様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２７　年　　６　月　　３　日現在

機関番号：　６２６１５
研究種目：　挑戦的萌芽研究
研究期間：　2011～2014
課題番号：　２３６５００１９

研究課題名（和文）ソフトウェアシステムの柔らかな不具合の検出と修正の方法

研究課題名（英文）Detection and Repair of Soft-Faults in Software Systems

研究代表者
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

交付決定額（研究期間全体）：（直接経費）　　2,800,000円

研究成果の概要（和文）：Webアプリケーションに代表されるオープンなシステムでは，開発者が予期しなかった利用者の振る舞いによって，機能的には正しいが運用者が期待しないという不具合を示すことがある．このような状況は，プログラムバグとは異なり完全に除去しなければならないものではないことから「柔らかな不具合」と命名した．本研究課題では，この柔らかな不具合を統一的に取り扱う理論的な枠組みを提示する．自己改変Webアプリケーションへの適用を具体例として，提案方法が有効であることを示した．

研究成果の概要（英文）：Open systems such as Web applications may fall into undesirable situations by unpredictable behavior of users or clients. The situations are such that the system is functionally correct, but exhibits behavior different from what the system owner expect from it. Such faulty behavior is not a program bug that must be removed, and is called “Soft Faults” here. This research project proposes a general theory to account for the Soft Faults, and shows that the theory is effective by applying it to a self-adaptive Web application system.

研究分野：　ソフトウェア工学

キーワード：　自己適応システム　Webアプリケーション　実行時検証　柔らかな不具合

１．研究開始当初の背景

ソフトウェアシステム開発の根本的な難しさは，システムが持つべき機能や性質を表す要求仕様を，開発段階で決定することが困難という事実に起因することが多い．

要求工学の標準的な考え方では，システム開発に関わる多様な利害関係者（ステークホルダ）の調整・妥協の産物が要求仕様であるとする．システム運用開始後に，開発時に想定した状況が変化し，その結果，機能的には正しくても，あるステークホルダにとって期待と異なる結果を示すことがある．本研究課題では，このような状況を「柔らかな不具合」と命名した．

この「柔らかな不具合」は，システム稼働によって，はじめて顕在化する．特に，Webアプリケーションのような「オープンなシステム」では同様の不具合が頻発する．その理由は，利用者がどのような振る舞いを示すかを開発時に予測することの困難さにある．

今後，多様なシステムがネットワーク接続されることによって，オープンなシステムの重要性が増す．「柔らかな不具合」への対応を可能とする技術の確立が求められている．

２．研究の目的

本研究課題は，柔らかな不具合の検出と修正の方法について，技術的な解決策を確立することを目的とする．

柔らかな不具合は，システム稼働中に顕在化するものであり，開発時に想定した前提条件や仮定が，システム実行時に満たされないことによって生じる．最初に，3 つの要素（開発時の仮定・システム機能・ステークホルダの期待）の関係を整理した統一的な枠組みを整理する．2 番目に，検出した柔らかな不具合を修正する方法を明らかにし，自己改変のアーキテクチャを整理する．3 番目として，自己改変の方法が新たな不具合をもたらさないことを確認する自動検査の方法を明らかにする．

以上によって，柔らかな不具合を統一的に取り扱う新しい理論を整理し，具体的なソフトウェアシステムの構成アーキテクチャを示すことを目的とする．

３．研究の方法

要求工学・自己改変システム・自動検証に関する既存の研究成果をもとに，具体的な Web アプリケーションを題材として，柔らかな不具合に関わる研究を進める．

(1) 柔らかな不具合の理論的な枠組み：
要求工学の研究成果として知られている M. ジャクソン（独立コンサルタント）の適合性規則を精密化することで，柔らかな不具合が混入することを説明する理論的な枠組みを考案する．特に，柔らかな不具合の検出法の妥当性を裏付けることが可能な方法の確立に注力する．

(2) 自己改変の実現アーキテクチャ：
一般的には，自己改変システムは，実行監視・改変の診断・置き換え（修正），といった 3 つのステップを必要とする．(1)の成果をもとに，具体的な Web アプリケーションを題材として，これら 3 つの関係を明らかにする．自己改変 Web アプリケーションを試作することで，提案する実現アーキテクチャの妥当性を実証的に確認する．

