

通信挙動に基づいたスキャン攻撃検知

山下 智也^{1,a)} 宮本 大輔^{1,b)} 関谷 勇司^{1,c)} 中村 宏^{1,d)}

受付日 2021年3月9日, 採録日 2021年9月9日

概要: ネットワーク上の攻撃者は、攻撃を行う準備としてまずスキャン攻撃を行い、ネットワーク上のホストが持つ脆弱性に関する情報の収集を試みる。したがってスキャン攻撃の検知は、さらなる本格的な攻撃を未然に防ぐための重要な課題といえる。スキャン攻撃を検知するシステムとして侵入検知システム (IDS) が提案、利用されている。しかし、通信の時間間隔を大きくしてスキャンを行うスロースキャン攻撃や、複数のホストを利用してスキャンを行う分散スキャン攻撃の検知は容易ではない。そこで本論文では、スキャン攻撃を行うホストと正常な通信を行うホストの通信挙動の違いをとらえることのできる特徴量を提案し、この特徴量を用いたスキャン攻撃の検知手法を提案する。実験により、提案手法がスロースキャン攻撃や分散スキャン攻撃の検知に有効であることを確認する。

キーワード: セキュリティ, スキャン攻撃検知, 通信挙動, スロースキャン, 分散スキャン

Scan Attack Detection Based on Communication Behavior

TOMOYA YAMASHITA^{1,a)} DAISUKE MIYAMOTO^{1,b)} YUJI SEKIYA^{1,c)} HIROSHI NAKAMURA^{1,d)}

Received: March 9, 2021, Accepted: September 9, 2021

Abstract: Cyberattacks often begin with a port scan attack, which is used to find exploitable vulnerabilities on targeted systems. Therefore, quick detection of scanning attacks is by far important to avoid further attacks. Intrusion detection systems (IDS) have been proposed to detect scanning attacks. However, it is difficult to detect slow scan attacks, in which the time interval between successive communications is increased, or distributed scan attacks, in which multiple hosts are used for scanning. Therefore, in this paper, we propose a method for detecting scan attacks that focuses on the difference in communication behavior between scanning hosts and hosts that perform normal communication. Through experiments, we confirm that the proposed method is effective in detecting slow scan attacks and distributed scan attacks.

Keywords: security, scan attack detection, communication behavior, slow scan attack, distributed scan attack

1. 背景

近年のコンピュータネットワークの発展と普及により、情報ネットワークは人々にとって身近な存在となった。しかし、コンピュータネットワークの普及とともに、ネットワーク上の攻撃も年々増加している。ネットワーク上の攻撃者は、攻撃準備として、まずスキャン攻撃を行い、ネットワーク上のホストに存在する脆弱性についての情報の

収集を試みる。そして、収集した情報を利用して本格的な攻撃を行う。そのため、スキャン攻撃の段階で攻撃を検知することができれば、後に続く本格的な攻撃に対して事前に対策を打つことができると考えられる。したがって、スキャン攻撃の検知はセキュリティ分野における重要な課題の1つといえる。現在、スキャン攻撃を検知する手法の1つに侵入検知システム (IDS) が存在する [1]。IDS はシステムやネットワーク上で発生するイベントを監視、分析することでネットワーク上の攻撃検知を行う。既存のIDSでは、シグネチャと呼ばれる攻撃通信のパターンに通信データを照らし合わせて攻撃通信を検知するシグネチャ検知が主流である。しかし、長い時間をかけて低速にスキャンを実行するスロースキャン攻撃や、複数のホストを利用し

¹ 東京大学
The University of Tokyo, Bunkyo, Tokyo 113-8654, Japan
a) yamashita@hal.ipc.i.u-tokyo.ac.jp
b) daisu-mi@nc.u-tokyo.ac.jp
c) sekiya@nc.u-tokyo.ac.jp
d) nakamura@hal.ipc.i.u-tokyo.ac.jp

てスキャンを実行する分散スキャン攻撃に対し、網羅的にシグネチャを用意することは困難である。そのため、既存のIDSではこれらのスキャン攻撃は検知が困難とされている。さらに、現在では、暗号化された通信が主流になりつつあり、検知のために通信データの中身、ペイロードを利用することが困難である。

既存のIDSにおけるこれらの問題点を解決する方策として、通信挙動に基づいたアノマリ検知が考えられる。シグネチャ検知が、攻撃通信のパターンを列挙することで検知を行う検知手法であるのに対し、アノマリ検知は正常な通信の特徴を学習し、その特徴から外れた通信を検知する検知手法である。したがって、アノマリ検知においてシグネチャは不要であり、シグネチャ検知では検知が困難であったスロースキャン攻撃や分散スキャン攻撃にも対応できると考えられる。さらに通信挙動に着目して検知を行うアノマリ検知では、通信データのペイロードは不要なため、暗号化された通信データに対しても検知が可能と考えられる。

アノマリ検知においては、検知にどのような特徴量を用いるかが重要なポイントとなる。アノマリ検知に着目したスキャン攻撃検知に関する既存研究はいくつか存在するが、検知に有用な特徴量は確立されておらず、スロースキャン攻撃や分散スキャン攻撃に対して、十分な検知性能を持つ検知手法ははまだ提案されていない。

本論文では、まず正常な通信とスキャン攻撃の通信挙動の違いをとらえることのできる特徴量を提案する。そして提案する特徴量を用いた、スキャン攻撃の検知手法を提案する。実験により、提案する検知手法がスロースキャン攻撃や分散スキャン攻撃の検知に有効であることを確認する。なお、本論文で提案する特徴量は著者らが文献[2]において提案したものと同一である。しかし、文献[2]では、分散スキャン攻撃に対する検知手法の提案・評価は行っていない。また、文献[2]では、スロースキャン攻撃の検知性能の評価に関して、時間あたりの攻撃頻度を変えた際のIDSの検知性能との比較を行っていない。本論文ではこれらの点を加え、新たに手法の提案と有効性の評価を行う。

本論文の構成を述べる。まず2章で既存研究について述べる。そして、3章でスキャン攻撃検知に利用する特徴量の提案を行い、4章で提案した特徴量を用いたスキャン攻撃の検知手法の提案を行う。5章で、提案手法の評価実験を行い、6章に結論を述べる。

2. 既存研究

本章では既存研究として、アノマリ検知に着目したスキャン攻撃の検知手法に関する研究をいくつかあげる。

2.1 エントロピーを利用したスキャン攻撃検知

エントロピーを利用したスキャン攻撃検知に関する研究がある[3], [4], [5]。文献[3], [4], [5]ではトラフィック量を

見るだけではとらえることのできなかつた通信挙動の特徴を、エントロピーを利用することでとらえることができる」と述べられている。文献[3]では、トラフィック量に対しシャノンエントロピーへの変換を施し、変化点検知を行うことで、攻撃通信があった時間の特定を試みている。文献[4]では、トラフィック量に対し、いくつかのエントロピー変換を施し、機械学習を用いて攻撃通信の検知を試みている。実験によって、Tsallis エントロピー、もしくはRenyi エントロピーに変換した場合が最も検知結果が良いことが示されている。文献[5]ではパケットヘッダから得られるデータ（フローサイズ、ポート番号の分布、IP アドレスの分布）をエントロピーに変換したものに加えて、通信の送信元と宛先に着目した特徴量をエントロピーに変換したものを利用した検知手法を提案している。実験では、いくつかの攻撃通信を用意し、それぞれの攻撃通信を検知できる特徴量の調査を行っている。

