一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
IN2017-57(2017-12)

特徴量写像関数の学習による類似インシデント検索

大下　裕一†　　村田　正幸†

† 大阪大学 大学院情報科学研究科
E-mail: †{y-ohsita,murata}@ist.osaka-u.ac.jp

あらまし　インシデントが発生した際には、管理者はそのインシデントに対して、迅速に対応することが求められる。インシデントの対応には、過去に発生したインシデントに関する情報は有用であり、過去の類似のインシデントの情報から、新たに発生したインシデントが早急な対応が必要なインシデントか否かといった判断や、インシデントの対応方法に関して参考となる情報を得ることができる。そこで、本稿では、このようなインシデント情報を蓄積し、新たなインシデントが発生した際に、過去に蓄積したインシデントから当該インシデントに類似したインシデントに関する情報を提示できるシステムについて議論する。新たなインシデントが検知された際には、当該インシデントで発生したフロー等の特徴量を把握できる。しかしながら、それらの特徴量間の距離が近いインシデントが同種のインシデントとは限らない。そこで、本稿では、インシデントの特徴量を、類似のインシデントは近くに、異なるインシデントは遠くに写像するような写像関数をインシデントの対応結果の情報から学習し、写像関数で写像後の位置が近い過去のインシデントを検索する手法を提案する。評価により、提案手法により、過去に経験した同種のインシデントを高い精度で検索できることを示す。
キーワード　インシデント、蓄積、分類、検索

Similar incident retrieval by learning feature mapping function

Yuichi OHSITA† and Masayuki MURATA†

† Graduate School of Information Science and Technology, Osaka University
E-mail: †{y-ohsita,murata}@ist.osaka-u.ac.jp

Abstract　When a security incident is detected, the manager must handle it as soon as possible. The investigation of the incident is important to handle the security incident, and the information of the previously handled incidents is useful to investigate the incident. By using the information of the similar incidents, the manager obtains the hints to handle the incident. In this paper, we discuss the system that can search the similar incidents. When a security incident is detected, the manager obtains the features of the incident. In our system, the features are used as the key to search the similar incidents. The similarity used to search the incidents should be defined so that the incidents of the same kind have the large similarity. In our method, we use the mapping function learned by using the incident reports to search the incidents considering the similarity; our system trains the mapping function so that the incidents of the same kinds are mapped to the near points. In this paper, we evaluate our system and demonstrate that our system can retrieve the incidents with the same kind accurately.
Key words　Incident, Store, Classification, Search

1. はじめに

従来からインターネットに接続されきたパソコンやスマートフォンに加え、IoT 機器と呼ばれる様々な機器がインターネットに接続されるようになった。インターネットに接続される機器が増加するにつれ、それらの機器が攻撃者から狙われるなど、セキュリティリスクが高くなっている。すでに、IoT 機器を対象とした攻撃も実際に発生している。2016 年には、Mirai と呼ばれる IoT 機器を対象としたマルウェアが登場し、その亜種の感染も広がっている [1]。今後、IoT 機器を対象とした新たな種類の攻撃が発生する可能性もあり、IoT によるサービスを提供する業者は、それらの新たな攻撃に対しても、迅速な対処が求められる。

攻撃に対して迅速な対応を行うためには、異常検知技術 [2] を用い、インシデントを迅速に検出するだけでなく、そのインシデントについて分析することが必要となる。インシデントを

分析することにより、外部からポートスキャンを受けた場合や、ブルートフォース攻撃を受けたものの、侵入に失敗した場合のように、被害が発生しておらず、早急の対処は必要ではない場合なのか、あるいは、機器への侵入が成功し、機器が踏み台として用いられている場合のように、迅速に対応することが必要な場合なのかを把握することが可能となる。また、インシデントの分析の結果、過去に同種のインシデントが発生し、対処した経験があれば、その経験をもとに、新たに発生したインシデントへ対応することが可能となる。

このようにインシデントへの対応には、過去に発生したインシデントに関する情報は有用である。特に、IoT 機器に対するインシデントは、これまでに経験の蓄積が少ないため、新たにインシデントが発生し、そのインシデントを今後発生するインシデント対応に利用できる形で蓄積することは重要である。このような脅威に関する情報を共有するため、脅威情報の記述方法等についての議論も勧められている [3]。

