

平成21年5月22日現在

研究種目：基盤研究（C）
研究期間：2007～2008
課題番号：19510148
研究課題名（和文） ソフトウェアサイバネティクスに基づいた自律的信頼性評価技術の開発
研究課題名（英文） A Development on Autonomous Reliability Assessment Technologies Based on Software Cybernetics
研究代表者
土肥 正（TADASHI DOHI）
広島大学・大学院工学研究科・教授
研究者番号：00243600

研究成果の概要： 通常、ソフトウェアのコーディングが完了した時点で、当該製品の仕様書と詳細設計書に基づいて作成されたテストケースを投入し、ソフトウェアのデバッグ作業が実施される。テストの進捗状況を逐次監視しながらソフトウェア信頼度を高い精度で予測し、「当たり前品質としての信頼性」を定量的に評価することが行われる。本研究では、ソフトウェアサイバネティクスと呼ばれる新しい概念を導入することにより、自律的に信頼性評価を行うためのスキームを提案し、テストの進捗状況を学習しながら信頼度を推定する適応オンライン評価システムのプロトタイプを世界に先駆けて開発した。具体的には、(a) フォールト検出数に関するデータや各種メトリクスデータに基づいて、フィールド情報を過不足なく信頼性評価に活用するための統計的推論機構の開発、(b) 自律的かつ適応的にソフトウェア信頼性を評価するオンラインアルゴリズムの開発、(c) フィードバック原理と自己組織化原理に基づくテスト工程の制御、などを行うための方法論を展開した。

交付額

(金額単位：円)

	直接経費	間接経費	合計
2007年度	1,900,000	570,000	2,470,000
2008年度	1,500,000	450,000	1,950,000
計	3,400,000	1,020,000	4,420,000

研究分野：複合新領域**科研費の分科・細目：**社会・安全システム科学，社会システム工学・安全システム**キーワード：**ソフトウェア，信頼性評価，サイバネティクス，自律計算，適応計算

1. 研究開始当初の背景

現在、我々を取巻く高度情報化社会において、ソフトウェアシステムへの依存性は極端に増加しており、コンピュータシステムの信頼性とソフトウェアの信頼性は **nearly equal** の関係にあると言っても決して過言ではない。すなわち、コンピュータシステムにおけるシステム障害はソフトウェアに内

在するフォールトに起因する 경우가ほとんどであり、一旦システム障害が発生すると、非常に大きい社会的・経済的損失を被る事例が少なくない。このような背景から高信頼化ソフトウェアを開発するために数多くの高信頼化技術が提案されてきたが、費用対効果の観点から、現実のソフトウェア開発現場においてこれらの技術が実践された例はそれ

程多くない。

一方で、知的生産物としての工業製品であるソフトウェアの品質向上に対する取組みは、ソフトウェア工学の創設当初から継続して議論されてきた課題であり、未だに完全に解決される目処が立っていない。ソフトウェア工学における究極の目的は、最終成果物であるソフトウェア製品の高い品質を保持しながら健全な生産プロセスを完全自動化することであろう。しかしながら、ソフトウェア工学における自動化技術はランダムテストにおけるテストケース生成技術や設計技術などのごく一部に限られており、仕様定義、検証、コーディング、テスト、品質評価、保全など、いずれの工程においても開発管理者の手を介した知的作業に基づいているのが実状である。また、ソフトウェア工学における多くの知見は事例に基づいた実証的研究成果であり、経験科学としての色彩が非常に強く、理論的かつ普遍的な技術体系を確立するのは困難な状況にある。

2. 研究の目的

本研究の目的は、ソフトウェア開発の最終工程であるテスト工程において実施される信頼性評価に着目し、ソフトウェア製品の信頼性評価を完全自動化（知能化）するための次世代技術の開発を行うことである。通常、ソフトウェアのコーディングが完了した時点で、当該製品の仕様書と詳細設計書に基づいて作成されたテストケースを投入し、ソフトウェアのデバッグ作業が実施される。テストの進捗状況を逐次監視しながらソフトウェア信頼度を高い精度で予測し、「当たり前品質としての信頼性」を定量的に評価することが行われる。本研究では、ソフトウェアサイバネティクスと呼ばれる新しい概念を導入することにより、自律的に信頼性評価を行うためのスキームを提案し、テストの進捗状況を学習しながら信頼度を推定する適応オンライン評価システムのプロトタイプを世界に先駆けて開発する。具体的には、(a) フォールト検出数に関するデータや各種メトリクスデータに基づいてフィールド情報を過不足なく信頼性評価に活用するための統計的推論機構の開発、(b) 自律的かつ適応的にソフトウェア信頼性を評価するオンラインアルゴリズムの開発、(c) フィードバック原理と自己組織化原理に基づくテスト工程の制御、などを行うための方法論を展開する。