2.2 ウェーブレット変換を利用したスキャン攻撃検知

ウェーブレット変換を利用したスキャン攻撃検知に関する研究がある[6], [7]。パケットサイズの時系列データに対し、ウェーブレット変換を施すことで、時系列データの局所的な変化をとらえて攻撃通信検知を行うことができると述べられている。文献[6]では、通信フローデータから15種類の時系列の特徴量を抽出し、ウェーブレット変換にかけてGMMモデルに入力することで攻撃通信の検知を試みている。実験により、既存の検知手法に比べ高い検知性能を持つことが示されている。文献[7]ではポートスキャン攻撃、ステルススキャン攻撃が含まれるデータセットを用いて実験を行い、それぞれの攻撃に対し、適切なウェーブレット関数を選択すれば攻撃通信を検知できるということを示している。

2.3 深層学習を利用したスキャン攻撃検知

深層学習を利用したスキャン攻撃検知に関する研究がある[8], [9], [10], [11]。文献[8]では、通信データに含まれる送信元IPアドレス、送信元ポート、宛先IPアドレス、宛先ポートそれぞれの分布のエントロピーを時間ウィンドウで切って特徴量として利用している。その4つの特徴量をDeep Auto Encoderの入力として学習、検知を試みている。実験においては、データセットに対して攻撃の度合いの異なる擬似的なポートスキャン攻撃を加え、攻撃の度合いの大きなものは検知できるということを示している。文献[9]では、Auto Encoderを拡張したStacking Dilated Convolutional Auto Encoderを用いて通信データから攻撃通信の検知に有用な特徴量を取り出すことを試みている。Dilated Convolutional Auto Encoderとは、中間層が畳み込みニューラルネットワークになったAuto Encoderであり、広い領域の情報を伝えることができるという特徴があ

る。実験の結果、複雑な攻撃通信を検知することができたと述べられている。文献 [10] では、深層学習を利用することで、Wi-Fi のネットワークに対する攻撃通信の検知と分類を試みている。深層学習に利用する活性化関数の候補をいくつか用意し、検知性能の比較を行った。実験の結果、98.67%の精度で攻撃通信を分類できることを示している。文献 [11] では、Auto Encoder とサポートベクターマシンを組み合わせた侵入検知システムの提案がなされている。Auto Encoder の特徴量生成によって、より検知にとって重要な情報が抽出されると述べられている。実験の結果、提案手法が既存の手法（ナイーブベイズ、ランダムフォレスト、サポートベクターマシン）に比べ、高い検知性能を持つことを示している。

2.4 Fuzzy Rule を利用したスキャン攻撃検知

Fuzzy Rule を利用したスキャン攻撃検知に関する研究がある [12], [13], [14]。Fuzzy Rule とはスキャン攻撃検知に利用する特徴量に対し、攻撃通信か否かという結論を対応づけたルールである。セキュリティの専門家が前もってこの Fuzzy Rule を定めて検知に利用する。Fuzzy Rule を用いることで攻撃通信か否かだけでなく、個々の通信の攻撃の強さを特徴量の値に応じて決めてしまうことが可能である。文献 [13], [14] における、Fuzzy Rule を用いた検知に関する研究では、各ホストの単位時間あたりのパケットの送受信数に着目した特徴量を用いられている。この特徴量に対し、Fuzzy Rule を用いた検知実験を行い、一般的なIDS (Snort) では検知が困難であったスロースキャン攻撃に対する検知性能の向上が確認できたと述べられている。ただし実験では、テスト用に擬似的に構築した小規模のネットワーク環境を用いた検知性能の評価のみにとどまっておき、実際の通信データに対する検知性能については言及されていない。

3. 特徴量の提案

3.1 既存研究の課題と提案手法の概要

エントロピーを利用したスキャン攻撃検知やウェブレット変換を利用したスキャン攻撃検知に関する研究 [3], [4], [5], [6], [7] における課題として、適切なエントロピーやウェブレット関数の選択が困難であることがあげられる。また、文献 [12], [13], [14] における課題として、検知に利用する特徴量が時間依存性を持つということがあげられる。本論文において、時間依存性を持つ特徴量とは単位時間あたりの情報をとらえる特徴量と定義する。このような時間依存性を持つ特徴量を用いた検知では、正常な通信と同程度の速度でスキャンを行うスロースキャン攻撃への対応はしばしば困難になると考えられる。また、深層学習を利用したスキャン攻撃検知に関する研究 [8], [9], [10], [11] における課題として、深層学習を利用

した検知では軽量の検知が困難であることがあげられる。ネットワーク型IDS (NIDS) を想定したスキャン攻撃検知では、検知器はネットワーク上に存在する計算能力の乏しい機器に設置されることが想定される。したがってNIDSを考えるうえでは、軽量の検知手法であることは重要なポイントであると考えられる。

これらの課題をふまえ、本論文では、時間依存性を持たない特徴量を利用した、アノマリ検知によるスキャン攻撃の検知手法を提案する。そこで本論文ではまず、スキャン攻撃の検知に利用する特徴量を提案する。本論文で提案する特徴量は、通信フローデータの情報から計算できるものである。通信フローデータは通信データのペイロードを必要としないデータであるため、暗号化された通信データに対しても、特徴量を計算することができる。さらに、通信データのペイロードを利用する検知手法に比べて保持するデータ量を減らすことができ、軽量の検知が可能と考えられる。

3.2 通信フローデータ

本論文では、通信フローデータの情報をを用いてスキャン攻撃の検知を行うことを考える。通信フローデータは、送信元ホストと宛先ホストとの間の双方向のパケットのストリームである。送信元ホストと宛先ホストはそれぞれ、ネットワーク層の送信元および宛先のIPアドレスと、トランスポート層の送信元および宛先のポートによって定義される。通信フローデータは、 $F = (\text{srcIP}, \text{srcPort}, \text{dstIP}, \text{dstPort}, t_s)$ の5要素からなるタプル形式で表現される。srcIPは送信元IPアドレス、srcPortは送信元ポート、dstIPは宛先IPアドレス、dstPortは宛先ポート、 t_s は通信が行われた時刻である。定義より通信フローデータは、どこから、どこに、いつ、どのような通信が行われたかという通信挙動の情報を持つデータになっていることが分かる。通信フローデータを利用する際にはこれら5要素以外のペイロードは破棄される。

