様式 C-19

科学研究費補助金研究成果報告書

平成２１年　６月　１日現在

研究種目：若手研究（B）
研究期間：2007～2008
課題番号：19700029
研究課題名（和文）　Reverse Ajax による分散協調的統合システム検証環境の構築

研究課題名（英文）　Development of a Multi-user, Multi-platform, and Multi-method System Verification Environment with Reverse Ajax

研究代表者
森本 祥一（SHOICHI MORIMOTO）
産業技術大学院大学・産業技術研究科・助教
研究者番号：00433186

研究成果の概要：本研究では，利用者の OS やネットワーク接続環境，個々の形式手法や検証ツールに依存しない情報システム仕様記述・検証のための総合環境を開発した．この環境を用いることにより，手法やユーザの環境に依存せず，Web ブラウザのみを用いて検証対象を形式的に記述・検証することができる．また，複数人で同時に協調して作業することにより，形式的記述・検証過程における知見や経験などを共有し，検証の負担を軽減，開発者を支援する．

交付額

（金額単位：円）

	直接経費	間接経費	合　計
2007 年度	600,000	0	600,000
2008 年度	500,000	150,000	650,000
年度			
年度			
年度			
総　計	1,100,000	150,000	1,250,000

研究分野：総合領域
科研費の分科・細目：情報学・ソフトウエア
キーワード：ソフトウエア工学

１．研究開始当初の背景

（１）従来ソフトウェア工学の分野では，国家機密事項が関わる軍事用のシステムや人命が関わる航空管制・医療用システム等，些細なバグや誤動作も許されないミッション・クリティカルな情報システムにおいて，形式手法による仕様記述と検証が不可欠とされてきた．そのシステムは本当に信頼し得るかを数学的に厳密に検証するためである．一方で，Web 技術や組込み技術の発展に伴ってソフトウェアは我々の生活の様々な局面に利用されるようになり，その規模や用途は年々多様化・複雑化している．よって，あらゆる情報システムにおいて，形式手法によるシステム検証が欠かせない状況となってきている．

（２）一般的に形式手法では，検証対象のシステムを形式言語で記述し，更にその検証対象のシステムが満たすべき性質を検証者自らが作成しなければならないが，これには専門的な知識を必要とする．このため，専門的な知識を持たない検証者は検証すべき性質が何なのか，どう記述してよいのか分からないこともあり得る．また，形式手法をサポートしている大抵のツールは，大学等の研究機関によって開発され公開されており，公開以後ツール単体としての機能改善は停滞・打切りしているものが多い．

以上のような理由から，よりソフトウェア開発の現場で導入しやすい実用的なツールが求められており，UML といったソフトウェアの現場で広く利用されている記法から

形式的記述を導き出す手法など，様々な試行錯誤がなされている．しかし，現状ではこれらのアプローチは個々に定義されており，また利用されている基盤技術や形式的な記法もまちまちであり，実際に利用者側から見てどの手法・記法・ツールが適用することができるのか，開発しているシステムに最も適しているのか，判断することは難しい．

２．研究の目的

本研究では，手法・記法によらないシステム検証のための統合環境を構築する．また，開発現場で用いること，形式手法の専門的知識の格差を吸収することを前提とし，複数のユーザで分散協調的に検証作業を行える環境を構築する．

現行の様々な形式的表記法をサーバ上で保持し，ユーザはインターネット等のネットワークを介してサーバにアクセスし，Web ブラウザ上で検証対象のシステムを形式的に記述，検証する．同一サーバにアクセスすることにより，複数人が同時に同じシステムの記述・検証をグループワークとして協調的に作業することができる．『三人寄れば文殊の知恵』という格言にもあるように，1 人では解決できない問題を複数人でコミュニケーションを取りながら作業することで対応可能にする．遠隔地からネットワークを介して専門家の助言をうけることもできる．また，新たに形式的記述法を追加する場合には，サーバ上に記法の定義をアップロードすることにより，クライアント側では特に環境を変えることなく新記法を利用できるようにする．

実現方式としては，Ajax（Asynchronous JavaScript + XML)と Latex スタイルファイルを用いる予定である．この分散協調的統合システム検証環境を用いることにより，記法やユーザの環境に依存せず，Web ブラウザを用いて検証対象のシステムを形式的に記述・検証することを可能にする．また，複数人で同時に協調して作業することにより，システムの形式的記述・検証過程における知見や経験などを共有し，システム検証の負担を軽減，開発者を支援する．

３．研究の方法

具体的な開発としては，DWR（Direct Web Remoting）というオープンソースの JavaScript～Java 間連携用フレームワークと，Latex のスタイルファイルを用いる．DWR は，Reverse Ajax という技術を実現可能であり，あるクライアントがブラウザ上で行った更新を，サーバにアクセスしている他のブラウザにリアルタイムで反映することができる．