3. 研究の方法

【平成19年度】 システムテストに対する信頼性評価技術の開発

(1) ソフトウェアメトリクスデータの活用技術 (H19.4-5) : ソフトウェアテスト工程において観測される各種メトリクスデータとフォールト検出頻度データを融合した新しい信頼性モデルを定式化した。基本的なアイデ

アはマルコフ依存ポアソン回帰に基づく比例強度モデルを改良することであり、必要なメトリクス情報（プロダクトメトリクス、資源メトリクス、プロセスメトリクス）とモジュール構造の実行過程を全て組み入れた動的信頼性モデルの開発を行った。(2) 自律的ソフトウェア信頼性評価ツールにおけるデータ処理機能の開発 (H19.4-7) : モジュールテスト、結合テスト、システムテストを実施する過程で観測される各種メトリクスデータをデータベース上に記録し、さらに各々のテストにおいて観測されたフォールト検出頻度データを時系列情報として格納するためのファイルシステムを開発した。(3) パラメータ推定アルゴリズムの改良 (H19.5-7) : ソフトウェア内に含まれる残存フォールト数の不偏推定量を矛盾なく推定することは最尤法の枠組みでは不可能であり、ソフトウェアテストの初期から中期段階においては必ずしも十分な数のデータを取得できないことが問題点として挙げられる。そこで、ベイズ推定に基づいたいくつかの方法が小標本問題に対して有効であることが知られているが、ベイズ推定では超パラメータと呼ばれる下層パラメータのチューニングや事後分布の検証などが必要とされ、ソフトウェアの自律的信頼性評価を実施することは事実上困難であると考えられてきた。しかしながら、最近になって統計物理学でその有効性が認識され始めた変分ベイズ法を適用すれば、申請者らが開発した EM アルゴリズムに基づいたパラメータ推定法をベイズ推定の枠組みで改良することが可能となり、前述の残存フォールト数の推定問題も解決することができた。モデルに含まれる超パラメータの自動チューニングには、ABIC (Akaike's Bayese Information criterion) と呼ばれる情報量基準に基づいて逐次更新を行う方式を採用した。(4) 分散開発環境をシミュレートするための実験環境の整備 (H19.8-9) : 購入予定のパーソナルコンピュータをローカルネットワークで連結し、分散開発環境下でのシステムテスト環境を仮想的に模擬するための実機システムを整備した。このシステムを利用することで、開発予定の信頼性評価システムに基づいて推定される信頼性評価尺度の統計的性質（一致性、漸近正規性、十分性、不偏性）をシミュレーション実験を通じて検証することが可能となった。(5) 階層ベイズモデルの自己組織化と自律計算技術の開発 (H19.8-11) : (3) で改良したアルゴリズムに基づいて SRATS を改良し、さらに階層ベイズ構造に発見的自己組織化 (GMDH) アルゴリズムを適用することで環境（採集されたデータ）に応じて信頼性モデルを学習させるための自律計算技術を開発した。(6) システムテスト用信頼性評価ツールの作成

(H19.10-12) : (1)-(5) の理論的成果を統合し、システムテスト環境に対して自律的に適合しながら進化する信頼性評価アルゴリズムを開発し、(4) で整備した実機システムにこれを実装した。ランダムテストを想定したシミュレーション実験を行い、システムテストに対する自律的信頼性評価技術の有効性を実験的に検証した。

