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

令和　５ 年　 ６ 月　 ５ 日現在

機関番号：３２６８９
研究種目：基盤研究(B)（一般）
研究期間：2018～2021
課題番号：１８Ｈ０３２２５

研究課題名（和文）想定に漏れた環境変化にしなやかに耐える実行時モデルフレームワーク

研究課題名（英文）Models@run.time Framework for Graceful Degradation

研究代表者
鄭　顕志（TEI, Kenji）

早稲田大学・理工学術院・准教授（任期付）

研究者番号：４０４３４２９５

交付決定額（研究期間全体）：（直接経費）　　12,800,000円

研究成果の概要（和文）：本研究では「開発時の想定から漏れた変化」に対しても最大限の安全性を保証するGraceful Degradationを実現するために，システム自身が実行時にモデルを活用して保証を伴う自己適応を実現する実行時モデル更新技術を確立した．具体的には，(1)開発時の想定に漏れた変化をモデルに反映し，(2)更新された環境モデル下で安全性を保証する動作仕様を実行時に自動導出する技術を確立した．また，構築した技術を反映した実行時モデルフレームワークを開発し，IoTシステムやロボットシステムでの評価実験を通じて手法の有効性と限界を明らかにした．

研究成果の学術的意義や社会的意義
開発時の想定のみに頼る従来の安全性保証技術では，本質的に想定漏れを避けることが困難な近年のソフトウェアシステムで十分な安全性を保証することができない．近年のIoTシステムやCPSが対象とするオープン環境ではシステムの動作に影響を与えうる事象が無数に存在する．あらゆる可能性を想定しようとすると工数が増大し，また想定漏れは本質的に防ぎきれない．そこで本研究では開発時の想定に漏れた環境変化が起きてもシステムが即応的に適応し，その時点で可能な最大限の安全性を保証するよう段階的に動作を変更するGraceful Degradationを実現する技術を構築した．

研究成果の概要（英文）：We aimed to realize Graceful Degradation, which guarantees maximum safety even in the case of "changes that were not assumed at the time of development". For this purpose, this research established Models@run.time techniques in which the system itself utilizes the model at runtime to realize self-adaptation with guarantees. Specifically, we have established techniques that (1) reflect changes that were not assumed during development in the model and (2) automatically synthesize at runtime a behavior specification that guarantees safety under the updated environmental model. We also developed a models@run.time framework that reflects the established technology, and clarified the its effectiveness and limitations through evaluation experiments on IoT systems and robot systems.

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　Models@run.time　離散制御器合成　モデル学習

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

開発の早期段階においてソフトウェア動作の安全性を保証する手法としてモデル検査等の形式的検証がある．システムの実行環境を分析して環境の状態遷移モデルを構築し，環境モデルが満たすべき安全性を時相論理式等で記述する．加えてソフトウェアの動作仕様も状態遷移モデルとして表し，動作仕様による環境モデルへの影響を網羅的にチェックし，動作仕様の安全性を検証，保証する． 例えばドローン監視システムの場合，監視対象地域やドローンの情報を環境モデルとして表し，それら環境内の機器を監視，制御するソフトウェアの動作仕様モデルが期待される安全性が満たされるかを検証する．だがこの方式では開発時に想定した環境下でしか安全性が保証されない．オープン環境下では，突風，濃霧，ゲリラ豪雨，落雷といった気象変動や他のドローン・鳥類の有無など，ドローン監視システムの動作に影響を与えうる事象が無数に存在する．あらゆる可能性を想定しようとすると工数が増大し，また想定漏れは本質的に防ぎきれない．このことは変化の激しい実世界と密に連動するソフトウェアにおいて顕著な問題となる．開発時の想定に漏れた環境変化が起きてもシステムが即応的に適応し，その時点で可能な最大限の安全性を保証するよう段階的に動作を変更する Graceful Degradation を実現することが望まれる．

開発時の想定のみに頼る従来の安全性保証技術では，本質的に想定漏れを避けることが困難な近年のソフトウェアシステムで十分な安全性を保証することができない．本研究では「開発時の想定に漏れた環境変化に対して即応的に適応し最大限の安全性を保証する Graceful Degradation を行うシステムをどのようにして実現するのか？」という問いを扱う．

