ディペンダビリティ工学講座
情報システムの信頼性向上を目指して

研究室紹介

土　屋　達　弘*

The Dependability Engineering Laboratory:
Towards Improved Dependability of Information Systems

Key Words：Dependability, Dependable systems, Software, Testing

はじめに

ディペンダビリティ（dependability）とは、最近では「総合信頼性」とも訳される言葉で、広い意味で信頼性を表す[1)]。ディペンダビリティ工学講座は、我々が運営している研究室の正式名称であり、大阪大学 大学院情報科学研究科に設置されている。本研究室では、情報システム、特にソフトウェアシステムを対象として、信頼性向上に関連する研究を行っている。

私が教授として着任したのは2012年4月であり、前任の菊野亨先生（大阪大学名誉教授）の後任という立場であった。本講座の前身は基礎工学研究科の計算機構学研究室であり、情報科学研究科の創設にともなって現在の名称となった。私自身は、学生、助手、講師、准教授、そして現在教授として、足掛け30年近く在籍していることになる。もともと信頼性に興味があったわけではなく、何となく研究室を選んだというのが実情なのだが、次第に研究に没頭していって現在に至っている。

学生として研究室に配属された90年代でも、情報システムの信頼性は重要な課題であったが、当時と比較して社会の情報技術への依存はますます進み、信頼性への要求は更に高まっている。重要性と比較して派手さのないこの課題を、地道に探究しているのが本研究室である。本稿では、研究室で取り組んでいるいくつかのテーマを取り上げて簡単に紹介したい。

* Tatsuhiro TSUCHIYA
1972年3月生まれ
大阪大学　大学院　基礎工学研究科
物理系専攻　博士前期課程（1995年）
現在、大阪大学　大学院情報科学研究科
情報システム工学専攻　教授
博士（工学）　専門／情報工学
TEL：06-6879-4535
FAX：06-6879-4539
E-mail：t-tutiya@ist.osaka-u.ac.jp

ソフトウェアテスト

情報システムを開発する場合、正しく動作するかを確認するテスト工程が、全体の開発コストの半分以上を占めることも珍しくない。システムに十分な信頼性を保ちながら、テストのコストを低減することは、実用上非常に重要な課題である。

組み合わせテストは、この二つの矛盾した目標を解決する手法として、広く実践されている。

今、情報システムとしてプリンタを考え、そのテストを想定して、レイアウト、用紙サイズ、カラー印刷、両面印刷、の四つの因子について、それぞれ二つの選択肢があるものとする。これらを組み合わせたシステムの構成の総数は16であり、異なる構成は一つずつテストする必要があるものとする。以下は、16の構成から五つを、ある条件を満たすように抽出したものである。各行がテストする構成を表している。

レイアウト	用紙サイズ	カラー印刷	両面印刷
縦	A4	カラー	両面
縦	A4	白黒	片面
縦	B5	白黒	両面
横	A4	白黒	両面
横	B5	カラー	片面

ここで「ある条件」とは、二つの因子をどのように選んでも、値のペアがすべてどこかでテストされていることである。たとえば、レイアウトとカラーという二つの因子に注目すると、四つのペア（横，白黒）（縦，白黒）（横，カラー）（縦，カラー）が、いずれかの行に出現していることが分かる。特定の

2個の因子間のインタラクションによって不具合がしばしば生じることが知られており、このようにうまくテストする構成を選択することで、少ないコストで効率の良いテストを実施することができる。

ただし、実際のシステムでは因子が100を超えることも多いので、人手でこのようなテストを設計することは現実的ではなく、コンピュータを用いることが必要となる。そこで本研究室では、CIT-BACH[2]と名付けた組み合わせテスト用のテスト設計ツールを開発し、フリーソフトウェアとして公開している。

また、この数年では、組み合わせテストを拡張して、不具合の存在を検出するだけでなく、どこに不具合があるのかも特定できるようなテストを設計することにも取り組んでいる。

ある構成をテストした際、システムに異常が見られなければ、そのテストはパスしたという。逆に、異常が生じた場合は、そのテストはフェイルしたという。先の5通りの構成をテストした際、結果が上から順にパス、パス、フェイル、パス、パスだったとする。すると、フェイルした構成に含まれるインタラクションの中で、(縦, 白黒)(縦, 両面)(白黒, 両面)はパスした構成に含まれているので異常の原因ではないといえるが、残った(縦, B5)(B5, 白黒)(B5, 両面)のうち、どれが原因なのかは判定できない。

下の表も先程と同様にテストする構成を表したものであるが、少し数が多くなっている。

レイアウト	用紙サイズ	カラー印刷	両面印刷
縦	A4	カラー	両面
縦	A4	白黒	片面
縦	B5	カラー	片面
縦	B5	白黒	両面
横	A4	白黒	両面
横	B5	カラー	両面
横	B5	白黒	片面

仮に、(B5, 白黒)が異常の原因だったとする。すると、これらの構成を実行したとき、結果は上からパス、パス、パス、フェイル、パス、パス、フェイルとなる。フェイルした構成すべてに出現するインタラクションは(B5, 白黒)だけあり、テストをパスしたどの構成にも含まれていない。したがって、(B5, 白黒)が異常の原因であると結論できる。実は、どのインタラクションが原因であっても、必ず一意に特定できるように、上の表は設計されている。