【平成20年度】モジュールテストと結合テストに対する信頼性評価技術の開発

(1) ソフトウェア・アーキテクチャモデルの開発 (H20.4-6) : 多数のモジュール (コンポーネント) から構成されるソフトウェア・アーキテクチャ上で、モジュールテストの実行プロファイルを記述するための信頼性モデルを定式化した。これは最近になって注目を集めているセミマルコフ変調過程 (もしくは MAP) に基づいた信頼性評価モデルの非定常過程版であり、信頼度成長現象をモデル内で矛盾無く表現出来ることが特徴となっている。実行プロファイルの推移率や結合テストの失敗確率はすべて可観測ではないため、パラメータの推定には EM アルゴリズムと変分ベイズアルゴリズムを用いた。これにより、システムテストに移行する直前の各モジュールの信頼度を推定することが可能となった。アーキテクチャモデルの開発は、米国 Duke 大学の K. S. Trivedi 教授と共同で行った。(2) 実験システムの追加整備 (H20.4-5) : 分散開発環境下でのモジュールテスト環境を仮想的に模擬するために実機システムを整備した。これにより、モジュールテスト、結合テスト、システムテストという一連のテスト環境を連続してシミュレート出来る実験環境が整った。(3) 適応オンライン推定に基づくテスト進捗過程の再構成 (H20.7-9) : 前年度(6)で開発されたシステムにモジュールテストに対する信頼度推定機能(1)を付加し、テスト工程全般を通じて信頼度を推定するためのスキームを確立した。ここでは開発パラダイムとして Water Fall Model を仮定し、各推定フェーズにおいて推定された信頼度がある閾値を下回った場合にはテストケースを追加し、テスト要員や資源を増加するための警告機能を設定し、テスト進捗状況の監視機能に対してフィードバック構造を導入した。この機能のもうひとつの重要な目的は、不完全デバッグが事後的に判明した場合に信頼度を再計算するためであり、典型的なフィードバック構造を仮定して推定モデルの再構成機能を設計した。(4) テスト環境の変化への対応(H20.10-12) : ソフトウェアの開発プロジェクトで頻繁に発生する「プロジェクト混乱」と同様に、テスト工程においても「フォールトの検出傾向の変化」が度々発生する。このような傾向変化時点を統計的に予測する問題を「変化点検出問

題」と呼び、理論統計学における興味深い問題を提供している。変化点を検出することが遅れたならば、異なる環境の下で信頼度を推定し続けることになり、自己組織化機能により精度が回復するまでかなりの学習回数 (期間) を要する。よって、前年度の(2)において開発されたシステムに同質データの変化点を検出する機能を追加し、テスト環境の変化 (モデルの構造変化) に対応することの出来るロバストな推定スキームに変更した。(5) ウェブアプリケーションの開発と実証研究 : 得られた理論的成果を基に、自律的ソフトウェア信頼性評価を実施するためのウェブアプリケーションの開発と、実工程で観測されたデータに基づいて実証研究を行った。ソフトウェア著作権の問題から、システムのアクセスを堅固なものにする必要がある。そのため、基礎をなす PC クラスタサーバは広島大学が所有する大型計算機環境の利用を避け、独自の機器構成に基づいてシステム構築を行った。(6) 研究とりまとめ (H21.1-3) : モジュールテストと結合テストに対する信頼性評価技術の研究とりまとめを行い、査読付フルペーパーとして投稿した。

4. 研究成果

各年度毎の研究成果を以下に記す。

【平成19年度】ソフトウェアメトリクスデータの活用技術を精査し、ソフトウェアテスト工程において観測される各種メトリクスデータとフォールト検出頻度データを融合した、新しい信頼性モデルを定式化した。自律的ソフトウェア信頼性評価ツールにおけるデータ処理機能の開発を目標に掲げ、モジュールテスト、結合テスト、システムテストを実施する過程で観測される各種メトリクスデータをデータベース上に記録し、さらに各々のテストにおいて観測されたフォールト検出頻度データを時系列情報として格納するためのファイルシステムを開発した。ソフトウェア信頼性モデルにおけるパラメータ推定においては、EM アルゴリズムに基づいたパラメータ推定法をベイズ推定の枠組みで改良し、残存フォールト数の推定問題に適用した。モデルに含まれる超パラメータの自動チューニングのために、ABIC に基づいて逐次更新を行う方式を開発した。また、分散開発環境をシミュレートするために、システムテスト環境を仮想的に模擬するための実機システムを整備した。改良したパラメータ推定アルゴリズムに基づいて、既存の信頼性評価ツール SRATS を拡張し、さらに階層ベイズ構造に発見的自己組織化 (GMDH) アルゴリズムを適用することで、環境 (採集されたデータ) に応じて信頼性モデルを学習させるための自律計算技術を開発した。最終的に、得られた理論的成果を統合し、システムテスト環境に対して自律的に適合しなが