２．研究の目的

本研究では「開発時の想定から漏れた変化」に対しても最大限の安全性を保証する Graceful Degradation を実現するために，システム自身が実行時にモデルを活用して保証を伴う自己適応を実現する実行時モデル更新技術を確立する(図 2)．具体的には，(1)開発時の想定に漏れた変化をモデルに反映し，(2)更新された環境モデル下で安全性を保証する動作仕様を実行時に自動導出する技術を確立することを目的とする．

【目的 1: 環境モデルの実行時更新技術の確立】従来，開発時に人手で行われていた「環境モデルの構築」を自動化し，実行時に検知した想定漏れの変化を環境モデルに対して迅速かつ正確に反映する技術を確立する．

【目的 2: 保証を伴う動作仕様の実行時自動導出技術の確立】 従来開発時に人手で行われていた「安全性を保証する動作仕様の導出」を自動化し，更新された環境モデル下で最大限の安全性を保証するシステム動作モデルを実行時に実用的な速度で生成する技術を確立する．

３．研究の方法

本研究では想定漏れの変化に耐える Graceful Degradation を実現する実行時モデル更新技術を確立(実施項目 1,2)し，その技術を反映した実行時モデルフレームワークを用いた実証実験(実施項目 3)により本手法の有効性と限界を明らかにする．

実施項目 1: 環境モデルの実行時更新技術の確立(担当：鄭，本位田)

【提案内容】実行中に得られた実行トレースから Labeled Transition System (LTS)形式の環境モデルを更新する．想定漏れが起きた場合，実行トレースが示す「実際に起きた環境変化」が環境モデルでは受理できなくなる．この不整合を解消するため，実行トレースによって判明した「実際に起きた環境変化」に対して過不足ない遷移をもつ LTS 形式の環境モデルとなるように実行時に更新する手法を提案する．

【解決すべき課題】開発時に環境モデルを構築する従来手法では多量の実行トレースを，勾配降下法をベースとしたバッチ処理で解析することで環境モデルを構築していた[1]．実行時に適用した場合，バッチ処理方式ではモデル構築の計算時間が課題となる．研究代表者の事前実験の結果では一度のモデル構築に十数分を要した．開発時であれば許容範囲内であるが，実行時に活用する場合，現実的な計算時間ではない．

[1] D.Sykes, et.al., Learning revised models for planning in adaptive systems, ICSE2013

【解決のアプローチ】本研究では，バッチ処理を避け，環境モデルを差分更新する手法を提案する．確率的勾配降下法を応用し，実行時に得られた実行時に新規に得られたトレースの差分から，逐次的にモデル更新するオンライン更新手法を提案する．バッチ処理を避けた逐次更新を実現することで，モデル構築時間の大幅な短縮を試みる．

実施項目 2: 保証を伴う動作仕様の実行時導出技術の確立(担当：鄭)

【提案内容】実行時に更新された LTS 形式の環境モデルに対して，時相論理式で記述された安全性を最大限保証する動作仕様を自動で導出する技術を確立する．開発時に優先順位付けされた安全性要求群から，現在の環境下で保証が可能な最大限の安全性要求を判定し，その要求を満た

すことが保証された動作仕様を自動導出する．本実施項目は Discrete Controller Synthesis(DCS)技術を実行時に実用的な速度で実行可能とするよう拡張することで達成する．DCS は与えられた環境モデル下で要求充足が保証された LTS 形式のシステム動作仕様をゲーム理論に基づき自動で導出する．DCS により解となる LTS が生成された場合，その要求は現在の環境下で保証可能であり，その解は保証を伴う動作仕様となる．

【解決すべき課題】環境変化に対して実行時に適応するためには，動作仕様の導出を高速に実行可能でなければならない．しかしながら，従来の DCS は入力された環境モデルの空間探索を一から行うため実行時に用いる場合，実用に耐える実行速度ではない．研究代表者による予備実験では仕様モデル導出に数十分の時間を要した．

【解決のアプローチ】本研究では，実行時に更新された環境モデルの差分に着目して効率化を試みる．環境モデル更新の差分を分析し，生じた変化が影響する箇所の部分的な再探索のみで動作仕様を導出することで効率化を図る．

