

CNNを用いたネットワークトラフィック異常検知と 異常トラフィックからの脅威情報抽出

池端 悠人^{1,a)} 木村 航佑¹ 松尾 美咲¹ 加藤 雅彦¹

概要: 近年、サイバー攻撃による被害が頻発しており、政府機関や民間企業などでは、攻撃を念頭に置いたセキュリティ対策が急務となっている。そのような脅威を防止するための効果的なセキュリティ対策を行うためには、実際にどのような脅威が迫っているのかを、前もって正確に把握しておくことが必要である。本研究では、悪性および良性のネットワークトラフィック画像データを学習させたCNNを用いて、ネットワークトラフィック画像データをもとに不審なネットワークトラフィックを検出し、サイバー攻撃に関する脅威情報を抽出することによって、脅威への対策に役立てるための手法を提案する。取得した悪性または良性のネットワークトラフィックを含むPCAPを利用してCNNに学習させ、実際に不審なネットワークトラフィックが検出されることを検証し、不審なネットワークトラフィックから、攻撃に関するものと思われる脅威情報が抽出されることを確認した。

キーワード: トラフィック分類, PCAP, CNN, アノマリ検知, OSINT

Anomaly Detection of Network Traffic Using CNN and Threat Information Extraction from Anomaly Traffic

YUTO IKEBATA^{1,a)} KOSUKE KIMURA¹ MISAKI MATSUO¹ MASAHIKO KATO¹

Abstract: Recently, damages due to cyber attacks have occurred frequently, and immediate and effective measures for cybersecurity are urgently needed by government agencies and companies. For effective measures to prevent such threats, it is necessary to accurately grasp in advance what kind of threats are actually approaching. This research proposes the method which enables to detect suspicious network traffic by CNN trained with malicious and unmalicious network traffic image data and to provide useful threat information about cyber attacks which are coming. Actually the suspicious network traffic was detected by CNN trained with gathered malicious and unmalicious network traffic, and more, threat information which was likely to be related to attacks was extracted from suspicious network traffic.

Keywords: Traffic Classification, PCAP, CNN, Anomaly Detection, OSINT

1. はじめに

近年、サイバー攻撃による被害が頻発しており、政府機関や民間企業などでは、攻撃を念頭に置いたセキュリティ対策が急務となっている。そのような脅威を防止するための効果的なセキュリティ対策を行うためには、実際にどのよ

うな脅威が迫っているのかを、前もって正確に把握しておくことが必要である。IDS（侵入検知システム）やIPS（侵入防止システム）は、ルールやアノマリに従って攻撃を検知することができるが、具体的にどのような脅威が存在するのか、詳細に知ることは困難である。また、OSINT^{*1} [1] を使ってサイバー攻撃に関する詳細な情報を得ることがで

