A Parameterless Learning Algorithm for Behavior-based PortScan Detection and its Evaluation

王, 璨
九州大学システム情報科学研究院 | 九州先端科学技術研究所

馮, 尭鏘
九州大学大学院システム情報科学研究院 | 九州先端科学技術研究所

川本, 淳平
九州大学大学院システム情報科学研究院 | 九州先端科学技術研究所

堀, 良彰
佐賀大学全学教育機構 | 九州先端科学技術研究所

他

出版情報：Symposium on Cryptography and Information Security. 2015, pp.1A1-2-, 2015-01-20
バージョン：
権利関係：

SCIS 2015 The 32nd Symposium on
Cryptography and Information Security
Kokura, Japan, Jan. 20- 23, 2015
The Institute of Electronics,
Information and Communication Engineers

挙動に基づくポートスキャン検知に向けたパラメータなしの学習アルゴリズムの提案とその性能評価

A Parameterless Learning Algorithm for Behavior-based PortScan Detection and its Evaluation

王 サン*‡　フォン ヤオカイ*‡　川本 淳平*‡　堀 良彰†‡

Can Wang　Yaokai Feng　Junpei Kawamoto　Yoshiaki Hori

櫻井 幸一*‡

Kouichi Sakurai

あらまし　近年，インターネットが益々便利になると共に，ネットの安全性確保が一つの課題になってきた．多くの攻撃者は本格的な攻撃を行う前に良くポートスキャンという技術を利用し，ターゲットの弱点を探す．この準備段階のスキャンを検知できれば，本格的な攻撃への対処が容易になる．そのため，ポートスキャンの早期検知が重要な課題の一つである．挙動に基づく検知手法は学習データから抽出した通常モードを利用して異常検知を行うため，事前に通常と異常を分類する閾値を決める必要がないという利点がある．挙動に基づく検知手法では，通常モードを抽出するために，事前に与えられた度数分布図に対して学習アルゴリズムを適用する．しかしながら，度数分布図に学習アルゴリズムを適用する際，パラメータチューニングが必要であるという問題がある．それを解決するために，本研究では挙動に基づく検知手法において，パラメータなしの学習アルゴリズムを提案する．また，討議および実験により，本提案の学習アルゴリズムはインターネット攻撃の検知に有効であることを示す．

キーワード　ネットワークセキュリティ，ポートスキャン，挙動に基づく検知，学習アルゴリズム

1　はじめに

近年, インターネットの利用率が益々高くなってきている．総務省によると，平成 25 年インターネットの利用率は 82.8%であり，近年の最大値となっている．その中で，81.4%の利用者は個人情報の保護に不安を感じている[1]. そのため, 安全・安心なインターネット環境を構築することが重要な課題である．特に，個人や企業の知らないところで, 機密情報が不正者に窃取されると，大きな損失となり得る．そこで，多くの研究者がサイバー攻撃に関する研究を行ってきた. しかし, 発生している攻撃の検知や防御, また潜在的な脅威の予測などは未解決な課題である.

サイバー攻撃を検知するために, 様々な手法が提案されてきた．侵入検知システム（IDS）や侵入阻止システム（

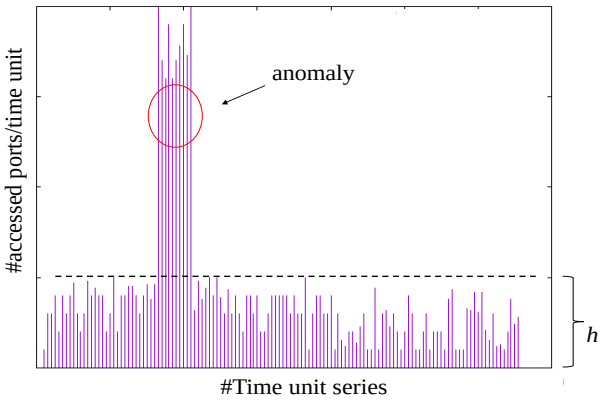

図 1 挙動に基づく手法の一例

* 九州大学システム情報科学研究院, 福岡県福岡市西区元岡 744 番地,
† 佐賀大学全学教育機構, 佐賀県佐賀市本庄町 1 番地
‡ 九州先端科学技術研究所, 福岡市早良区百道浜 2 丁目 1 番地 22 号 福岡 SRP センタービル 7 階