3.3 宛先ポートの数と宛先IPアドレスの数の比

攻撃者がスキャン攻撃を行う際には、標的とするホストやネットワークの情報を収集することを目的としている。水平ポートスキャン攻撃を行う攻撃者は、標的とする少数のIPアドレスに対して、多数の宛先ポートを用いた通信を行うと考えられる。一方、垂直ポートスキャン攻撃を行う攻撃者は標的とするネットワーク上の多数のIPアドレスに対して、特定の少数の宛先ポートを用いた通信を行うと考えられる。この通信挙動は正常な通信を行うホストにはめったに見られないものであると考えられる。したがって、この通信挙動の違いをとらえることのできる特徴量として、Ports Per IPs (PPI) を提案する。

表 1 正常な Web アプリの通信フローデータ (PPI : 5.15)

Table 1 Communication flow data of a normal web server.

srcIP	srcPort	dstIP	dstPort
198.51.100.35	443	203.0.113.212	43922
198.51.100.35	443	203.0.113.212	43922
198.51.100.35	443	203.0.113.212	44062
...
198.51.100.35	443	203.0.113.212	33650
198.51.100.35	443	203.0.113.212	33710

$$PPI = \log \frac{\text{ホストが通信に用いる宛先ポートの種類数}}{\text{ホストが通信を行う宛先 IP アドレスの種類数}}$$

水平ポートスキャン攻撃を行うホストは、少数の宛先 IP アドレスに対して、多数の宛先ポートを用いて通信を行うため、PPI の値は大きなものになると考えられる。一方、垂直ポートスキャン攻撃を行うホストは、多数の宛先 IP アドレスに対して少数の宛先ポートを利用して通信を行うため、PPI の値は小さなものになると考えられる。正常な通信を行うホストの場合、通信を行う宛先 IP アドレスの種類数と、通信に用いる宛先ポートの種類数に大きな偏りが出ることはめったになく、PPI の値はゼロに近いものになると考えられる。

ただし、PPI の問題として、スキャン攻撃を行っていない Web サーバや DNS サーバの中に、大きな PPI をとるホストが存在するということがあげられる。これは Web サーバや DNS サーバに対して、少数のクライアントホストが複数の接続を確立することが、しばしば起こるからである。表 1 に大きな PPI をとる Web サーバの通信フローデータを示す。通信フローデータを見ると、ホスト 198.51.100.35 は単一の宛先 IP アドレスに対して、多数の宛先ポートを用いて通信を行っている。これは、水平ポートスキャン攻撃の通信挙動に類似しており、PPI も比較的大きな値をとっている。しかし、このホストの送信元ポートが 443、すなわち HTTPS の通信を行っているということと、宛先ポート 43922 に重複があることから、このホストは水平ポートスキャン攻撃を行っているとは考えにくい。このホストは単一のクライアントと複数の接続を確立した Web サーバであると考えられる。PPI を用いてスキャン攻撃の検知を行った場合、このような Web サーバや DNS サーバを誤検知する可能性がある。そこで、このような誤検知を回避するためのもう 1 つの特徴量を提案する。

3.4 送信元フロー数と宛先フロー数の比

前節で述べた、PPI の問題を解決するための特徴量を提案する。すなわち、スキャン攻撃を行っている攻撃者と、スキャン攻撃を行っていない Web サーバや DNS サーバの通信挙動の違いをとらえることのできる特徴量である。一般に Web サーバや DNS サーバは、ネットワーク上のクライアントから通信を受け取り、クライアントが要求する

サービスを提供するサーバである。したがって Web サーバや DNS サーバは、自らが送信元として開始する通信よりも、自らを宛先として開始する通信を主に行うと考えられる。一方、スキャン攻撃を行う攻撃者は、自らが送信元として開始する通信を主に行い、自らを宛先として開始する通信はめったに行わないと考えられる。この通信挙動の違いをとらえることのできる特徴量として、以下の特徴量 Src Per Dst (SPD) を提案する。

$$SPD = \log \frac{\text{自らが送信元として開始する通信フロー数}}{\text{自らを宛先として開始される通信フロー数}}$$

スキャン攻撃を行っていない Web サーバや DNS サーバは、自らが送信元として開始する通信フローの数よりも、自らを宛先として開始される通信フローの数が多くなるため、SPD の値は小さなものになると考えられる。一方、スキャン攻撃を行う攻撃者は、自らが送信元として開始する通信フローの数が、自らを宛先として開始される通信フローの数を大きく上回るため、SPD の値は大きなものになると考えられる。したがって、SPD を用いることで、スキャン攻撃を行う攻撃者と、スキャン攻撃を行っていない Web サーバや DNS サーバを区別することができると考えられる。

3.5 提案する特徴量のまとめ

水平ポートスキャン攻撃を行うホストの PPI, SPD はともに大きな値となると考えられる。一方、垂直ポートスキャン攻撃を行うホストは PPI が小さな値となり、SPD は大きな値となると考えられる。そして、スキャン攻撃を行っていないホストの PPI と SPD はスキャン攻撃を行う攻撃者の PPI, SPD とは大きく異なる値をとると考えられる。したがって、PPI と SPD を用いることで、スキャン攻撃を行う攻撃者とスキャン攻撃を行っていないホストの区別が可能になると考えられる。

4. PPI, SPD を用いたスキャン攻撃検知手法の提案

4.1 スキャン攻撃検知の手順

本章では、提案した特徴量 PPI, SPD を用いたスキャン攻撃の検知手法を提案する。スキャン攻撃を検知する際には、以下の手順をとる。

- (1) 通信データに含まれる各ホストの PPI と SPD を計算。
- (2) PPI, SPD を用いて検知を行う際の検知閾値を設定。
- (3) ホストのグルーピング処理を行ったうえで PPI, SPD を再計算。
- (4) 検知閾値を超えたホストを検知。

以下の節で、手順 (2) の検知閾値の設定方法、手順 (3) のホストのグルーピングについて説明する。

4.2 検知閾値の設定方法

提案した特徴量を用いて検知を行うためには、閾値の設

定を行う必要がある。提案手法では、以下の理由により既存のIDSであるSnortの検知結果を利用して閾値を設定することとする。Snortはシグネチャと呼ばれる不正な通信パターンを保持し、通信データと比較することで攻撃を行うホストを検知するNIDSであり、一般的なスキャン攻撃に対して高い検知性能を持つ。しかし、時間依存性を持つ通信パターンを用いるためスロースキャン攻撃に対する検知性能は高くない。一方で、提案手法は時間依存性を持たない特徴量を用いた検知手法である。そこで、高い検知性能を有するSnortの利点を活用することで、一般的なスキャン攻撃を検知できる閾値を設定し、提案する特徴量が時間依存性を持たないという利点によりスロースキャン攻撃をも検知することを旨とする。以下、具体的な例とともに詳細を説明する。図1は、東京大学のネットワークにおいて取得された、通信データに含まれる各ホストの、PPI, SPDによるマッピングである。通信データの取得日時は、2019年10月11日の14時58分から15時13分までの15分間である。オレンジのプロットがSnortによって検知されたホストを示している。図1より、左上の領域、すなわちPPIが小さく、SPDが大きい領域にSnortによって検知されたホストのプロットのクラスタが確認できる。これらのオレンジのプロットのホストの通信フローデータの1つを表2に示す。

表2のホストは多数の宛先IPアドレスに対して、宛先ポート515の通信を行っている。ポート515は多機能周辺機器(MFP)上で実行されているLPRサーバが利用しているポートである[15]。LPRサーバにはバッファ

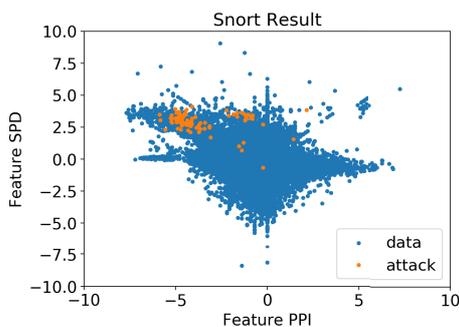


図1 Snortによる検知
Fig. 1 Detection by Snort.

