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　４ 年　 ６ 月　 ３ 日現在

機関番号：１２６０１
研究種目：挑戦的研究（萌芽）
研究期間：2020～2021
課題番号：２０Ｋ２１７８８

研究課題名（和文）深層学習と仮想化技術の融合によるバンキングマルウェア対策

研究課題名（英文）Combining deep learning and virtualization technologies to defend against banking malware

研究代表者
品川　高廣（Shinagawa, Takahiro）

東京大学・情報基盤センター・准教授

研究者番号：４０３６１７４５

交付決定額（研究期間全体）：（直接経費）　　5,000,000円

研究成果の概要（和文）：本研究では、深層学習と仮想化技術を融合したバンキングマルウェア対策に関する研究をおこなった。バンキングマルウェアには亜種が多いという特徴を活用して、深層学習により高い精度で亜種の分類をおこなうことができる手法を研究した。また、仮想化技術との融合を目指して、仮想化技術で取得可能なバイナリレベルでのデータからマルウェア画像を生成して検知可能な技術に関する研究をおこなった。秘匿化対策のためのラベルの工夫なども取り入れた上で、深層学習の様々なモデルとパラメータの組み合わせを探索した結果、最新のモデルで転移学習の程度を低めに抑えることで高い分類精度が得られることがわかった。

研究成果の学術的意義や社会的意義
近年は非常に多数のマルウェアが登場しており、実際に様々なセキュリティ上の被害が継続的に発生し続けているのが現状である。本研究では、最新の深層学習技術と仮想化技術を融合することで、高い精度でマルウェアを検知することができて、かつマルウェアが回避できないシステムの構築に向けた基礎研究を実施した。この技術を発展させることにより、将来的にマルウェアによる被害を大幅に低減できるシステムが実用化されることが見込まれる。

研究成果の概要（英文）：In this study, we conducted research on countermeasures against banking malware by integrating deep learning and virtualization technologies. We studied a method that can classify variants with high accuracy by deep learning, taking advantage of the fact that banking malware has many variants. We also studied a technique that can generate and detect malware images from binary-level data that can be obtained by virtualization technology, with the aim of integrating deep learning technique with virtualization technology. We explored various models and parameter combinations for deep learning, including the use of labels for confidentiality measures, and found that the latest models provide high classification accuracy with a low degree of transition learning.

研究分野：オペレーティングシステム

キーワード：仮想化技術　セキュリティ　深層学習

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

マルウェア検出に深層学習を用いる試みは近年多数おこなわれているが、マルウェアをバイナリレベルで扱う手法では、良い学習データを生成することが難しい点が課題となっている。一方、仮想化技術を用いると、マルウェアからは迂回できない強力な保護を実現できる一方、OSレベルの情報が失われて検出率の向上が難しかったり、仮想化技術の導入が面倒で実際の利用者の環境への導入には敷居が高かったりする等の問題があった。

２．研究の目的

本研究の目的は、近年著しく進歩した深層学習の技術と応募者オリジナルの技術である準パススルー型軽量仮想化技術を新たな視点で融合させることで、バンキングマルウェアという実際の金銭的被害が大きいセキュリティ問題に特化した強力な対策手法を実現することである。本研究では、バンキングマルウェアに特化して検出率の高い学習データを生成するとともに、仮想化技術によるクライアント側での前処理とクラウドでの後処理とを組み合わせることで、高効率・高検出率で強力なバンキングマルウェア対策を低コストで導入可能にするという挑戦的試みであり、実際に起こっている金銭被害を迅速かつ強力に防止できるという意義がある。