(3) 柔らかな不具合の発生確率予測：
(2)の成果から，検知した柔らかな不具合を修正することが可能になる．一方，検知の方法は実行監視を基にしており，これは実行時性能の低下をもたらす．柔らかな不具合は，その定義から深刻な影響を与えない．仮に発生頻度が小さければ無視するという運用判断もあり得る．そこで，システム稼働時に，どのくらいの確率で特定の柔らかな不具合が発生するかを知る方法を考案する．

(4) 置き換え可能性の検査：
自己改変を行う場合，その改変の方法が，システムに新たな不具合をもたらしてはならない．通常のバグ修正であれば，修正後に期待する性質が満たされることを確認すれば良い．一方，柔らかな不具合の場合，改変によって無効になる性質と有効になる性質の両方を考える必要がある．題材とする Web アプリケーションを具体例として検討し置き換え可能性が満たすべき性質を考察する．

４．研究成果

得られた研究成果を，３節に示した 4 つの項目に対応して報告する．

(1) 柔らかな不具合の理論的な枠組み：
前出の M. ジャクソンによる適合性規則は，関わる 3 種類の情報（ドメイン・システム・要求）の関係を表す．C. ゲッチ教授（ミラノ工科大学）は，ドメインが変化した時に，要求が壊れないようにシステムを変更することを自己適応性と定義した．本研究課題では，要求を，満たさなくてはならない最小機能の集合と，前者から構成される高次機能の集合に分割する．後者の高次機能は要求工学の分野でポリシーとも呼ばれるもので，ステークホルダの意図を表す．そして，高次の機能が壊れることを「柔らかな不具合」と定義した．機能的には正しいが特定ステークホルダの期待に反する．

(2) 自己改変の実現アーキテクチャ：
実行監視には，自動検証の技術であるロジック・モデル検査のテスティングへの応用から生まれた「実行時検証」の方法

を用いる．プログラム実行箇所に監視ポイントを設定し，実行に伴って生成される監視ポイント列が，期待する列になっているかを判断する．期待の列を有限状態オートマトン（監視オートマトン）で表すことにより，文字列（実行監視ポイント列）の受理問題に置き換える．改変の診断には，列を受理した監視オートマトンの種類に応じて，置き換えるプログラムコンポーネントを選ぶ方法を採用した．複数のコンポーネント候補が存在することを，フィーチャダイアグラムで表す．最後の置き換え方法は，対象システムの実行基盤や用いるプログラミング言語に依存する．題材の Web アプリケーションでは，PHP 言語で記述したプログラムファイルの置き換えによって実現できる．図１（報告書末尾に掲載）に考案した「自己適応 Web アプリケーション・アーキテクチャ」を示した．

以上の成果を，(1)と合わせることで，学会発表[3]と雑誌論文[4]として公表した．

(3) 柔らかな不具合の発生確率予測：
発生確率予測の基本的な方法は，モンテカルロ法である．つまり，利用者の振る舞いを乱数で規定し，その影響によって，どのくらいの確率で不具合が発生するかを調べる．柔らかな不具合の発生確率予測が難しい原因は，そもそも，発生確率が極めて小さいことによる．そこで，統計モデル検査法でも採用された「重点サンプリング」による稀なイベント・シミュレーション法を用いた．題材の Web アプリケーションによる実験を通して，提案方法が妥当であることを示した．

以上の成果を学会発表[2]と雑誌論文[3]として公表した．

(4) 置き換え可能性の検査：
一般に，置き換え可能性は，オブジェクト指向プログラミング言語のサブタイピング関係や，形式手法のリファインメント関係で定義されている．これらは，新たなコンポーネントが機能を追加しても良いという規則になっている．一方，自己改変の場合，新たなコンポーネントが持つ機能を制限したい．そこで，セキュリティ分野で議論されるインテグリティ関係を導入する方法を着想した．題材の Web アプリケーションでの機能制限的な置き換え可能性を理論的に説明することができる．

以上の成果を学会発表[1]と雑誌論文[2]として公表した．

本研究課題で得られた成果は，雑誌論文 3 件・国際学会発表 3 件として公表され，近年話題を集めている自己適応システムの研究者に影響を与えた．特に，J. クラマー教授（英国インペリアルカレッジ），C.ゲッチ教授（イタリア・ミラノ工科大学）とは，個別に研究議論を行った．また，最近，プログラム・テストの分野では，相対的な正しさのテストを，どのように考えるか，が新しい研究テーマとして認識されはじめた．D.ローゼンブラム教授（国立シンガポール大学）は，「Known Unknowns」と呼んでいる．本研究課題の「柔らかな不具合」も相対的な正しさの取り扱いに着目したものであり，今後，多様な展開を期待できる．ソフトウェア工学の新しい方向性を先取りした研究と云える．

