研究課題別評価

1 研究課題名：高信頼性 Web サービス

2 研究者氏名：中島 震

3 研究の狙い：

インターネットの発展と共に Web サービスの技術が新しい業務サービスの基盤として登場した。当初は、ひとつの機能を提供する単独 Web サービスが主流であったが、最近では、複数の Web サービスを統合して新しいサービスを提供する複合サービスの技術に注目が集まっている。複合化によって多数のビジネスパートナーと連携したサービス提供が可能になる。

Web サービスの世界では、異なるベンダが開発したソフトウェア基盤がネットワーク上で情報交換する。そのため、W3C (World Wide Web Consortium) や OASIS (Organization for the Advancement of Structured Information Standards) といった中立組織を中心とする技術標準化の活動が活発になっている。Web サービス複合化の技術も、ベンダ提案段階から OASIS での標準化活動に進み、WS-BPEL (Web Service Business Process Execution Language) と呼ぶ一種の分散協調システム記述言語が提案される段階に至った。複合サービスを WS-BPEL のプログラムとして表現する。

複合サービスを表現する連携のことをオーケストレーションと呼ぶことがある。多数の演奏者である Web サービスの全体調整を行うことが特徴であり分散協調システムとみなせることを示す簡潔な用語である。一般に、分散協調システムは動作振る舞いが複雑なため、処理が進行しないデッドロックによるシステム停止などの不具合を除去することが難しい。ある複合サービスが実行中に停止すると、関連する Web サービス提供者にも影響を与える。これを安全性の問題と呼ぶ。WS-BPEL の記述を対象として安全性の観点から不具合がないことを確認する必要がある。

次にセキュリティに関する問題を考える。企業が活動の効率化を目的として、外部のコンサルタント会社等に、従来は社内で行っていた業務を外部委託することが増えている。コンサルタント会社は顧客会社の情報を入手してはじめて有用なアドバイスができる。

Web サービス技術を用いたコンサルタント業務は便利な反面、問題も大きい。顧客企業は必要な情報を Web サービスとして提供し、コンサルタント会社はノウハウを組み込んだ業務ロジックを WS-BPEL のプログラムとして表現する。顧客企業の情報や市場動向調査レポートなどの一般情報を全て Web サービスの技術を用いて収集することが可能になる。

顧客会社からみると、コンサルタントに必要とはいえ、社外秘情報が外部に出るため、取り扱いに慎重になる。コンサルタント業務を表現する WS-BPEL のプログラムが何らかの誤りによって、大切な情報を流出することがないという証拠を、コンサルタント会社に求める。WS-BPEL 記述を対象としてセキュリティの観点からの不具合がないことを確認しなければならない。

本研究課題では、WS-BPEL のプログラムを解析し、安全性ならびにセキュリティという上記の 2 つの観点からの不具合がないことを、インターネット上で実行する前に確認する技術を検討した。

4 研究成果：

4.1 安全性の解析

当初の研究目的は、WSFL (Web Service Flow Language) のプログラムを対象としてデッドロック等の不具合があるかないかを解析する技術を確立することであった。本研究課題の開始時点では、WSFL と呼ぶ Web サービス連携記述言語が提案された段階で、まだ WS-BPEL は、その基になった BPEL4WS (Business Process Execution Language for Web Service) も含めて提案されていなかった。

WSFL の言語仕様を調査すると、業務の作業連鎖を記述するワークフローの考え方を Web サ

ービスに転用したものであることが判明した。WSFL は外部 Web サービス起動をノードとし、この起動順序を指定する制御フローならびに外部 Web サービスと交換するデータのやりとりをデータフローで表現する一種のネットワーク指向並行記述言語である。

そこで、WSFL プログラムの構成要素を、並行システム記述言語である Promela を用いて表現する方法を考案した。これによって、Promela を入力とするモデル検査ツール SPIN を用いて、デッドロックの有無などを自動解析する方法を実現できる。モデル検査の方法で WSFL プログラムの振舞いチェッカが実現できることを示した。

また、いくつかの実験を行った結果、WSFL の言語仕様に不備があり、デッドロックを除去することが難しいことを指摘した。デッドロックを除去する方法を提案し、提案方式が問題を解決していることを具体的な実験を行うことで確認した。