３．研究の方法

本研究では 2 つの手法を並行して研究し、当初目的の実現に目処をつけることを目指す。まず、(1) 深層学習によりバンキングマルウェアを高精度に検出する手法を研究する。これまでの予備研究で得られたバンキングマルウェア固有の特徴を活用して、深層学習に適したデータ変換をおこなって、高効率・高検出率のバンキングマルウェア対策を行う。並行して、(2) 準パススルー型軽量仮想化ソフトウェアを用いてバンキングマルウェアのバイナリデータを取得する方法の工夫や、深層学習のための前処理の仕方の工夫などをおこなって、上記の深層学習によるバンキングマルウェア検知手法と親和性の高い軽量仮想化ソフトウェアの構築を目指す。

４．研究成果

本研究では、深層学習と仮想化技術を融合したバンキングマルウェア対策に関する研究をおこなった。バンキングマルウェアには亜種が多いという特徴を活用して、深層学習により高い精度で亜種の分類をおこなうことができる手法を研究した。また、仮想化技術との融合を目指して、仮想化技術で取得可能なバイナリレベルでのデータからマルウェア画像を生成して検知可能な技術に関する研究をおこなった。秘匿化対策のためのラベルの工夫なども取り入れた上で、深層学習の様々なモデルとパラメータの組み合わせを探索した結果、最新のモデルで転移学習の程度を低めに抑えることで高い分類精度が得られることがわかった。

具体的には、24 種類の ImageNet 事前学習済み CNN モデルと 5 段階の微調整パラメータを用いた 120 通りの組み合わせを用い、深層学習モデルや転移学習の程度が画像ベースのマルウェア分類精度に与える影響について網羅的に調査した。その結果、事前学習したパラメータを全く、あるいは 1/4 だけ凍結して微調整した EfficientNetB4 モデルが、Malimg（98.96%）および Drebin（93.65%）のデータセットで最も高い分類精度を持つことが分かった（図１及び図２）。これは、クロスバリデーションで検証した結果では、これまでで最も高い分類精度である。

また、最近の実在するマルウェアについては、VirusTotal May 2020 Windows データセットにおいて、1/2 の凍結パラメータで微調整した EffieicnetB5 モデルが 98.78%の最高分類精度を達成し、VirusTotal May 2020 Android データセットにおいて、凍結パラメータなしの EfficientNetB3～B5 モデルが 100%の精度を達成したことが分かった。

実験結果から、マルウェア亜種の分類精度は、転移学習の度合いが比較的低い最新の深層学習モデルを使用した場合に最も高くなる傾向があることが分かった。最適なモデルを探索するための現実的なアプローチとしては、最新のモデルをファインチューニングしながら、凍結パラメータを半分から徐々に減らしていくことが考えられる。