一般的に形式手法の表記法は，Latex のスタイルファイルとして配布されているため，このスタイルファイルをサーバ上に配置し，Latex コンパイルした結果の形式的表記をクライアントのブラウザ上に表示する．新たに記法を追加する場合は，その記法のスタイルファイルをアップロードするようにする．ユーザはまず，サーバ上にプロジェクトを作成し，プロジェクトメンバーを設定する．プロジェクトメンバーは各自ブラウザからプロジェクトにアクセスしログインするとメンバー共通の作業を行うことができるようにする．各メンバーのブラウザでの作業の結果はそれぞれのブラウザに反映され，協調的に作業を進めていく．クライアント側で記述したシステム記述と検証式はサーバ上で保持し，表示/編集はクライアント側で行う MVC（Model-View-Controller）構造を取る．

検証自体の機能は，それぞれの記法ごとに対応した検証エンジンをサーバ上に配置しておき，クライアントからの指示でサーバ側で保持している記述と検証式をサーバ上の検証ツールで検証させ結果をクライアントに表示，というやりとりをクライアント側に隠蔽して行う．

また記述・検証以外の機能として，クライアント同士のコミュニケーション用のツールも用意する．ユーザが形式的記述法を知らなくても学びながら利用できるように，サーバ上にそれぞれの記法のチュートリアル等も用意しておき，また Wiki のように誰でもチュートリアルを作成/編集できるような環境を用意する．更に，作業時には Google Suggest のように，形式記述や検証式を打ち込んでいくとリアルタイムで後に続く要素をサーバ上で推測し補完する候補を表示するようにし，記法独自の論理記号等は入力用のボタンを設け，使用する記法を切り替えると動的にボタンも切り替わるようにする等，形式手法の専門家でないユーザをサポートする．

４．研究成果

本研究は，利用者のオペレーティング・システムやネットワーク接続環境，更に個々の形式手法や検証ツールに依存しない情報システム仕様記述・検証のための総合環境を構築することを目指している．2007 年度は主に以下のような研究成果を上げた．

（１）本研究で提案するシステムと，その基盤となる分散協調的作業を実現するフレームワークの設計を行った．本システムでは，形式手法に関する既存のツールや記法のた

めのファイルをサーバ上にアップロードし，これらに異なるオペレーティング・システムやネットワーク接続環境からアクセスしてWeb ブラウザ上で仕様の記述や検証が行えるようにする．その他，利用者ごとの形式手法に関する専門知識の格差を補うためのチュートリアル機能を設計した．

（2）設計したフレームワークを，Reverse Ajax 技術を用いて構築した．このフレームワークを用いると，分散されたネットワーク接続環境下で Web ブラウザを介して複数人による協調作業を行えるアプリケーションを実装可能である．

（3）上記のフレームワークを利用して，まずはZ記法という形式手法の既存の検証ツールをサーバにアップロードでき，更にインターネットを介して複数人で仕様の記述・検証ができる環境を実装した．

（4）同様に，既存のモデル検査ツール 2 種（SPIN，SMV，UPPAAL）をサーバ上にアップロードし，システムの記述・検証ができる Web アプリケーションを実装した．

また，2008 年度は前年度の成果を踏まえ，主に以下のような研究成果を上げた．

（1）前年度に開発したシステムと，その基盤となる分散協調的作業を実現するフレームワークの改良を行った．本システムでは，形式手法に関する既存のツールや記法のためのファイルをサーバ上にアップロードし，これらに異なるオペレーティング・システムやネットワーク接続環境からアクセスしてWeb ブラウザ上で仕様の記述や検証が行えるようにする．その他，利用者ごとの形式手法に関する専門知識の格差を補うためのチュートリアル機能の充実を図った．特に，データベースを用いた仕様記述の再利用機能と，これらを用いた入力補完機能を強化した．

（2）開発したフレームワークを，様々な検証へ応用できることを示した．このフレームワークを用いると，分散されたネットワーク接続環境下で Web ブラウザを介して複数人による協調作業を行えるアプリケーションを実装可能である．

（3）開発したフレームワークを利用して，isabelle，Coq，PVS，SPIN，SMV とった検証ツールを用いてインターネットを介して複数人で仕様の記述・検証ができることを確認した．また性能評価も行った．

（4）前年度と今年度の研究成果やその応用を国内のシンポジウムや国際会議において発表した．更に，雑誌論文にも公表した．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 6 件）