インシデント情報を新たなインシデント発生時に活用するには、蓄積された情報から、類似するインシデントの情報を取得できることが求められる。インシデントの対応は、異常検知技術により、何らかの異常が検知された後に行われる。そのため、新たに検知されたインシデントの特徴（インシデント発生時に通信が行われていた宛先ポート番号や通信量等）が得られ、この特徴をもとに過去に蓄積されたインシデントの情報から、類似のインシデントを検索する。このような検索を実現する単純な方法としては、インシデントの特徴をベクトルとしてあらわし、特徴量ベクトル同士を比較し、新たに発生したインシデントの特徴量ベクトルとの差がもっとも小さいインシデントの情報を得るという方法が考えられる。しかしながら、インシデントの特徴量ベクトルの差が小さいインシデントが、同種のインシデントとは限らず、インシデントの分析において、有用な情報が取得できない可能性がある。そのため、同一種類のインシデントを類似のインシデントとして抽出できるように、各インシデントの特徴を踏まえた上で、類似か否かの判断を行う必要がある。

本稿では、上記を踏まえ、写像関数の学習を通して、類似のインシデントを検索することができるシステムを提案する。本システムでは、インシデント対応後に管理者が投入する情報から把握できるインシデントの種類をもとに、類似のインシデントが近くに、異なる種類のインシデントが遠くに写像されるように、インシデントの特徴量ベクトルの写像関数を学習する。そして、新たなインシデントが発生した際には、学習された写像関数を用い、写像後の位置が近いインシデントを検索することにより、新たに発生したインシデントに類似したインシデントの情報を得る。

2. インシデント情報蓄積・検索システム

2.1 概　　要

新たなインシデントが検出された際、管理者は当該インシデントの特徴を示す特徴量を把握している。しかしながら、そのインシデントがどのような種類のインシデントであるのかまでは判明していない。本稿では、そのような場合に、把握されたインシデントの特徴量を検索の入力として投入すると、過去に蓄積された対応済みインシデントの情報から、類似のインシデントの情報を抽出し、管理者に提示することにより、当該インシデントの対応に活用できるシステムを構築する。ただし、ここで抽出すべきインシデントの情報は、発生したインシデントと同種のインシデントの情報であり、単に特徴量が類似しているインシデントではない。同種のインシデントであれば、その種類のインシデント固有の特徴がある。例えば、マルウェアに感染したデバイスが、新たな感染先を探しているときには、同一ポート番号宛のポートスキャンを行うといった特徴的な通信が発生する。このような特徴をもつインシデントは同種のインシデントとしてみなす必要があるが、特徴量の単純な比較だけでは、上記のような各インシデントの特徴を考慮した検索を実現できない。

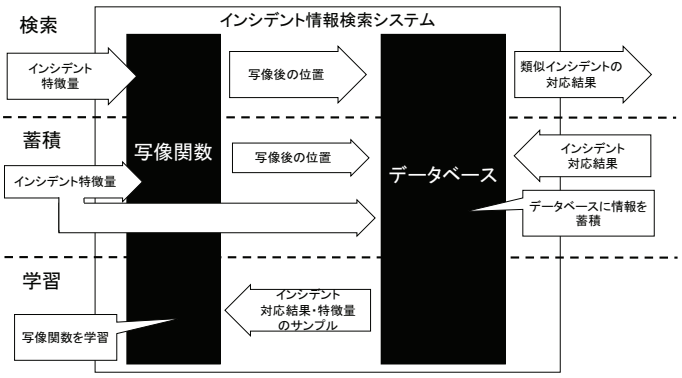

図 1　概　　要

そこで、本システムでは、写像関数を導入する。写像関数の入力としてインシデントの特徴量を与えた場合に、同種のインシデントは近い位置に、異なるインシデントは遠い位置に写像されるように、過去に蓄積されたインシデントの対応結果をもとに写像関数を学習する。そして、写像関数の入力として、新たに発生したインシデントの特徴量を与え、写像後の位置を得、得られた写像後の位置が近い過去のインシデントを抽出することにより、類似のインシデントを抽出することが可能となる。