実施項目 3．実証実験・公開（担当：本位田・鄭）

実施項目 1,2 で構築した技術を，以前に開発した実行時モデルフレームワーク上に反映し，2 回の実証実験を通して確立した技術の有用性，限界を評価する．初回の実験ではクローズドな環境で動作する自動倉庫管理システムを，2 回目の実験ではオープン環境で動作するドローン監視システムをフレームワーク用いて開発し，想定漏れの変化に対する品質維持能力や実行時モデル更新のオーバヘッドを評価する．

４．研究成果

本研究によって得られた実施項目 1,2 の研究成果詳細と，実施項目 3 による実験を通して得られた性能評価結果の概要について説明する．

実施項目 1：環境モデルの実行時更新技術の確立(担当：鄭，本位田)

Sykes らのバッチ処理方式による環境モデル学習手法を拡張して，実行時の環境モデル学習手法を構築(図 1)した．具体的には，環境モデル LTS を構成する状態と遷移を<事前条件，アクション，事後条件>のトリプルで表されるルールに変換し，学習によって各ルールの尤度を推定する．この尤度の学習は，得られた実行トレースを最も確からしく説明できるように行われる．この尤度更新を，確率的勾配降下法(Stochastic Gradient Decent: SGD)を用いたオンライン学習としてモデル化することで，実行時の環境モデル学習を実現する．SGD では，本来，ランダムでサンプルをピックし尤度更新を行うが，本手法では実行時に得られた最新のトレースをランダムピックとみなし，尤度更新を行う．

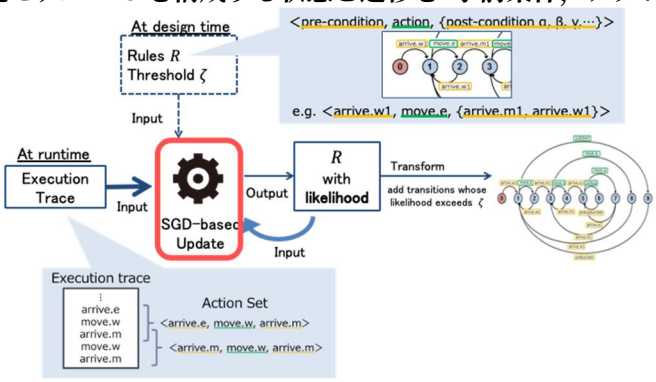

図 1 確率的勾配降下法を用いた実行時環境モデル学習手法

また，本研究では提案した実行時環境モデル学習手法の精度と学習時間を，従来の Sykes らの手法を単純に実行時に用いた場合を比較対象として評価した．実証実験の一つである自動倉庫管理システムの例に適用した際の性能比較結果を図 2 に示す．精度の観点では，両手法は収束後の精度は同程度であることが確認できた．一方で，収束の速度は提案手法の方が大幅にはやく収束できることが確認できた．これは，従来のバッチ処理では時間ウィンドウ内のトレースデータを全て学習に使用するが，環境変化が起きた直後は大半のデータが変化前のトレースデータであるためであると考えられる．一方で，提案手法は最新のトレースデータを学習に強く反映するため，変化に対して追従性の高い学習が可能となっている．また，実行時間の観点でも，SGD を用いた提案手法では従来のバッチ処理方式と比べ，最大で 10 万倍の高速化が確認できた．

