様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　６　月　１７　日現在

機関番号：　６２６１５
研究種目：　挑戦的萌芽研究
研究期間：　2015～2016
課題番号：　１５Ｋ１２０１２

研究課題名（和文）実行時ゴールモデル追跡による想定外の検出

研究課題名（英文）Detection of Unexpected by Runtime Goal Model Tracking

研究代表者
石川　冬樹（Ishikawa, Fuyuki）

国立情報学研究所・コンテンツ科学研究系・准教授

研究者番号：５０４５５１９３

交付決定額（研究期間全体）：（直接経費）　　2,500,000円

研究成果の概要（和文）：より深く物理的な環境や人の活動に踏み込むシステムでは，あらゆる状況や前提条件などを十分に想定し，システムによるゴールの達成方法やその適応を定めることが非常に難しい．これに対し本研究では，実行時にゴールの達成に関する追跡を行い，ゴールの達成に関する論理が想定と合わなくなっている箇所を検出することにより，原因追及を支援する手法を提案，評価する．これにより，「システム自身の助けを得て人と共に想定外をデバッグする」というアプローチの確立を目指す．

研究成果の概要（英文）：It is very difficult to define the way of goal realization and its adaptation by supposing all possible situations and conditions as systems have increasingly intensive interactions with physical environments and human activities. In this work, we investigate methods to analyze root causes of gaps between the assumptions on the goal realization logic and the reality. For this purpose, we apply runtime monitoring of goal realization. Thus, we challenge to establish the collaboration between human and the system itself to debug the "unexpected."

研究分野：　ソフトウェア工学

キーワード：　ゴールモデル　不確かさ　障害原因分析　サイバーフィジカルシステム

１．研究開始当初の背景

近年，実世界に多数のセンサー・アクチュエーターを埋め込み活用し，より深く物理的な環境や人の活動に踏み込むシステムが多く提案されている．そのため実世界への影響が大きくなり，システムの動作環境やその変化への適切な対応が求められる．一方，人の振る舞いや障害物など実世界の影響が大きくなり，環境やその変化を，机上で予め十分に洗い出すことは難しい．

ここでシステムの動作（仕様）を適切に定めるためには，システムがゴールを達成するためのサブゴールや代替ゴール，環境に求める前提条件などゴールモデルの分析を行うこととなる（ゴール指向要求分析や，アシュアランスケースなど）．従来のシステム開発では，これらの分析を開発時に人が行い，それを基に設計を得てプログラムに書き起こす．しかし前述のように，机上，事前の分析であらゆる状況を考慮し尽くすことは難しい．さらに，ゴールモデルとプログラムのギャップが大きくなる（相関が暗黙的になる）．このため，プログラムを実行して問題が顕在化した際，元の分析（想定）のうちどの部分が問題の根源であるかを追求するのが困難である．

環境変化への対応のためのアプローチとしては，従来開発時に机上で検討されるのみであったモデルを，実行時にシステムにも保持させ扱わせることが提起されている（自己適応システムのためのソフトウェア工学[1]，Requirements-Aware Systems[2]）．しかし現状の取り組みは，あるゴールの前提条件が成り立たないときに分析結果に基づき代替ゴールの実現を目指す[3]など，システムが機能実現の過程などをより明示的に理解，監視し推論や振る舞いの再生成を行うもので，（想定している命題の真偽ではなく）隠れた仮定や因果関係，競合を扱っているものではない．

想定外の状況でのシステムの実行結果として障害などの問題が顕在化したとき，それは結果であり，その根源としてどのような想定外があるかは自明でない．さらに想定とは異なる実行が進んでいるが問題としてなかなか表面化しないこともありうるほか，問題の原因が単にバグ（想定およびゴール達成方針ではなく実現方法の誤り）である可能性もある．そもそも「想定外（思いもしていない）」という意識の問題も併せると，想定外に対する原因追及は非常に困難な問題である．

[1] 鄭ら，自己適応ソフトウェアのための自己適応性設計に関する研究動向，コンピュータソフトウェア，Vol. 31 No. 1，2014
[2] P. Sawyer et al, Requirements-Aware Systems: A Research Agenda for RE for Self-adaptive Systems, RE 2010
[3] L. Fu et al., Stateful requirements monitoring for self-repairing socio-technical systems, RE 2012

２．研究の目的

本研究では上記の問題に対し，ゴールモデルの実行時追跡を通して，想定外を検出する基礎技術を構築する．具体的には，以下の達成項目を扱う．

【達成項目１】ゴールの論理構造に対する想定外のパターン　を洗い出し，それに対し，
【達成項目２】ゴールモデルの実行時追跡に基づく想定外の検出手法　を定め
【達成項目３】様々な事例に対する評価　を行う．

図１に従来のシステム開発・保守プロセスと，本研究が想定する継続的なプロセスを示す．上部に示すように，注意深く分析を行っても，その想定が実際のソフトウェアで観測される事象とどう結びついているかが暗黙的であると，観測された事象から，その根源となる想定外を探し紐付けていくことは困難である．これに対し本研究のアイディアは，図の下部に示すように，システム自身が想定をたどり確認しつつ実行を進めることで，どの想定が崩れている可能性があるのかを検出することができるようにする．これは従来と大きく異なるアプローチである．

