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 １２ 日現在

機関番号：１７１０２
研究種目：基盤研究(B)（一般）
研究期間：2020～2022
課題番号：２０Ｈ０４１６８

研究課題名（和文）ステートフル深層学習システムに対する総合的解析と修復技術の確立

研究課題名（英文）Comprehensive Analysis and Repairing Techniques for Stateful Deep Learning Systems

研究代表者
馬　雷（MA, LEI）

九州大学・システム情報科学研究院・准教授

研究者番号：７０８４２０６１

交付決定額（研究期間全体）：（直接経費）　　13,600,000円

研究成果の概要（和文）：本研究では、回帰型ニューラルネットワーク（RNN）に対する系統的な分析と修正技術の確立を目的としています。具体的には、以下の成果を得ました。1) RNNの内部動作を近似する抽象モデルの抽出と分析基盤を構築しました。2) RNNの自動分析、テスト、修正、解釈などの早期フレームワークを開発しました。3) 提案された技術を実際のRNNシステムに適用することで、提案手法の有効性を検証できました。
本研究は、RNNについて早期に解釈可能な分析技術の基盤を確立することができ、今後、RNNがより影響力を持つことが予想されるため、信頼性の高いRNNを構築するために、この研究成果が役立つことが期待されています。

研究成果の学術的意義や社会的意義
RNNは、自然言語処理などの時系列信号処理において、社会基盤に関わる重要な分野での成果がますます期待されている。しかし、RNNはフィードバックと内部状態を使用するため、ブラックボックスの特性により、信頼性保証などが非常に困難となることがある。特に、信頼性が重要な産業界や日常社会の様々な応用において、誤った動作をする悪い影響に直面する可能性がある。そこで、本研究では、RNNに対する系統的解釈ができる分析技術の確立により、RNNにおける解釈可能な分析などにおいて、品質・安全保証技術の基盤とその支援環境が整い、信頼性と品質の高いRNNシステムを構築することができるようになるでしょう。

研究成果の概要（英文）：The purpose of this research is to establish a systematic analysis technique for recurrent neural networks (RNN). Specifically, the following outcome were achieved: 1) we design and develop a platform that can extract abstract models that can approximate the internal behavior of RNNs, which enables the in-depth analysis of RNN behaviors. 2) We design and develop a framework for automatic analysis, testing, repair, and interpretation of RNNs. 3) We evaluate and demonstrate the effectiveness and usefulness of the proposed technique by applying it to real-world RNN systems.
In this research, we have established a foundation for early interpretable analysis techniques and developed tools for RNNs. As RNN-liked AI models are expected to become more influential with more real-world applications in the future, it is expected that this research would inspire future research along this direction and facilitate the building of more trustworthy RNNs for real-world applications.

研究分野：ソフトウェア工学、機械学習工学

キーワード：知能ソフトウェア分析　深層学習　回帰型ニューラルネットワーク分析　機械学習品質保証　ソフトウェア工学　機械学習工学

１．研究開始当初の背景

人工知能の中核をなす深層学習（deep learning, DL）は、画像処理、音声認識、自然言語処理、囲碁などの応用面で華々しい成功をおさめ、自動運転車やロボットなど、社会基盤に関わる重要な分野での成果がますます期待されている。ただし、DL システムにおいて障害が発生する場合、社会や自然に大きな災害をもたらす可能性があるため、その信頼性と安全性に対する要求がますます高くなっている [1]。信頼性と安全性の高い DL システムを系統的な方法で効率よく開発することは、情報化社会からの大きな要請であり、情報化社会の安定と発展にとって火急な課題である。

順伝播型ニューラルネットワーク（FNN）と回帰型ニューラルネットワーク（RNN）は、DL システムの最も広く使用されている 2 つのカテゴリである。FNN は状態無き（stateless）であり、出力が行われるまで入力が層ごとに順番に処理される。特に、FNN の代表的な種類の 1 つである畳み込みニューラルネットワーク（CNN）は、大規模な画像処理やオブジェクト検出などにうまく適用されている。一方、RNN はフィードバックと内部状態を使用し設計されており、音声入力、自然言語などの時系列信号を処理する際の利点を示しています。RNN は複雑な設計、状態ありおよびブラックボックスの特性により、その解析とテストは非常に困難である。当初、FNN に対するいくつかの解析とテスト技術が開発されたが、RNN に対する解析とテストはほとんど提案されていません。この状況より、特に信頼性と安全性が重要な RNN 産業応用が誤った動作をする危険に直面する可能性が高いと言える。RNN の潜在的な信頼性と安全性の問題を早期に発見するために、RNN に対して効果的な解析とテストが鍵となっている。