IPS）は，よく利用される技術の一つである．侵入検知システムは IP パケットをモニタリングすることで不審なアクセスをリアルタイムで検知するシステムである[2]．そこでシは，グネチャー型 IDS と異常検出型 IDS などの種類がある．シグネチャー型 IDS では事前に設定されるルールやシグネチャーで不正侵入を検知する．適当なシグネチャーがあれば検知率が高いというメリットがあるが，未知の攻撃への対応ができない[3]．異常検出型 IDS は通常挙動モードを抽出し，それを用いて異常検知を行う．通常モードをうまく抽出できれば，未知な攻撃も検知することができる．異常検出型の検知手法として，D. E. Denning は挙動に基づく検知手法を提案した[4]．図 1 は挙動に基づく検知手法を示す．横軸は時間単位の時系列で，縦軸の定義は応用により違う．この例では、縦軸は各時間単位にアクセスされた終点ポート数を示す．図 1 に示したように，通常な状況ではアクセスされた終点ポートの数が h を超えない．一方，丸で囲まれる部分では，トラフィック時間単位ごとにアクセスされた終点ポートの数が特に大きいため，それを異常とみなす．このような場合では *h* を通常モードと呼ぶ．もし過去のデータから *h* の範囲を抽出できれば，異常を簡単に検知できる．従って，過去のデータから通常モードを抽出することは，挙動に基づく検知手法における異常検知の核心になる．十分な時間に渡るノイズの少ないデータがあれば通常モードは簡単に抽出できる．しかし，現実的にはそのような状況は難しい．そのため，観測データにノイズが含まれている状況でも通常モードを抽出する学習アルゴリズムが必要である．Feng らは，そのような学習アルゴリズムの一つである FHST アルゴリズム[5]を提案している．本研究ではその学習アルゴリズムを FHST 学習アルゴリズムと呼び，第三章で詳しく紹介する．

挙動に基づく検知手法はいくつかのメリットがある．例えば，監視する実際のネットワークのトラフィック特徴を反映することができることと，実際の通信状況によって通常モードは自動的に更新できることが挙げられる．更に，同じネットワークに対しても，幾つかの通常モードを抽出すれば，異なる状況にも対応できる[5]．従って， 挙動に基づく検知手法はよく注目されてきた．挙動に基づく検知手法において，学習アルゴリズムは核心な役割を担っている．しかしながら，既存の学習アルゴリズムでは，幾つかのパラメータを事前に設定しなければならない．FHST アルゴリズムでも，二つのパラメータを利用している．

本研究では，挙動に基づく検知手法に向けて、初めてパラメータのチューニングが要らない学習アルゴリズムを提案した．実験の結果により，過去のデータから抽出された通常モードは信頼性と応用性があることを示した．また，本研究はポートスキャンを具体例として学習アルゴリズムの仕組みを検証したが，ポートスキャン攻撃に限らず，他のサイバー攻撃（例えば分散型 DOS 攻撃など）も検知できる．異なる種類の攻撃を検知する場合は，攻撃種類ごとに度数分布図を作成すれば良い．

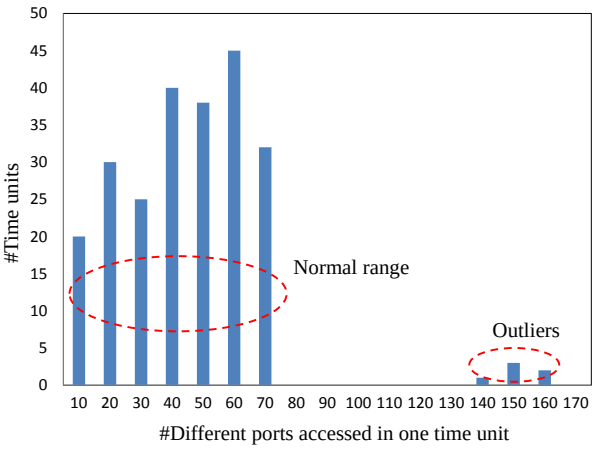

図 2 時間単位内にアクセスされたポート数の度数分布図

本稿の構成を以下に示す．第 2 章はポートスキャンに関する予備知識を紹介する．第 3 章は挙動に基づくポートスキャン検知を説明する．第 4 章は FHST 学習アルゴリズムを紹介し，第 5 章が本研究の中核な部分として，パラメータが必要でない学習アルゴリズムを提案する．第 6 章は実験結果を示す．第 7 章は結論と今後の課題である．

2 ポートスキャン

不正者はターゲットの計算機へ侵入するために，ターゲットの脆弱性情報を収集することが多い[6]．そこで，ポートスキャンという技術がよく用いられる．ポートスキャンによってセキュリティホールを発見すると，本番の攻撃を行うことができる．ポートスキャンは危険性が高い行為であるため，その早期検知は課題になってきた．