表2 Snortに検知されたホストの通信フローデータ (112フロー)

Table 2 Communication flow data of the host detected by Snort.

srcIP	srcPort	dstIP	dstPort
198.51.100.39	45889	192.0.2.11	515
198.51.100.39	38660	192.0.2.32	515
198.51.100.39	53118	192.0.2.5	515
...
198.51.100.39	50891	192.0.2.87	515
198.51.100.39	50714	192.0.2.43	515

オーバーフローの脆弱性があることが知られており、ホスト198.51.100.39はLPRサーバを標的とした垂直ポートスキャン攻撃を行ったのではないかと考えられる。PPIが小さく、SPDが大きな領域に分布するオレンジのプロットのホストの通信フローデータの多くは、このホストの通信フローデータに類似したものとなっていることが確認できた。したがって、これらの左上のオレンジのプロットのホストの多くは垂直ポートスキャン攻撃を行うホストであると考えられる。なお、Snortによって検知されたホストのうち、左上のクラスタに含まれないホストの通信フローデータを確認したところ、ポートスキャン攻撃ではないと考えられる通信挙動を持つホストが多く含まれることが確認できた。これらのホストはスキャン攻撃以外の攻撃を行っているホストがSnortによって検知されたものであると考えられる。

そこでPPI, SPDを用いてスキャン攻撃検知における検知閾値を設定する際には、Snortに検知されたホストのうち、PPIが小さく、SPDが大きな領域に存在するオレンジのプロットのクラスタの重心を、垂直ポートスキャン攻撃の検知閾値と定めることとする。一方、水平ポートスキャン攻撃に関しては、図1に示すとおり、PPI, SPDがともに大きな領域にはホストがほとんど存在しておらず、Snortの検知結果を利用して検知閾値を設定することは困難である。そこで、垂直ポートスキャン攻撃検知の閾値をSPD軸対称に反転して、水平ポートスキャン攻撃検知の閾値として利用することとする。PPIの提案の際に述べたことから、SPD軸対称に反転して検知閾値を設定することで、垂直ポートスキャン攻撃の検知閾値と同程度の攻撃強度の水平ポートスキャン攻撃を検知できることを期待する。Snortの検知結果からクラスタを取り出す際には、X-meansと呼ばれるクラスタリング手法を用いる。なお、オレンジのプロットのクラスタが存在する領域には青色のプロットも存在している。これらのホストの通信フローデータを確認したところ、この領域に存在するオレンジのプロットと同様、垂直ポートスキャン攻撃と考えられる通信挙動を持つホストが多く存在していることが確認できた。これらの青色のホストの多くは、垂直ポートスキャン攻撃を行う攻撃ホストであり、Snortはこれらの攻撃ホストの検知に失敗したのではないかと考えられる。

また、Snortが誤検知を起こす可能性が考えられるが、一般にネットワークトラフィックにはSnortが検知できるスキャン攻撃が多く含まれると考えられる。提案手法では、Snortが検知したホストのクラスタのうち、垂直ポートスキャン攻撃を行っていると考えられる左上のクラスタを閾値の設定に利用しており、少数の誤検知が閾値の設定に大きな影響を及ぼすことは少ないと考えられる。そこで、本論文では、Snortがスキャン攻撃と判断したホストのPPIとSPDの値を、提案手法が用いる閾値として設定した。次

節では、分散スキャン攻撃の検知に対応するためのグルーピング処理について説明する。

4.3 ホストのグルーピング

本節では、ホストのグルーピングについて説明する。まず、ホストのグルーピングの必要性について説明する。図 2 に、あるデータセットに含まれる各ホストに対して PPI, SPD を用いたマッピング結果を示す。

図 2 を見ると、黒枠内にクラスタの存在が確認できる。黒枠内に含まれるホストの通信フローデータを表 3, 表 4 に示す。

表 3, 表 4 を見ると、通信フローデータの送信元ポートがすべて 32766 で同一であったということ、通信フローデータの宛先 IP アドレスがすべて 203.0.113.21 で同一であったということ、さらに宛先ポートに重複がないということが確認できた。したがって、黒枠内のこれらのホスト

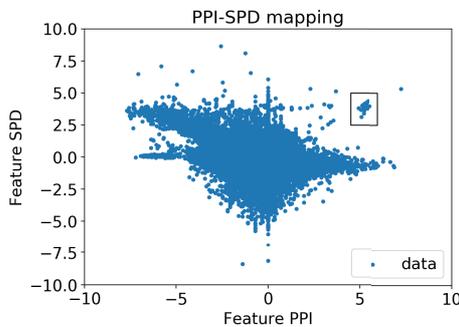


図 2 分散スキャン攻撃を行っていると考えられるホスト群
 Fig. 2 Hosts thought to be conducting distributed scanning attacks.

表 3 分散スキャン攻撃と考えられる通信フローデータ 1 (235 フロー)

Table 3 Communication flow data considered to be a distributed scanning attack.

srcIP	srcPort	dstIP	dstPort
192.0.2.50	32766	203.0.113.21	39327
192.0.2.50	32766	203.0.113.21	48516
192.0.2.50	32766	203.0.113.21	25107
...
192.0.2.50	32766	203.0.113.21	30974
192.0.2.50	32766	203.0.113.21	58542

表 4 分散スキャン攻撃と考えられる通信フローデータ 2 (208 フロー)

Table 4 Communication flow data considered to be a distributed scanning attack.

srcIP	srcPort	dstIP	dstPort
192.0.2.72	32766	203.0.113.21	27179
192.0.2.72	32766	203.0.113.21	2719
192.0.2.72	32766	203.0.113.21	21540
...
192.0.2.72	32766	203.0.113.21	11070
192.0.2.72	32766	203.0.113.21	29759

