

研究種目：基盤研究（A）  
 研究期間：2006～2009  
 課題番号：18200001  
 研究課題名（和文） 生産性と安全性向上のためのアスペクト指向ソフトウェア開発に関する研究  
 研究課題名（英文） Aspect-Oriented Software Development Methodology for Enhancing Productivity and Safety  
 研究代表者  
 玉井 哲雄（TAMAI TETSUO）  
 東京大学・大学院総合文化研究科・教授  
 研究者番号：60217172

研究成果の概要（和文）：「生産性と安全性向上のためのアスペクト指向ソフトウェア開発に関する研究」と題した研究を2006年度から2009年度まで4年間実施し、アスペクト指向モデルの型安全性を実際的に検証する理論とツールを整備し、高度な機能を備えたアスペクト指向言語の設計と、高い処理能力と使いやすさを兼ね備えた言語処理系を作成した。また、WebサービスのBPELによる記述に関するセキュリティの検証という応用で、この研究で開発した方法の実用性を明らかにするとともに、アスペクト指向を用いたソフトウェアの開発方法論を整備した。

研究成果の概要（英文）：We conducted a research project titled “Aspect-Oriented Software Development Methodology for Enhancing Productivity and Safety” in the fiscal years from 2006 to 2009. In the project, we developed a theory and tools for validating type-safety of aspect-oriented models, designed a new aspect-oriented language with highly advanced features and built a language processor that has high performance as well as flexible usability. We also applied our method to security validation of Web services written in BPEL and constructed a software development methodology for employing aspect-oriented technologies.

交付決定額

（金額単位：円）

	直接経費	間接経費	合計
2006年度	11,800,000	3,540,000	15,340,000
2007年度	11,000,000	3,300,000	14,300,000
2008年度	7,300,000	2,190,000	9,490,000
2009年度	7,300,000	2,190,000	9,490,000
年度			
総計	37,400,000	11,220,000	48,620,000

研究分野：ソフトウェア工学

科研費の分科・細目：情報学・ソフトウェア

キーワード：(1) アスペクト指向プログラミング (2) セキュリティ (3) ソフトウェア工学  
 (4) ディスペンダブル・コンピューティング (5) UML (6) 形式手法  
 (7) ソフトウェア開発効率化・安定化 (8) 要求工学

## 科学研究費補助金研究成果報告書

## 1. 研究開始当初の背景

現代のソフトウェアは社会に広く浸透しながら、その姿は一般の目からはますます見えにくくなっている。携帯電話、家電、カーナビ、デジタルカメラなどに組み込まれたおびただしい種類と量の組み込みソフトウェアや、インターネットを介して提供されるさまざまな種類のサービスを実現するソフトウェアに代表されるように、ソフトウェアはあらゆる人にあらゆる時と場所で享受されながら、その存在はほとんど意識されない。しかし日常生活から産業経済、公共活動にわたるあらゆる場面で、必要なソフトウェアが的確に供給され、また正しく動作することは現代社会に不可欠な要件となっている。

このため、ソフトウェアの供給者は、ますます短縮化される開発サイクルと多様なニーズにこたえる多種類のバリエーションの提供、という厳しい条件下での開発を要請されている。さらに、そうして提供したソフトウェアに不具合があったり、予期せぬ環境変化や悪意を持った攻撃に脆弱なものであったりした場合は、回収や修理に膨大なコストが発生するだけではなく、社会的な責任も強く問われることになる。

## 2. 研究の目的

このような困難さを伴うソフトウェア開発には、根本的に新しい方法論が必要である。その基本となるのは、システムに対する個別の要求特徴(feature)や関心事に明確に対応したソフトウェア単位(モジュール)を部品として用意し、それらの組み合わせでシステムを構築していくという考え方である。各ソフトウェア単位は明確な外部との境界と意味を持ち、その内部構造と振舞いの正しさは保証されなければならない。また、それぞれが十分に汎用的で、他の部品との自由な組み合わせを許すものでなければならない。さらに、部品によるシステムの構成の方法が明確に定められ、構成されたシステムが安全で正しく動作することが保証されなければならない。