２．研究の目的

本研究では、回帰型ニューラルネットワーク(RNN)に対する系統的解析と修正技術の確立を目的としています。以下の問題を解決するために、具体的な取り組みを行います。

1. RNN の内部動作を近似する抽象モデルを抽出し、解析基盤を構築します。
2. RNN の自動解析とテスト生成フレームワークを構築します。
3. RNN の自動修正技術を開発します。
4. 本研究で提案した手法を、4 つの実用的な RNN システムに適用し、有効性を検証します。

本研究の進展により、RNN における系統的な解析技術やテスト技術とその支援環境が整い、信頼性と安全性の高い RNN システムを構築することが期待されます。

３．研究の方法

■研究スゲジュール: 本研究では、2020 年度からの 3 年間計画で、以下の研究項目 A、B、C、D に分けて実施する。

[研究項目 A]　RNN の内部動作を近似する抽象モデルの抽出と詳細化する。

[研究項目 B]　モデルに基づく解析とテストフレームワークの開発と構築 。

[研究項目 C]　RNN システムにおける自動修正技術の開発。

[研究項目 D]　実用的 RNN システムへの適用より提案手法の有効性を検証する。

各研究項目と実施計画について下のように小項目を設定の通りである。

表中の□は当該研究の予備調査時期、■は当該研究を主として実施する時期、◇は成果公表評価、システム試用評価の時期、○は当該研究のとりまとめ時期を、概ね 2 ヶ月ごとに示したものである。

項目	小項目	2020 年	2021 年	2022 年
A	A1	■■■■■■	■■■◇◇◇	◇◇○○○○
	A2	■■■■■■	■■■◇◇◇	◇◇○○○○
B	B1	□□■■■■	■■■◇◇◇	◇◇○○○○
	B2	□□□■■■	■■■■■■	■■◇◇○○
C	C1	□□□■■■	■■■■■■	■◇◇◇○○
	C2	□□□□■■	■■■■■■	■■◇◇○○
D		□□□□■■	■■■■■■	■■■◇○○

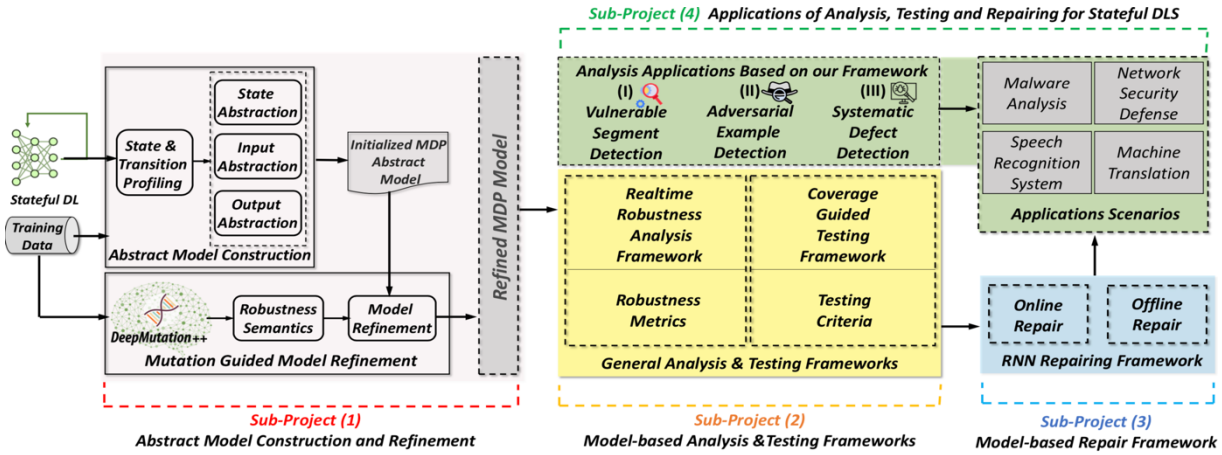


図 2: 本研究開発全体項目分配とワークフロー概要

研究項目 A：RNN の内部動作を近似する抽象モデルの抽出と詳細化

■小項目 A1:　RNN から抽象モデルの抽出と初期化

RNN の状態遷移動作を解析しやすいモデルで近似すると、ホワイトボックス解析と理解が可能になる。本項目では、状態、遷移、およびトレースの詳細な統計的動作を特徴付けるマルコフ決定プロセス（MDP）の強力な表現力により、RNN から MDP を活用して抽出し、近似する。図 2 に示すように、まずトレーニングデータを使用し、RNN のプロファイリングを行い、具体的な状態遷移を取得する。図 3(a)は、2 次元空間に投影されるプロファイルされた状態遷移の例を示している。s_i は具体的な状態を表し、有向エッジは状態遷移であり、入力と出力セグメント x_i, y_i はエッジの上に示され、各バケットは抽象状態を表し、バケット内のすべての具体的な状態は一つ抽象状態に見られる。実際には、状態の次元が高く、トレーニングデータを超えた RNN の潜在的な動作をより適切に近似できるモデルを実現するために、具体的な状態が要約される PCA（主成分解析）による状態、入力および出力の抽象化を実行する主要な PCA コンポーネントを使用し、抽象状態にする。状態の入出力の抽象化に基づいて、MDP 抽象モデルを初期化できる。図 3(b)は、図 3(a)から抽象化された対応する MDP を示している。