4.2 セキュリティの解析

Web サービスは開放型ネットワークであるインターネットを土台としているため、標準化でもセキュリティに関する議論が活発である。Web サービスの基本通信メッセージである SOAP を暗号化し通信路で情報が漏えいしないことを保障する技術として WS-Security が、また、指定 Web サービスへのアクセスを許可するか否かをあらわすアクセス制御ポリシー表現、ならびにアクセス制御実現のためのプロトコルなどが WS-Authorization として提案されている。

ところが、暗号技術とアクセス制御の技術だけでは、情報漏えいの問題を扱うことができない。従来から情報システムセキュリティの分野で、ラティスに基づく情報フロー制御の方法が提案されていた。本研究課題では、WS-BPEL を対象として、情報フロー制御の方法を用いて情報漏えいの有無を解析する方法の適用可能性を検討した。これは、現在の Web サービス技術体系では未だ取り扱っていない問題である。冒頭のコンサルタント会社のような先進的な Web サービスを実現する上で必須の技術になると考え、先行して研究を進めた。

ラティスに基づく情報フロー制御の方法では、セキュリティからみた情報の重要さを導入し、重要さを表すセキュリティラベルに順序関係を与える。この順序関係を dominates 関係と呼び、これがラティスとなることが方式名の由来である。代表的な例では、「秘密文書」、「公開文書」などを考えることができ、「秘密文書」は「公開文書」よりも dominates 関係が大きい、あるいは支配的であるという。次に、利用主体と資源の双方にセキュリティラベルを与え、dominates 関係を満たす方向だけに情報の流れを許可する。機密関係の高い方向にだけ情報の流れを許可するため Flow-Up と呼ぶ。

Flow-Up だけでは、高いレベルの利用主体が読んだデータは2度と読み出すことができないという問題がある。アクセスの都度、dominates 関係の支配的な方向に情報が動き、最終的に、誰も読み出すことができない「ブラックホール」のような超高機密レベルに落ち込む。この問題を避けるために、クラス低下 (Declassification) と呼ぶ方法を導入する。

今、利用主体 P1 が資源 T1 から読み出したデータを資源 T3 に書き込む場合を扱い、次の関係が満たされているとする。ここで、L (P1) は P1 が持つセキュリティラベルを示す。

L (P1) dominates L (T1)
L (P1) dominates L (T3)
L (T3) dominates L (T1)

3つめの dominate 関係を考えるかぎり資源 T1 から T3 へのフローは許可される状況にある。しかし、利用主体 P1 がデータをアクセスするために、P1 が T1 から得たデータのセキュリティラベルが表面上、P1 と同一になる。そのため、2番目の関係から P1 から T3 へのフローが禁止され、T1 から T3 へのフローを禁止すべきと結論してしまう。条件が厳しすぎるという問題である。

この問題を解決するために、クラス低下により、利用主体 P1 のラベルを一時的に下げる。次のような関係を満たす一時的なラベル DCL が見つかればよい。

L (P1) dominates L (DCL)

L (DCL)　　dominates　L (T1)
L (T3)　　dominates　L (DCL)

1番目は DCL が P1 よりも小さいこと、2番目は DCL によって T1 からのフローが許可されること、3番目は DCL から T3 へのフローが許可されることを示す。この例では、L (T1) に一致するように L (DCL) を選べばよい。一般的には数多くの dominates 関係を満たすように、DCL の値をうまく選ぶ必要がある。

ラティスに基づく方法は、上の例を一般化することで次のように整理することができる。ある実行経路上に現れる全てのアクセスごとに dominates 関係を集め、すべての dominates 関係を満たすような一時ラベル DCL が存在するかを調べる。DCL の値を具体的に求めることができれば、情報フローに誤りがなく、したがって、情報漏えいがないといえる。一方、DCL の値がなければ情報漏えいの問題があると結論することができる。

上に述べたように、情報漏えいの問題は、流れるデータに付随するセキュリティラベルの値がラティスを形成し、その値を比較することで集めてきた dominates 関係が解を持つか否かを判定することである。この処理は2つの問題に分割することができる。実行経路を網羅的に生成し当該経路上の dominates 関係を集めてくる1番目の処理、さらに、集めてきた dominates 関係の制約を解く2番目の処理である。

