

研究課題別 事後評価結果

1. 研究課題名: Webサービス・セキュリティ技術

2. 研究代表者: 中島 震 (国立情報学研究所 アーキテクチャ科学研究系 教授)

3. 研究内容及び成果

近年、インターネットを活用した新しいビジネスソフトウェアの基盤技術として、Webサービスが注目を集めており、コンソーシアム組織OASIS(Organization for the Advancement of Structured Information Standards)ではWebサービス連携記述言語WS-BPEL(Web Services Business Process Execution Language)の標準化が進んでいる。Webサービスの基盤となるインターネットは開放型の実行環境であるため、安全性並びにセキュリティの確保が大切である。特に、複数のWebサービスを組み合わせた高度なWebサービス連携は分散協調システムであり複雑な振舞いを示すため、論理的な機能振舞いについてデッドロック等の不具合を起こさない等の安全性の確認が必要である。さらに、機密レベルの高い情報が不用意に漏洩しないようにセキュリティに配慮する必要がある。

本研究は、WS-BPELで記述されたプログラムが安全性ならびにセキュリティの観点から不具合を持つか否かを、事前に解析する技術を開発するとともに、産業界に示せるような具体的な技術として解析ツールを試作・整備することを目標とした。特に、ソフトウェア科学の成果であるモデル検査法の技術を拡張する研究を行った。

安全性検証については、WS-BPELプログラムを並行システム記述と見なして、モデル検査法を適用すれば良いことから、既存のモデル検査ツールPromela/SPINを利用した一方、WS-BPELは通常のプログラミング言語と同様な記述を可能とするために多様な言語機能を提供しており、中間表現の導入や制御変数の抽象化といった新たな方法を導入するという工夫を行った。その結果、BPEL4WS(Business Process Execution Language for Web Services)(v1.1)仕様書記載の例題全てを正しく解析することに成功した。

情報漏洩の有無を調べるセキュリティ問題を取り扱うためには、WS-BPELに新たな概念を導入する必要がある。本研究においては、ラティスに基づくアクセス制御を用いた情報フローの方法をWS-BPELに導入するとともに、一時的なクラス低下と呼ばれる方法を採用した。また、情報フローの検査を行う手順に用いるモデル検査法について、安全性検証で用いたPromela/SPINでは順序に関わる制約条件を記号的に表現出来ず、プリミティブなデータ型にコード化しなければならないため、コード化の正しさを保証することが難しいという問題に直面した。そこで、新たな研究のアイデアとして、有限状態遷移システムであり記号的な制約条件を明示的に取り扱うことが出来る制約オートマトンを試作し、予備的な実験を行って制約オートマトンを用いる方法の有効性を確認した。

本研究は、従来から知られていたソフトウェア科学の成果であるモデル検査法という基礎

技術を背景に、Webサービス連携技術における信頼性に関わる問題点を指摘し、その解決の一つの方法を示した点に重要性がある。ほぼ同時期に、欧米各国でも同様な目的の研究が進行し発表された。初期に発表した論文が先行研究として引用されている事実から、ここに述べた本研究の意義を裏付けることが出来る。

4. 事後評価結果

4-1. 外部発表(論文、口頭発表等)、特許、研究を通じての新たな知見の取得等の研究成果の状況

期間中の外部発表、特許等の実績を示す。

発表論文： 4 件

口頭発表： 15 件

現在のwebサービスの広がり和社会基盤化を考えた場合、Webサービスの記述言語としてのWS-BPELとその言語によって実現されたシステムについて、セキュリティ面からの検証基盤を構築することは必要性が高く、その着眼点も良い。また、言語仕様の拡張も視野に入れた上でWS-BPELの安全性解析を実現したことや、情報漏洩解析法を具体化して解析ツールを試作したこと等、高く評価出来る。権威ある論文誌等での発表数も十分あり、価値ある成果を得ただけでなく広く周知させている。ただし、WS-BPELの標準化プロセスについて研究成果のフィードバックは十分ではなく、研究成果の産業界での活用を課題として残している。しかし、技術の重要性および今後の普及の可能性を考慮すると評価出来る成果である。費用対効果の面からしても少額の研究費で十分な成果と言える。

4-2. 成果の戦略目標・科学技術への貢献

本研究は、仕様記述言語からのシステム評価という観点で、新たな研究領域を切り拓き、確立し、その実用的な成果を生み出したと言える。しかしながら、標準化団体OASISが取り扱うWS-BPELの標準化プロセスと独立に研究が実施されたため、WS-BPELの標準化プロセスに十分な影響を与えることが出来なかったことは残念である。WS-BPELについては、新たな版(v2.0)が標準化され言語機能が強化されたこと、Web Service (WS) におけるセキュリティ機能の基本的なフレームワークが標準化されたことから、本研究の直接的な研究成果(手法およびツール)を現在のWS-BPELやWSに対して展開することは難しいのではないかと考えられる。一方、ソフトウェアの検証手法としてのモデル検査法については、ソフトウェアの検査に対する需要が高まりつつある現在、さらなる展開が期待出来る。このため、WS-BPELに特化している部分と、より汎用的にソフトウェア検査に活用出来る研究成果を峻別し、汎用性の高い成果を用いてさらなる研究展開が期待出来る。

4-3. その他の特記事項(受賞歴など)

本研究では、平成18年12月1日に「形式手法ワークショップ」を開催し、ソフトウェア検査・評価に対する形式手法をより広く理解してもらうための活動を展開している。このようなアウトリーチ活動が研究に含まれることは、学術性の強い研究活動と産業界における開発実態との差異を相互に理解し、より多くの成果を生み出すことに貢献するものであり、高く評価出来る。