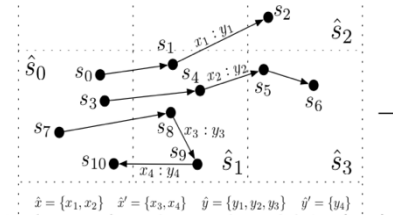
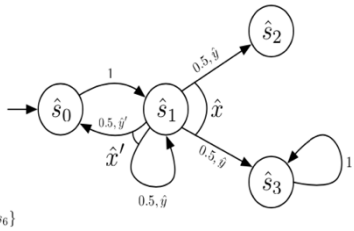


図 3: (a) 具体的な状態の遷移の例。$\hat{s}_i$ は抽象状態を表します。



(b) (a)からの抽象化な状態によって構築されたMDP

■小項目 A2：抽象 MDP モデルのミューテイションに基づく詳細化

初期化された MDP には、状態がどの程度頑健性があるかについての意味なしで、統計的な遷移情報のみが含まれている。状態と頑健性など性質のつながりをさらに確立するために、我々が開発した DeepMutation++[9,13]を活用し、頑健性のオフライン解析を

行う。次に、このような頑健性情報を MDP モデルに持たせて、MDP モデルがリアルタイムの頑健性解析に使用できる頑健性情報を保持できるようにする。複数の入力セグメントが抽象状態で一貫した頑健性に達しない場合、正確な頑健性になるまで状態分割によって状態の詳細化をさらに実行する。 DeepMutation++による頑健性解析は非常にコスト高いなので、リアルタイムには使用できない。一方、改良後の MDP モデルは、その頑健性情報を保持し、リアルタイムの頑健性解析を可能である。MDP モデリングは、RNN の解析の基盤を設定し開拓する。

研究項目 B：モデルに基づく解析とテストフレームワークの開発

■小項目 B1：リアルタイム頑健性解析フレームワークの設計と解析

時系列入力 $T = \{t_1,t_2,\cdots,t_n\}$が RNN に与えると、RNN が t_i で誤った判断をしないように、各セグメント t_i に対する頑健性をリアルタイムで解析することが重要である。 この目標に向けて、本項目では、最初に、項目(A)で得られた MDP モデルに基づいて頑健性メトリクスの集合を提案する。特に、メトリクスは、それぞれの抽象状態での頑健性情報とその次の状態と遷移を特徴づける。新しい入力が入るとき、そのセグメントが順番に処理されると、MDP の状態も遷移する。 不正確な挙動推定のために，将来の遷移確率と到達可能性と組み合わせて，現在の頑健性情報を活用した解析枠組みを設計する。モデルに基づきの解析は非常に効率的であるため、脆弱なセグメント検出のためのリアルタイム解析に適用できる。

■小項目 B2：カバレッジに基づくテストフレームワークの開発

本項目では、RNN のカバレッジに基づくテストフレームワークを開発する。最初に、RNN 専用の状態レベル、遷移レベルでのテスト基準を提案する。これは、主要な機能領域とコーナーケース領域の側面からテストの十分性を解析する。特に、主要な機能領域は主にトレーニングデータでカバーされている。これらの主要な機能領域を十分テストにカバー必要がある。また、より良いテストは、実際に潜在的な欠陥を検出するためのコーナー領域もカバーする必要がある。テスト基準に基づいて、RNN の体系的なテストに特化したカバレッジ誘導テストフレームワークをさらに開発する。提案されたテスト基準は、テスト生成のガイダンスとして使用される。汎用的に使用するために、時系列テスト生成用の一般的なミューテーション変換の一般的なセットを設計する。さらに、自然言語、マルウェア解析などの特定のアプリケーション向けに、ユーザーが新しいミューテーション変換（変容変換など）をさらに設計および拡張できるように、ミューテーション変換を拡張可能にする。