ポートスキャンは一般的に 4 つの種類がある[5]．

1) Vertical Scan：単一な始点 IP アドレスからある標的のホストに対して，そのホストの幾つか（もしくはすべて）のポートをスキャンする行為．
2) Horizontal Scan：単一な始点 IP アドレスからある脆弱性があるポートに対して，複数のホストをスキャンする行為．
3) Distributed Vertical Scan：複数の始点 IP アドレスから標的なホストの複数のポートをスキャンする行為．
4) Distributed Horizontal Scan：複数な始点 IP アドレスからある脆弱性があるポートに対して，複数のホストをスキャンする行為．

表 1 挙動に基づくポートスキャン検知

1. 学習データを収集
2. 各時間単位内にアクセスされたポート数を集計
3. 度数分布図を作成
4. 学習アルゴリズムで度数分布図から通常モードを抽出
5. 異常検知

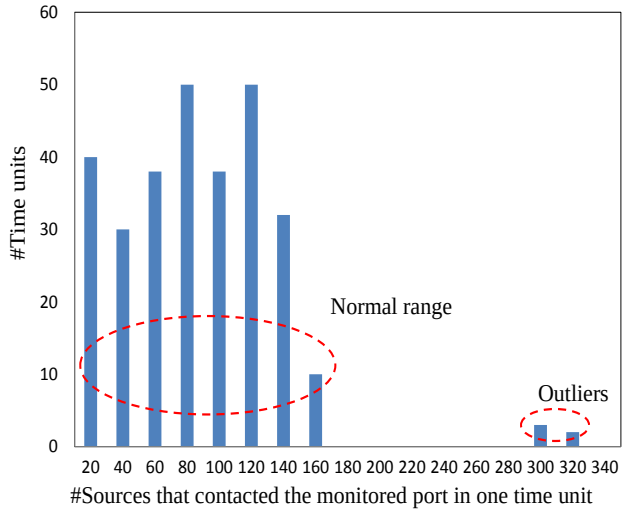

図 3　Feng ら提案で用いた度数分布図

表 2　FHST 学習アルゴリズム初期化

Input: Frequency Distribution of the number of accessed different ports in one time unit **Output**: Normal behavior mode	
	Descriptions
Initializing	**Input**: Frequency Distribution diagram **Output**: Normal behavior mode ***α***:*A* Threshold **β%**:*Another* Threshold ***d***: Distance to the next bin **Ω**: Group of checked bins **Area(Ω)**: The number of time units in Ω

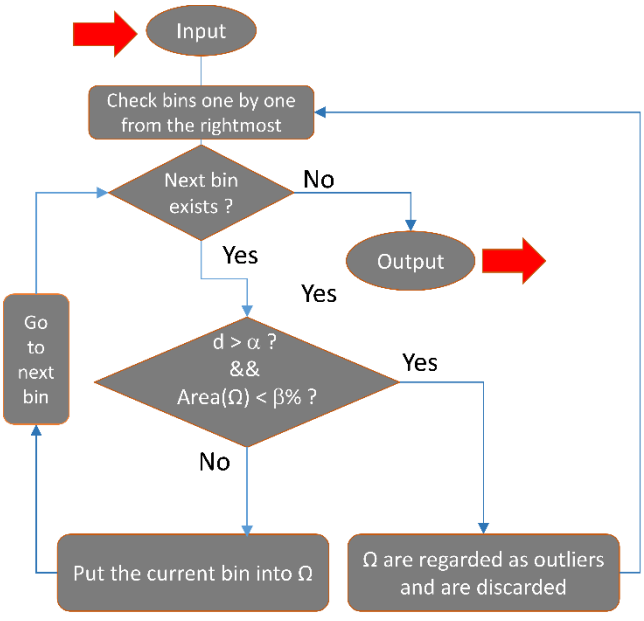

図 4　FHST 学習アルゴリズム

また，攻撃者はポートスキャンを極力隠したいため，よく stealth scan を行う[7]．例えばスキャン頻度を下げてスローポートスキャンを行ったり[8, 9]，SYN パケットを送ってポートの状況を確認したりすることを行う[10]．

上記の 3 番目と 4 番目は分散型スキャンのため，高度なスキャン攻撃だと考えられている[11]．本研究の学習アルゴリズムを説明するために，3 番目の Distributed Vertical Scan を例とする．これから本稿に言及されるポートスキャンは，Distributed Vertical Scan を指す．

