トップエスイー修了制作

ERPバッチ処理フレームワークへのモデル検査の適用

SCSK株式会社　齋藤 誉　h.saitoh@scsk.jp

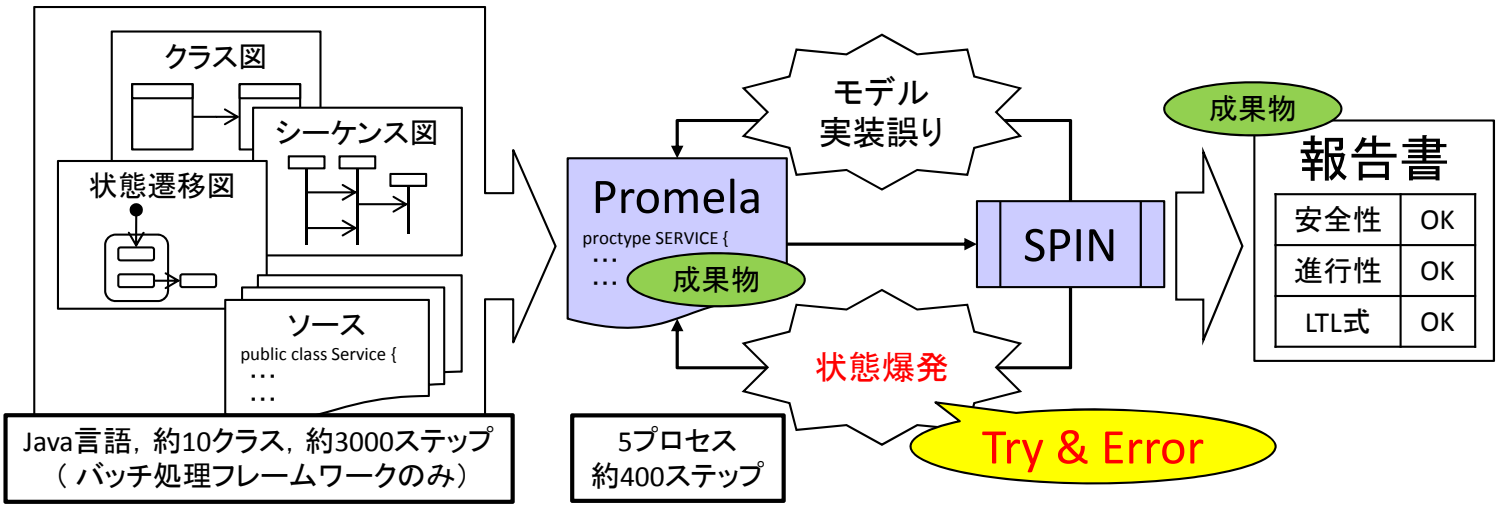
開発における問題点

フレームワークに対する「業務処理に障害があっても，システム全体としては停止することなく処理を継続する」要件に対して，従来のテストによる検証では，タイミングにより稀に発生する想定外の「状態」を再現することが困難であり，完全な検証が不可能だった．

手法・ツールの適用による解決

フレームワークに対して，モデル実装言語 ”Promela”，モデル検査ツール “SPIN” を使用したモデル検査手法を適用することにより，「発生しうる状態を網羅」した厳密な検証が可能となる．
開発プロセスへのモデル検査手法導入に向けて，作業工程，成果物の整理，工数の測定，課題の洗い出しを行う．

モデル検査の作業工程と成果物



検査結果・検証工数

1. 検査結果
「業務処理に障害があっても，システム全体としては停止することなく処理を継続する」要件に対して，設計上の問題がないことを確認．
2. 検証工数
検証モデル作成・検査実施： 6.0人日
状態爆発対応のTry & Error： 7.0人日

検査項目	状態数	メモリ使用量	処理時間
安全性	6,564,761	965MB	13秒
進行性	36,445,494	5,373MB	676秒
LTL式	13,425,041	1980MB	199秒

テストでは実施不可能な状態網羅

導入への課題

1. 状態爆発への対策
・状態爆発対応を少なく抑える．
・早期に対応工数を見積もる．
→ 進行性検査，LTL式検査での増加傾向を考慮し，安全性検査における状態数・メモリ使用量・処理時間の上限を設定し，モデルの改善を行う．

2. ノウハウの蓄積・マニュアル化
・JavaクラスとPromelaプロセスの対応
・内部状態遷移の削除 → 状態爆発防止
・処理ブロックのatomic化 → 状態爆発防止
・・・etc.
→ シンプルなマニュアルを作成する．

NII 国立情報学研究所 National Institute of Informatics
トップエスイー ～サイエンスによる知的ものづくり教育プログラム～