2.2 構 成 要 素

図 1 に本システムの構成を示す。本システムは、情報を蓄積するデータベースと、学習により更新可能な写像関数からなる。以降、本システムの詳細について述べる。

2.2.1 データベース

本システムでは、データベース内に、各インシデントについて以下の情報を蓄積する。

- インシデント特徴量：当該インシデントの特徴づける情報
- インシデント対応結果：当該インシデントに対応した結果、判明したインシデントの種類や、対応方法の情報
- 写像後位置：　検索に用いる後述の写像関数で写像した後の位置

そして、写像後の位置を検索のキーとして利用できるようにデータベースを構成することにより、類似したインシデントに関する情報の検索ができるようになる。

以下、データベースに蓄積される上記の各情報について説明する。

a) インシデント特徴量

インシデント特徴量は、当該インシデントを特徴づける特徴量で、インシデント検知時に把握可能な情報のみからなる情報である。例えば、当該インシデント検知時に、インシデントが発生した機器が通信を行っていたフローの本数や、宛先の種類の数、フローのサイズ等の特徴量が考えられる。インシデント特徴量に含める情報については、システムの運用開始時にあらかじめ設定するものとし、インシデント特徴量はベクトルで表現可能であるとする。以降、インシデント i の特徴量をベクトル表現したものを v_i とする。

b) インシデント対応結果

インシデント発生が検知されると、管理者はそのインシデントの調査を行い、インシデント対応を行う。その結果、インシデントの種類といったインシデントに関する情報や、インシデントへの対応方法を管理者は把握することができる。本稿では、これらのインシデントの調査やインシデント対応の結果、管理者が把握できた情報をインシデント対応結果と呼ぶ。管理者は、インシデント対応結果を本システムに投入し、本システムがインシデント対応結果を蓄積することにより、今後、類似インシデント発生時に、それらの情報を有効活用できるようにする。

c) 写像後の位置

2.2.2 で述べる写像関数の入力として v_i を与えた際に得られる出力を、各インシデントについて蓄積する。本情報は、本データベースから、インシデントを検索する際のキーとして用いられる情報となる。具体的なインシデントの検索手順については、2.3.1 で述べる。

2.2.2 写像関数

本システムでは、写像関数 f を保持する。写像関数 $f(v_i)$ により、インシデント情報を低次元な空間に写像する。その際に、同種のインシデント同士は、写像先同士の距離が近くなるように、異なるインシデントの写像先は離れた位置になるように写像関数を設定する。本関数を用い、写像後の位置をキーとしてデータベースの検索を行うことにより、単に特徴量ベクトル v_i が似ているインシデントではなく、同種のインシデントに関する情報を抽出することができる。

2.3 動作

2.3.1 インシデントの検索

新たなインシデントが発生すると、当該インシデントの特徴量 v_i が得られる。v_i を学習済みの写像関数 f に入力し、$f(v_i)$ を得る。$f(v_i)$ をキーとして、類似した写像後の位置をもつインシデントをデータベースから検索する。

2.3.2 インシデントの蓄積

インシデントの調査やインシデント対応の結果、当該インシデントの詳細が分かると、管理者は、インシデント特徴量とインシデント対応結果の組をシステムに投入する。システム側では、当該インシデント量を写像関数に入力し、写像後の位置を得た上で、インシデント特徴量、インシデント対応結果、写像後の位置をデータベースに保存する。

2.3.3 写像関数の学習

本システムでは、定期的に写像関数の学習を行う。写像関数の学習の際には、データベースに蓄積されたインシデント情報から、一部をサンプリングし、インシデント特徴量とインシデント対応結果の組を一定数得る。得られたインシデント対応結果をもとに、インシデント同士の類似度を計算する。インシデント間の類似度の計算方法は、あらかじめ設定した任意の計算方法が適用できる。そして、得られたインシデントの類似度をもとに、類似度が高いインシデントは写像後の位置が近く、類似度が低いインシデントは写像後の位置が遠くなるように、写像関数を学習する。具体的な学習方法の例は、次節で述べる。

写像関数の学習後、写像後の位置を大きく変わることがあれば、これまでにデータベース内に蓄積された写像後の位置は、学習後の写像関数と合致しないものとなる。この場合、新しい写像関数に合わせてデータベース内の写像後の位置を更新する。

3. 異常フローの関連情報抽出への適用

本稿では、送信元・宛先 IP アドレス、ポート番号が一致する通信をフローとし、異常検知時のフローについて、過去に経験した類似のフローの情報を得るという、異常フローを検索するシステムとして、前節のシステムを具体化する。以降、本応用における特徴量、対応結果、写像関数とその学習方法について述べる。

