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　 ６ 日現在

機関番号：３２６６５
研究種目：基盤研究(C)（一般）
研究期間：2020～2022
課題番号：２０Ｋ１１７５３

研究課題名（和文）DevOpsアシュアランスケースによる機械学習システムのディペンダビリティ保証

研究課題名（英文）Dependability Assurance of Machine Learning Systems by DevOps Assurance Cases

研究代表者
松野　裕（MATSUNO, Yutaka）

日本大学・理工学部・准教授

研究者番号：７０５３４２２０

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：ディープラーニング、機械学習技術の実用化が本格化しつつある中、機械学習システムのディペンダビリティ保証が重要な課題になっている。本研究ではその解決策として、システム保証の手法であるアシュアランスケースを発展させ、機械学習システムの開発と運用が一体となったDevOpsアシュアランスケース手法とツールを提案する。本研究では、研究室とリモートでコミュニケーションすることができるミニロボットの開発において、提案手法およびツールを試行した。その結果、実用化に関する課題を抽出することができた。それらの結果を自動運転技術のベンチャー企業と議論することにより、その会社との共同研究を開始することができた。

研究成果の学術的意義や社会的意義
研究成果の学術的意義は、開発と運用を通じた、機械学習システムのディペンダビリティ保証手法とツールを提案し、試行したことである。機械学習システムなどのシステムの保証、分析手法は国際規格などでその必要性が言われているが、具体的な手法やツールをどのように構築すればよいか明らかではなかった。本研究によりその具体化の１例を示したことは学術的意義があると考える。研究成果の社会的意義は、本研究課題の成果により、日本でも注目されている自動運転のスタートアップ企業との共同研究を開始することができたことである。このことにより、産学の共同研究を実施することができ、大学の研究による社会貢献を目指すことができる。

研究成果の概要（英文）：As the practical application of deep learning and machine learning technology is becoming more established, ensuring the dependability of machine learning systems is becoming a significant issue. In this study, we propose a method and tools for DevOps assurance cases, an enhancement of system assurance methods, as a solution to this issue. This allows for the development and operation of machine learning systems to become integrated. In this study, we tested the proposed method and tools in the development of a mini robot capable of communicating remotely with the lab. As a result, we were able to identify challenges related to practical application. By discussing these results with a startup company in the field of autonomous driving technology, we were able to initiate joint research with the company.

研究分野：ソフトウェア工学

キーワード：アシュアランスケース　機械学習システム　システム保証　ウエブベースツール

１．研究開始当初の背景

ディープラーニング、機械学習技術は飛躍的な発展をしており、歩行者検出機能などへの適用による自動運転車の実現が視野に入ってきている。しかし機械学習システムのディペンダビリティ（安全性やセキュリティを総合した概念）を保証する手法は確立されていない。ディープラーニングで入力に対する出力が間違った場合に、原因となったネットワーク部分は特定しづらく、できたとしてもその値の持つ意味を説明することは困難である。そのため従来のシステムのように出力の正しさの、演繹的な説明をすることができないという課題があった。

２．研究の目的

この背景において、本研究課題は「機械学習システムのディペンダビリティ保証は可能か?」という学術的「問い」に答えることを目的とした。

機械学習システムのディペンダビリティ保証には原理的な困難さがある。現実解は、システム開発(Development)と運用(Operations)が一体となって連携し、合意していくマネジメントを確立することだと考える。本研究はこのマネジメント支援のための、開発時のテストや仕様書などと運用時のモニタリングが一体となった DevOps アシュアランスケース手法とツールの開発評価を目的とした。

３．研究の方法

解決策として、アシュアランスケース(Assurance Cases)による機械学習システムのディペンダビリティ保証議論構築が注目を集めている。アシュアランスケースは システムの安全性などの主張を木構造により分解し議論構造を構成し、最終的にテスト結果などの証拠により主張が成り立つことを示す手法である。 例として、GSN と呼ばれる代表的なアシュアランスケース表記法による簡単な例を示す(図 1)。システムの安全性について、ハザード A と B がリスク分析より得られたとき、それぞれに対して対処できていることを、テスト結果を証拠として用いている。従来の既存研究では、自動運転における歩行者検出機能をディープラーニングで実装するケースを例に取り、想定する歩行者のクラスをすべて列挙することなどを前提とするアシュアランスケースを提案している。しかしこの前提の達成はほぼ不可能である。このように既存研究では、実現が困難な前提や議論構造を定義するのみで、実現手段を明示していない。