ら進化する信頼性評価アルゴリズムを開発し、整備した実機システム上にこれを実装した。

【平成20年度】前年度の成果に基づいて、モジュールテストと結合テストに対する信頼性評価技術の開発を行った。具体的には次のように要素技術を列挙することができた。(a) ソフトウェア・アーキテクチャモデルの開発：多数のモジュール（コンポーネント）から構成されるソフトウェア・アーキテクチャ上で、モジュールテストの実行プロファイルを記述するための信頼性モデルを定式化した。(b) 実験システムの追加整備：分散開発環境下でのモジュールテスト環境を仮想的に模擬するために実機システムを整備した。(c) 適応オンライン推定に基づくテスト進捗過程の再構成：前年度に開発されたシステムにモジュールテストに対する信頼度推定機能を付加し、テスト工程全般を通じて信頼度を推定するためのスキームを確立した。(d) テスト環境の変化への対応：テスト工程において発生する「フォールトの検出傾向の変化」時点を統計的に検出する機能を追加し、テスト環境の変化（モデルの構造変化）に対応することの出来るロバストな推定スキームに変更した。(e) ウェブアプリケーションの開発と実証研究：得られた理論的成果を基に、自律的ソフトウェア信頼性評価を実施するためのウェブアプリケーションの開発と、実工程で観測されたデータに基づいて実証研究を行った。

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33件）

1. K. Ohishi, H. Okamura and T. Dohi, Gompertz software reliability model: estimation algorithm and empirical validation, J. Systems and Software, 82, 535-543, 2009 (査読有) .
2. T. Ozaki, T. Dohi and N. Kaio, Numerical computation algorithms for sequential checkpoint placement, Performance Evaluation, 66, 311-326, 2009 (査読有) .
3. H. Okamura and T. Dohi, Software reliability modeling based on capture-recapture sampling, IEICE Trans. on Fundamentals (A), E92-A, 2009 (掲載決定) (査読有).
4. H. Okamura, T. Dohi and K. S. Trivedi, Markovian arrival process parameter estimation with group data, IEEE/ACM Trans. on Networking, 172, 2009 (掲載決定) (査読有).
5. T. Uemura and T. Dohi, A security match management model, Proc. IASTED Int'l Conf. on Software Engineering, 巻なし, 114-119, ACTA Press, 2009 (査読有) .
6. X. Xiao and T. Dohi, On equilibrium distribution properties in software reliability modeling, Proc. 4th Int'l Conf. on Availability, Reliability and Security, 巻なし, 158-165, IEEE CS Press, 2009 (査読有) .
7. K. Rinsaka and T. Dohi, Estimating the optimal software rejuvenation schedule with small sample data, Quality Technology and Quantitative Management, 6 (1), 55-65, 2008 (査読有) .
8. H. Okamura and T. Dohi, Software reliability modeling based on mixed Poisson distributions, Int'l J. Reliability, Quality and Safety Engineering, 15(1), 9-32, 2008 (査読有) .
9. K. Iwamoto, T. Dohi and N. Kaio, Estimating periodic software rejuvenation schedule in discrete operational circumstance, IEICE Trans. on Information & Systems (D), E91-D (1), 23-31, 2008 (査読有) .
10. T. Ishii, T. Fujiwara and T. Dohi, Bivariate extension of discrete software reliability modeling with number of test cases, Int'l J. Reliability, Quality and Safety Engineering, 15 (1), pp. 1-17, 2008 (査読有) .
11. H. Okamura and T. Dohi, Analysis of a software system with rejuvenation, restoration and checkpointing, Service Availability (ISAS 2008), LNCS 5017, 110-128, Springer-Verlag, 2008 (査読有) .
12. H. Eto, T. Dohi and J. Ma, Simulation-based optimization approach for software cost model with rejuvenation, The 5th International Conference on Autonomic and Trusted Computing (ATC 2008), LNCS 5060, 206-218, Springer-Verlag, 2008 (査読有) .
13. L. Z. Jin and T. Dohi, How good is gamma process modeling for software reliability assessment, Proc. of 2008 Asian International Workshop on Advanced Reliability Modeling, 巻なし, 567-574, McGraw-Hill, 2008 (査読有) .
14. K. Rinsaka and T. Dohi, Adaptive software rejuvenation schedule based