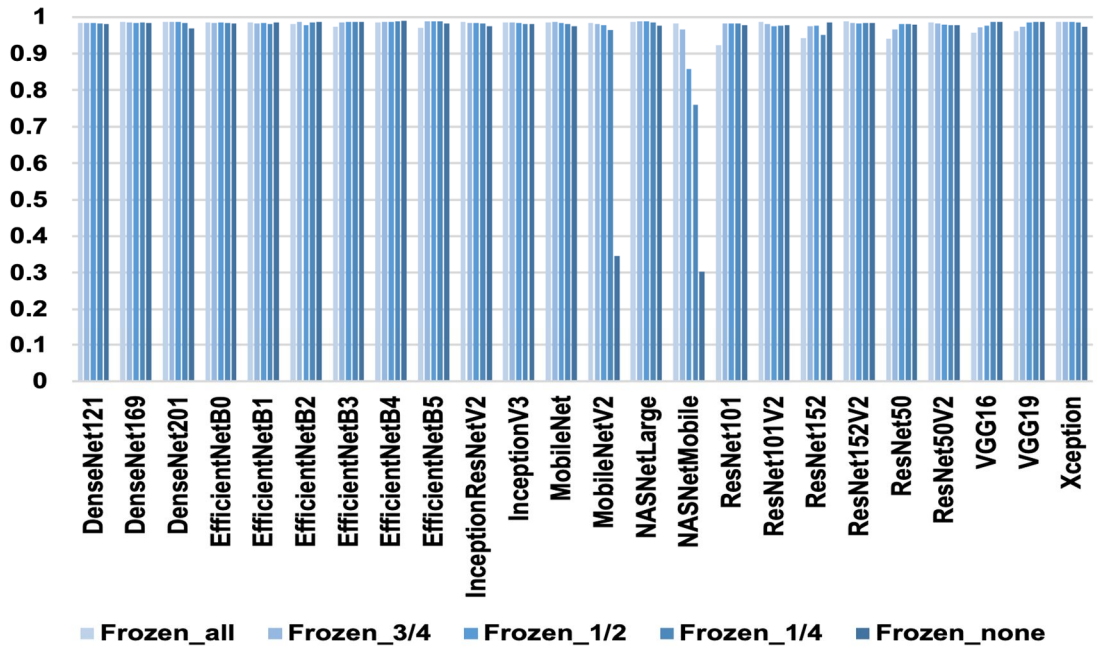

図１　Malimg の分類結果

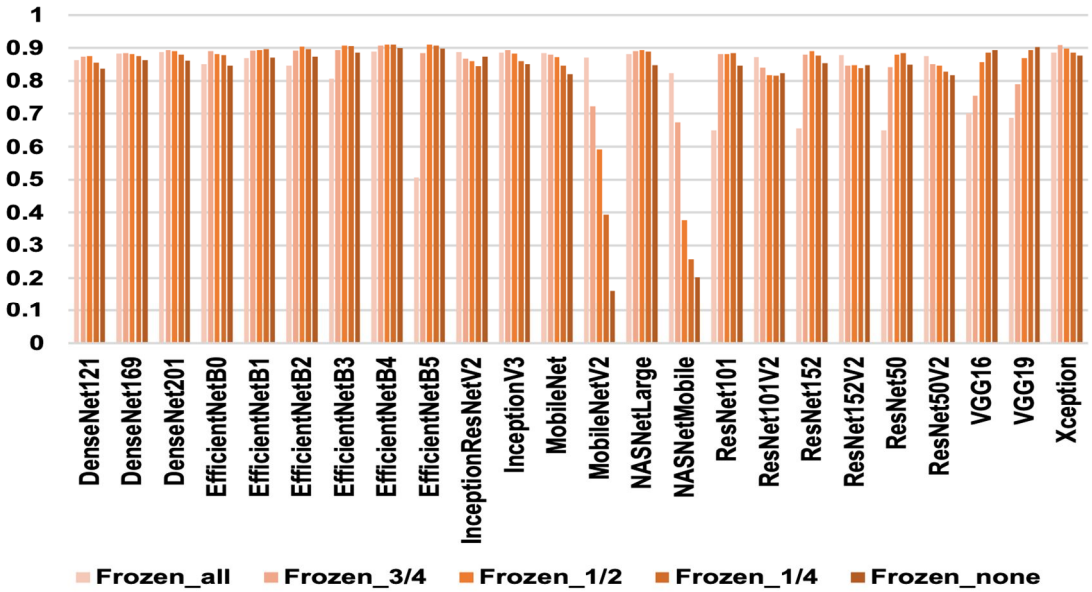

図２　Drebin の分類結果

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 Rikima Mitsuhashi, Takahiro Shinagawa	４．巻 -
２．論文標題 Exploring Optimal Deep Learning Models for Image-based Malware Variant Classification	５．発行年 2022年
３．雑誌名 In Proceedings of the IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC 2022)	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） 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 －

〔学会発表〕　計1件（うち招待講演　0件／うち国際学会　1件）

１．発表者名 Rikima Mitsuhashi, Takahiro Shinagawa
２．発表標題 Deriving Optimal Deep Learning Models for Image-based Malware Classification
３．学会等名 37th ACM/SIGAPP Symposium On Applied Computing (ACM SAC 2022)（国際学会）
４．発表年 2022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

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