研究項目 C：RNN システムにおける自動修正技術の開発

■小項目 C1： RNN システムのオンライン修正技術の開発

項目(B)で開発される解析フレームワークを使用すると、入力の脆弱なセグメントとオンラインでの入力全体の両方をリアルタイムで解析できる。これらの検出された問題を修正するために、本項目では、入力 $T = \{t_1, t_2, \cdots, t_n\}$に対する RNN システムのリアルタイムオンライン修正技術を設計する。t_1 から t_n は順次入力のセグメントを表す。脆弱で不確実な問題は、主に現在のセグメントが RNN を脆弱な状態にトリガーするために発生する[11]。オンライン修正は、2 つの独立した部分で構成されており、つまり、(1)実行時にモデル側からの修正、入力セグメント t_i が脆弱な状態 s_i をトリガーすると、モデルを修正し、将来の入力セグメントに対するこの脆弱なケースの影響を軽減する。(2)実行時に入力側からの修正である、自然言語のような多くのドメイン時系列入力には、強力な統計的情報がある。したがって、現在の入力セグメントのコンテキストに、統計的推論手法使用し入力修復できる。修正はもっと効果があるため、モデル側と入力側のオンライン修正は一緒に使用する。

■小項目 C2： RNN システムの解析誘導オフライン修正技術の開発

オンライン修正とは異なり、オフライン修正では、再トレーニングや微調整など、より集中的な計算を実行する。項目(B)では、RNN の脆弱性および欠陥の問題を体系的に検出されたデータを体系的に修正するには、まず、訓練データとこれらの脆弱なデータを使用し、RNN のメモリセルとゲートのアクティベーション状況解析し、それらを強力、中、および弱いアクティベーションに分ける。問題を解決する主なロジックの原因となる強力な中程度のアクティブ化されたケースの重みを凍結し、弱いアクティブ化されたメモリとゲートの重みを調整することによって、項目(B)から検出されたこれらの問題を修正する。これは、新しい RNN バージョンの更新とリリース中に定期的にシステムを修正することに適している。

研究項目 D：実用システムへの適用より提案した手法の有効性の検証

本項目では、項目 (A、B、C) で提案した RNN のモデリング、解析、テスト、及び修正手法を四つの RNN を含む実用的なアプリケーションへ適用し、その有効性を検証する。特に、(1) マルウェアコード解析と(2)ネットワークセキュリティ防御は、現在の RNN システムが最先端のパフォーマンスを達成した代表的なセキュリティクリティカルなシステムである。モデリング技術により、一部のマルウェアおよびネットワークトラフィック攻撃が DL セキュリティディテクターをバイパスできる理由を解析および理解できる。また、これらのセキュリティクリティカルなアプリケーションに向けって、より優れた RNN ソリューションを構築できる。さらに、提案された技術を実世界の(3) 音声認識、および(4) 機械翻訳システムに適用して、信頼性と安全性の保証に関する現在の緊急の産業需要を解決する。特に、潜在的な脆弱性と頑健性の問題を明らかにするために、体系的な解析と修復を実行する。本研究で提案された技術では、潜在的な問題を解析、検出、修正してより多くの人々に利益をもたらすために、信頼性と安全性が重視される企業応用向けの RNN システムで大規模な評価を行う。

４．研究成果

本研究では、回帰型ニューラルネットワーク（RNN）に対する系統的な分析と修正技術の確立を目的としています。具体的には、以下の成果を得ました。1) RNN の内部動作を近似する抽象モデルの抽出と分析基盤を構築しました。2) RNN の自動分析、テスト、修正、解釈などの早期フレームワークを開発しました。3) 提案された技術を実際の RNN システムに適用することで、提案手法の有効性を検証できました。本研究は、RNN について早期に解釈可能な分析技術の基盤を確立することができ、今後、RNN がより影響力を持つことが予想されるため、信頼性の高い RNN を構築するために、この研究成果が役立つことが期待されています。

この研究では、3 年間にわたって、ステートフル深層学習ソフトウェアに対する解析、理解、及び修正技術などを研究し、一連の技術方法などを提出し、有効性を評価しました。それぞれの技術については、国際会議や論文投稿などで発表されました。当初の計画内容が完成でき、最後の研究成果が当初の計画よりも優れていました。

RNN は、自然言語処理などの時系列信号処理において、社会基盤に関わる重要な分野での成果がますます期待されている。しかし、RNN はフィードバックと内部状態を使用するため、ブラックボックスの特性により、信頼性保証などが非常に困難となることがある。特に、信頼性が重要な産業界や日常社会の様々な応用において、誤った動作をする悪い影響に直面する可能性がある。そこで、この課題に関する一連の研究成果により、信頼性の高い AI ソフトウェアの構築に向けた基礎や土台が早期に築かれました。今後信頼性・品質の高い RNN システムを構築することができるようになるでしょう。