3.1 特徴量

本応用においては、監視対象となる機器を定め、当該機器が送受信するトラヒックを観測するものとする。観測は、フロー単位で行われ、当該フローが異常検知された後に、当該フローと類似のフローの情報を検索により得る。この検索においては、各フローについて、異常検知時に得られる情報を特徴量として用いる。本稿において、各フローについて用いた特徴量を表 1 に示す。

3.2 対応結果

本応用では、インシデントについて調査を行った結果、属性（DoS 攻撃に関するフローやブルートフォース攻撃に関するフローなど）が判明したフローについて、判明した属性やその詳細に関する情報を対応結果に含め、システムに投入する。写像関数の学習の際には、対応結果に含まれている属性情報を用い、同種のフローかの判断を行う。

3.3 写像関数

3.3.1 写像関数の構成

本実装では、入力として、表 1 の特徴量ベクトルを与え、写像先の値が出力されるような多層ニューラルネットワークとして構成する。各層の構成について、以下に述べる。

a) 入力層

特徴量ベクトルの各要素を一つのノードへ、そのまま入力として与える。

表 1　特　徴　量

説明	値
同時刻の同一 IP アドレス宛のフロー数	整数値
同時刻の同一 IP アドレス発のフロー数	整数値
同時刻の同一ポート番号宛のフロー数	整数値
同時刻の同一ポート番号発のフロー数	整数値
フロー中の監視対象機器への総パケット数	整数値
フロー中の監視対象機器への総トラヒック量（Byte)	整数値
フロー中の監視対象機器からの総パケット数	整数値
フロー中の監視対象機器からの総トラヒック量 (Byte)	整数値
フロー中の監視対象機器への平均パケットレート（packets/sec）	実数値
フロー中の監視対象機器からの平均パケットレート（packets/sec）	実数値
フロー中の監視対象機器への平均トラヒックレート（Byte/sec）	実数値
フロー中の監視対象機器からの平均トラヒックレート（Byte/sec）	実数値
フロー中の監視対象機器の送信トラヒック量と対象機器の受信トラヒック量の比	実数値
監視対象機器側のポート番号	代表的なポート番号について One Hot 化した値
監視対象機器の通信相手側のポート番号	代表的なポート番号について One Hot 化した値
プロトコル番号	代表的なプロトコルについて One Hot 化した値
開始 TCP フラグ	各フラグについて ON なら 1、OFF なら 0
逆方向開始 TCP フラグ	各フラグについて ON なら 1、OFF なら 0

b）　一層目の隠れ層

入力ベクトル v の各要素について、閾値を設け、閾値を超えているかで、0 または 1 を出力することにより、入力ベクトルから特徴を抽出する。本写像関数では、一層目の隠れ層で、このような特徴量の抽出を行う。以降では、各入力要素につき、n 個の特徴量を抽出する。これを行うための処理として、一層目の出力の各要素は、以下の関数によって得る。

$$y_{in+j}^{(1)} = \sigma\left(a_{in+j}^{(1)} v_i + b_{in+j}^{(1)}\right)$$

ただし、$a_i^{(1)}$、$b_i^{(1)}$ は学習によりチューニングされるパラメータであり、$\sigma()$ はシグモイド関数である。

c）　二層目以降の隠れ層

二層目以降の隠れ層は、前の層の出力を全結合して、出力する。活性化関数は、ReLU を用いる。つまり、n 層目の出力は、以下の関数により得られる。

$$y_i^{(n)} = \max\left(0, \sum_j \left(a_j^{(n)} y_j^{(n-1)} + b_j^{(n)}\right)\right)$$

ただし、$a_i^{(n)}$、$b_i^{(n)}$ は学習によりチューニングされるパラメータである。

d）　出　力　層

二層目以降の隠れ層を多段組み合わせ、最上位層で得られた出力を、写像結果とする。

3.3.2　学 習 方 法

本実装では、フロー f_1 と f_2 の間の類似度 $S(f_1, f_2)$ が、既知のデータベースに登録されたフローのすべてについて得られた場合に、以下を最小化するように、ニューラルネットワークで構成された写像関数 f を学習する。

$$\sum_{f_1, f_2 \in F} \left(S(f_1, f_2) \left(\frac{f(v_{f_1}) - f(v_{f_2})}{\alpha} \right)^2 \right)$$

$$+ \sum_{f_1, f_2 \in F} \left((1 - S(f_1, f_2)) \frac{1}{\left(\frac{f(v_{f_1}) - f(v_{f_2})}{\alpha} \right)^2} \right)$$