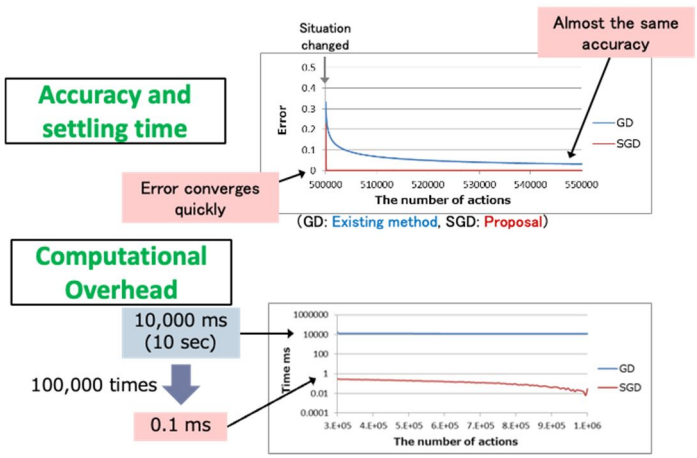

図 2 環境モデル学習手法の性能比較

実施項目 2：保証を伴う動作仕様の実行時導出技術の確立(担当：鄭)
DCS は 2 人プレイヤーゲーム理論に基づいており，入力となる LTS 形式の環境モデルをゲーム空間に変換し，ゲーム空間上で(1)勝利領域分析と(2)勝利戦略抽出を行い，得られた勝利戦略を LTS 形式に変換することで，保証を伴う動作仕様を合成する．本研究では，この(1)勝利領域分析アルゴリズムと(2)勝利戦略抽出アルゴリズムに着目し，環境変化に起因するゲーム空間での変化差分から部分的なゲーム空間再探索で勝利領域，勝利戦略を抽出する差分分析アルゴリズムを提案した．ゲーム空間の種類は扱う要求の種類によって異なる．本研究では，安全性要求に着目し，安全性ゲーム(Safety Game)の既存アルゴリズムを拡張することによって差分分析アルゴリズムを構築した(図 3)．
また，本研究では構築した差分分析アルゴリズムの性能評価を，従来の勝利領域分析アルゴリズム，勝利戦略抽出アルゴリズムと比較して行った．実証実験の例題の一つであるドローン監視システムのシナリオで評価したところ，従来手法と比較し，全体の約 20%, 30%の状態際探索のみで，従来手法と等価な動作仕様を合成することが確認できた．

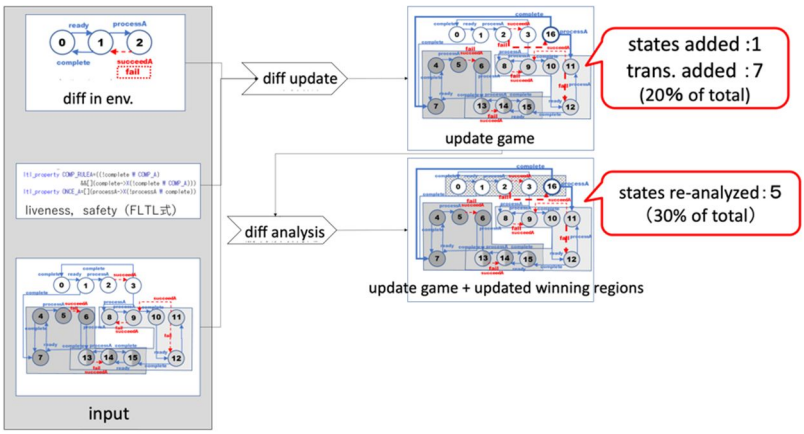

図 3 ゲーム空間差分分析アルゴリズム

５．主な発表論文等

〔雑誌論文〕　計8件（うち査読付論文　8件／うち国際共著　2件／うちオープンアクセス　1件）

１．著者名 相澤 和也、鄭 顕志、本位田 真一	４．巻 61
２．論文標題 活性と同時に保証可能な安全性特定のためのゲーム分析アルゴリズム	５．発行年 2020年
３．雑誌名 情報処理学会論文誌	６．最初と最後の頁 853～862
掲載論文のDOI（デジタルオブジェクト識別子） 10.20729/00204236	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 相澤 和也、鄭 顕志、本位田 真一	４．巻 J103-D
２．論文標題 違反状態抽象化による保証可能な安全性特定のための分析空間削減	５．発行年 2020年
３．雑誌名 電子情報通信学会論文誌D 情報・システム	６．最初と最後の頁 238～246
掲載論文のDOI（デジタルオブジェクト識別子） 10.14923/transinfj.2019PDP0018	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Nahabedian Leandro、Braberman Victor、Dippolito Nicolas、Honiden Shinichi、Kramer Jeff、Tei Kenji、Uchitel Sebastian	４．巻 46
２．論文標題 Dynamic Update of Discrete Event Controllers	５．発行年 2020年
３．雑誌名 IEEE Transactions on Software Engineering	６．最初と最後の頁 1220～1240
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TSE.2018.2876843	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 相澤 和也，鄭 顕志，本位田 真一	４．巻 60(4)
２．論文標題 環境変化時に保証可能な安全性を特定するためのゲーム分析アルゴリズム	５．発行年 2019年
３．雑誌名 情報処理学会論文誌	６．最初と最後の頁 1025～1039
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 田邉 萌香，鄭 顕志，本位田 真一	4．巻 60(10)
2．論文標題 自己適応システムのための環境モデル実行時更新手法	5．発行年 2019年
3．雑誌名 情報処理学会論文誌	6．最初と最後の頁 1617～1630
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Munan Li, Kenji Tei, Yoshiaki Fukazawa	4．巻 8
2．論文標題 An Efficient Adaptive Attention Neural Network for Social Recommendation	5．発行年 2020年
3．雑誌名 IEEE Access	6．最初と最後の頁 63595～63606
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2020.2984340	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 L. Nahabedian, V. Braberman, N. DIppolito, S. Honiden, J. Kramer, K. Tei, S. Uchitel	4．巻 early access
2．論文標題 Dynamic Update of Discrete Event Controllers	5．発行年 2018年
3．雑誌名 IEEE Transactions on Software Engineering (TSE)	6．最初と最後の頁 1～21
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TSE.2018.2876843	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 T. Kobayashi, F. Ishikawa, S. Honiden	4．巻 31
2．論文標題 Consistency-preserving refactoring of refinement structures in Event-B models	5．発行年 2019年
3．雑誌名 Formal Aspects of Computing	6．最初と最後の頁 287～320
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s00165-019-00478-z	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計21件（うち招待講演　0件／うち国際学会　17件）