は、協働して水平ポートスキャン攻撃を仕掛けているホストではないかと考えられる。このような分散スキャン攻撃は、各ホストからのスキャン攻撃が軽微なものであっても、協働してスキャン攻撃を行っているホスト全体の通信データをまとめると、甚大なスキャン攻撃を行っている可能性がある。したがって、ホストを適切にまとめて検知を行う必要があると考えられる。本論文では分散スキャン攻撃への対策として、ホストのグルーピングを提案する。本節ではホストのグルーピングの方針について説明する。まず、水平ポートスキャン攻撃を行うホストは、標的とする少数の宛先 IP アドレスに対して、多数の宛先ポートを利用して通信を行う。この少数の宛先 IP アドレスは、分散スキャン攻撃を仕掛ける場合、攻撃を行うホスト全体が標的とする宛先 IP アドレスになると考えられる。したがって、水平ポートスキャン攻撃を行っていると考えられるホストについては、この少数の宛先 IP アドレスをヒントにグルーピングを行うことを考える。一方、垂直ポートスキャン攻撃を行うホストは、多数の宛先 IP アドレスに対して、標的とする少数の宛先ポートを利用して通信を行う。この少数の宛先ポートは、分散スキャン攻撃を仕掛ける場合、攻撃を行うホスト全体が標的とする宛先ポートになると考えられる。したがって、垂直ポートスキャン攻撃を行っていると考えられるホストについては、この少数の宛先ポートをヒントにグルーピングを行うことを考える。この方針に従いホストのグルーピングを行うことで、攻撃の標的を同一とするようなホストをまとめることができると考えられる。

ホストのグルーピングを行う際には、宛先 IP アドレス、もしくは宛先ポートのヒストグラムを利用する。そしてホスト間のヒストグラムが類似していることをホストをまとめる際の条件とする。ヒストグラムの類似度はホスト間のヒストグラムどうしの二乗誤差をもって、測ることとする。ホストのグルーピングの具体的な方法について説明する。通信データ内の各ホストに対して、PPI, SPD の値を計算する。そして、PPI, SPD の差がともに 1 以下かつ宛先 IP アドレス、もしくは宛先ポートのヒストグラムの二乗誤差が 0.2 以下のホストは同一グループと見なして IP アドレスをまとめることとする。この際、PPI, SPD がともに 0 以上の領域に含まれるホストについては宛先 IP アドレスのヒストグラムを利用し、PPI が 0 以下、SPD が 0 以上の領域に含まれるホストについては宛先ポートのヒストグラムを利用することとする。

PPI, SPD の値が近いことをグルーピングの条件とすることで、通信挙動が類似したホストをまとめることができると考えられる。また、宛先 IP アドレス、もしくは宛先ポートのヒストグラムが類似していることをグルーピングの条件とすることで、攻撃の標的を同一とするホストをまとめることができると考えられる。

5. スキャン攻撃検知手法の評価

本章では実験により、提案手法がスロースキャン攻撃や分散スキャン攻撃の検知に有効であることを確認する。本論文では、有効性の確認は、既存のIDSであるSnortと比較することで行う。Snortは様々なファイアウォールに搭載されている実用的なNIDSであり、実データを用いた比較実験の対象として適切だと考えられるからである。

5.1 実験に利用するデータセット

スロースキャン攻撃の検知実験と分散スキャン攻撃の検知実験では、東京大学のユーザ端末が主に接続されているネットワークにおいて取得された通信データを利用する。スロースキャン攻撃の検知実験では、2020年2月1日の8時14分から14時14分までの6時間に得られた通信データを用いる。このデータセットに含まれるパケット数は2,320,992,126個、データセットの大きさは1.38TBである。また、このデータセットには1,834,013個のIPアドレスが含まれており、組織への流入フローの割合が40.9%、組織からの流出フローの割合は59.1%である。分散スキャン攻撃の検知実験では、2019年10月11日の14時58分から15時13分までの15分間に得られた通信データを用いる。このデータセットに含まれるパケット数は357,672,714個、データセットの大きさは189GBである。このデータセットには188,831個のIPアドレスが含まれており、組織への流入フローの割合が47.9%、組織からの流出フローの割合が52.1%であることが確認できた。また、本論文で用いるデータセットは現実のデータセットであるために、攻撃通信は含まれていると考えられる。なお、本論文ではIPアドレスをRFC5737[16]にしたがって変換することで、データの匿名性を担保する。

5.2 スキャン攻撃検知の閾値

東京大学のネットワークから得られた通信データに対して、Snortによる検知とX-meansによるクラスタリングを施し、PPI, SPDを用いてマッピングした結果を図3に示す。なお、データの取得日時は2019年10月11日の14時

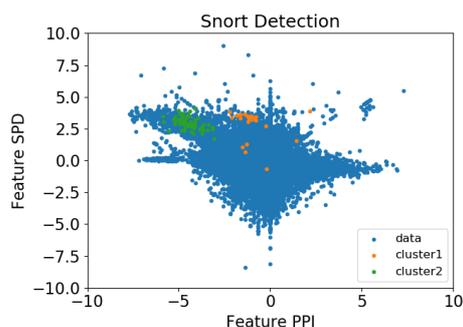


図3 X-meansによる攻撃ホストのクラスタリング結果1
Fig. 3 Clustering results of attack hosts by X-means.

58分から15時13分までの15分間であり、図1のデータと同一のものである。図3より、Snortによって検知されたホスト群がX-meansによって、2つのクラスタにクラスタリングされていることが分かる。そして、Snortに検知されたホストのいくつかについて通信フローデータを確認すると、cluster2のホストは垂直ポートスキャン攻撃と考えられる通信挙動を持っていること、またcluster1のホストは垂直ポートスキャン攻撃とは考えにくい通信挙動を持っていることが確認できた。垂直ポートスキャン攻撃の検知の閾値は、左上のクラスタの重心をとって、 $PPI = -4.52$, $SPD = 2.98$ とする。また、水平ポートスキャン攻撃の検知の閾値は、垂直ポートスキャン攻撃の検知閾値をSPD軸で反転させ、 $PPI = 4.52$, $SPD = 2.98$ とする。

5.3 スロースキャン攻撃に対する有効性の評価実験

スロースキャン攻撃の検知実験では、まずデータセットに対し、スロースキャン攻撃を行う擬似的なホストの通信データを挿入する。そして、提案手法により、この擬似的なホストを検知できることを確認し、提案手法のスロースキャン攻撃の検知に対する有効性を確認する。本実験において挿入する、擬似的なスロースキャン攻撃を行うホストは、30分あたり15スキャン程度の頻度で水平ポートスキャン攻撃を行うホストとする。一般的なポートスキャンツールであるNmapは、デフォルトで0.2秒あたり1スキャンを実行する。したがって、本実験で挿入する擬似的な水平ポートスキャン攻撃は、十分に低速なスロースキャン攻撃であるといえる。なお、挿入するスキャン攻撃はデータセットの8時14分から14時14分の6時間、利用するデータセットの全時間にわたって挿入する。そして、データセットの1時間分と6時間分に対して提案手法による検知を行う。データセットの時間が長いものになるにつれて、よりスキャン攻撃が進行したものになる。

5.4 スロースキャン攻撃に対する有効性の評価結果と考察

スロースキャン攻撃を行う擬似的なホストの通信データを含むデータセットに対し、PPI, SPDを用いて各ホストをマッピングした結果を図4、図5に示す。青色のプロットがデータセットに含まれるホストのプロットであり、オレンジ色のプロットが擬似的なスキャン攻撃を行うホストのプロットである。そして、赤色の領域が水平ポートスキャン攻撃の検知領域、緑色の領域が垂直ポートスキャン攻撃の検知領域である。