ただし、類似度 $S(f_1, f_2)$ は、0 以上 1 以下の値をとり、類似する際に 1 に近い値となり、異なる場合に 0 に近い値をとるものとする。本誤差関数は、類似度の高いフローの写像後のユークリッド距離が近くなり、類似度の低いフローのユークリッド距離が遠くなるほど、小さな値をとる。

しかしながら、多量のデータを与え、上述の目的関数を用いて、誤差逆伝搬法によりニューラルネットワークの学習を行うと、局所解から脱することができず、類似度の低いフロー同士の距離が小さいままとなってしまうことも起こりうる。そこで、この問題を解消するために、以下の手順で、学習を行う。

（1）　学習時に代表となるフローを、代表として選択されたフロー同士の類似度が低くなるように、選択

（2）　代表となるフロー間の距離が大きくなるように写像関数を学習

（3）　代表となるフローを基準に、そのほかのフローの情報を用いて写像関数を学習

ここで、代表となるフローは、すでに代表として選択されたいずれのフローとも類似度が低いフローを選択する。そのようなフローが複数存在する場合は、候補となるフローのうち、類似度が高いフロー同士でクラスタを作成し、クラスタ内の全フローの現在の写像関数での写像後の位置を計算、写像後の位置の中央値に近いフローを選択する。これにより、当該クラスタに属するフロー群について、クラスタの中心に近いフローを代表となるフローとして選択することが可能となる。以降、この選択されたフローの集合を F^{rep} と表す。

次に、選択された代表となるフロー間で、現在の写像関数における写像後の位置を計算する。代表となるフロー間の写像後の位置のユークリッド距離が、いずれも閾値 T 以上であれば、

類似度の低いフロー同士は、十分離れた距離に写像されているとみなすことができる。しかしながら、ユークリッド距離が閾値 T 以下のフローの組み合わせが存在すると、類似度の低いフロー同士が近くに写像されており、適切な写像関数となっていない。この場合、代表として選択されたフロー同士の写像後の位置が離れた位置となるように、以下の誤差関数を最小化するように、ニューラルネットワークで構成された写像関数を誤差逆伝搬法により、学習する。

$$\sum_{f_1,f_2\in F^{\mathrm{rep}}}\left((1-S(f_1,f_2))\frac{1}{\left(\frac{f(v_{f_1})-f(v_{f_2})}{\alpha}\right)^2}\right)$$

これにより、代表として選択されたフロー同士は、離れた位置に写像されるように、写像関数を学習することができる。

代表となるフローの写像後の位置が離れた位置となるように写像関数を学習できると、代表となるフローの写像後の位置を基準として用い、そのほかのフローの写像後の位置が類似するフローの写像後の位置と近くなるように、写像関数を学習する。その際、以下の誤差関数を最小化するように学習を行う。

$$\sum_{f_1\in F^{\mathrm{sample}},f_2\in F^{\mathrm{rep}}}\left(S(f_1,f_2)\left(\frac{f(v_{f_1})-f'(v_{f_2})}{\alpha}\right)^2\right)$$

ただし、F^{sample} は学習に用いるサンプリングされたフローの集合、f' は本学習をする前の写像関数を表す。これにより、代表として選択されたフローの写像後の位置を基準に、各フローについて、代表として選択されたフローのうち、類似したフローの写像後の位置の近くに写像されるように、写像関数を学習することができる。

4. 評　　価

4.1 評 価 方 法

4.1.1 評価に用いたデータ

本評価では、仮想ネットワーク上に、攻撃者ノードと被害者ノードを配置、表 2 に示す攻撃トラヒックを攻撃者ノード・被害者ノード間に発生させた。そして、tcpdump を用いて当該フローをキャプチャし、表 1 の特徴量を抽出し、評価に用いた。攻撃トラヒックは、各種類につき、通信レートやダウンロード・アップロードするファイルのサイズ、辞書攻撃に用いる辞書等の攻撃時に設定するパラメータをランダムに変化させつつ、1000 回発生させた。また、学習の際には、学習に利用する各フローについて、表 2 の分類が分かり、管理者は当該分類結果をシステムに投入するものとする。また、本分類結果をもとに、同一の種類に分類されるフローについては、類似度は 1、それ以外は類似度は 0 となるものとした。