¹ 長崎県立大学
University of Nagasaki
^{a)} bs216005@sun.ac.jp

^{*1} 公開情報から生成されるインテリジェンスで、特定のインテリジェンス要件への対処を目的として収集され、利用され、適時に、適切な対象者に提供される。

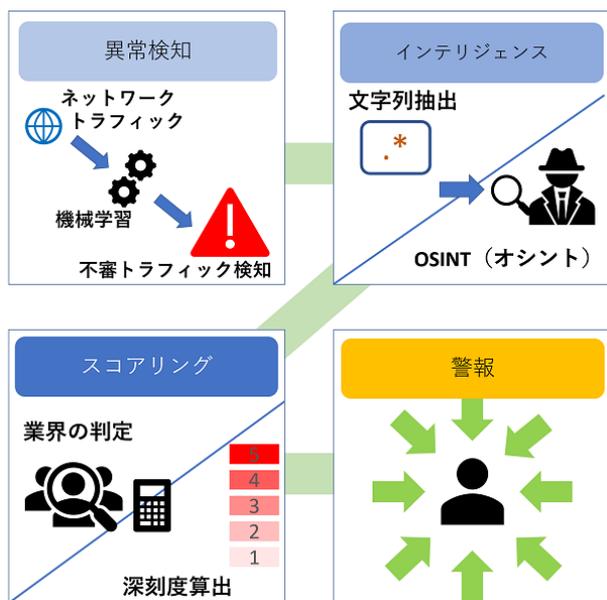


図 1 提案システムの全体像
Fig. 1 Proposed Framework

きるが、OSINT には高度な技術が必要であるため、気軽に導入するのは難しい。

そこで、本研究グループでは、図 1 に示すシステムを提案する。このシステムにより、ネットワークトラフィックをもとに必要な脅威情報を集約することを可能にし、他組織で発生している攻撃の情報や、すでに発生している攻撃についての情報を被害発生前に提供することによって、利用者は自動的に、自ネットワークに特化した、脅威に関する情報を得ることができる。このシステムは、ネットワーク通信の中から不審なネットワークトラフィックを検知する”Anomaly Detection (異常検知)”，検知した不審なネットワークトラフィックをもとにサイバー攻撃に関する脅威情報を抽出する”Intelligence (インテリジェンス)”，取得した脅威情報をもとに対応の必要性を表す重要度を算出する”Scoring (スコアリング)”，脅威情報を集約し必要な情報のみを利用者に提供する”Warning (警報)”の 4 つのフェーズから構成される。

2. 関連研究

ネットワークトラフィック分類に関する様々な手法が提案されている。

Nguyen らは、2008 年に、機械学習を用いたネットワークトラフィック分類の手法に関するサーベイ論文を発表している [2]。この調査によると、2008 年以前は、Moore ら、Park ら、Nguyen ら、Haffner ら、Williams ら、Erman ら、Bonfiglio らの手法で採用されていたナイーブベイズや、Barnaille ら、Erman らの手法で採用されていた K-means などによる手法が主であった。Zhou らは、順伝播型ニューラルネットワークを用いたネットワークトラフィッ

ク分類の手法 [3] を、Mathewos らは、パラレルニューラルネットワークを用いたネットワークトラフィック分類の手法 [4] を、Bekerman らは、機械学習を用いたネットワークトラフィック分類によるマルウェア検知の手法 [5] を提案している。Ang らは、多層パーセプトロンを用いたネットワークトラフィック分類の手法 [6] を、Wang らは、画像認識などで使われる、畳み込みニューラルネットワーク (Convolutional Neural Network, 以下「CNN」) を用いたマルウェアトラフィックの分類の手法 [7] を、Lopez-Martin らは、CNN と再帰型ニューラルネットワーク (Recurrent Neural Network, 以下「RNN」) を組み合わせた、CRNN(Convolutional Recurrent Neural Network) を用いた IoT 向けのネットワークトラフィック分類の手法 [8] を提案している。Jain らは、CNN を用いたネットワークトラフィック分類の手法 [9] を、Lim らは、CNN と Residual Network(ResNet) を用いた、パケットベースのネットワークトラフィック分類の手法 [10] と、多層 LSTM または CNN と LSTM を組み合わせたモデルを用いた、ペイロードベースのネットワークトラフィック分類の手法 [11] を提案している。

[5,7] の手法は、マルウェアのトラフィックのみを対象としているが、悪性トラフィックの中にはマルウェア以外によるトラフィックも含まれているため、マルウェア以外の悪性トラフィックを検知できない可能性がある。また、[7] の手法は既知のマルウェアのマルウェアトラフィック分類を目的としているため、未知のマルウェアトラフィックを検知することはできない。さらに、[3-11] はネットワークトラフィック分類、またはマルウェア分類を目的としているため、ネットワークトラフィック分類のみを行っているが、ネットワークトラフィック分類を行っただけでは、実際にどういった脅威があるのか、深く知ることは困難である。

近年、ネットワークトラフィック分類に機械学習、特にニューラルネットワークを用いる手法が広く採用されている。本研究では、CNN を用いてネットワークトラフィックの異常検知を行い、さらに、そのトラフィックデータをもとに、サイバー攻撃に関する有用な脅威情報を抽出し、提供するための手法を提案する。

3. 提案手法

提案システム実現のため、機械学習を用いて不審なネットワークトラフィックを検知し、そのトラフィックの中から、攻撃に関する脅威情報を抽出する手法を提案する。本論文では、図 1 に示したシステムにおける、トラフィックの中から不審なトラフィックを検知する”Anomaly Detection”，検知した不審なトラフィックをもとにサイバー攻撃に関する脅威情報を抽出する”Intelligence”の 2 つのフェーズについての手法を提案する。以下、それぞれのフェーズについ