図4、図5より、データセットの時間が長いものであるほど、オレンジのプロットが右上に位置していることが分かる。これは、時間が長くなるにつれて、擬似的なホストによる水平ポートスキャン攻撃が進行し、PPI, SPDがスキャン攻撃の通信挙動をとらえることができたためと考えられる。そして6時間のデータセットを用いた場合のマッ

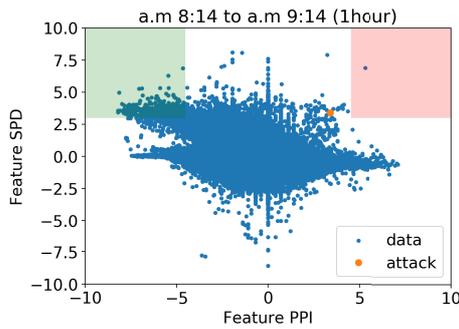


図 4 1 時間のデータセット
Fig. 4 One hour dataset.

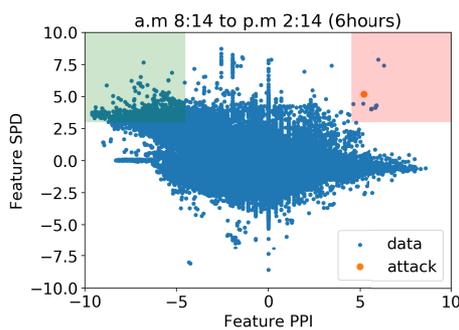


図 5 6 時間のデータセット
Fig. 5 Six hours dataset.

表 5 Snort によるスキャン攻撃の検知結果

Table 5 Detection results of scanning attacks by Snort.

30分あたりのスキャン数	10	100	1,000	10,000
検知結果	×	×	○	○

ピングにおいてオレンジのプロットが赤色の領域、すなわち水平ポートスキャン攻撃の検知領域に含まれていることが確認できる。したがって、低速にスキャンが実行されるスロースキャン攻撃であっても、一定程度スキャン攻撃が進行すると、提案手法によって検知が可能であることが確認できた。また、Snort による検知結果を表 5 に示す。データセットに対して、時間あたりの攻撃頻度を变化させた擬似的な水平ポートスキャン攻撃を挿入し、Snort を用いて検知を試みた結果である。表 5 を見ると、30 分あたり 100 スキャン以下の水平ポートスキャン攻撃は Snort によって検知できないことが確認できた。一方、提案手法では検知に利用する特徴量が時間あたりの攻撃頻度とは無関係の特徴量であるため、いずれのスロースキャン攻撃も検知することができる。本実験によって、提案手法によるスキャン攻撃検知は Snort では検知できないようなスロースキャン攻撃を検知できることが確認できた。

スロースキャン攻撃を行う場合、攻撃者は正常な通信を行うホストと同程度の速度でスキャンを行う。したがって、単位時間あたりのトラフィック量などの情報を基にスキャン攻撃の検知を試みる Snort では、スロースキャン攻撃を検知することは困難である。しかし、本論文で提案し

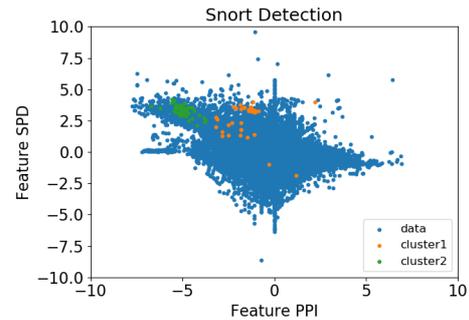


図 6 X-means による攻撃ホストのクラスタリング結果 2
Fig. 6 Attack hosts clustering for datasets on different day.

た PPI と SPD という特徴量はホストの長期的な通信挙動をとらえることのできる特徴量である。したがって、攻撃者のスキャン攻撃の進行をとらえることができ、評価実験においてスロースキャン攻撃を検知することができたと考えられる。

なお、付録 A.1 に今回の実験で検知されたホストのうちいくつかの通信フローデータを示す。表 A-1, A-2 は、今回の実験で水平ポートスキャン攻撃を行っている と検知されたホストの通信フローデータである。表 A-1, A-2 を見ると、これらのホストは単一のホストに対して、多数の宛先ポートを利用して通信を行っていることが確認できる。したがって、これらのホストは水平ポートスキャン攻撃を行っていると考えられる。今回の実験で水平ポートスキャン攻撃を行っている と検知されたホスト 21 個の通信フローデータを確認したところ、すべてこれら 2 つのホストと類似する通信フローデータを持つことが確認できた。一方、表 A-3, A-4 は、今回の実験で垂直ポートスキャン攻撃を行っている と検知されたホストの通信フローデータである。表 A-3, A-4 を見ると、これらのホストは多数のホストに対して、単一の宛先ポート 445 を利用して通信を行っている。445 ポートは、SMB サーバが利用するポートである。SMB サーバには脆弱性があることが知られており、WannaCry というマルウェアの標的とされている。したがって、表 A-3, A-4 の通信フローデータは、WannaCry に感染したホストが次の標的ホストを探すために垂直ポートスキャン攻撃を行っているのではないかと考えられる。今回の実験で垂直ポートスキャン攻撃を行っている と検知されたホスト 1,839 個の通信フローデータのうちいくつかを確認したところ、多くの通信フローデータはこれら 2 つのホストと類似する通信フローデータを持つことが確認できた。したがって、今回の実験で検知されたホストの多くはスキャン攻撃を行うホストであると考えられる。

また、図 6 に、実験と同一のネットワークにおいて別の日に得られたデータセットに対する PPI, SPD を用いた各ホストのマッピング結果を示す。このデータセットの取得日時は 2019 年 10 月 12 日の 14 時 58 分から 15 時 13 分である。このマッピング結果をみると、Snort によって

検知されたホストのクラスタは図3のクラスタと類似したものであることが確認できる。各クラスタのホストの通信フローデータを確認したところ、cluster2のホストは垂直ポートスキャン攻撃と考えられる通信挙動を持っていること、またcluster1のホストは垂直ポートスキャン攻撃とは考えにくい通信挙動を持っていることが確認できた。そして、このデータセットに対して提案手法による検知を行った結果、スキャン攻撃を行っていると考えられるホストを正しく検知できていることを確認した。したがって、本論文で提案した閾値の設定は妥当であり、検知手法の有効性は一般性を持つものであると考えられる。

5.5 分散スキャン攻撃に対する有効性の評価実験

分散スキャン攻撃の検知実験では、データセットに対し、分散スキャン攻撃を行う擬似的なホスト群の通信データを挿入する。そして提案手法により、この擬似的なホスト群を検知できることを確認し、提案手法が分散スキャン攻撃の検知に有効であることを確認する。分散スキャン攻撃の検知実験においては、100台のホストを用いた計1,000スキャンの水平ポートスキャン攻撃を行うホスト群を、擬似的な攻撃ホスト群として挿入する。すなわち1ホストあたり10スキャンのスキャン攻撃を行うものとする。