3　挙動に基づくポートスキャン検知

3.1　一般的な流れ

挙動に基づくポートスキャン検知手法の一般的な流れを表 1 に示す．　ステップ 1 で学習データを収集し，ステップ 2 で各時間単位内にアクセスされたポート数を集計する．その後，ステップ 3 として度数分布図を描く．ステップ 4 は，学習アルゴリズムを利用して度数分布図から通常モードを抽出する．最後に通常モード（閾値）と比較することにより異常検知を行う．

上記のステップ 1、ステップ 2 とステップ 5 は単純な処理のため，ステップ 3 とステップ 4 を詳しく説明する．

表 3　本研究の学習アルゴリズム初期化

Input: Frequency Distribution of the number of accessed different ports in one time unit **Output**: Normal behavior mode	
	Descriptions
Initializing	**Left_Pointer**: pointing to endpoint of the left-most 1st bin-group **Right_Pointer**: pointing to the end point of the right-most bin-group **Span**: the difference between right-most and the left-most bins **Total_area**: summation of all bins **Dist_right**: the distance between Left_Pointer and its right-neighboring bin-group **Dist_left**: the distance between Right_Pointer and its left-neighboring bin-group **Area_right**: the area of the Left_Pointer's right-neighboring bin-group **Area_left**: the area of the Right_Pointer's left-neighboring bin-group