図 2 画像化プロセス
Fig. 2 Imaging process

て詳細に説明する。

3.1 Anomaly Detection

3.1.1 学習

悪性トラフィックと良性トラフィックの両方のトラフィックデータを収集し、データセットとして扱う。パケットキャプチャなどにより取得した PCAP ファイルを、TCP または UDP のコネクションごとに分割して保存する。ここでいう「コネクション」というのは、送信元 IP アドレス、送信元ポート番号、送信先 IP アドレス、送信先ポート番号、通信プロトコルの 5 つ (5-tuple) が一致する一連のパケット群のことである。さらに、パケットの IP アドレスを削除する。

1つの PCAP ファイルをバイナリとして読み込み、ASCII コードに変換して 2 次元配列にし、その 2 次元配列を画像に変換する。画像は、Bicubic を使って拡大または縮小し、縦横ともに 256 になるように整形する。再度 2 次元配列に変換し、全体を 255 で除算して、CNN に入力できるように変換する。概要図を図 2 に示す。

次に、図 3 に示すようなモデルを構築する。構築したモデルに画像変換データを入力して学習させる。使用したモデルと得られた重み (weights) データを保存しておき、未知トラフィック判定の際に再利用できるようにしておく。

3.1.2 判定

学習によって得られたモデルと重みデータを利用して、良性か悪性かの判定を行う。学習の際と同様の手順で、得られた PCAP ファイルを画像データに変換し、CNN に入力して判定させる。

3.2 Intelligence

Anomaly Detection の判定で悪性と判定されたトラフィックデータから、正規表現を使って、クォーテーションで括られた文字列と、アルファベットが連続している単語様の文字列や、IP アドレス、ドメイン名と見られる文字列を抽出する。さらに、抽出した文字列を、外部のデータベースで検索し、より詳細な情報を取得する。