- on non-parametric predictive inference: an expected cost model, Proc. of 2008 Asian International Workshop on Advanced Reliability Modeling, 巻なし, 591-598, McGraw-Hill, 2008 (査読有).
15. Y. Yamaguchi, H. Okamura and T. Dohi, Estimating a mixture of Erlang distributions based on variational Bayes, Proc. of 2008 Asian International Workshop on Advanced Reliability Modeling, 619-626, McGraw-Hill, 2008 (査読有).
 16. H. Okamura and T. Dohi, Availability optimization in operational software system with aperiodic time-based rejuvenation scheme, Supplementary Proc. of 19th Int'l Sympo. on Software Reliability Engineering, 1-6, IEEE CS Press, 2008 (査読有).
 17. K. Rinsaka and T. Dohi, Non-parametric predictive inference of adaptive software rejuvenation schedule, Supplementary Proc. of 19th Int'l Sympo. on Software Reliability Engineering, 7-12, IEEE CS Press, 2008 (査読有).
 18. T. Ishii and T. Dohi, A new paradigm for software reliability modeling - from NHPP to NHGP -, Proc. of 14th Pacific Rim Int'l Sympo. on Dependable Computing, 巻なし, 224-231, IEEE CS Press, 2008 (査読有).
 19. H. Okamura and T. Dohi, Hyper-Erlang software reliability model, Proc. of 14th Pacific Rim Int'l Sympo. on Dependable Computing, 巻なし, 232-239, IEEE CS Press, 2008 (査読有).
 20. T. Dohi, N. Kaio and S. Osaki, Estimating cost-effective checking request policies, Quality Technology and Quantitative Management, 4 (2), 1-13, 2007 (査読有).
 21. K. Shibata, K. Rinsaka and T. Dohi, Dynamic software reliability modeling with discrete-test metrics; how good is it?, Int'l J. Industrial Engineering, 14 (4), 332-339, 2007 (査読有).
 22. H. Okamura, T. Sakoh and T. Dohi, A note on Markov chain Monte Carlo for software reliability models with group data, Proc. of 2007 Int'l Workshop on Recent Advances in Stochastic Operations Research, 221-228, 2007 (査読有).
 23. K. Rinsaka and T. Dohi, Effective algorithms for the optimal software rejuvenation schedule under censoring, Proc. of 2007 Int'l Workshop on Recent Advances in Stochastic Operations Research, 243-250, 2007 (査読有).
 24. K. Rinsaka and T. Dohi, A faster estimation algorithm for periodic preventive rejuvenation schedule maximizing system availability, Service Availability (ISAS 2007), LNCS 4526, 94-104, Springer-Verlag, 2007 (査読有).
 25. H. Okamura, M. Grottke, T. Dohi and K. S. Trivedi, Variational Bayesian approach for interval estimation of NHPP-based software reliability models, Proc. of 2007 Int'l Conf. on Dependable Systems and Networks, 698-707, IEEE CS Press, 2007 (査読有).
 26. H. Okamura and T. Dohi, Confidence intervals of software release time based on Bayesian estimation, CD-ROM Proc. of 5th Int'l Conf. on Mathematical Methods in Reliability, 1-9, 2007 (査読有).
 27. K. Rinsaka, K. Shibata and T. Dohi, Empirical stopping rule for testing a software - theory and application -, CD-ROM Proc. of 5th Int'l Conf. on Mathematical Methods in Reliability, 10-17, 2007 (査読有).
 28. T. Ishii, T. Dohi and H. Okamura, Bivariate software fault-detection models, Proc. of 31st Annual Int'l Computer Software and Applications Conf., 535-538, IEEE CS Press, 2007 (査読有).
 29. H. Okamura, Y. Kamahara and T. Dohi, Estimating Markov-modulated compound Poisson process, Proc. of 2nd Int'l Conf. on Performance Evaluation Methodologies and Tools, 1-10, ACM Press, 2007 (査読有).
 30. K. Rinsaka and T. Dohi, Non-parametric predictive inference of preventive rejuvenation schedule in operational software systems, Proc. of 8th Int'l Sympo. on Software Reliability Engineering, 247-256, IEEE CS Press, 2007 (査読有).
 31. K. Shibata, K. Rinsaka, T. Dohi and H. Okamura, Quantifying software maintainability based on a fault-detection/correction model, Proc. of 13th Pacific Rim Int'l Sympo.