このような目的に応じて近年とくに注目を浴びている方法に、アスペクト指向モデル化手法がある。アスペクトは1つの関心事に対応するソフトウェア構成単位である。従来のシステムは、たとえば手続きあるいはオブジェクトという単位をモジュールとして構成されてきたが、セキュリティ、性能、実行時データ分析などの関心事はそれらのモジュールを横断して存在する。それらの記述をモジュールごとに分散させていたのでは、可読性、保守性、再利用性が悪い。そこでそのような横断的関心事をアスペクトとして独立に記述し、それらと元のシステムを合成する

ことにより、高い生産性と信頼性をもったソフトウェア開発を行う、というのがアスペクト指向ソフトウェア開発の基本的な考え方である。

われわれは、このアスペクト指向分野で世界をリードする研究を行ってきたという自負をもっているが、これからはこの技術を実用化に向けて本格的に展開する時期であると認識している。そこで、アスペクト指向技術のさらなる展開と、それを体系化したソフトウェア開発方法論を確立することを目的として、アスペクト指向技術を用いたソフトウェアの設計・記述・検証方法を構築する。

より具体的には、以下の3点を目的とする。

(1) 今後増加することが大いに見込まれるアスペクト指向技術を利用したソフトウェアの信頼を高めるために、アスペクト指向技術向きの設計手法・プログラミング言語・検証方法を提案すること

(2) セキュリティや冗長性などの安全性・信頼性向上のための機能や記述を含むソフトウェアを、アスペクト指向技術によってモジュール化して開発や保守の効率を高めること

(3) これらの技術をベースとして体系的なアスペクト指向開発方法論を確立すること

## 3. 研究の方法

アスペクトをプログラミングレベルの技術としてのみ捉えるのではなく、新しいモジュール化の概念として、ソフトウェア開発の全工程にわたって位置づける。

分析フェーズやアーキテクチャ設計フェーズでのアスペクト概念の導入については、UMLによるモデル記述にアスペクトを明示的に記述できるようにするだけではなく、形式手法と結びつけてその意味の厳密化と検証を可能とする方法を開発する。そしてその結果を後のソフトウェア開発工程に系統的に反映させる体系を構築する。

計算モデルやプログラミング言語レベルでは、これまでもわれわれはアスペクト指向言語の原理や実現方式を詳細に議論するための土台として、理論的なモデル化を行ってきた。それをさらに展開させ、よりモジュール性の高いアスペクト指向プログラムを記述するため、アスペクト中でデータや制御の関係を簡潔に扱うことのできる言語機能の拡張する。またその処理系として、これまで開発した Javasssit や、dflow ポイントカット、連想アスペクト、SCoPE コンパイラあるいは EpsilonJ 処理系をベースとして、より完成度の高い処理系を作成する。

理論面では、上の言語設計と関連して、導入したアスペクト指向言語概念の意味定義を厳密に与えるとともに、型システムによる安

全性の検証を推進する。

#### 4. 研究成果

研究成果を年度ごとに記述すると、以下のようになる。

[2006 年度]

初年度として基礎的な技術の調査と開発を行った。

##### 1) 安全性のための理論構築に着手

・機密性の高い情報資源へのアクセス権について、ユーザの認証とアクセス承認を管理する JAAS 手法に対し、形式手法を用いてその正当性を検証する仕組みを開発し、成果を得た。

##### 2) アスペクト指向言語の拡張と処理系の開発

・安全性のためのアスペクトの再利用性を高めるために、細粒度のジョインポイントを持ったアスペクト指向言語を設計し、その実装を行って効果を確認した。

##### 3) 上流工程での要件定義への応用

・プロダクトライン型の開発で重要な要求特徴を抽出するモデルに対し、アスペクト指向の考え方を導入するという応用を提案し、成果を得た。

##### 4) UML に基づく開発方法論へのアスペクトの導入

・UML のクラスベースのモデルと振舞いベースのモデルのそれぞれでアスペクト概念を導入する記法とその意味論につき研究し、成果を得た。

[2007 年度]

