トップエスイー修了制作

エンタープライズ系システムへのAlloyの適用の検討

東芝ソリューション株式会社　橋本憲幸　hashimoto.noriyuki@toshiba-sol.co.jp

開発における問題点

高品質なシステムを開発する手段として形式手法が提案されている．近年，形式手法をエンタープライズ系システムへ適用する試みがなされているが，形式手法のツールの1つであるAlloyの適用事例は少なく，現場で実際に使うためのノウハウが不足している．

手法・ツールの適用による解決

Alloyをエンタープライス系システムの検証に試用し，Alloyが有効な問題領域を評価する．高品質なシステムの開発には，上流工程の品質が重要となる．そこで，上流工程の代表的な成果物である業務フローを対象に試用を行う．

業務フローについて

業務フローの検証項目

フローの進捗：業務処理が滞ることなく，正しい状態で業務が終了すること
データの変化：業務の過程で操作されるデータ（帳票や管理台帳）に，矛盾や不整合が発生しないこと

業務フローの特性

・業務パターンが全て網羅されない．
・主要なフローが記述され，例外処理や代替処理は省略される．

発注者に仕様を確認しながら要件を決定

Alloyの特徴と選択理由

1)集合や関係，命題論理を基盤に持ち，データ構造やその制約を扱える

データ構造の記述力が豊富で，データの変化の検証に適する

2)与えられた仕様に対して，制約条件を満たすインスタンスの集合を生成し，具体例を示してくれる

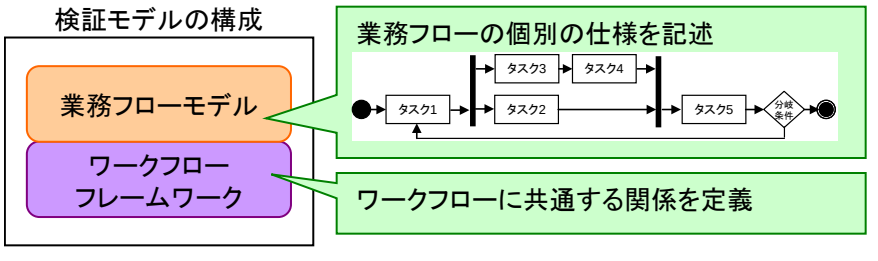
3)与えられた仕様に対して，制約条件を満たさないインスタンスの集合を生成し，反例を示してくれる

例を出して実感を深めながらモデルを検証できる

仕様が曖昧で試行錯誤することが多い上流工程において，確定した仕様からインクリメンタルに検証するのに適している

検証モデルの構成

ワークフローを記述するためのフレームワークと，検証対象の業務フローの2層構造とした．



業務フローモデル：業務フローを構成するプリミティブな要素を記述
ワークフローフレームワーク：ワークフローの枠組みと，ワークフローを実行させる仕組みを定義

フレームワークの注意点
フレームワークの制約で，デッドロックの集合を除外していたため，業務フローモデルでデッドロックの反例が発見できなかった．フレームワークの制約は，”正しくない”業務フローモデルの集合も含めないと期待した結果とならない．

評価

フローの進捗：フローを実行させる仕組みをモデル化する必要があるが，デッドロックが発生してフローが止まる例を発見できた．
データの変化：複数のフローが同時に実行されると，データを一意に特定できなくなり，間違った承認をする例を発見する目処がついた．

今後の課題

- 今回の試用で，業務フローの進捗とデータの変化の検証にAlloyが有効であることを確認できた．他の形式手法のツールとの比較評価や，別の問題領域に対する有効性の評価が今後の課題である．
- 検証モデルのフレームワーク部分を完全に独立化することができなかった．他の業務フローも扱えるように，汎用化・独立化するのが望ましい．