大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

トップエスイー ソフトウェア開発実践演習

分散システムにおけるモデル検査の利用と実システムとの比較

東芝デジタルソリューションズ株式会社　志田信之
株式会社日立製作所　木下崇央
株式会社リンクレア　永島裕之

注目した課題

分散システムにおける設計では、通信の遅延、データ整合性、可用性について考慮する必要がある。
モノリシックなシステムの設計と比較し、設計漏れや応答時間の増大などが発生しやすい。
そこで、分散システムの設計についてモデル検査を利用して有効性や限界を把握したい。

解決のアプローチ

マイクロサービスシステムを設計してデータ整合性と応答時間が検証できるユースケースを特定。
実システムとモデル検査を作成して、以下を実施。

- 設計とモデル検査の比較
- 実装したシステムとモデル検査の比較検証

アプローチ

要件定義 → 設計 → 検証

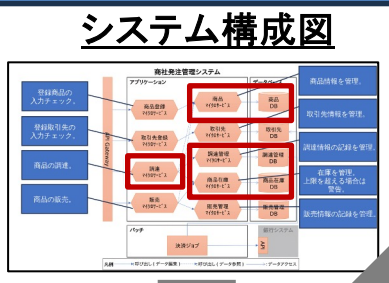
発注管理システム

1. **商品調達**
倉庫に空きがあれば商品在庫追加し、調達記録更新。

2. **商品販売**
倉庫に商品在庫があれば商品在庫を減らし、調達記録更新。

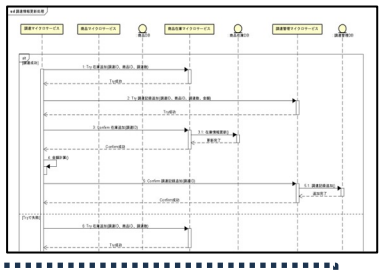
：

システム構成図

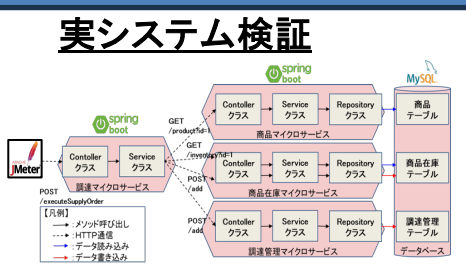


システム構成図を作成し、実装範囲を決定
実装範囲についてシーケンス図作成

シーケンス図

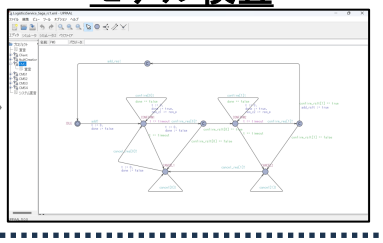


実システム検証



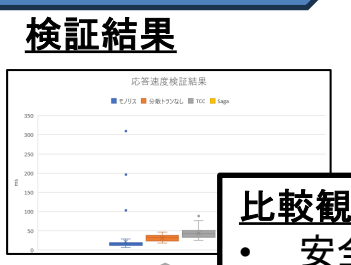
検証：モノリス、分散トランなし、あり(TCC)、あり(Saga)

モデル検査



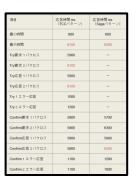
シーケンス図を基に実システムと検査モデルを作成

検証結果



検証結果

特性	概要	検査式	結果(TCC)	結果(Saga)
安全特性	デッドロックしない	A[] (not deadlock) or (User.SUCCESS) or (User.FAILED)	TRUE	TRUE
活性特性	要求が必ずいつかは必ず入口処理が完了する	User.REQUESTED --> User.SUCCESS	TRUE	TRUE
データ関依存	マイクロサービス間の状態が一致	A[] (User.SUCCESS imply (Child1.completed == true and Child2.completed == true))	TRUE	TRUE
データ関依存	追加要求した数量分在庫が増加する	A[] (User.SUCCESS imply Child1.stock == 15) （※）	TRUE	TRUE



比較観点を基に双方を検証して、結果を比較

比較観点

- 安全特性
- 活性特性
- データ依存
- 応答時間

検証結果

設計面について

設計の妥当性確認に有効。
設計漏れ・意図しない動作を発見可能。

性能面について

応答時間の見積もりに有効。
環境毎の見積もりの精度向上が必要。

実適用の課題と対策

【課題】
応答時間見積もり精度向上のため、クラウド実装時にネットワーク環境を反映した適切なモデルのパラメータ設定が必要。

【対策】
ネットワークモデルの導入。
ネットワーク環境における事前実測。
クラウド基盤におけるカタログスペック調査。