５．主な発表論文等

〔雑誌論文〕　計10件（うち査読付論文　10件／うち国際共著　7件／うちオープンアクセス　0件）

１．著者名 Yu Bing、Qi Hua、Qing Guo、Juefei-Xu Felix、Xie Xiaofei、Ma Lei、Zhao Jianjun	４．巻 -
２．論文標題 DeepRepair: Style-Guided Repairing for Deep Neural Networks in the Real-World Operational Environment	５．発行年 2021年
３．雑誌名 IEEE Transactions on Reliability	６．最初と最後の頁 1～16
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TR.2021.3096332	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 Ding Yepeng、Sato Hiroyuki	４．巻 12
２．論文標題 Formalism-Driven Development: Concepts, Taxonomy, and Practice	５．発行年 2022年
３．雑誌名 Applied Sciences	６．最初と最後の頁 3415～3415
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/app12073415	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 Hua Qi, Zhijie Wang, Qing Guo, Jianlang Chen, Felix Juefei-Xu, Fuyuan Zhang, Lei Ma, Jianjun Zhao	４．巻 n.a.
２．論文標題 ArchRepair: Block-Level Architecture-Oriented Repairing for Deep Neural Networks	５．発行年 2023年
３．雑誌名 ACM Transactions on Software Engineering and Methodology (TOSEM 2023, CORE Rank A*, Impact Factor 3.685)	６．最初と最後の頁 n.a.
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 該当する

１．著者名 Yuheng Huang, Lei Ma, Yuanchun Li	４．巻 -
２．論文標題 PatchCensor: Patch Robustness Certification for Transformers via Exhaustive Testing	５．発行年 2023年
３．雑誌名 ACM Transactions on Software Engineering and Methodology (TOSEM 2023, CORE Rank A*, Impact Factor 3.685)	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3591870	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 Xiaofei Xie, Tianlin Li, Jian Wang, Lei Ma, Qing Guo, Felix Juefei-Xu, Yang Liu	4．巻 -
2．論文標題 NPC: Neuron Path Coverage via Characterizing Decision Logic of Deep Neural Networks.	5．発行年 2022年
3．雑誌名 ACM Transactions on Software Engineering and Methodology (TOSEM 2022, CORE Rank A*, impact factor 3.685)	6．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3490489	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 Yuta Ishimoto, Masanari Kondo, Naoyasu Ubayashi, Yasutaka Kamei	4．巻 155
2．論文標題 PAFL: Probabilistic Automaton-based Fault Localization for Recurrent Neural Networks	5．発行年 2023年
3．雑誌名 Information and Software Technology, Volume 155, Article number: 107117, 2023. (Impact factor 3.862)	6．最初と最後の頁 107-117
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.infsof.2022.107117	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 Shuncheng Tang, Zhenya Zhang, Yi Zhang, Jixiang Zhou, Yan Guo, Shuang Liu, Shengjian Guo, Yan-Fu Li, Lei Ma, Yinxing Xue, Yang Liu	4．巻 -
2．論文標題 A Survey on Automated Driving System Testing: Landscapes and Trends	5．発行年 2023年
3．雑誌名 ACM Transactions on Software Engineering and Methodology (TOSEM 2023, CORE Rank A*, impact factor 3.685)	6．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3579642	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 Zhenya Zhang, Deyun Lyu, Paolo Arcaini, Lei Ma, Ichiro Hasuo, Jianjun Zhao	4．巻 49
2．論文標題 FalsifAI: Falsification of AI-Enabled Hybrid Control Systems Guided by Time-Aware Coverage Criteria	5．発行年 2022年
3．雑誌名 IEEE Transactions on Software Engineering (TSE 2022, CORE Rank A*, Impact Factor 9.322)	6．最初と最後の頁 1842-1859
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TSE.2022.3194640	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 Xuhong Ren, Jianlang Chen, Felix Juefei-Xu, Wanli Xue, Qing Guo, Lei Ma, Jianjun Zhao, Shengyong Chen	4．巻 131
2．論文標題 DARTSRepair: Core-failure-set guided DARTS for network robustness to common corruptions	5．発行年 2022年
3．雑誌名 Pattern Recognition, Elsevier, 2022 (Impact Factor 8.544)	6．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.patcog.2022.108864	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 Xiongfei Wu, Jinqiu Yang, Lei Ma, Yinxing Xue, and Jianjun Zhao	4．巻 2022
2．論文標題 On the usage and development of deep learning compilers: an empirical study on TVM	5．発行年 2022年
3．雑誌名 Empirical Software Engineering volume 27, 172, Sep. 2022 (EMSE 2022, Impact Factor 3.762)	6．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s10664-022-10221	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