4. 実装

提案手法で挙げた”Anomaly Detection”と”Intelligence”について、実装を行った。

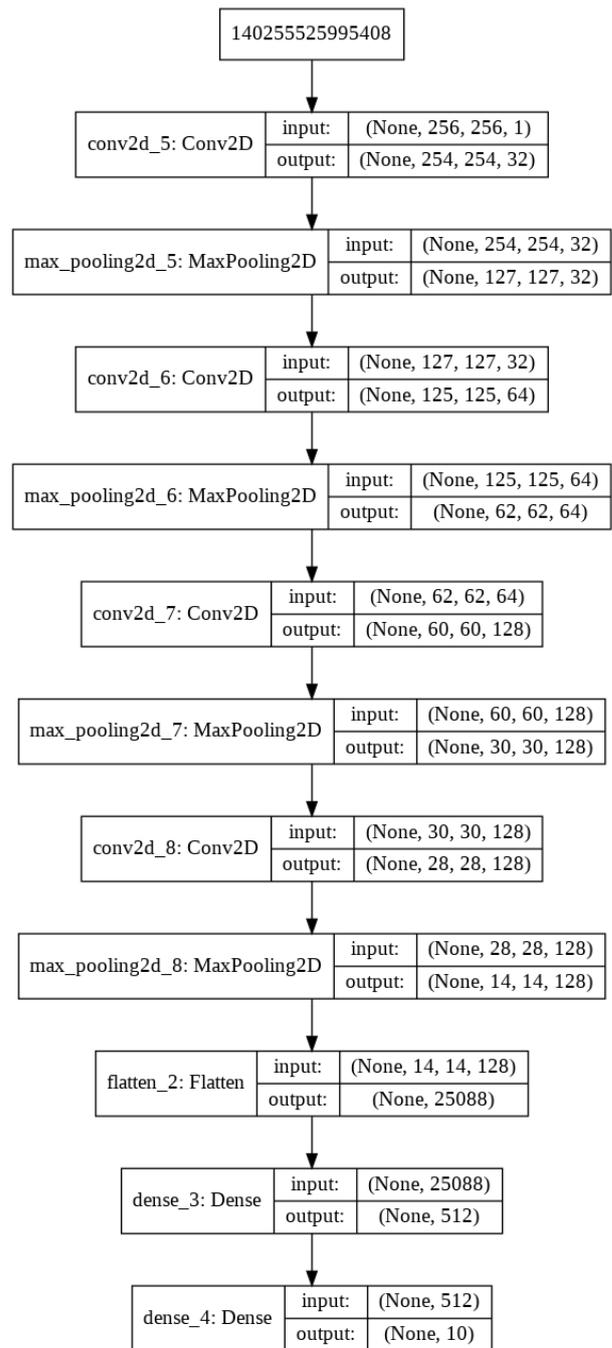


図 3 CNN モデル概要図

Fig. 3 CNN Model

4.1 実行環境

実装を行うにあたり、表 1 に示す環境を用いた。VM は、VMware vSphere^{*2}上に構築した CentOS 7.3 の仮想マシンである。Google Colaboratory は、完全にクラウドで実行される Jupyter ノートブック環境である。設定不要で、無料で利用できる。Colaboratory を使用すると、コードの記述と実行、解析の保存や共有、強力なコンピューティングリソースへのアクセスなどをブラウザからすべて無料で行える [12]。

*2 VMware 社が提供する、ハイパーバイザ型サーバ仮想化ソフトウェア。

表 1 使用した環境

Table 1 Machines for practice

	VM	Google Colaboratory	物理マシン
OS	CentOS 7.3	Ubuntu 18.04.2 LTS	CentOS 7.6
CPU	Intel Xeon E5	Intel Xeon	Intel Xeon E3
RAM	62GB	12GB	32GB
GPU	—	Tesla K80	—

表 2 CNN の学習に使用したデータセット

Table 2 Dataset for CNN Training

Train 7500 個				Test 2500 個			
Malicious 3750 個		Unmalicious 3750 個		Malicious 1250 個		Unmalicious 1250 個	
MTA	SUN	Mine	Others	MTA	SUN	Mine	Others
1875 個	1875 個	1875 個	1875 個	625 個	625 個	625 個	625 個

4.2 Anomaly Detection

使用したデータセットの内訳としては表 2 の通りである。75 % が学習用の Train データセットで、25 % がテスト用の Test データセットとなっている。悪性トラフィックのデータとして、Malware-Traffic-Analysis.net で配布されているマルウェアトラフィックを含む PCAP ファイル (MTA データセット) と、本学科攻撃収集ネットワークでキャプチャしたトラフィック (SUN データセット) を含む PCAP ファイルを使用した。良性トラフィックのデータとして、ネットサーフィンや動画視聴時のネットワークトラフィックをキャプチャして保存した PCAP ファイル (Mine データセット) を使用した。悪性か良性かの判定は、ProtectWise 社のセキュリティチームである 401TRG の情報 [13] を参考に、“Emerging Threats Suricata ruleset” を適用した Suricata [14] を使って行った。なお、Others データセットは、MTA と SUN のうち、Suricata の判定の際に良性であると判定されたデータ群である。Google Colaboratory の環境で、Keras [15] を使って CNN のモデルを構築した。CNN の学習曲線を図 4 に示す。“accuracy” が正解率，“loss” が損失である。正解率と損失の推移をもとに、エポック数を 100 とすることにす。

4.3 Intelligence

不審であると判定した PCAP の中から、主に正規表現を使って URL や IP アドレスなどの文字列を抽出し、それを外部のデータベースの検索キーワードとして脅威情報の検索を行うシステムを構築する。外部のデータベースとして、情報通信研究機構が開発し、OSS として公開した EXIST (サイバー脅威情報集約システム) [16] や、Google 検索を利用した。なお、EXIST は Docker を使って構築した。

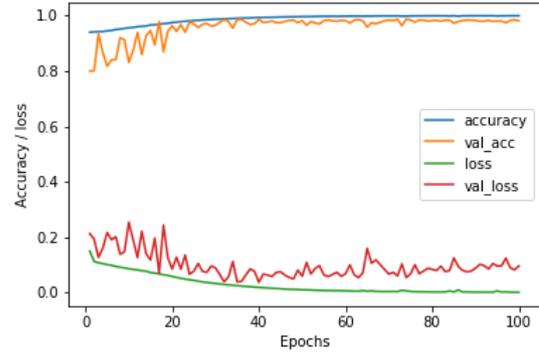


図 4 CNN の学習曲線

Fig. 4 Learning curve of CNN

表 3 CNN の評価に使用したデータセット

Table 3 Dataset for CNN Evaluation

Valid 5000 個			
Malicious 2500 個		Unmalicious 2500 個	
MTA	SUN	Mine	Other
1250 個	1250 個	1250 個	1250 個