本研究課題で提案する手法は、1番目の処理に 4.1 節で検討したモデル検査の方法を用いる。すなわち、セキュリティラベルを付加できるように拡張した WS-BPEL を対象として、4.1 節で用いたモデル検査の方法を適用する。2番目の制約計算処理は大小関係の比較演算で実現できることがわかった。

以上、本研究によって、Web サービス連携の記述を対象とする情報漏えいの解析がはじめて可能となる。

5 自己評価:

本研究課題では、並行システムのモデル検査やラティスに基づく情報フロー制御といった科学的な裏づけのある研究成果が、ビジネス主導の技術である Web サービスの世界でも重要な役割を果たすことを具体的に実感できた。

研究開始当初は、WSFL のプログラムを対象にして検討を進めた。この研究成果は Web サービス連携記述の解析にモデル検査の方法を適用した先駆的な研究として一定の評価を得て、諸外国の研究者から論文を引用されている。一方、WSFL は同時期に提案された XLANG と統合され、BPEL4WS として主要ベンダが共同提案して、現在の WS-BPEL になった。

本研究課題のように、ビジネスが密接に絡むソフトウェア技術を研究対象とする場合、実用的な貢献が明確である反面、急なビジネス環境の変化によって、計画の変更を余儀なくされた。幸い、WS-BPEL は WSFL の特徴であるネットワーク指向並行処理記述を部分言語として持つため、WSFL の方式を WS-BPEL の安全性解析を行う方法に適用することができ、研究が無駄にならずにすんだ。

本当に実用的な解析ツールを開発するためには、解決すべき課題が多く残っている。また、本研究課題の中で、ラティスに関する制約処理をモデル検査と統合する必要があり、これを一般化することで新しい研究課題をみつけた。今後、実用的なツールの実現ならびに、新たな課題を解決するための基礎研究を行いたいと考えている。

6 研究総括の見解:

中島氏の研究は，インターネット上のウェブサービスの安全な構成法に関するものであり，研究期間中2つの研究成果を出した．複数のウェブサービスを組み合わせて複合サービスを構成する場合には，全体として調和して動作し，デッドロックなどを起こさないことが必要である．中島氏はウェブサービスに関する国際標準言語WSFLの仕様にデッドロックに関する問題点があることを，

モデル検査技術によって明らかにした．この結果は国際的に高い評価を得た．中島氏の2番目の研究成果は，ウェブサービスにおけるセキュリティに関するものであり，数学的束理論とモデル検査を用いて，安全にデータを移動させる方法を研究した．いずれの研究も，現実の問題を最新の情報科学の手法とツールを用いて解決したもので大変優れた研究成果であると評価される．

7 主な論文等：

(1) 論文誌

1. 中島 震，玉井 哲雄 ：EJBコンポーネントアーキテクチャのSPINによる振舞い解析，コンピュータ・ソフトウェア，Vol.19, No.2, pp.2-18 (2002年3月)．
2. 中島 震：Web サービスフロー記述のモデル検査検証，情報処理学会論文誌，Vol.44, No.3, pp.942-952 (2003年3月).
3. 中島 震：コンポーネントフレームワーク振舞い解析への多値遷移システムの応用，コンピュータ・ソフトウェア，Vol.21, No.2, pp.32-36 (2004年3月).

(2) 国際会議

1. S. Nakajima : Verification of Web Services Flows with Model-Checking Techniques, International Symposium on Cyber World (CW 2002), pp. 378-385 (2002年11月).
2. S. Nakajima : Behavioural Analysis of Component Framework with Multi-Valued Transition Systems, Asia-Pacific Software Engineering Conference (APSEC 2002), pp.217-226 (2002年12月).
3. S. Nakajima : Model-Checking of Safety and Security Aspects in Web Service Flows, International Conference on Web Engineering (ICWE 2004), pp. 488-501 (2004年7月).

(3) 依頼原稿

1. 中島 震：書評－G.J.Holzmann著 The SPIN Model Checker，コンピュータ・ソフトウェア，Vol.21, No.2, pp.61-69 (2004年3月).
2. 中島 震：組込みソフトウェアへのモデル検査の応用，情報処理，Vol.45, No.7, pp.690-693 (2004年7月)．

(4) 表彰

1. 2003年度日本ソフトウェア科学会論文賞受賞 (2004年6月)．