〔学会発表〕　計33件（うち招待講演　0件／うち国際学会　33件）

1．発表者名 Zhijie Wang, Yuheng Huang, Da Song, Lei Ma, Tianyi Zhang
2．発表標題 DeepSeer: Interactive RNN Explanation and Debugging via State Abstraction
3．学会等名 The ACM CHI Conference on Human Factors in Computing Systems (CHI 2023, CORE Rank A*)（国際学会）
4．発表年 2023年

1．発表者名 Da Song, Zhijie Wang, Yuheng Huang, Lei Ma, Tianyi Zhang
2．発表標題 DeepLens: Interactive Out-of-Distribution Data Detection in NLP Models
3．学会等名 The ACM CHI Conference on Human Factors in Computing Systems (CHI 2023, CORE Rank A*)（国際学会）
4．発表年 2023年

１．発表者名
Qiang Hu, Yuejun Guo, Xiaofei Xie, Maxime Cordy, Lei Ma, Mike Papadakis, Yves Le Traon

２．発表標題
Aries: Efficient Testing of Deep Neural Networks via Labeling-Free Accuracy Estimation

３．学会等名
The 45th International Conference on Software Engineering (ICSE 2023, CORE Rank A*) (国際学会)

４．発表年
2023年

１．発表者名
Qiang Hu, Yuejun Guo, Xiaofei Xie, Maxime Cordy, Lei Ma, Mike Papadakis, Yves Le Traon

２．発表標題
CodeS: Towards Code Model Generalization Under Distribution Shift

３．学会等名
The 45th International Conference on Software Engineering, NIER Track (ICSE 2023, CORE Rank A*) (国際学会)

４．発表年
2023年

１．発表者名
Xuan Xie, Fuyuan Zhang, Xinwen Hu, Lei Ma

２．発表標題
DeepGemini: Verifying Dependency Fairness for Deep Neural Network

３．学会等名
The Thirty-Seventh AAAI Conference on Artificial Intelligence (AAAI 2023, CORE Rank A*) (国際学会)

４．発表年
2023年

１．発表者名
Jiayang Song, Deyun Lyu, Zhenya Zhang, Zhijie Wang, Tianyi Zhang, Lei Ma

２．発表標題
When Cyber-Physical Systems Meet AI: A Benchmark, an Evaluation, and a Way Forward

３．学会等名
The 44th International Conference on Software Engineering, SEIP Track (ICSE 2022, CORE Rank A*) (国際学会)

４．発表年
2023年

１．発表者名
Yuheng Guo, Hiroyuki Sato

２．発表標題
Traceable In-Air Signature 3D Restoration Record Structure and In-Air Dominant Hand Biometric Based on Dynamic Time Warping Algorithm

３．学会等名
The 6th International Conference on Artificial Intelligence and Big Data (ICAIBD 2023) , 2023（国際学会）

４．発表年
2023年

１．発表者名
Yuta Ishimoto, Ken Matsui, Masanari Kondo, Naoyasu Ubayashi, Yasutaka Kamei

２．発表標題
An Initial Analysis of Repair and Side-effect Prediction for Neural Networks

３．学会等名
The 2nd International Conference on AI Engineering - Software Engineering for AI (CAIN 2023)（国際学会）

４．発表年
2023年

１．発表者名
Zhennan Wu, Yang Li, Yifei Huang, Lin Gu, Tatsuya Harada, Hiroyuki Sato

２．発表標題
3D Segmenter: 3D Transformer based Semantic Segmentation via 2D Panoramic Distillation

３．学会等名
The 11th Int'l Conference on Learning Representations (ICLR Core rank A*), 2023.（国際学会）

４．発表年
2023年

１．発表者名
Qing Guo, Ziyi Cheng, Felix Juefei-Xu, Lei Ma, Xiaofei Xie, Yang Liu, and Jianjun Zhao

２．発表標題
Learning to Adversarially Blur Visual Object Tracking

３．学会等名
International Conference on Computer Vision, Montreal, Canada, 2021 (ICCV 2021, CORE Rank A*)（国際学会）

４．発表年
2021年

１．発表者名
Xiaofei Xie, Wenbo Guo, Lei Ma, Wei Le, Jian Wang, Lingjun Zhou, Yang Liu, Xinyu Xing

２．発表標題
Automatic RNN Repair via Model-based Analysis

３．学会等名
The 38th International Conference on Machine Learning, 2021 (ICML 2021, CORE Rank A*) (国際学会)

４．発表年
2021年

１．発表者名
Zhenya Zhang, Deyun Lyu, Paolo Arcaini, Lei Ma, Ichiro Hasuo and Jianjun Zhao

２．発表標題
Effective Hybrid System Falsification Using Monte Carlo Tree Search Guided by QB-Robustness