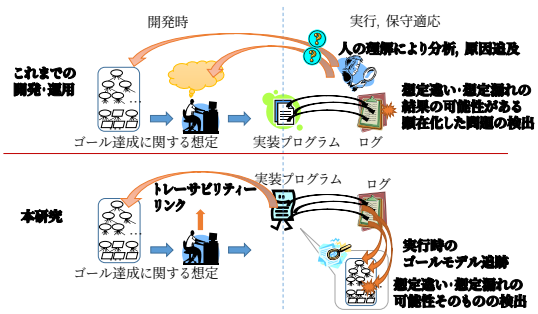

図 1 本研究のアプローチ

研究期間内に扱うゴールの種類としては，時相論理で表現できるものなど機能的なゴール（論理的に達成されるゴール）のみを扱う（利用者の満足感などは扱わない）．

本研究の特色は，想定されていない命題や因果関係，競合に対し，システム自身がその可能性を検出し，人による原因追求を支援するという課題のチャレンジ性にある．その成果は，シミュレーションやテスト，さらに実運用を通して想定外を発見し，システムを継続的に適応・進化させていくプロセスの基礎となる．その発展により，「想定外」に向き合い続けていくための工学技術への展開が期待される．これらの技術的な発展により，ロボットや家電，車，ウェアラブル端末などを用い，より深く物理的な環境や人の活動に踏み込んで支援を行うシステムの高信頼化，そのための継続的な開発・更新の効率化に寄

与する．

３．研究の方法

本研究で扱う「想定」とは，ゴール達成に関する例えば下記のような命題である．

- ゴール g を達成するためにはサブゴール sg1，sg2 の両方を達成することが必要十分条件である．
- ゴール sg1 を達成する手段の一つは m1 でありその実行には環境に関する前提条件 p の成立が必要である．別の手段 m2 は前提条件 p を必要としない．

こういった想定は一般にゴールモデルとして表現されてきた．要求分析にて活用されているほか，近年ではアシュアランスケースと呼ばれる信頼性の議論・証拠の表現にも用いられている．

ここで例えば上記の命題 1 つ目について，モデル上に表現されていない要因（他アプリケーションとの干渉やユーザの振る舞いなど）により，「サブゴール sg1 と sg2 が成り立っていてもゴール g が成り立つとは限らない」ことがわかったとする．これは本研究にて扱う想定外の一例であり，「必要なはずだが想定から漏れている（暗黙の仮定となっている）サブゴールが存在する」というパターンである．この例の場合，システムの実行時に「sg1 と sg2 が成り立っているが sg が成り立っていない」という条件を監視することにより検出することができる．これは最も単純で自明な場合であるが，このようなパターンを明示的に意識することにより，実行時の監視内容を定める．

最初に，達成項目１（ゴールの論理構造に対する想定外のパターン）について，理論的，系統的な洗い出しと，実例からの洗い出しの双方を行うことにより，洗い出しを行った．すなわち，ある論理体系内での網羅性と，実用上の重要性とを考えて必要となるものを含めるような進め方を採った．

続いて，達成項目２（ゴールモデルの実行時追跡に基づく想定外の検出手法）に関し，抽出した個々のパターンに対して，その検出手法の基本検討を行った．ここで，ゴールモデルと，実際のシステムにて監視されるイベントや条件との対応については，既存研究などで扱われているようにトレース可能であることを仮定している．観測された事象に対して，ゴールモデルで表現された命題の集合にて説明が付かない（矛盾がある）場合が想定外の発生と見なされる．ここで，一部の命題や因果関係を変更することにより説明が付くようになるのであれば，それが一つの想定外の可能性を示唆することになる．ただし，そのような説明は複数存在しうるため，それらを制約充足ソルバーなどにより列挙することを試みる．

最後に，達成項目３（様々な事例に対する評価）に取り組んだ．研究体制にて示すように研究代表者らが取り組んできた様々なプロジェクトにおけるゴールモデルを用いて評価を行う．既存のゴールモデルの初期版を用いる，あるいは洗練されたゴールモデルに抜けを埋め込むなどして，既知の想定外を含むゴールモデルを作成する．それらのゴールモデルに基づくシステム実現を，実行あるいはシミュレーションし，実行時の観測に相当する情報を得る．この情報を基に，埋め込まれた想定外をどの程度検出できるかを評価した．その他，提案を用いない場合における検出の困難さ，構築した技術の発展の可能性と必要性などについても，定性的に議論，評価を行った．

４．研究成果

以上のように本研究においては，不確かさの存在が前提となるシステム開発に対し，ゴールモデルの実行時追跡のアプローチを追求した．想定外のパターンとして 6 個のパターンを得て，その検出手法の試行を行った．基本的にはアプローチの有効性を確認することができた．

一方，観測された情報だけでは想定外の根元を一意には特定できない状況が少なからずあった．プログラムに対する障害原因の推定（Fault Localization）と同様に，統計的，経験的な手法も交えた総合的なアプローチを採り，今後も引き続き取り組んでいく．

５．主な発表論文等

〔雑誌論文〕（計 0 件）

〔学会発表〕（計 0 件）

〔図書〕（計 0 件）

〔産業財産権〕

○出願状況（計 0 件）

○取得状況（計 0 件）

〔その他〕

６．研究組織

(1)研究代表者
石川　冬樹（ISHIKAWA, Fuyuki）
国立情報学研究所・コンテンツ科学研究系・准教授
研究者番号：50455193

(2)研究分担者
本位田　真一（HONIDEN, Shinichi）
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：70332153

(3)連携研究者

(4)研究協力者