トップエスイー修了制作

Webベース監視制御システムにおける View model同期の信頼性評価とその検証

株式会社東芝インダストリアルICTソリューション社　古城仁士　masashi.kojo@toshiba.co.jp

開発における問題点

監視制御システムとしてのWebアプリケーションは,サーバ側での状態変化を一定時間内に表示できる必要があるなど,高い動的性と信頼性が求められる.このためブラウザ上のView modelをサーバ側にも設け,これらを自動同期させる構造を採用しているが,通信ロスや通信断,並列動作時にも同期が正しく行われることを通常のテストでは確認困難.

手法・ツールの適用による解決

弊社フレームワークのView model同期処理コードを対象とし,通常のテストでは検出困難なタイミング問題等の不具合が無いかどうかをSPINによるモデル検査で確認.

検証項目と検証モデル

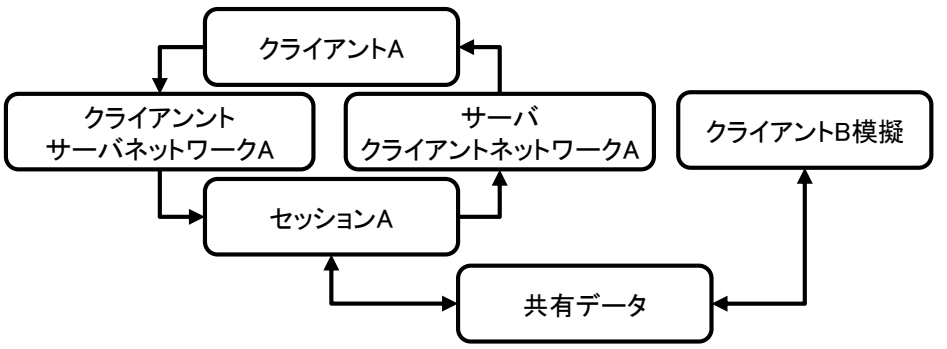
抽出した検証項目

- サーバ再起動後,ブラウザ保有のView model値に再同期される(またはその逆)
- 一時的通信断後View modelが再同期される
- 再同期時にView model値が振動しない
- 複数ブラウザが同一View modelを参照する場合にも正しく同期される

通信プロトコル上の制約

- 一方のみしか通信断を検知しない場合がある
- 通信ロス,順序入れ替えが発生しうる

使用した検証モデル



検証結果

各検証式の状態数と検証時間

検証式	状態数(百万)	所要時間(秒)
検証式1	5,790	406,000
検証式2	58	114
検証式3	77	151
検証式4	74	172
検証式5	37	82
検証式7	162	329
検証式8	162	321

ブラウザ側がループに陥る反例を1件検出.反例は実プログラム側にも存在することを確認し,修正を実施.

各国パケットロス率1～5%,毎秒0．05回メッセージとすると、反例は年間約1～40回発生.

反例発生後は再起動が必要.

Piggyback効果などにより反例は通常のテストにて見つけることは困難であり,モデル検査が有効.