３．学会等名
The 33rd International Conference on Computer-Aided Verification, 2021 (CAV 2021, CORE Rank A*) (国際学会)

４．発表年
2021年

１．発表者名
Yan Zheng, Yi Liu, Xiaofei Xie, Yepang Liu, Lei Ma, Jianye Hao, and Yang Liu

２．発表標題
Automatic Web Testing using Curiosity-Driven Reinforcement Learning

３．学会等名
The 43rd International Conference on Software Engineering (ICSE 2021, CORE Rank A*) (国際学会)

４．発表年
2021年

１．発表者名
Maryam V. Pour, Li Zhuo, Lei Ma and Hadi Hemmati

２．発表標題
A Search-Based Testing Framework for Deep Neural Networks of Source Code Embedding

３．学会等名
IEEE International Conference on Software Testing, Verification and Validation (ICST 2021, CORE Rank A) (国際学会)

４．発表年
2021年

１．発表者名
Xiyue Zhang, Xiaoning Du, Xiaofei Xie, Lei Ma, Yang Liu, Meng Sun

２．発表標題
Decision-Guided Weighted Automata Extraction from Recurrent Neural Networks

３．学会等名
Thirty-Fifth AAAI Conference on Artificial Intelligence (AAAI 2021, CORE Rank A*)（国際学会）

４．発表年
2021年

１．発表者名
Qing Guo, Jingyang Sun, Felix Juefei-Xu, Lei Ma, Xiaofei Xie, Wei Feng, Yang Liu, and Jianjun Zhao

２．発表標題
EfficientDeRain: Learning Pixel-wise Dilation Filtering for High-Efficiency Single-Image Deraining

３．学会等名
Thirty-Fifth AAAI Conference on Artificial Intelligence (AAAI 2021, CORE Rank A*)（国際学会）

４．発表年
2021年

１．発表者名
Shogo Tokui, Susumu Tokumoto, Akihito Yoshii, Fuyuki Ishikawa, Takao Nakagawa, Kazuki Munakata and Shinji Kikuchi

２．発表標題
NeuRecover: Regression-Controlled Repair of Deep Neural Networks with Training History

３．学会等名
The 29th IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER 2022), March 2022（国際学会）

４．発表年
2022年

１．発表者名
Matias Duran, Xiao-Yi Zhang, Paolo Arcaini, Fuyuki Ishikawa

２．発表標題
What to Blame? On the Granularity of Fault Localization for Deep Neural Networks

３．学会等名
The 32nd International Symposium on Software Reliability Engineering (ISSRE 2021 Practical Experience Reports), pp.264-275, October 2021（国際学会）

４．発表年
2021年

１．発表者名
Yuta Ojima, Shingo Horiuchi, Fuyuki Ishikawa

２．発表標題
Model-based Data-Complexity Estimator for Deep Learning Systems

３．学会等名
The 3rd IEEE International Conference on Artificial Intelligence Testing (IEEE AI Tests 2021), pp.1-8, August 2021（国際学会）

４．発表年
2021年

１．発表者名
Li Shaowen, Li Gen, SATO Hiroyuki

２．発表標題
Dynamic resource allocation among collocated applications via reinforcement learning

３．学会等名
Proc. IEEE 6th Int'l Conf. Cloud Computing and Big Data Analytics, A0014, Chengdu, April, 2021（国際学会）

４．発表年
2021年

１．発表者名
G. Li, L. Zhang and H. Sato

２．発表標題
In-air Signature Authentication Using Smartwatch Motion Sensors

３．学会等名
2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC), 2021（国際学会）

４．発表年
2021年

１．発表者名
Yepeng Ding, Hiroyuki Sato

２．発表標題
Formalism-Driven Development of Decentralized Systems

３．学会等名
Proc. 26th Int'l Conf. Engineering of Complex Computer Systems, March, 2022（国際学会）

４．発表年
2022年

１．発表者名
Xiyue Zhang, Xiaoning Du, Xiaofei Xie, Lei Ma, Yang Liu, Meng Sun

２．発表標題
Decision-Guided Weighted Automata Extraction from Recurrent Neural Networks

３．学会等名
Thirty-Fifth AAAI Conference on Artificial Intelligence (AAAI 2021, CORE Rank A*)（国際学会）

４．発表年
2021年

１．発表者名
Qing Guo, Jingyang Sun, Felix Juefei-Xu, Lei Ma, Xiaofei Xie, Wei Feng, Yang Liu, and Jianjun Zhao

２．発表標題
EfficientDeRain: Learning Pixel-wise Dilation Filtering for High-Efficiency Single-Image Deraining