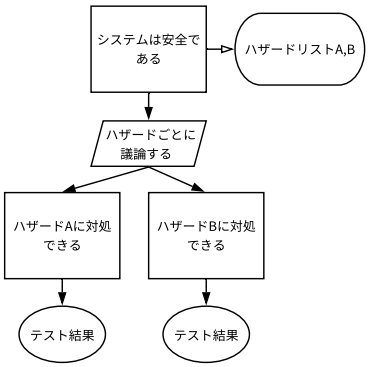

図 1 GSN の例

本研究ではアシュアランスケースのゴールにモニタリング値による動的な証拠をリンクし、モニタリング値が異常値になった場合、開発時の情報をもとにしたアシュアランスケースに遷移する仕組みを開発した。顔認識システムを例に取り説明する(図 2)。

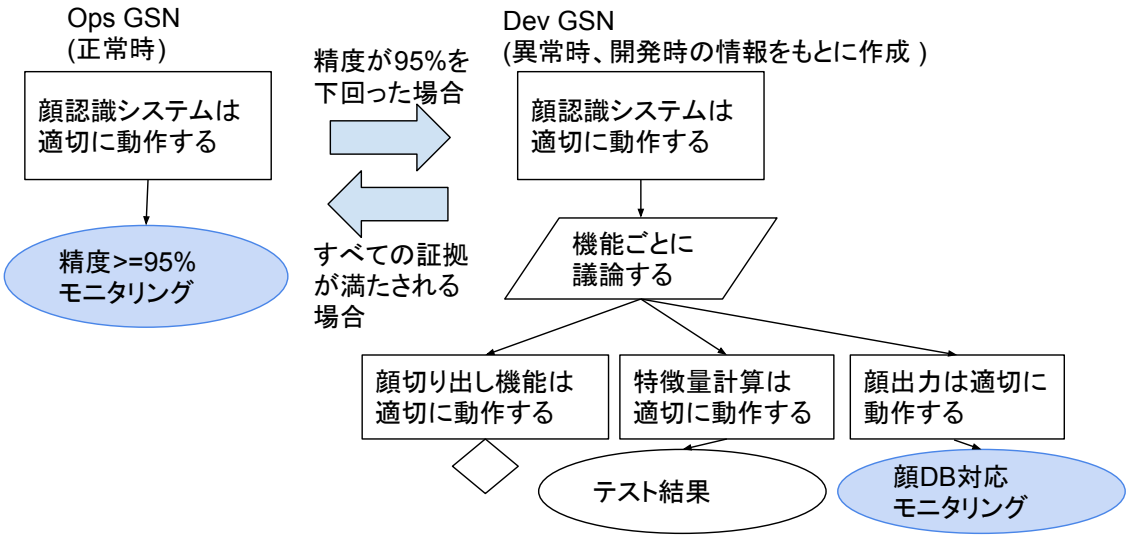

図 2 顔認識システムの DevOps アシュアランスケース

トップゴールは顔認識システムの機能性である。正常時は精度が 95%以上であるモニタリングデータを証拠とする Ops GSN(図 2 左)になる。これが成り立たなくなると、右の開発時の情報をもとにした Dev GSN に遷移する(図 2 右)。顔認識システムは顔切り出し、特徴量計算、顔 DB より特徴量に該当する顔の出力の 3 つの機能よりなる。この例では、顔切り出し機能に証拠がついて

おらず、問題があることがわかる。障害対応(再学習など)が成功すれば、顔切り出し機能のモニタリングによる証拠がリンクされる(顔切り出し機能レベルの Dev GSN, Ops GSN 間の遷移)。すべてのサブゴールに証拠が再びリンクされ、図 2 左の Ops GSN に遷移する。開発時の想定と異なり、Dev GSN のすべての証拠が満たされても、精度が 95%を超えない場合もありうる(逆もありうる)。その場合でも Dev GSN は障害対応に有用であり、システム改修に対応して Dev GSN を更新すればよい。