4.1.2 評 価 手 順

提案手法では、学習した写像関数を用いることにより、特徴量ベクトルのみからは分からない類似したインシデントを抽出することができることに特徴がある。そのため、発生したインシデントと類似のインシデントの数が少ない場合であっても、類似したインシデントを抽出することができる。そこで、本メリットについて示すために、ある種類のインシデントに関する情報の蓄積が少ない場合に注目し、正しくインシデントの抽出ができるのかを調べた。本評価は、以下の手順で行う。

（1） 評価対象以外のフローの学習

評価対象の種類以外の全フローを学習に用い、写像関数を学習する

（2） 評価対象のフローの学習

評価対象の攻撃トラヒックを 1 回発生させ、本トラヒックに含まれるフローを学習

（3） 精度の評価

評価対象の全フローについて、各フローの特徴量をキーとして提案システムにおいて、類似したフローを検索し、検索の精度を評価。

（4） 2 へ戻る

上記の手順を繰り返すことにより、フローに関する情報の蓄積により、検索精度がどのように向上するのかについて調べる。以降、本評価では、検索精度は、各フローについて、写像後の距離がもっとも近い学習済みのフローを取得し、その取得されたフローの種類が評価に用いたフローと同一であったものの数をカウント、カウントされた値を評価に用いたフロー数で割った値とする。

4.1.3 比 較 対 象

提案手法では、学習した写像関数を用いることにより、類似した種類のフローを検索可能としている。そこで、本評価では、写像関数を用いずに、入力として与えられた特徴量 v 同士を比較し、学習済みのフローのうち、特徴量同士のユークリッド距離が最も小さいフローを得る手法と比較を行った。

4.2 結　　果

本評価では、隠れ層の数が 5、各隠れ層のノード数は 100、出力層が 2 ノードのニューラルネットワークとして写像関数を構成し、上述の手順で、フロー情報を蓄積、検索を行った際の精度について評価を行った。図 2 に telnet による遠隔操作のトラヒックを評価対象とした場合の結果を示す。図より、写像関数を用いない場合、写像関数の学習を行う場合、いずれも、経験した telnet による遠隔操作のトラヒックの数が増えるにつれ、検索精度が向上していることが分かる。これは、telnet による遠隔制御のトラヒックの蓄積が進むにつれ、精度の評価時に用いたフローと類似したフローがデータベース内に含まれる確率が高まるためである。

また、図より、写像関数を用いない場合には、蓄積されたトラヒック数に対して、精度は単調増加であるのに対して、写像関数の学習を行った場合は、学習済みのインシデント数が少ない場合には、精度の変化が大きく、新たなトラヒックを学習した結果、精度が悪化することも起きている。これは、少ないフローの情報から、telnet の写像後の位置を決定しているためであり、新たに観測された telnet のフローに合わせて写像関数を学習した結果、写像関数が大きく変化することが原因である。しかしながら、ある程度以上の telnet に関するフローの情報を蓄積し、写像関数の学習に用いることにより、学習結果との写像関数が大きく変化することはなくなり、新たなフローの観測