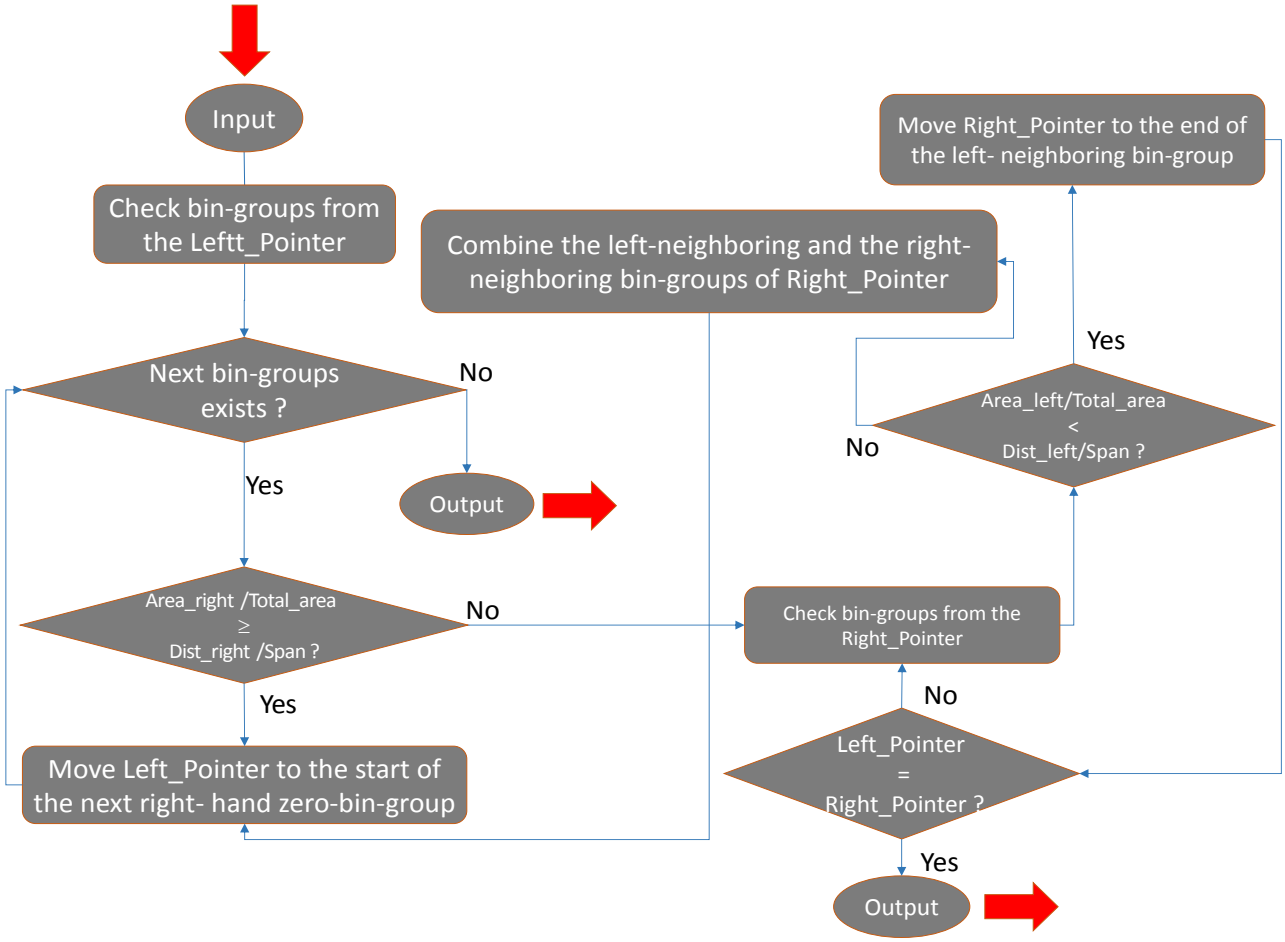

図 5　本研究で提案した学習アルゴリズム

通常モードを抽出するための度数分布図の作成方法を説明する．まず，アクセスされたポート数の範囲はを量子化させ，bin の形で横軸を表示する．次は各 bin に対して発生した時間単位数を集計して縦軸を構成する．図 2 は度数分布図の一例である。例えば，縦軸は 49 であり，横軸は 40 から 50 までの場合は，学習期間の内に 49 個の時間単位が，アクセスされたポート数は 40 から 50 までの範囲であったことを意味する．

3.2　FHST 学習アルゴリズム

本章は，Feng らに提案された学習アルゴリズムを紹介する．検知段階から論じると，もしあるポートに対して現在の送信元ホスト数は過去のデータから抽出した通常モードを超えたら，アラートを出す [3]．その度数分布の一例は図 3 で示す．ただし，検知対象は違うので横軸ラベルが図 2 と異なる．学習アルゴリズムの仕組みは表 2（初期化部分）と図 4（主体部分）で表している．

4　パラメータなしの学習アルゴリズムの提案

提案した学習アルゴリズムの目的は度数分布図から通常モードを抽出し，異常検知のための閾値設定をパラメータを用いず自動化すること．攻撃者はスキャンすることによりできるだけ多くの情報を収集したいため，一定期間内に多くのポートをアクセスすることはポートスキャンの特徴だと考えられる．既存のポートスキャンの特徴を度数分布図に反映させれば，新たに行われるより多数のポートへのスキャン通信はヒストグラムの右側に集まることになる．そのため，度数分布図の両側からすべての bin をチェックして通常に分類される bin-group と異常に分類される bin-group を区別できれば閾値を学習できる．そこで，本提案の学習アルゴリズムは 2 つのポインタを度数分布図の両側に設置し，各々を内側に向かって移動させることにより，出会った点を閾値とする．

本研究に提案した学習アルゴリズムは表 3（初期化部分）と図 5（主体部分）で説明する．そこで，すべての bin は幾つかの zero-bin に分割されているとする．ただ一つの bin-group しか存在しない場合は，このような bin-group をすべて正常通信だと仮定し，この bin-group の右端を学習結果とする（ステップ 1）．bin-group の面積はその bin-group にあるすべての bin の度数の合計を意味する．

5　実験

学習アルゴリズムを適用する前には，度数分布図を作成する必要がある．そこで，時間単位と bin 幅を決める必要

がある．我々の先行研究[12]では，この二つのパラメータがどのように学習の結果を影響するかを調査した．しかし，そこで使ったダークネットデータセットは，ground-truth はないので検知性能を評価できていない．

その発展として，本稿では提案学習アルゴリズムの学習性能を実証した上で，データを人工的に作ってポートスキャン検知に応用する際の検知性能を具体的に検証する．

6.1 データ

今回作ったデータは，当研究室のサーバで収集されたものである．研究室が外部との通信は，すべてこのサーバを経由しているため，日常的な Web 観覧や電子メールなどの通信ログを記録されている．本実験ではこのような通信を正常通信として扱う．

一方，攻撃を含まれる異常データを作るために，Nmap というオープンツールを利用した．Nmap は，ポートスキャン機能や OS 検出機能など多くの機能を兼ね備えているため，セキュリティスキャナとしてよく利用される[13].