5. 評価

5.1 Anomaly Detection

5.1.1 評価方法

以下の実験で評価を行う。

(実験 1) 学習用のデータとは別に評価用のデータを用意し、CNN にデータを入力して、CNN 自体の性能の評価を行う。

(実験 2) 用意したデータセットではない、実際のネットワークトラフィックをキャプチャした PCAP を使い、CNN による不審なネットワークトラフィックの検知能力を評価する。

5.1.2 評価結果

Train, Test データセットとは別に用意した、表 3 に示す Valid データセットを使用して、実験 1 を行った。その結果を表 4 に示す。Accuracy (正解率), Precision (適合率), Recall (再現率) の値はそれぞれ True Positive, True Negative, False Positive, False Negative の値をもとに、以下の数式を用いて算出した。

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

$$Precision = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP + FN}$$

表 5 に示す擬似攻撃のネットワークトラフィックを用い

表 4 CNN の評価

Table 4 CNN Evaluation

TP	TN	FP	FN
3417(46.6%)	3253(44.3%)	375(5.1%)	290(4.0%)
Accuracy	Precision	Recall	
90.9%	90.1%	92.2%	

表 5 実験 2 で使用した擬似攻撃

Table 5 Simulated attacks for Experiment 2

使用したツール	攻撃の種類
Nmap	TCP SYN Port Scan UDP Port Scan
Metasploit	vsftpd 2.3.4 Backdoor WordPress Admin Shell Upload

表 6 擬似攻撃の検知率

Table 6 Detection Rate of Simulated attacks

攻撃の種類	総数	TP	FN	検知率
TCP SYN Port Scan	65535	63778	1757	97.3%
UDP Port Scan	131246	127638	3608	97.3%
vsftpd 2.3.4 Backdoor	4	4	0	100%
WP Admin Shell Upload	18	14	4	77.8%

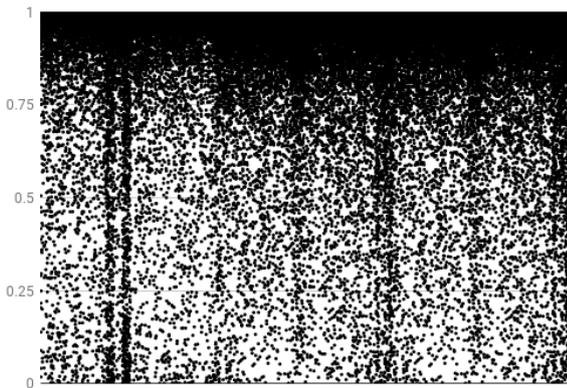


図 5 悪性トラフィックの確率

Fig. 5 probability of being Malicious Traffic

て、実験 2 を行った。その結果を表 6、図 5、図 6 に示す。表 6 は、攻撃の種類ごとの検知率を示している。図 5 は、CNN が判定した、ネットワークトラフィックが悪性である確率を、プロットしたものである。図 6 は、擬似攻撃トラフィックの悪性度の割合を示している。