５．主な発表論文等

〔雑誌論文〕（計　４件）

[1] 中島震、要求変化へのソフトウェア工学、電子情報通信学会誌、査読有、98 巻、2015、124-129。
[2] 中島震、自己適応システムにおけるコンポーネントの安全な置き換え、コンピュータソフトェア、査読有、31 巻、2014、259-269。
[3] 中島震、実行時干渉の発生確率予測、コンピュータソフトウェア、査読有、30 巻、2013、95-101。
[4] 中島震、自己適応 Web アプリケーションシステム：概念アーキテクチャと実現フレームワーク、コンピュータソフトウェア、査読有、29 巻、2012、54-69。

〔学会発表〕（計　７件）

[1] Shin Nakajima、Safe Substitution of Components in Self-Adaptive Web Applications 、 The 20th Asia-Pacific Software Engineering Conference、2013 年 12 月 5 日、バンコク（タイ）
[2] Shin Nakajima、Importance Sampling of Runtime Interference、The 19th Asia-Pacific Software Engineering Conference、2012 年 12 月 7 日、香港（中国）
[3] Shin Nakajima 、An Architecture of Dynamically Adaptive PHP-based Web Applications 、 The 18th Asia-Pacific Software Engineering Conference、2011 年 12 月 7 日、ホーチミン（ベトナム）
（他４件の発表）

〔その他〕
ホームページ等
http://researchmap.jp/nkjm/

６．研究組織

(1)研究代表者

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

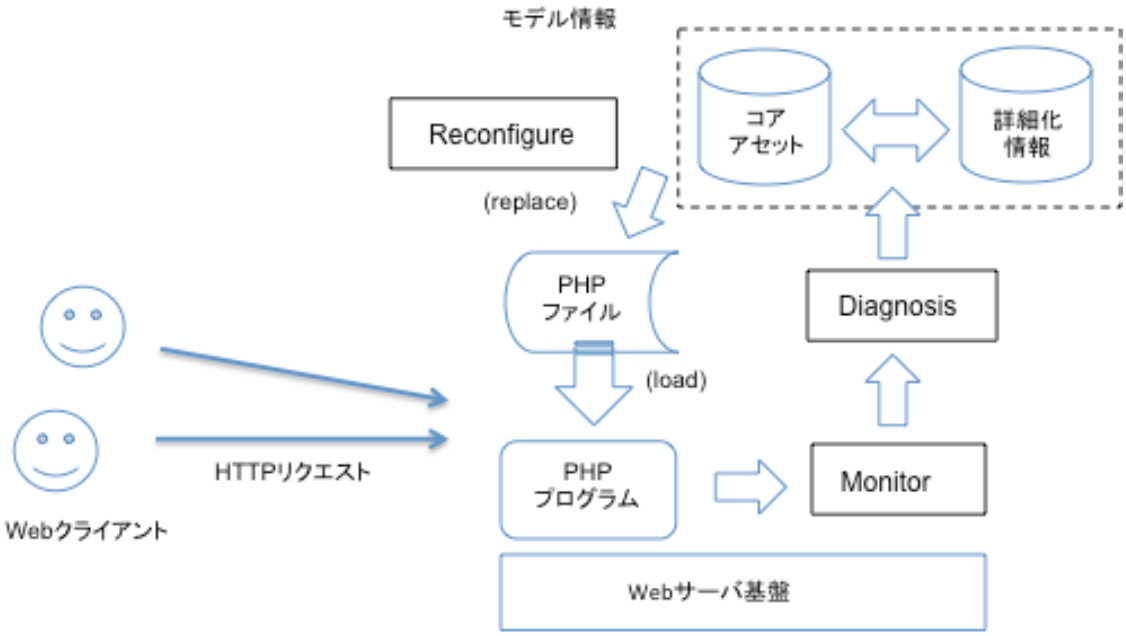

図1　自己適応Webアプリケーション・アーキテクチャ