本研究では、上記の DevOps アシュアランスケース手法およびツールを以下の手順で実現を目指した。

(1) 初年度に DevOps アシュアランスケースツールを開発する。松野研究室で開発した、モニタリング機構を持つアシュアランスケースツールを拡張し、Dev GSN と Ops GSN 間を遷移する機能を実装する。同時に既存の顔認証システムの精度保証方法を調査し、Dev GSN, Ops GSN を試作する。関助手が開発経験のある画像認識システムを応用し、顔認証入退室システムを開発する。開発が困難な部分は開発費用を注力する。

(2) 2 年目は所属大学で実際に運用するシステム(研究室、実験室入退室管理)へ開発したツールを適用する。障害発生時に Dev GSN, Ops GSN を用いて対応し、その有効性を評価する。うまくいかない場合は、顔認証システムの専門家に聞き、ユースケースを作成することにより有効性を示す。ツールの改善は継続する。

(3) 最終年度は自動運転システムのシミュレータ(Autoware など)を用い、歩行者検出機能を対象としたデモを作成する。シミュレータは高度であり、うまくいかない可能性があるが、その場合は文献調査によりユースケースを作成する。それらを元に、自動車関連団体 JASPAR でプレゼンを行い、本研究課題の成果の JASPAR 参加企業への導入、自動車安全性国際規格案 ISO/PAS21448 への、JASPAR 提案の一つとして取り入れられることを目指す。

４．研究成果

初年度において、DevOps アシュアランスケースツールの基本機能を実装することができた。しかし 2 年目以降、COVID-19 の影響により、実験室入退室管理システムは実現できず、研究室入退室管理システムは実装できたが、利用することができなかった。そこで実験対象となるシステムをオンラインコミュニケーション小型ロボット(図 3)に変更し、2 年目に企業とのディスカッションを通じて要件定義を行い、DevOps アシュアランスケースのためのプロセスを抽象的に定義した。3 年目にオンラインコミュニケーション小型ロボットは完成し、DevOps アシュアランスケースの記述試行を行ったが、利用までには至らなかった。しかしこの過程で得られた知見から、自動運転技術を開発している企業との共同研究を現在、実施している。共同研究の内容は以下である。自動運転の社会実装が進みつつあるが、自動車会社、自動運転技術開発会社、一般利用者、あるいは社会全体における自動運転の安全性やディペンダビリティの合意形成は大きな課題である。自動運転企業との共同研究では、本研究課題の成果を用い、多様なステークホルダー間での安全性やディペンダビリティの合意形成をするための手法およびツールを研究開発している。現在、自動運転企業の実際のユースケースにおいて、本研究課題で開発した基礎的な手法やプロトタイプツールの適用実験を行っている。今後、企業との共同研究をさらに進め、本研究課題の社会実装をより進めていきたい。

図 3 オンラインコミュニケーション小型ロボットシステム(現在の開発成果物)

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 Matsuno Yutaka、Yamagata Yoriyuki、Nishihara Hideaki、Hosokawa Yuichiro	４．巻 1
２．論文標題 Assurance Carrying Code for Software Supply Chain	５．発行年 2021年
３．雑誌名 2021 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)	６．最初と最後の頁 276-277
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ISSREW53611.2021.00077	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3件（うち招待講演　1件／うち国際学会　0件）

１．発表者名 高井利憲
２．発表標題 社会生活に密接に関わるSystem of Systems開発のためのDigital Twin+ACアプローチ
３．学会等名 DSW2021（招待講演）
４．発表年 2021年

１．発表者名 小池湧大、大熊拓海、高井利憲、岡田学、松野裕
２．発表標題 DevOpsアシュアランスケースによる自動運転システムの安全性保証
３．学会等名 電子情報通信学会KBSE研究会
４．発表年 2021年

１．発表者名 大熊拓海、小池湧大、松野裕
２．発表標題 DevOpsアシュアランスケースによるディペンダビリティ保証
３．学会等名 日本ソフトウェア科学会DSW研究会
４．発表年 2021年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

D-Case Communicator Githubレポジトリ(オープンソース) https://github.com/cstmatsulab/dcase_com DevOpsアシュアランスケースツールウエブページ http://www.matsulab.org/dcase/login.html

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	関　弘翔 (SEKI Hiroto) (00755043)	日本大学・理工学部・助教 (32665)	
研究分担者	高井　利憲 (TAKAI Toshinori) (10425738)	奈良先端科学技術大学院大学・先端科学技術研究科・客員准教授 (14603)	

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