5.2 Intelligence

5.2.1 評価方法

悪性のネットワークトラフィックの中から文字列の抽出、脅威情報の検索を行い、どのような情報が抽出されるか検証する。

5.2.2 評価結果

本学科攻撃収集ネットワークでキャプチャしたネット

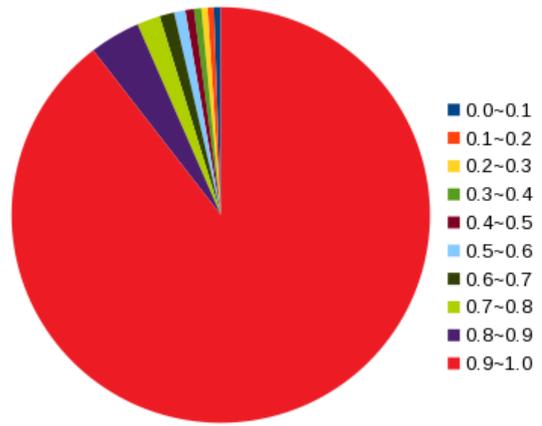


図 6 擬似攻撃トラフィックの悪性度の割合

Fig. 6 Percentage of Simulated attacks

表 7 抽出された文字列例

Table 7 Sample of Extracted Strings

community.sicherhei
aYLogin incorrectlogin:
Nordrhein Westfalen1
myip
Cookie: mstshash=
*/bin/busybox iDdosYou
shell:rm /data/local/tmp/dlr;
rm /data/local/tmp/bin;
rm /data/local/tmp/adb
msftncsi
http://ocsp.digicert.com0B
lJ@Vul
Lhmac-sha2-256,hmac-sha2-512,
hmac-sha1,hmac-sha1-96,
hmac-md5,hmac-md5-96,none
2DOWNGRD
.conexant@
whoami
ns1digitalocean
hunt57596
(ho4uku6at

ワークトラフィックのうち、Anomaly Detectionによって不審であると判定されたネットワークトラフィックを用いて、文字列の抽出を行った。なお、False PositiveとFalse Negativeはトレードオフに近い関係にあり、ネットワークセキュリティにおける侵入検知では、False Negativeを少なく抑えるためにある程度のFalse Positiveを許容する機会が多い。このシステムにおいてもそれが望ましいと考え、今回は一例として、Anomaly DetectionでのCNNによる不審なトラフィック検知の基準値を0.4に設定した。抽出された文字列の例を表 7 に示す。

さらに、抽出された文字列について、Google 検索や EXIST を利用して脅威情報の検索を行った。検索結果のうち、

表 8 脅威情報検索結果

Table 8 Search Results of Threat Information

検索文字列	Google 検索	EXIST
/bin/busybox iDdosYou	11 件	—
Cookie:mstshash=	94 件	—
myip	100 件	1 件
ttnet	101 件	1 件
(ho4uku6at	50 件	—

http://myipcheck121.pro/enter.php	
IP Address	217.107.34.53
Domain	
URL	http://myipcheck121.pro/enter.php
Date	2019-07-28 14:10:10
Source	CyberCrime Tracker
Description	sTDS
Referrer	https://cybercrime-tracker.net/index.php
CountryCode	

図 7 "myip"EXIST 検索結果

Fig. 7 Search Result of "myip" on EXIST

http://bottnet.site90.com/PHP/index.php?p=Login	
IP Address	31.170.162.223
Domain	
URL	http://bottnet.site90.com/PHP/index.php?p=Login
Date	2019-07-28 14:10:11
Source	CyberCrime Tracker
Description	Warbot
Referrer	https://cybercrime-tracker.net/index.php
CountryCode	

図 8 "ttnet"EXIST 検索結果

Fig. 8 Search Result of "ttnet" on EXIST

脅威情報である可能性があるものを表 8 に示す。Google 検索の結果の件数には、関連性の低いものも含まれている。なお、"myip"と"ttnet"という文字列が、EXIST の横断検索で該当したものの、検索結果(図 7, 図 8)を確認すると、意図した結果と異なっていた。

6. 考察

まず、Anomaly Detection については、表 4 の通り、誤検知を低く抑えつつ、90%以上の精度で、検知することができた。擬似攻撃ネットワークトラフィックを使用した場合

でも、95%以上のネットワークトラフィックを悪性であると判定することができたため、CNN を使って不審なネットワークトラフィックを検知することは、可能であると推測される。しかし、擬似攻撃のうち、WordPress Admin Shell Upload の検知率があまり高くなかったのは、この攻撃が HTTP POST メソッドを使用するため、正常な POST との判別が難しかったことが原因であると考えられる。今後は、パケット全体ではなく、特にアプリケーション層のペイロードに着目することで、DPI のような詳細な検知が可能になると考える。CNN に関しては、過学習を防止する効果のある Dropout 層のモデルへの追加や、より精度の高いデータセットの採用などによって、性能を向上させる余地があると考えられる。また、今回は CNN を採用したが、Lopez-Martin らの手法 [8] のように、時系列データを扱うことができる RNN を CNN と組み合わせた CRNN を利用することによって、より有用な結果を得ることができると可能性がある。