1) 学習データ

本実験は正常通信と異常通信を混在している 2 日間のトラヒックデータ（2014 年 11 月 8 日－2014 年 11 月 9 日）のトラフィックデータを学習データとする．具体的には，Nmap を使って 4 パターンのスキャン攻撃を行い，それぞれの学習結果を分析する．それにより，混ぜた異常通信の状況が変わったら学習結果にどのように影響するかについて検証する．

2) テストデータ

テストデータは次の 2 日間（2014 年 11 月 12 日－2014 年 11 月 13 日）にそれぞれ 1 回のスキャン攻撃を行って収集されたトラフィックデータである．

6.2 度数分布の作成

今回の実験は研究室のサーバでデータを収集するため，ダークネットのように大量な通信トラフィックを扱っていない．従って，この度は時間単位と Bin 幅を小さい数値で設定すれば提案の学習アルゴリズムの検知性能を実証することができると考えられる．今回の実験は時間単位を 3 分，Bin 幅を 2 とする．

6.3 学習結果

本セッションでは，次の 4 つのパターンのポートスキャン攻撃を実際に行い，各パターンの異常通信を混在した場合にどのように学習結果を影響するか検証する．

パターン 1 は，1 種類のスキャン攻撃を行った．そのスキャン攻撃は高速スキャンと呼ばれ，短期間で多くのポートをスキャンできるという利点があるため，よく使われる手段の一つである．そこで，その攻撃が含まれるデータを収集して度数分布図を作成した．学習結果は図 6 のように示した．学習結果は 33 のところであった．