- on Dependable Computing, 35-42, IEEE CS Press, 2007 (査読有) .
32. K. Shibata, K. Rinsaka and T. Dohi, PISRAT: Proportional intensity-based software reliability assessment tool, Proc. of 13th Pacific Rim Int'l Sympo. on Dependable Computing, 43-52, IEEE CS Press, 2007 (査読有) .
 33. T. Uemura and T. Dohi, Quantitative evaluation of intrusion tolerant systems subject to DoS attacks via semi-Markov cost models, Emerging Directions in Embedded and Ubiquitous Computing (EUC 2007 Workshops), LNCS 4809, 31-42, Springer-Verlag, 2007 (査読有) .

〔学会発表〕(計 10 件)

1. 岡村寛之, 土肥正, キッシュョー・トリベディ“自律的再稼動制御におけるオンライン適応アルゴリズム, 第 60 回 フォールトトレラントコンピューティング (FTC) 研究会, 山形, 1 月 29 日-31 日, 2009.
2. 岡村寛之, 土肥正, Estimating computer virus propagation using Markovian arrival processes, 待ち行列シンポジウム「確率モデルとその応用」報文集, pp. 168-177, 松本, 1 月 21 日-23 日, 2009.
3. 林坂弘一郎, 土肥正, コスト有効性に基づいたソフトウェアの適応的若化スケジューリング, 第 25 回電子情報通信学会アシュアランスシステム研究会技術研究報告, pp. 8-15, 神戸, 11 月 14 日, 2008.
4. 岡村寛之, 土肥正, 混合アーランソフトウェア信頼性モデル, 電子情報通信学会技術研究報告 (信頼性研究会), vol. 108, no. 125, pp. 7-12, 帯広, 7 月 11 日, 2008.
5. 岡村寛之, 徳實賢山, 土肥正, 脆弱性ライフサイクルとユーザプロファイルを考慮したソフトウェアシステムのセキュリティ評価, 電子情報通信学会技術研究報告 (信頼性研究会), vol. 108, no. 72, pp. 13-17, 神戸, 5 月 30 日, 2008.
6. T. Sakoh, H. Okamura and T. Dohi, A statistical approach for software release problem, 電子情報通信学会技術研究報告 (信頼性研究会), vol. 107, no. 137, pp. 27-32, 北見, 7 月 13 日, 2007.
7. T. Ishii, T. Dohi and H. Okamura, Bivariate software fault-detection models, 電子情報通信学会技術研究報告 (信頼性研究会), vol. 107, no. 137, pp. 33-38, 北見, 7 月 13 日, 2007.
8. 蒲原雄也, 岡村寛之, 土肥正, マルコフ変調複合ポアソン過程に基づいたパケットプロファイルによる統計的侵入検知, 電子情報通信学会技術研究報告 (信頼性研究会), vol. 107, no. 43, pp. 7-12, 東広島, 5 月 18 日, 2007.
9. 佐光哲哉, 岡村寛之, 土肥正, ベイズ推定に基づいたソフトウェアリリース時間の信頼区間, 電子情報通信学会技術研究報告 (信頼性研究会), vol. 107, no. 43, pp. 31-36, 東広島, 5 月 18 日, 2007.
10. 柴田和也, 林坂弘一郎, 土肥正, PISRAT: Proportional intensity-based software reliability assessment tool, 第 20 回電子情報通信学会アシュアランスシステム研究会技術研究報告, pp. 9-16, 横浜, 3 月 9 日, 2007.

〔図書〕(計 1 件)

1. S.-H. Shu and T. Dohi (eds.), Advanced Reliability Modeling III - Global Aspect of Reliability and Maintainability, McGraw Hill, 811 pages, 2008.

6. 研究組織

(1) 研究代表者

土肥 正 (TADASHI DOHI)
 広島大学・大学院工学研究科・教授
 研究者番号: 00243600

(2) 研究分担者

(3) 連携研究者