1．発表者名
Javier Camara, Alessandro Vittorio Papadopoulos, Thomas Vogel, Danny Weyns, David Garlan, Shihong Huang, Kenji Tei

2．発表標題
Towards Bridging the Gap between Control and Self-Adaptive System Properties

3．学会等名
15th International Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS2020)（国際学会）

4．発表年
2020年

1．発表者名
Jialong Li, Kazuya Aizawa, Kenji Tei and Shinichi Honiden

2．発表標題
Efficient Difference Analysis Algorithm for Runtime Requirement Degradation under System Functional Fault

3．学会等名
The 18th IEEE International Conference on Embedded and Ubiquitous Computing (IEEE EUC 2020)（国際学会）

4．発表年
2020年

1．発表者名
Takuto Yamauchi, Kenji Tei and Shinichi Honiden

2．発表標題
Method for Low-Cost Environment Partitioning Modeling in Dynamic Update

3．学会等名
IEEE Third International Conference on AI and Knowledge Engineering (AIKE)（国際学会）

4．発表年
2020年

1．発表者名
Kengo Kuwana, Kenji Tei, Yoshiaki Fukazawa and Shinichi Honiden

2．発表標題
Method of Applying Df-pn Algorithm to On-the-fly Controller Synthesis

3．学会等名
IEEE Third International Conference on AI and Knowledge Engineering (AIKE)（国際学会）

4．発表年
2020年

１．発表者名
Jialong Li, Kenji Tei and Shinichi Honiden

２．発表標題
Identifying achievable goals for adaptive replanning against runtime environment change

３．学会等名
The 20th International Conference on Intelligent Systems Design and Applications (ISDA)（国際学会）

４．発表年
2020年

１．発表者名
Munan Li, Kenji Tei, and Yoshiaki Fukazawa

２．発表標題
Heterogeneous Information Network based Adaptive Social Influence Learning for recommendation and explanation

３．学会等名
The 2020 IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT'20)（国際学会）

４．発表年
2020年

１．発表者名
Jialong Li, Zhenyu Mao, Zhen Cao, Kenji Tei, Shinichi Honiden

２．発表標題
Self-adaptive Hydroponics Care System for Human-hydroponics Coexistence

３．学会等名
2021 IEEE 3rd Global Conference on Life Sciences and Technologies

４．発表年
2020年

１．発表者名
安曽 徳康，小川 雅俊，松塚 貴英，鄭 顕志

２．発表標題
モデル予測制御と離散制御器合成による外部環境の動的特性を考慮した適応制御手法

３．学会等名
マルチメディア、分散、協調とモバイルシンポジウム(DICOMO2020)

４．発表年
2020年

１．発表者名
荒井 滉平，本位田 真一，鄭 顕志

２．発表標題
Event-Bによるリファインメントのパターン最適化

３．学会等名
日本ソフトウェア科学会第37回大会

４．発表年
2020年

１．発表者名
李 家隆，相澤 和也，鄭 顕志，本位田 真一

２．発表標題
離散制御器合成における設計誤りを特定するための反例出力手法

３．学会等名
IPSJ/SIGSEソフトウェアエンジニアリングシンポジウム2020(SES2020)