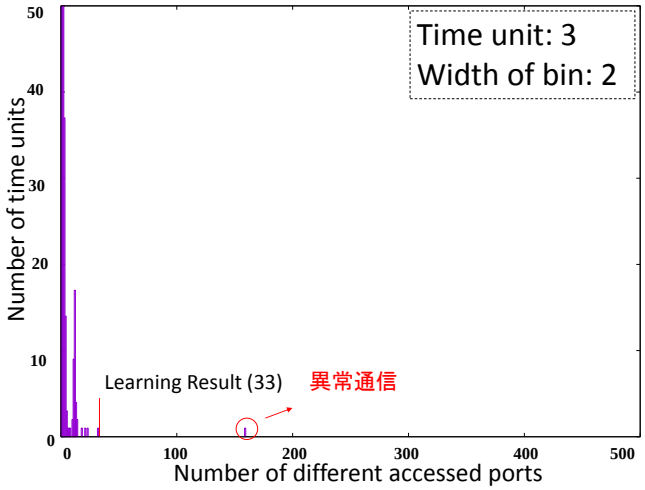

図 6　度数分布図（パターン 1 の場合）：学習結果＝33

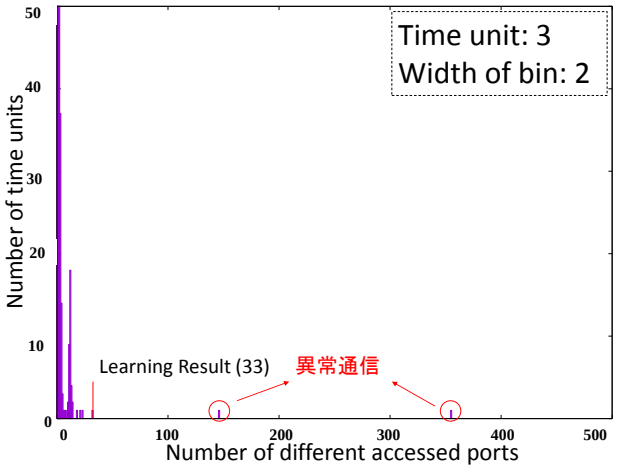

図 7　度数分布図（パターン 2 の場合）：学習結果＝33

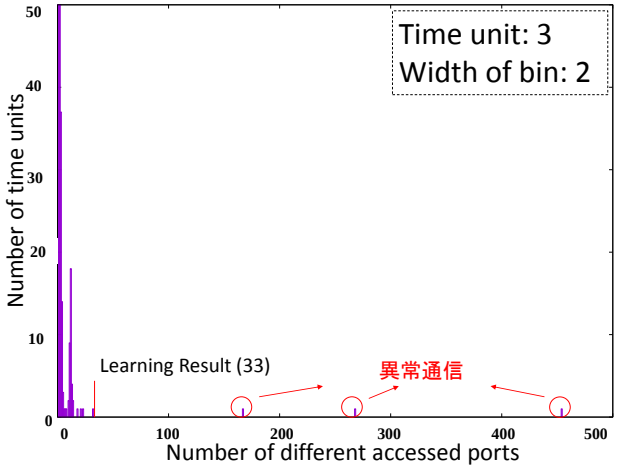

図 8　度数分布図（パターン 3 の場合）：学習結果＝33

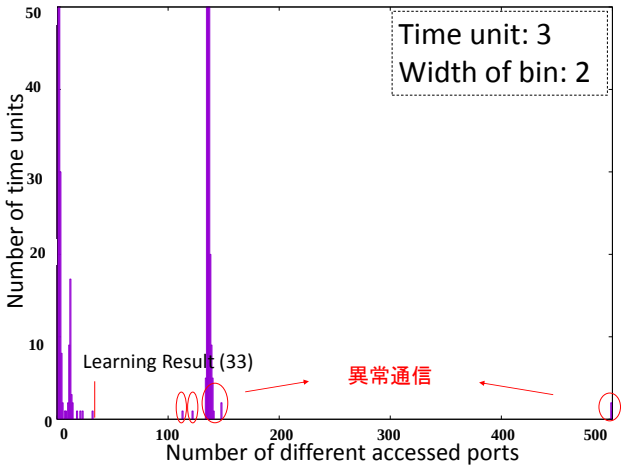

図 9　度数分布図（パターン 4 の場合）：学習結果＝33

パターン 2 は，2 種類のスキャン攻撃を行った．1 つは高速スキャンであり，もう 1 つはデフォールトスキャンである．デフォールトスキャンとは， nmap のデフォールト設定をそのまま利用してスキャンを行う手法である．初心者でもすぐ使えるので，簡単という利点がある．そこで，提案の学習アルゴリズムを適用すると，同じく 33 というところで図 7 から学習結果が得られた．

パターン 3 は，3 種類のスキャン攻撃を行った．2 つはそれぞれ高速スキャンとデフォールトスキャンであり，新規の 1 つはノーマルスキャンである．ノーマルスキャンとは， 高速スキャンより遅い速度でスキャンを行うことである． そこで，学習結果は図 8 に示したように，33 である．

パターン 4 は，前述した 3 つのスキャンのほかに，スローポートスキャンを加えた．スローポートスキャンとは，スキャン速度を極力下げて，スキャンにかかる時間を代価として秘匿性を得る手法である．スローポートスキャンは検知システムに発見されにくいので，危険性が高いと思われる．そこで，図 9 に示したように，この場合でも学習結果は 33 になるので，本提案の学習アルゴリズムがスローポートスキャンでも検知できるという結論を確認できた．

図 6 から図 9 まではスキャン通信を含まれる各パターンの度数分布図である．6.1 節は時間単位と Bin 幅が度数分布図に対するどのような影響があるかについて論じした．今回は大量なデータを扱っていないため，時間単位と Bin 幅を小さい数値で設定した．ここではそれぞれ 3 と 2 になる．

以上の実験結果より，違う種類の異常通信が含まれても学習結果が変わらないことを示した．それは，本研究で提案した学習アルゴリズムはロバストであることを意味する．

6.4 学習アルゴリズムの実行時間

データを収集するのは時間がかかるので，6.2 節の実験はすべて 2−3 日間（500MB 程度）のデータしか扱っていない．実験環境は Core i7 4960k の CPU と 8G のメモリに構築される仮想マシンである．そこで，収集されたデータで度数分布図を作ってから学習アルゴリズムの処理時間は 1 秒以内に収まった．度数分布図を作る時間を含めれば 10 秒に過ぎないという結果を得た．データ量が大きくなっても，学習アルゴリズムの実行時間は Bin の数と Bin の分布しか依存しないので，データ量の多少と関係がない．しかしながら，度数分布を作成するにかかる時間は，データ量とは線型関係である．全てのデータを 1 回スキャンする必要があるからである．

6.5 提案した学習アルゴリズムのポートスキャン検知への応用

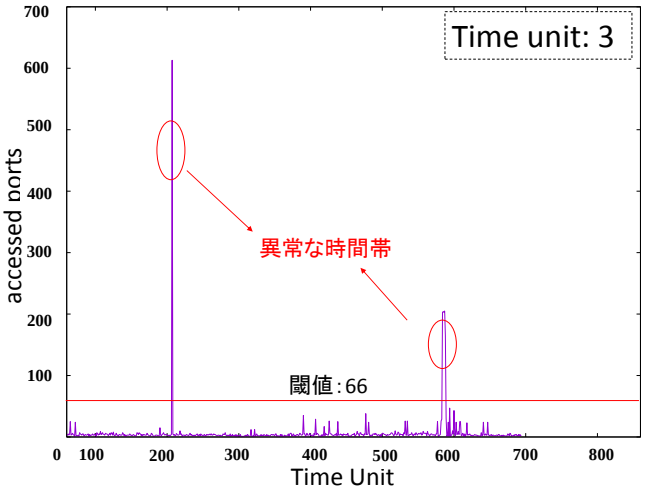

図 10　テストデータ：通信トラフィック時系列

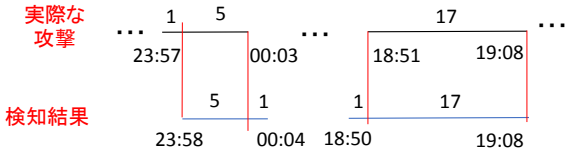

図 11　テストデータ：実際に攻撃があった時間帯

表 4　検知結果の評価

検知率	誤検知率	見逃し率
$\frac{5+17}{6+17}$ =95.7%	$\frac{1+1}{6+18}$ =8.3%	$\frac{1}{6+17}$ =4.3%