前年度に行った研究計画策定、関連研究調査、基本作業の着手という実績を踏まえ、核となる研究成果の獲得に向け具体的な研究開発作業を行った。

##### 1) 安全性のための理論構築

・アスペクト指向モデルの型安全性を実際的に検証するための基礎理論を構築した。

・関数型アスペクト指向言語上のアスペクトの意味論モデルを構築した。

・アスペクト指向設計モデルの振舞いに関するモデル検査手法を実証するための実験を行った。

##### 2) 言語と処理系の開発

・型つきポイントカット機構やテストベース・ポイントカット機構を持つアスペクト指向言語を開発した。

・アスペクト指向言語 Josh をもとに、GluonJ や Remote Pointcut を開発した。

##### 3) 問題分野への適用

・Web サービスの BPEL による記述についてのセキュリティ要件の表現と検証手法を開発した。

##### 4) 開発方法論の提案

・アスペクト指向を用いたソフトウェア開発方法論として UML を用いた手法を提案した。

[2008 年度]

前年度に行った基盤となる手法の構築、言語と処理系の開発、応用としての Web 上のセキュリティ要件の検証、開発方法論の策定、という実績を踏まえ、これらの研究成果の拡張、統合、実証を目標とする研究開発作業を行った。

##### 1) 安全性のための理論構築

・プログラムの健全性と記述の柔軟性の両者の要求を満たす型システムを持った言語を提案し、その型安全性を理論的に検証した。

・アスペクト指向プログラミングにおける基本構成要素の持つべき条件について、原理的な理論化を行った。

##### 2) 言語と処理系の開発

・データフローポイントカット機構を持つアスペクト指向言語を開発した。

・横断的関心事を抽象化して記述する機構について提案し、開発を行った。

##### 3) 問題分野への適用

・Web アプリケーションの実行時監視によるセキュリティ検証の手法を、アスペクト指向の応用として開発した。

##### 4) 開発方法論の提案

・アスペクト指向を用いてソフトウェア開発を行う際に、形式仕様に基づく事象解析を行って信頼性を高める方法を提案した。

[2009 年度]

この 4 年間の基盤研究 (A) の最終年度として、これまでに開発したソフトウェアを統合した環境を構築し、また手法を整備して利用価値の高い成果物を取りまとめた。具体的には以下のような作業を行った。