① 森本祥一，複数人によるシステム検証を支援するWebアプリケーションの開発，産業技術総合研究所システム検証センター算譜科学研究速報（テクニカルレポート），PS-2009-001，p. 115－122，2009 年，査読無
② 森本祥一，A Survey of Formal Verification for Business Process Modeling，International Journal of Operations and Quantitative Management Vol. 14, No. 4，pp. 237－247，2008 年，査読有
③ 長尾雄行，土屋陽介，森本祥一，中鉢欣秀，JavaScriptと非同期HTTPリクエストによる共同作業支援ミドルウェアの構築，産業技術大学院大学紀要，第 2 号，pp. 165－173，2008 年，査読有
④ 森本祥一，中鉢欣秀，シナリオの図解化による業務フロー分析，産業技術大学院大学紀要，第 2 号，pp. 193－208，2008 年，査読有
⑤ 森本祥一，中鉢欣秀，ソフトウェア開発工程における支援研究と実用化への課題，産業技術大学院大学紀要，第 1 号，pp. 105－110，2007 年，査読有
⑥ 堀江大輔，森本祥一，後藤祐一，程京徳，情報セキュリティ工学データベースシステムISEDSの開発と応用，情報処理学会論文誌Vol. 48, No. 8，pp. 2684－2698，2007 年，査読有

〔学会発表〕（計 14 件）

① 矢島賢一，森本祥一，Noor Shelia Azreen，後藤祐一，程京徳，FORVEST: A Support Tool for Formal Verification of Security Specifications with ISO/IEC 15408，The 4th International Conference on Availability, Reliability and Security (ARES 2009)，2009 年 3 月 19 日，福岡
② 森本祥一，An Educational Analysis of Consensus-Building Process in Business Domain Analysis with Conceptual Data Modeling，The IADIS International Conference on Information Systems 2009，2009 年 2 月 26 日，バルセロナ
③ 森本祥一，A Study of Value of Business Process Models from a Managerial

Viewpoint , The International Conference on Innovation in Software Engineering (ISE 2008), 2008 年 12 月 10 日, ウィーン

④ 森本祥一, 複数人によるシステム検証を支援するWebアプリケーションの開発, 日本ソフトウェア科学会 ディペンダブルシステム研究会 第 5 回システム検証の科学技術シンポジウム, 2008 年 11 月 19 日, つくば

⑤ 森本祥一, A Survey of Formal Verification for Business Process Modeling , The 8th International Conference on Computational Science (ICCS 2008), 2008 年 6 月 24 日, クラクフ

⑥ 森本祥一, Documentation Components of Software Development and their Management Based on International Standards , The 10th Workshop on Learning Software Organizations (LSO 2008), 2008 年 6 月 23 日, フラスカーティ

⑦ 堀江大輔, 森本祥一, 後藤祐一, 程京徳, ISEDS: An Information Security Engineering Database System Based on ISO Standards , The 3rd International Conference on Availability, Reliability and Security (ARES 2008), 2008 年 3 月 6 日, バルセロナ

⑧ 長尾雄行, 土屋陽介, 森本祥一, 中鉢欣秀, JavaScriptと非同期HTTPリクエストによる共同作業支援ミドルウェアの構築, 情報処理学会第 67 回プログラミング研究会, 2008 年 1 月 25 日, 仙台

⑨ 森本祥一, Classification, Formalization and Verification of Security Functional Requirements, The 34th Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM 2008), 2008 年 1 月 23 日, スモコヴェッツ

⑩ 森本祥一, Formal Musical Composition Analysis Using Music Notation and Text Processing , The inaugural International Conference on Music Communication Science (ICoMCS 2007), 2007 年 12 月 5 日, シドニー

⑪ 森本祥一, 中鉢欣秀, SBVA法によるビジネスプロセスモデリング, 情報システム学会第 3 回研究発表大会, 2007 年 12 月 1 日, 新潟

⑫ 長尾雄行, 森本祥一, 土屋陽介, 清水將吾, 村尾俊幸, 川田誠一, 情報アーキテクト育成のための PBL 教育支援についての一考察, 日本 e-Learning 学会 第 2 回 IT 専門職養成のための PBL 型教育シンポジウム, 2007 年 11 月 21 日, 熱海

⑬ 河野善彌, 陳慧, 高野英樹, 森本祥一, 学生チームによる組込システムの開発 ～10 年間の教育から～, 日本科学技術連盟 第 26 回ソフトウェア品質シンポジウム, 2007 年 9 月 6 日, 東京

⑭ 森本祥一, 程京徳, A Security Specification Library with a Schemaless Database , The 7th International Conference on Computational Science (ICCS 2007), 2007 年 5 月 29 日, 北京

〔その他〕
ホームページ等
http://www.aise.ics.saitama-u.ac.jp/~morimo/

６．研究組織
(1)研究代表者
森本 祥一 (SHOICHI MORIMOTO)
産業技術大学院大学・産業技術研究科・助教
研究者番号：00433186

(2)研究分担者
(　　)
研究者番号：

(3)連携研究者
(　　)
研究者番号：