5.6 分散スキャン攻撃に対する有効性の評価結果と考察

まず、本実験で用いるデータに対し検知にかかる時間を計測し、提案手法とSnortとで比較する。時間計測は5回行い、その平均をとって比較する。実験に用いるデータ形式は、提案手法はNetFlow形式のデータ、SnortはPCAP形式のデータである。NetFlow形式のデータ、PCAP形式のデータともにデータ収集の際にOn-the-Flyに取得できるデータである。また、本実験はXeon E5-2620v4 2.10 GHzの32コアCPU、64GBメモリの物理ハイパーバイザ上でVMを立てて、VM上で行った。VMは8コアCPU、32GBメモリとしており、資源の競合はないことを確認している。時間計測の結果、提案手法による検知にかかる時間は平均 7.7×10 [s]、Snortによる検知にかかる時間は平均 1.5×10^3 [s]であることを確認した。したがって、提案手法はSnortに比べて20倍程度軽量の検知が可能であることが分かる。これは、Snortによる検知では個々の通信データをペイロードまで精査する必要があるのに対し、提案手法による検知では通信データのIPヘッダの情報から得られるデータのみを利用するためであると考えられる。

次に擬似的な分散スキャン攻撃を挿入したデータセットに対する、PPI, SPDを用いたマッピング結果を図7, 図8に示す。図7は、グルーピング処理を加えずに、PPI, SPDを用いた検知を行った結果である。そして、図8は、グルーピング処理を加えたうえで、PPI, SPDを用いた検知を行った結果である。オレンジのプロットが、擬似的に

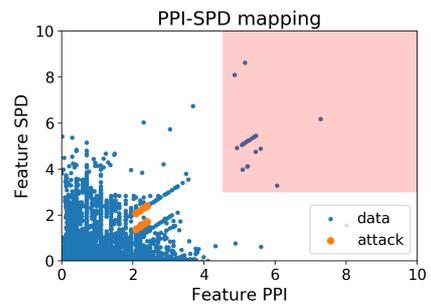


図7 グルーピングを行っていない場合のマッピング結果
Fig. 7 Mapping results without grouping.

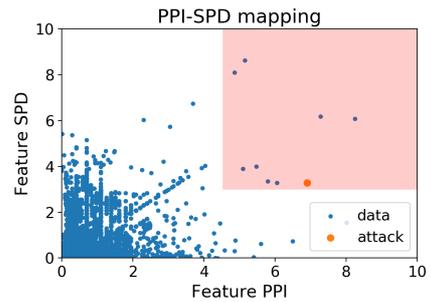


図8 グルーピングを行った場合のマッピング結果
Fig. 8 Mapping results with grouping.

加えた分散スキャン攻撃を行うホストのプロットである。図7を見ると、グルーピング処理を行っていない場合、擬似的な分散スキャン攻撃を行うホストそれぞれのPPI, SPDはともに約2.0程度であり、この分散スキャン攻撃を検知することはできない。しかし、グルーピング処理の結果、分散スキャン攻撃を行うホスト群が1つのグループにまとめられ、PPIは約7.0, SPDは約3.8となり、赤色の領域、すなわち水平ポートスキャン攻撃の検知領域に入っていることが確認できる。したがって、分散スキャン攻撃に対して、グルーピング処理を加えた検知手法が有効にはたらくことが確認できた。一方、Snortには複数台のホストからスキャン攻撃が来た場合に、攻撃ホストをまとめて検知を行うという機能はなく、今回挿入した擬似的な分散スキャン攻撃を検知することはできないということが確認できた。本実験によって、提案手法によるスキャン攻撃検知は、Snortでは検知できないような分散スキャン攻撃を検知できることが確認できた。また、4.3節で示した、データセットに元から含まれていた、分散スキャン攻撃を行っていると考えられるホスト群も、グルーピング処理の結果、1つのグループとしてまとめられることが確認できた。通信データに含まれていた分散スキャン攻撃を行っていると考えられるホスト群は図7のPPIが約5.4, SPDが約5.0の領域に分布するプロットである。これらのホスト群はグルーピング処理の結果、1つにまとめられ、図8においてPPIが約8.2, SPDが約6.0の位置にプロットされている。

分散スキャン攻撃を行う場合、攻撃者は複数のホストを用いてスキャンを行う。したがって、個々のホストのス

キャン攻撃は軽微なものとなり、Snort では分散スキャン攻撃を検知するのは困難である。しかし、提案手法では、PPI, SPD の値の近さと Histogram の類似度を利用してホストのグルーピングを行う。これによって、通信挙動が類似したホストかつ、攻撃の標的を同一とするホストをまとめることができ、評価実験において分散スキャン攻撃を検知することができたと考えられる。

5.7 誤検知と検知漏れについての考察

本論文で提案した特徴量 PPI は 1 つの宛先 IP アドレスあたり、いくつかの種類の宛先ポートを用いて通信を行ったかをとらえる特徴量である。したがって、特定のポートのみを用いて多数のサーバとアクセスするホストに対しては誤検知を起こす可能性がある。たとえば、ネットサーフィンなどといった多数の Web サーバを徘徊するようなホストが、80 ポートのみを用いて多数の Web サーバにアクセスした場合、提案手法では垂直ポートスキャン攻撃を行っているか誤検知を起こす可能性があると考えられる。ただし、このようなホストとポートスキャン攻撃を行うホストの通信挙動の違いとして、攻撃対象となる宛先 IP アドレスもしくは宛先ポートに対して重複した通信を行うか否かという点があげられる。したがって、宛先 IP アドレスもしくは宛先ポートに重複した通信を行っているか否かを精査することでこのような誤検知を回避できると考えられる。また、水平ポートスキャン攻撃と垂直ポートスキャン攻撃を混合して行うようなスキャン攻撃を考えた場合、PPI の値がゼロに近い値となりうることが考えられる。したがって、本論文の提案手法ではこのようなスキャン攻撃に対し検知漏れを起こす可能性があると考えられる。

6. 結論

本論文では、正常な通信とスキャン攻撃の通信挙動の違いをとらえることのできる、時間依存性を持たない特徴量と、提案した特徴量を用いたスキャン攻撃の検知手法の提案を行った。評価実験では、擬似的なスロースキャン攻撃を行うホストと、擬似的な分散スキャン攻撃を行うホストを準備し、提案手法の検知性能についての評価実験を行うことで、提案手法がスロースキャン攻撃や分散スキャン攻撃の検知において有効であることを確認した。

参考文献

- [1] 進入検知および進入防止システム (IDPS) に関するガイド, 入手先 (<https://www.ipa.go.jp/files/000025364.pdf>).
- [2] Yamashita, T., Miyamoto, D., Sekiya, Y. and Nakamura, H.: Slow scan attack detection based on communication behavior, *2020 the 10th International Conference on Communication and Network Security (ICCNS 2020)* (2020).
- [3] Wagner, A. and Plattner, B.: Entropy based worm and anomaly detection in fast IP networks, *14th IEEE Inter-*

national Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise (WETICE '05), pp.172–177, IEEE (2005).