研究室では、このようなテスト設計を自動的に行う手法を世界に先駆けて開発している[3]。

文章に基づくテスト充足度の分析

情報システムの開発現場では、システムのテストを他の会社にアウトソーシングすることも多い。テストを担当する会社では、行った一つ一つのテストを文章として記録し、発注元の会社に報告する。このような文章を手掛かりに、システムの機能が十分にテストされているのか、あるいは、もっとテストを行うべき機能はどれか、といったことを明らかにできれば、システムの品質管理にとって有用で、信頼性の向上につながる。

研究室では、企業と共同で、実際のシステムのテスト工程で作成されたこのような文章と、システムの機能を記述した文章との類似度を測定することで、実施したテストがカバーしている機能の範囲を特定し、可視化する方法を開発した[4]。テストを記述した文章と機能を記述した文章が同じ言葉や話題に触れているのであれば、それら二つの文章は類似度が高いと見なし、そのテストはその機能をテストしていると判断する。

幸い、近年、人工知能関連技術が極めて容易に利用可能になっており、機械的に文章の話題を抽出する潜在的ディリクレ配分法（LDA）などを用いて、このような解析を実現することができた。

サイバーフィジカルシステムの高信頼化

電力システムなど、物理的なシステムと情報システムが融合されたサイバーフィジカルシステムでは、構成要素同士が複雑に依存しあっており、その結果、ある構成要素の初期障害が、別の構成要素の障害を引き起こし、結果として、連鎖的障害を生じさせることがある。このようなシステムにおいて、どの部分が最も脆弱なのか、あるいは、どの部分を強化すればシステムを頑強にできるのか、といった課題に取り組んでいる。

具体的な研究例としては、よく知られた連鎖障害

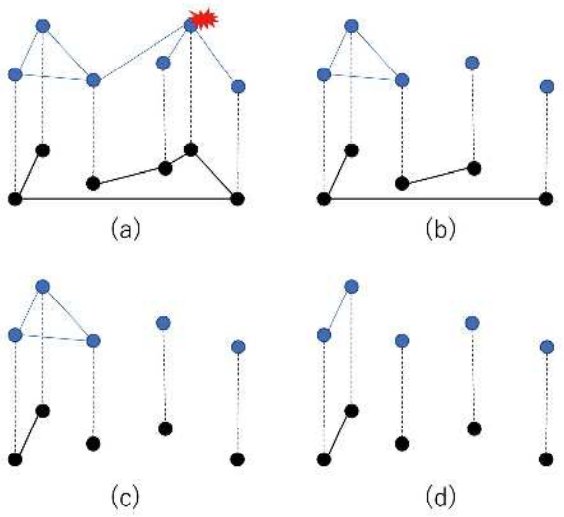

図１　連鎖的障害のモデル[6]。電力システムを相互に依存する電力ネットワーク（上）と情報ネットワーク（下）から構成されるシステムとしてとらえる。片方のネットワーク上の障害（a）が、もう一方のネットワーク障害（b）（c）を引き起こし、結果的にシステム全体に障害が波及する（d）

のモデル（図１）を基に、もっとも脆弱なポイントを探索する手法を開発した[5]。複数のポイントが初期障害を起こす場合、そのパターンは膨大となるため、一つ一つを調べるわけにはいかないのがこの問題の難しい点である。

そこで、提案した手法では、連鎖的障害のすべての発生パターンを、一つの方程式として「記号的に」表現する。方程式の変数の値によってある時点においてシステムの構成要素が正常か障害かを表し、方程式の解が連鎖的障害のパターンに一致するように式を構成する。方程式をコンピュータによって解くことで、そのようなパターンが存在するか、存在するならどの様に発生するかが分かる。

おわりに

本稿では、我々の研究室であるディペンダビリティ工学講座での研究テーマのいくつかについて紹介した。なお、更に最近になって取り組みをスタートしたテーマの一つとして、ブロックチェーン関連の信頼化技術があり、保存するデータの暗号化機構の実装などに取り組んでいる。また、人工知能のテストについても、メタモルフィック・テスティングと呼ばれる技術の可能性を検討している。

最後に、研究室を共に運営している中川博之准教授と小島英春助教へ感謝したい。

参考文献

1) 米田友洋，梶原誠司，土屋達弘：「ディペンダブルシステム―高信頼システム実現のための耐故障・検証・テスト技術」，共立出版（2005）
2) https://ja.osdn.net/users/t-tutiya/pf/cit_bach/
3) Tatsuya Konishi, Hideharu Kojima, Hiroyuki Nakagawa, Tatsuhiro Tsuchiya: Using simulated annealing for locating array construction, Information and Software Technology, Vol.126, 106346 (2020)
4) 松井勝利，中川博之，土屋達弘：文書間の類似度に基づいた要求カバレッジ可視化手法，コンピュータソフトウェア，Vol.35, No.1, pp.67-75 (2018)
5) Kenta Hanada, Tatsuhiro Tsuchiya, Yasumasa Fujisaki: Satisfiability-Based Analysis of Cascading Failures in Systems of Interdependent Networks, Proc. 24th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC 2019), pp.105-113 (2019)
6) Sergey Buldyrev et al.: Catastrophic cascade of failures in interdependent networks, Nature, Vol.464, pp.1025-1028 (2010)