表 2　評価に用いたトラヒック

トラヒックの種類	説明
ブルートフォース攻撃 (監視対象機器が攻撃先)	監視対象機器の telnet、ssh、ftp ポートで提供されるサービスのパスワード認証に対して辞書攻撃を発生
ブルートフォース攻撃 (監視対象機器が攻撃元)	監視対象機器から、監視対象外の機器の telnet、ssh、ftp ポートで提供されるサービスのパスワード認証に対して辞書攻撃を発生
DoS 攻撃 (監視対象機器が攻撃先)	監視対象機器に対して、SYN パケットを大量に生成 (SYN flood)、あるいは、ICMP パケットを大量に発生 (ICMP flood)
DoS 攻撃 (監視対象機器が攻撃元)	監視対象機器以外の特定の機器に対して、SYN パケットを大量に生成 (SYN flood)、あるいは、ICMP パケットを大量に発生 (ICMP flood)
ホストスキャン（監視対象機器が攻撃先）	特定の Well known ポートを対象として、当該ポートの空き状況をサブネット内の全機器に対して調査を行う通信を発生。（ただし、そのうち、監視対象機器に到達したもののみが観測）
ホストスキャン（監視対象機器が攻撃元）	監視対象機器から特定の Well known ポートを対象として、当該ポートの空き状況をサブネット内の全機器に対して調査を行う通信を発生。
ポートスキャン（監視対象機器が攻撃先）	監視対象の機器に対して、当該機器の空きポートを調査を行う通信を発生。
ポートスキャン（監視対象機器が攻撃元）	監視対象機器から監視対象の特定の機器に対して、当該機器の空きポートを調査を行う通信を発生。
遠隔制御	SSH や telnet で、監視対象機器を操作する通信を発生
ファイルのダウンロード	HTTP 経由で監視対象機器にファイルをダウンロード
ファイルのアップロード	HTTP 経由で監視対象機器からファイルをアップロード

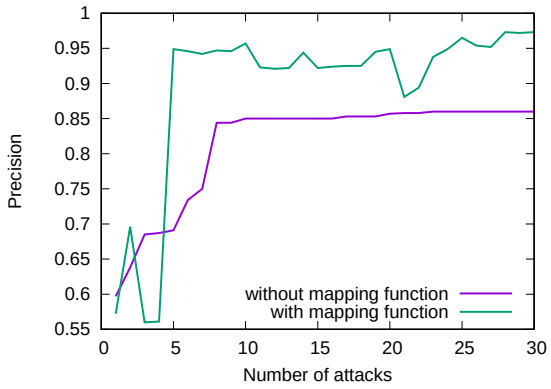

図 2　蓄積されたトラヒック数と検索精度

により、精度が著しく変化することはなくなる。

また、図より、telnet による遠隔操作に関するトラヒックを 5 回以上観測すると、提案手法では、0.95 程度の精度を達成可能であるのに対して、写像関数を用いない手法の精度は 0.85 から改善しない。これは、写像関数を学習する手法では、telnet による遠隔操作に関するフローを、他の種類のフローとは離れた位置に写像するような学習を行った結果、他の種類のフローを誤って抽出することが激減したのに対し、写像関数を用いない手法では、各フローについて、当該フローと特徴量ベクトルが近いフローが観測されない限り、精度を向上させることはできない。このように、写像関数の学習を通して、類似フローを検索することができる提案システムは、過去に蓄積された類似したフローを検索する際に、同種のフローの経験が少なくても、精度よく情報取得ができることが分かる。

本稿では、紙面の都合上、telnet による遠隔操作のトラヒックを評価対象とした場合の結果のみを示したが、他の種類のトラヒックを評価対象とした場合においても、同様に、一定数のトラヒックを学習に用いることにより、写像関数を用いない場合と比べ、提案手法の方がより高い検索精度を達成することができている。

5. ま と め

本稿では、写像関数の学習を通して、類似のインシデントを検索することができるシステムを提案した。そして、異常検知されたフローと類似するフローの検索に適用し、評価を行った。評価の結果、写像関数を用いずに、特徴量が類似するフローを検索する手法と比べ、より高い精度で類似フローの検索ができることが分かった。

今回の評価では、提案するインシデント検索を攻撃時に発生するフローに関する情報の検索に適用して評価を行った。しかしながら、現実に発生するインシデントは、複数のフローやログが関係し、それらを包括的に見ることにより、インシデントの識別が可能となる。そのような場合への本研究の適用は今後の課題である。

謝　　辞

本研究は、総合科学技術・イノベーション会議の戦略的イノベーション創造プログラム（SIP）「重要インフラ等におけるサイバーセキュリティの確保」（管理法人：NEDO）により実施された。

文　　献

[1] H. Sinanovic and S. Mrdovic, “Analysis of mirai malicious software,” in *Proceedings of SoftCOM*, Sept. 2017.

[2] 中津留毅, 五十嵐弓将, 南拓也, “IoT 機器の健全性劣化を検知する技術,” **電子情報通信学会総合大会**, Mar. 2017.

[3] S. Barnum, “Standardizing cyber threat intelligence information with the structured threat information expression (stix),” *MITRE Corporation*, vol. 11, pp. 1–22, 2012.