Intelligence については、URL や IP アドレス、文字列などをネットワークトラフィックから抽出し、それを外部のデータベースから検索することによって、攻撃に関係がある可能性のある情報を取得することができた。今回は、検索対象のソースが少なかったこと、情報を含んだ攻撃が少なかったことが影響して、取得することができた攻撃に関する情報が多くなかったが、検索対象のソースを増やすことによって、より多くの情報を集めることができると考える。また、バイナリをそのまま読み込んでいる影響により、文字列抽出の段階で、不要な文字列が大量に抽出される。ファイルの読み込み方法や、文字列抽出の方法を改善したり、抽出された文字列の中から不要な文字列を除去する手順を、あらかじめ行うことによって、情報を含んだ必要な文字列のみを抽出することができると考える。

近年、HTTPS のトラフィックが増加傾向にある [17]。同様に、暗号化された攻撃トラフィックも今後増加していくとみられている [18]。実際に、IoT マルウェアの一種である "Mirai" の亜種の一部は、C2 トラフィックを秘匿するために Tor を利用することが明らかになっている [19]。しかし、本研究では Anomaly Detection および Intelligence において、暗号化通信を考慮していない。現状ではどの程度の攻撃トラフィックが暗号化されているのか、不明確であるためである。今後、暗号化された攻撃トラフィックの状況が明らかとなり、暗号化されたトラフィックも扱う必要が出てくれば、TLS インスペクションなどにより復号の処理を行ったうえで、Anomaly Detection および Intelligence を行うといったことが考えられる。

さらに、このシステムにおいて、プライバシーの問題が存在していることが、実験を行っていくにつれて明らかとなった。ネットワークトラフィックから情報を抽出しているため、その際に利用者のプライバシー情報に触れてしまう可能

性が高い。また、脅威情報の検索を行う際に、内部の情報を不必要に漏洩してしまう可能性もあり、これは攻撃者からのインテリジェンスの餌食となってしまうことが考えられる。このシステムにおいても、適切な OPSEC(Operations Security)*³ [20], カウンターインテリジェンス*⁴ [21,22] を念頭に置く必要がある。

7. まとめ

本稿では、悪性または良性のネットワークトラフィック画像データを学習させた CNN を用いて、不審なネットワークトラフィックを検出し、そのネットワークトラフィックから脅威情報を抽出する手法を提案した。実験の結果、90%以上の精度で不審なネットワークトラフィックの検出を行うことができ、さらにそのネットワークトラフィックから抽出された文字列をもとに、攻撃に関係がある可能性のある情報を取得することができた。

