成できる。

- Apache Commonsのバグへの適用
- 会計伝票発行における無限ループ

発表とコメント

- CRUD の観点からシステムの振舞いを抽象化してモデル検査を適用するというアプローチは、現実的な形式検証の実現を目指す上で独創的かつ有望と考える
- 分析者が検査式（CTL式）をそのつど新規に書きくだす必要がなく，実務者向きの技術である
- CRUDは情報システムの基本という割り切りをもとに，形式手法導入の突破口としようという姿勢が読み取れ，興味深い

- 手法の理論的な妥当性、および現実のシステム検証に対してどの程度有用か
- 「CRUD以外」を特定の（複数の）用語でどう表現できるのか


ライブ論文賞

谷沢　智史　様

あなたは第十九回ソフトウェア工学の基礎ワークショップにおきましてライブ論文賞を獲得されました。ライブ論文賞は深い問題提起や優れたプレゼンテーションを行うなど、参加者に大きな貢献を与えた発表者に与えられる賞であり、その栄誉を称え、これを表彰します。

平成二四年十二月十五日

日本ソフトウェア科学会
ソフトウェア工学の基礎研究会
主査　杉山安洋

問題点と今後の課題

要件定義プロセスにおける要件定義の不整合の早期発見：

- コレクションとその要素に関する振舞い、オブジェクトとその属性であるオブジェクトの連動等の定義方法
- 要求分析モデルを段階的な形式化と複雑さの回避方法の検討

運用時の想定外の使用による不具合の特定：

- 無限ループ以外の不具合現象例のモデル化を要件定義プロセスの方針と合わせてステートマシンで定義し、検査式を自動生成することを検討
- 反例の解析により、修正を支援する方法の検討
- ソースコード理解の支援

マイグレーションによるシステムの再構築時のシステムの仕様の保証：

- 満たすべき性質を「着目するデータの振舞い」としてテーブルまたはステートマシン図を使用して定義することを検討
- 複数の言語に対応した検査ツールを実現することが必要