４．発表年
2020年

１．発表者名
Amel Bennaceur, Carlo Ghezzi, Kenji Tei, and et.al.,

２．発表標題
Modelling and Analysing Resilient Cyber-Physical Systems

３．学会等名
the 14th Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS2019)（国際学会）

４．発表年
2019年

１．発表者名
Piergiuseppe Mallozzi, Ezequiel Gustavo Castellano, Patrizio Pelliccione, Gerardo Schneider, Kenji Tei

２．発表標題
A Runtime Monitoring Framework to Enforce Invariants on Reinforcement Learning Agents Exploring Complex Environments

３．学会等名
2nd International Workshop on Robotics Software Engineering (RoSE 2019)（国際学会）

４．発表年
2019年

１．発表者名
Kazuya Aizawa, Kenji Tei, Shinichi Honiden

２．発表標題
The 16th IEEE International Conference on Advanced and Trusted Computing (ATC 2019)

３．学会等名
Analysis space reduction with state merging for ensuring safety properties of self-adaptive systems（国際学会）

４．発表年
2019年

１．発表者名
Munan Li, Kenji Tei, Yoshiaki Fukazawa

２．発表標題
An efficient co-Attention Neural Network for Social Recommendation

３．学会等名
IEEE/WIC/ACM International Conference on Web Intelligence (WI'19)（国際学会）

４．発表年
2019年

１．発表者名
Ezequiel Castellano, Victor Braberman, Nicolas D'Ippolito, Sebastian Uchitel, Kenji Tei

２．発表標題
Minimising Makespan of Discrete Controllers: A Qualitative Approach

３．学会等名
IEEE 58th Conference on Decision and Control (CDC2019)（国際学会）

４．発表年
2019年

１．発表者名
Kenji Tei

２．発表標題
Big Data, Cloud and IoT Technologies for Smart Cities: The M-Sec project paradigm, objectives, current status and related future research topics

３．学会等名
the 2nd International Workshop on Big data, cloud, and IoT technologies for smart cities (IWBigDataCity2020)（国際学会）

４．発表年
2020年

１．発表者名
Keita Tsukamoto, Yuta Maezawa and Shinichi Honiden

２．発表標題
AutoPUT: An Automated Technique for Retrofitting Closed Unit Tests into Parameterized Unit Tests

３．学会等名
the 33rd ACM/SIGAPP Symposium on Applied Computing (SAC ' 18) (国際学会)

４．発表年
2018年

１．発表者名
Kazuya Aizawa, Kenji Tei and Shinichi Honiden

２．発表標題
Identifying safety properties guaranteed in changed environment at runtime

３．学会等名
the 3rd IEEE International Conference on Agents (IEEE ICA 2018) (国際学会)

４．発表年
2018年

１．発表者名
Kenji Tei

２．発表標題
Assured Graceful Degradation by Models@run.time

３．学会等名
THE 7TH ASIAN-PACIFIC WORKSHOP OF ADVANCED SOFTWARE ENGINEERING (AWASE2018) (国際学会)

４．発表年
2018年

１．発表者名
Moeka Tanabe, Kenji Tei

２．発表標題
Updating Environment Model at Runtime for Self-Adaptive Systems

３．学会等名
THE 7TH ASIAN-PACIFIC WORKSHOP OF ADVANCED SOFTWARE ENGINEERING (AWASE2018) (国際学会)

４．発表年
2018年

１．発表者名 Kazuya Aizawa, Kenji Tei
２．発表標題 Reducing the size of two-player game for identifying guaranteeable safety property at runtime
３．学会等名 THE 7TH ASIAN-PACIFIC WORKSHOP OF ADVANCED SOFTWARE ENGINEERING (AWASE2018)（国際学会）
４．発表年 2018年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	本位田　真一 (Honiden Shinichi) (70332153)	早稲田大学・理工学術院・教授（任期付） (32689)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関			
アルゼンチン	ブエノスアイレス大学			
中国	北京大学			
英国	Imperial College London	Open University		
米国	カーネギーメロン大学			
スウェーデン	Chalmers University of Technology			
イタリア	Politecnico di Milano			
フランス	Lip6	Lyon 1 University		