今後は、CNN や文字列抽出手法の改善、CRNN 利用の検討や、OSINT の検索ソースの充実などを行いつつ、提案システム全体の実現を目指す。

参考文献

- [1] Office of the Director of National Intelligence: U.S. National Intelligence: An Overview 2011, Office of the Director of National Intelligence (online), available from https://www.dni.gov/files/documents/IC_Consumers_Guide_2011.pdf (accessed 2019-08-20).
- [2] Nguyen, T. T. and Armitage, G.: A survey of techniques for internet traffic classification using machine learning, *IEEE Communications Surveys & Tutorials*, Vol. 10, No. 4, pp. 56–76 (online), DOI: 10.1109/SURV.2008.080406 (2008).
- [3] Zhou, W., Dong, L., Bic, L., Zhou, M. and Cheng, L.: Internet traffic classification using feed-forward neural network, *2011 International Conference on Computational Problem-Solving (ICCP)*, IEEE, pp. 641–646 (online), DOI: 10.1109/ICCP.2011.6092257 (2011).
- [4] Mathewos, B., Carvalho, M. and Ham, F. M.: Network traffic classification using a parallel neural network classifier architecture, *Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research - CSIRW '11*, No. September, New York, New York, USA, ACM Press, p. 1 (online), DOI: 10.1145/2179298.2179334 (2011).
- [5] Bekerman, D., Shapira, B., Rokach, L. and Bar, A.: Unknown malware detection using network traffic classification, *2015 IEEE Conference on Communications and Network Security, CNS 2015*, pp. 134–142 (online), DOI: 10.1109/CNS.2015.7346821 (2015).
- [6] Ang, M. K., Valla, E., Neggatu, N. S. and Moore, A. W.: Network traffic classification via neural networks, No. 912 (online), available from <http://www.cl.cam.ac.uk/> (2017).
- [7] Wang, W., Zhu, M., Zeng, X., Ye, X. and Sheng, Y.: Malware traffic classification using convolutional neural network for representation learning, *International Conference on Information Networking*, pp. 712–717 (online), DOI: 10.1109/ICOIN.2017.7899588 (2017).
- [8] Lopez-Martin, M., Carro, B., Sanchez-Esguevillas, A. and Lloret, J.: Network Traffic Classifier With Convolutional and Recurrent Neural Networks for Internet of Things, *IEEE Access*, Vol. 5, pp. 18042–18050 (online), DOI: 10.1109/ACCESS.2017.2747560 (2017).
- [9] Jain, A. V.: Network Traffic Identification with Convolutional Neural Networks, *2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)*, IEEE, pp. 1001–1007 (online), DOI: 10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00142 (2018).
- [10] Lim, H.-K., Kim, J.-B., Heo, J.-S., Kim, K., Hong, Y.-G. and Han, Y.-H.: Packet-based Network Traffic Classification Using Deep Learning, *2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIIC)*, IEEE, pp. 046–051 (online), DOI: 10.1109/ICAIIIC.2019.8669045 (2019).
- [11] Lim, H.-K., Kim, J.-B., Kim, K., Hong, Y.-G. and Han, Y.-H.: Payload-Based Traffic Classification Using Multi-Layer LSTM in Software Defined Networks, *Applied Sciences*, Vol. 9, No. 12, p. 2550 (online), DOI: 10.3390/app9122550 (2019).
- [12] Google Colaboratory: Colaboratory へようこそ, Google Colaboratory (オンライン), 入手先 <https://colab.research.google.com/notebooks/welcome.ipynb?hl=ja> (参照 2019-08-06).
- [13] Logoyda, M. Y.: Using Emerging Threats Suricata Ruleset to Scan PCAP, 401TRG (online), available from <https://401trg.com/using-emergingthreats-suricata-ruleset-to-scan-pcap/> (accessed 2019-08-06).
- [14] Open Information Security Foundation: Suricata — Open Source IDS / IPS / NSM engine, Open Information Security Foundation (online), available from <https://suricata-ids.org/> (accessed 2019-08-20).
- [15] Keras: Keras Documentation, Keras (online), available from <https://keras.io/ja/> (accessed 2019-08-06).
- [16] 情報通信研究機構サイバーセキュリティ研究室: EXIST, 情報通信研究機構サイバーセキュリティ研究室 (online), available from <https://github.com/nict-csl/exist> (accessed 2019-08-20).
- [17] HTTP Archive: Report: State of the Web, HTTP Archive (online), available from <https://httparchive.org/reports/state-of-the-web> (accessed 2019-08-21).
- [18] Cisco Systems, Inc.: Cisco 2018 Annual Cybersecurity Report, Cisco Systems, Inc. (online), available from https://www.cisco.com/c/dam/m/ku_hu/campaigns/security-hub/pdf/acr-2018.pdf (accessed 2019-08-21).
- [19] Cyber Threat Research Team(CTRT): Tor ネットワークを利用する「Mirai」亜種 IoT マルウェアを発見, トレンドマイクロ株式会社 (オンライン), 入手先 <https://blog.trendmicro.co.jp/archives/21920> (参照 2019-08-21).
- [20] Naval Operations Security Support Team: OPSEC, Naval Operations Security Sup-

*³ 重要な情報を識別, 制御, 保護し, 軍事作戦やその他の活動に関連する友好的な行動を分析するために用いられる体系的手法。最終的に, OPSEC は敵から自身の情報と活動を保護する。

*⁴ 外国の勢力, 組織, 個人, そのエージェント, または国際的なテロ組織やその活動のために, またはそれらに代わって行われるスパイ活動や, その他の諜報活動, 妨害工作, 暗殺行為を識別, 欺瞞, 悪用, 防止するために収集された情報および活動のこと。

port Team (online), available from https://www.navy.mil/ah_online/OPSEC/terms.asp (accessed 2019-08-20).

[21] Reagan, R. W.: Executive Order 12333 – United States intelligence activities, United States of America (online), available from <https://www.archives.gov/federal-register/codification/executive-order/12333.html> (accessed 2019-08-20).

[22] Bush, G. W.: Further Amendments to Executive Order 12333, United States Intelligence Activities, United States of America (online), available from <https://www.federalregister.gov/documents/2008/08/04/E8-17940/further-amendments-to-executive-order-12333-united-states-intelligence-activities> (accessed 2019-08-20).