##### 1) 安全性のための理論とツールの整備

・アスペクト指向モデルの型安全性を実際的に検証する理論とツールを整備した。

##### 2) アスペクト指向言語と処理系の構築

・高度な機能を備えたアスペクト指向言語の設計とその処理系を完成させ、高い処理能力と使いやすさを兼ね備えた言語処理系を作成した。

##### 3) 応用

・Web サービスの BPEL による記述に関するセキュリティの検証という応用で、この研究で開発した方法の実用性を明らかにした。

##### 4) 開発方法論

・アスペクト指向を用いたソフトウェア開発方法論を整備した。

以上をまとめてこのような最終報告書を作成した。

#### 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 78 件)

① Hidehiko Masuhara, Atsushi Igarashi,

- Manabu Toyama, Type Relaxed Weaving, Proceedings of the 9th Int'l Conf. on Aspect-Oriented Software Development, 査読有, 2010, pp. 121-132
- ② Shin Nakajima, Semi-Automated Diagnosis of FODA Feature Diagram, Proceedings of the 25th ACM Symp. on Applied Computing, 査読有, 2010, pp. 2191-2197
- ③ Tetsuo Tamai, Social Impact of Information System Failures, Computer, Vol. 42, No. 6, 査読有, 2009, pp. 58-65
- ④ Shumpei Akai, Shigeru Chiba, Extending AspectJ for Separating Regions, Proceedings of the 8th Int'l Conf. on Generative Programming and Component Engineering, 査読有, 2009, pp. 45-54
- ⑤ Keiji Hokamura, Ryoto Naruse, Masaru Shiozuka, Naoyasu Ubayashi, Shin Nakajima, Akihito Iwai, AOWP: Web-specific AOP framework for PHP, Proceedings of the 24th IEEE/ACM Int'l Conf. on Automated Software Engineering, 査読有, 2009, pp. 679-681
- ⑥ Chieri Saito, Atsushi Igarashi, Self Type Constructors, Proceedings of OOPSLA 2009, 査読有, 2009, pp. 263-282
- ⑦ Kouhei Sakurai, Hidehiko Masuhara, Test-Based Pointcuts for Robust and Fine-Grained Join Point Specification, Proceedings of the 7th Int'l Conf. on Aspect-Oriented Software Development, 査読有, 2008, pp. 96-107
- ⑧ Naoyasu Ubayashi, Jinji Piao, Suguru Shinotsuka, Tetsuo Tamai, Contract-based Verification for Aspect-oriented Refactoring, Proceedings of 1st IEEE Int'l Conf. on Software Testing, Verification, and Validation, 査読有, 2008, pp. 180-189
- ⑨ Tetsuo Kamina, Tetsuo Tamai, Lightweight Dependent Classes, Proceedings of the 7th ACM Int'l Conf. on Generative Programming and Components Engineering, 査読有, 2008, pp. 113-124
- ⑩ Naoyasu Ubayashi, Akihiro Sakai, Tetsuo Tamai, An Aspect-oriented Weaving Mechanism Based on Component and Connector Architecture, Proceedings of the 22nd IEEE/ACM Int'l Conf. on Automated

- Software Engineering, 査読有, 2007, pp. 154-163
- ⑪ Kenichi Kourai, Hideaki Hibino, Shigeru Chiba, Aspect-oriented Application-level Scheduling for J2EE Servers, Proceedings of the 6th Int'l Conf. on Aspect-Oriented Software Development, 査読有, 2007, pp.1-13
- ⑫ Tetsuo Kamina, Tetsuo Tamai, Lightweight Scalable Components, Proceedings of the 6th ACM Int'l Conf. on Generative Programming and Components Engineering, 査読有, 2007, pp. 145-154
- ⑬ Tetsuo Tamai, Naoyasu Ubayashi, Ryoichi Ichiyama, Objects as Actors Assuming Roles in the Environment, Software Engineering for Multi-Agent Systems V, LNCS 4408, 査読有, 2007, pp. 185-203

[学会発表] (計 3 1 件)

- ① Shin Nakajima, Constructing FODA Feature Diagrams with a GUI-based Tool, SEKE 2009, 2009年7月1日, Hyatt Harborside at Logan Int'l Airport (Boston, USA)

[図書] (計 3 件)

- ① 中島震、オーム社、SPIN モデル検査入門、2010、262

## 6. 研究組織

### (1) 研究代表者

玉井 哲雄 (TAMAI TETSUO)  
 東京大学・大学院総合文化研究科・教授  
 研究者番号：60217172

### (2) 研究分担者

中島 震 (NAKAJIMA SHIN)  
 国立情報学研究所・アーキテクチャ科学  
 研究系・教授  
 研究者番号：60350211  
 (H20→H21：連携研究者)

千葉 滋 (CHIBA SHIGERU)  
 東京工業大学・大学院情報理工学研究科・  
 教授  
 研究者番号：80282713  
 (H20→H21：連携研究者)

鶴林 尚靖 (UBAYASHI NAOYASU)  
 九州大学・大学院システム情報科学  
 研究院・教授  
 研究者番号：80372762  
 (H20→H21：連携研究者)

増原 英彦 (MASUHARA HIDEHIKO)  
東京大学・大学院総合文化研究科・准教授  
研究者番号：40280937  
(H20→H21：連携研究者)

五十嵐 淳 (IGARASHI ATSUSHI)  
京都大学・大学院情報学研究科・准教授  
研究者番号：40323456  
(H20→H21：連携研究者)

紙名 哲生 (KAMINA TETSUO)  
東京大学・大学院人文社会系研究科・助教  
研究者番号：90431882  
(H20→H21：連携研究者)