- [4] Berezinski, P., Jasiul, B. and Szpyrka, M.: An entropy-based network anomaly detection method, *Entropy (Basel, Switzerland)*, Vol.17, No.4, pp.2367–2408 (2015).
- [5] Nychis, G., Sekar, V., Andersen, D., Kim, H. and Zhang, H.: An empirical evaluation of entropy-based traffic anomaly detection, *Proc. 8th ACM SIGCOMM Conference on Internet Measurement*, pp.151–156, ACM (2008).
- [6] Lu, W. and Ghorbani, A.A.: Network anomaly detection based on wavelet analysis, *EURASIP Journal on Advances in Signal Processing* (2009).
- [7] Huang, C.-T., Thareja, S. and Shin, Y.-J.: Wavelet-based real time detection of network traffic anomalies, *2006 Securecomm and Workshops*, pp.1–7, IEEE (2006).
- [8] Cordero, C.G., Hauke, S., Muhlhauser, M. and Fischer, M.: Analyzing flow-based anomaly intrusion detection using replicator neural networks, *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, pp.317–324, IEEE (2016).
- [9] Yu, Y., Long, J. and Cai, Z.: Network intrusion detection through stacking dilated convolutional autoencoders, *Security and Communication Networks*, Vol.2017, pp.1–10 (2017).
- [10] Thing, V.L.L.: IEEE 802.11 network anomaly detection and attack classification: A deep learning approach, *2017 IEEE Wireless Communications and Networking Conference (WCNC)*, pp.1–6, IEEE (2017).
- [11] Al-Qatf, M., Lasheng, Y., Al-Habib, M. and Al-Sabahi, K.: Deep learning approach combining sparse autoencoder with SVM for network intrusion detection, *IEEE Access*, Vol.6, pp.52843–52856 (2018).
- [12] Kim, J. and Lee, J.-H.: A slow port scan attack detection mechanism based on fuzzy logic and a stepwise policy, *4th International Conference on Intelligent Environments (IE '08)* (2008).
- [13] El-Hajj, W., Aloul, F., Trabelsi, Z. and Zaki, N.: On detecting port scanning using fuzzy based intrusion detection system, *2008 International Wireless Communications and Mobile Computing Conference*, pp.105–110, IEEE (2008).
- [14] Almseidin, M., Al-Kasassbeh, M. and Kovacs, S.: Detecting slow port scan using fuzzy rule interpolation, *2019 2nd International Conference on New Trends in Computing Sciences (ICTCS)*, pp.1–6, IEEE (2019).
- [15] MFP の脆弱性に関する調査報告書, 入手先 (<https://www.ipa.go.jp/files/000014073.pdf>).
- [16] Arkko, J., Cotton, M. and Vegoda, L.: IPv4 Address Blocks Reserved for Documentation, RFC 5737 (2010).

付 録

A.1 検知されたホストの通信フローデータ

A.1.1 水平ポートスキャン攻撃を行っているか判断されたホスト

検知の結果、水平ポートスキャン攻撃を行っているか判断されたホストは 21 個あることが確認できた。これらのホストのうち 3 つを表 A.1、表 A.2 に示す。

表 A.1 水平ポートスキャンと判断された通信フローデータ 1

Table A.1 Communication flow data considered to be a horizontal port scan attack 1.

srcIP	srcPort	dstIP	dstPort
192.0.2.80	32766	198.51.100.77	9355
192.0.2.80	32766	198.51.100.77	52661
192.0.2.80	32766	198.51.100.77	17435
...
192.0.2.80	32766	198.51.100.77	35585
192.0.2.80	32766	198.51.100.77	32971

表 A.2 水平ポートスキャンと判断された通信フローデータ 2

Table A.2 Communication flow data considered to be a horizontal port scan attack 2.

srcIP	srcPort	dstIP	dstPort
203.0.113.15	6838	198.51.100.24	6400
203.0.113.15	6838	198.51.100.24	2816
203.0.113.15	6838	198.51.100.24	14592
...
203.0.113.15	6838	198.51.100.24	16640
203.0.113.15	6838	198.51.100.24	11008

表 A.3 垂直ポートスキャンと判断された通信フローデータ 1

Table A.3 Communication flow data considered to be a vertical port scan attack 1.

srcIP	srcPort	dstIP	dstPort
198.51.100.7	47827	203.0.113.32	445
198.51.100.7	47827	203.0.113.11	445
198.51.100.7	47827	203.0.113.71	445
...
198.51.100.7	47827	203.0.113.20	445
198.51.100.7	47827	203.0.113.9	445

表 A.4 垂直ポートスキャンと判断された通信フローデータ 2

Table A.4 Communication flow data considered to be a vertical port scan attack 2.

srcIP	srcPort	dstIP	dstPort
192.0.2.81	51993	203.0.113.5	445
192.0.2.81	51993	203.0.113.49	445
192.0.2.81	51993	203.0.113.63	445
...
192.0.2.81	51993	203.0.113.56	445
192.0.2.81	51993	203.0.113.48	445

A.1.2 垂直ポートスキャン攻撃を行っていると思われるホスト

検知の結果、垂直ポートスキャン攻撃を行っていると思われるホストは、1,839 個あることが確認できた。これらのホストのうち 3 つを表 A.3、表 A.4 に示す。



山下 智也

2019 年東京大学工学部計数工学科卒業。2021 年同大学院情報理工学系研究科システム情報学専攻修士課程修了。2021 年日本電信電話に入社。AI セキュリティの研究に従事。



宮本 大輔 (正会員)

2000 年関西学院大学商学部卒業。2009 年奈良先端科学技術大学院大学情報科学研究科で博士(工学)学位取得。情報通信研究機構、東京大学情報基盤センター、奈良先端科学技術大学院大学を経て 2018 年より東京大学情報理工学系研究科准教授。サイバーセキュリティ、データマイニングの研究に従事。



関谷 勇司 (正会員)

1997 年京都大学総合人間学部卒業。2005 年慶應義塾大学大学院政策・メディア研究科後期博士課程修了。博士(政策・メディア)。USC/ISI 訪問研究員、東京大学情報基盤センター助手、講師、准教授を経て 2019 年より東京大学情報セキュリティ教育研究センター教授。ソフトウェアネットワーク技術、サイバーセキュリティに関する研究に従事。デジタル庁シニアネットワークエンジニア兼務。



中村 宏 (正会員)

1985 年東京大学工学部電子工学科卒業。1990 年同大学院工学系研究科電気工学専攻博士課程修了。工学博士。筑波大学電子・情報工学系助手、同講師、同助教授を経て 1996 年東京大学先端科学技術研究センター助教授。2010 年東京大学大学院情報理工学系研究科教授。2019 年より東京大学情報セキュリティ教育研究センター長を兼務。省電力コンピューティング、高性能・低消費電力 VLSI システム、サイバーセキュリティの研究に従事。本会フェロー。