３．学会等名
Thirty-Fifth AAAI Conference on Artificial Intelligence (AAAI 2021, CORE Rank A*)（国際学会）

４．発表年
2021年

１．発表者名
Qing Gu, Felix Juefei-Xu, Xiaofei Xie, Lei Ma, Jian Wang, Bing Yu, Wei Feng, Yang Liu

２．発表標題
Watch out! Motion is Blurring the Vision of Your Deep Neural Networks

３．学会等名
Thirty-fourth Conference on Neural Information Processing Systems (NeurIPS 2020, CORE Rank A*)（国際学会）

４．発表年
2020年

１．発表者名
Zi Peng, Jinqiu Yang, Tse-Hsun Chen, Lei Ma

２．発表標題
A First Look at the Integration of Machine Learning Models in Complex Autonomous Driving Systems: a Case Study on Apollo

３．学会等名
The 28th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE 2020, CORE Rank A*)（国際学会）

４．発表年
2020年

１．発表者名
Xiaoning Du, Yi Li, Xiaofei Xie, Lei Ma, Yang Liu, Jianjun Zhao

２．発表標題
MARBLE: Model-Based Robustness Analysis of Stateful Deep Learning Systems

３．学会等名
The 35th IEEE/ACM International Conference on Automated Software Engineering. (ASE 2020, CORE Rank A) (国際学会)

４．発表年
2020年

１．発表者名
David Berend, Xiaofei Xie, Lei Ma, Lingjun Zhou, Yang Liu, Chi Xu, Jianjun Zhao

２．発表標題
Cats Are Not Fish: Deep Learning Testing Calls for Out-Of-Distribution Awareness

３．学会等名
The 35th IEEE/ACM International Conference on Automated Software Engineering. (ASE 2020, CORE Rank A) (国際学会)

４．発表年
2020年

１．発表者名
Xuhong Ren, Bing Yu, Hua Qi, Felix Juefei-Xu, Zhuo Li, Wanli Xue, Lei Ma and Jianjun Zhao

２．発表標題
Few-Shot Guided Mix for DNN Repairing

３．学会等名
The 36th IEEE International Conference on Software Maintenance and Evolution, NIER Track (CORE Rank A) (国際学会)

４．発表年
2020年

１．発表者名
Hua Qi, Qing Guo, Felix Juefei-Xu, Xiaofei Xie, Lei Ma, Wei Feng, Yang Liu, Jianjun Zhao

２．発表標題
DeepRhythm: Exposing DeepFakes with Attentional Visual Heartbeat Rhythms

３．学会等名
Proceedings of the 28th ACM International Conference on Multimedia (ACM MM, CORE Rank A*) (国際学会)

４．発表年
2020年

１．発表者名
Run Wang,Felix Juefei-Xu, Yihao Huang, Qing Guo, Xiaofei Xie, Lei Ma, Yang Liu

２．発表標題
DeepSonar: Towards Effective and Robust Detection of AI-Synthesized Fake Voices

３．学会等名
Proceedings of the 28th ACM International Conference on Multimedia (ACM MM, CORE Rank A*)（国際学会）

４．発表年
2020年

１．発表者名
Run Wang,Felix Juefei-Xu, Yihao Huang, Qing Guo, Xiaofei Xie, Lei Ma, Yang Liu

２．発表標題
Amora: Black-box Adversarial Morphing Attack

３．学会等名
Proceedings of the 28th ACM International Conference on Multimedia (ACM MM, CORE Rank A*)（国際学会）

４．発表年
2020年

１．発表者名
Lingfeng Zhang, Hiroyuki Sato

２．発表標題
Automated Test Input Generation for Convolutional Neural Networks by Implementing Multi-objective Evolutionary Algorithms

３．学会等名
2020 Eighth International Symposium on Computing and Networking Workshops (CANDARW)（国際学会）

４．発表年
2020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	佐藤　周行 (Sato Hiroyuki) (20225999)	東京大学・情報基盤センター・准教授 (12601)	

6．研究組織（つづき）

	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	趙　建軍 (Zhao Jianjun) (20299580)	九州大学・システム情報科学研究院・教授 (17102)	
研究分担者	石川　冬樹 (Ishikawa Fuyuki) (50455193)	国立情報学研究所・アーキテクチャ科学研究系・准教授 (62615)	
研究分担者	鵜林　尚靖 (Ubayashi Naoyasu) (80372762)	九州大学・システム情報科学研究院・教授 (17102)	

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			
シンガポール	Nanyang Technological University	Singapore Management University		
カナダ	University of Calgary	Concordia University	University of Alberta	
中国	Peking University	Tsinghua University	Tianjin University	
米国	Purdue University	Iowa State University		
ルクセンブルク	University of Luxembourg			