今までの実験は，データの状況が変わると学習結果に対しての影響を考察した．そこで，本番な検知段階であれば，得られた学習結果がどの程度の攻撃を検知できるかということについて検証したい．本節は，学習で得られた閾値を検知に適用し，検知率、誤検知率と見逃し率を計算する．

学習アルゴリズムより，学習データから得られた学習結果は 66（33×2）になっている．ここで，33 は bin の通し番号であり，2 は bin 幅である．66 を閾値としてテストデータに適用すると，図 10 のように 2 つの時間帯を異常として検知できた．

今回のテストデータは異常通信を事前に記録されたので，それによって検知率や誤検知率を計算できる．そこで，実際攻撃の時間範囲と検知結果は図 11 で示す．図 11 では 1 分間を最小単位とし，検知率などを計る．検知結果の評価は表 4 で示す．

以上の実験結果より，提案した学習アルゴリズムの学習結果をポートスキャン検知に応用すれば，95%以上の検知率を達成した．

6　結論と今後の課題

本稿では挙動に基づく検知手法に対して，学習アルゴリズムの重要性を論じた．そこで，一般的な学習アルゴリズムはパラメータが必要であり，またパラメータを事前に決めるのが難しいという問題点がある．本研究では二つのポインタを利用することにより，パラメータが必要でない学習アルゴリズムを提案した．実験の結果により，提案学習アルゴリズムの有効性を示した．また，実験はポートスキャン攻撃の検知を注目したが，度数分布を作成する際に統計対象が変われば提案した学習アルゴリズムは他の異常検知にも利用できる．

今後の課題として，データをより多く収集した上で更なる提案の性能を実証する．また，本提案の学習アルゴリズムを他の検知（分散型攻撃など）に応用し，性能の実証を行う．

謝辞

この研究の一部は，総務省による「国際連携によるサイバー攻撃の予知技術の研究開発」および科学研究費（基盤研究（C) No. 25330131)の支援を受けている．

本研究を実施するにあたり，独立行政法人情報通信研究機構(NICT)よりダークネット観測データの提供を受けた．ここに記して謝意を表す．

参考文献

[1] 総務省：平成 26 年版情報通信白書，総務省（オンライン），入手先〈http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h26/html/nc253120.html〉（参照 2014-12-5）

[2] 山田正平，見神宏紀，木村啓二 ほか: 不正侵入検知システムにおけるマルチコア上でのシグネチャ割当によるレイテンシ削減手法，情報処理学会研究報告 2014-ARC-209(2), pp.1-8 (2012)

[3] C.Modia, D. Patela, B.Borisaniya, et al: A survey of intrusion detection techniques in Cloud, *Journal of Network and Computer Applications*, Vol.36, No.1, pp.42-57 (2013).

[4] D. E. Denning: An Intrusion-Detection Model, *IEEE Transactions on Software Engineering - Special issue on computer security and privacy*, Vol.13 No.2, pp.222-232 (1987).

[5] Y. Feng, Y. Hori, K. Sakurai, et al: A Behavior-Based Method for Detecting Distributed Scan Attacks in Darknets, *Journal of Information Processing*, Vol.21, No.3, pp.527-538 (2013).

[6] 情報処理推進機構：セキュリティ担当者のための脆弱性対応ガイド，情報処理推進機構（オンライン），入手先〈http://www.ipa.go.jp/files/000024184.pdf〉（参照 2014-12-5）

[7] 情報処理推進機構：ポートスキャン，情報処理推進機構（オンライン），入手先〈https://www.ipa.go.jp/security/fy14/contents/soho/html/chap1/scan.html〉（参照 2014/12/5）

[8] M.Dabbagh, A.Ghandour, K.Fawaz, et al: Slow Port Scanning Detection, *Proc. 7th International Conference on Information Assurance and Security* (IAS2011), pp.228-344 (2011).

[9] L.Aniello, G.Lodi, R.Baldoni: Inter-Domain Stealthy Port Scan Detection through Complex Event Processing, *Proc. the 13th European Workshop on Dependable Computing*, pp.67-72 (2011).

[10] M.Chowdhary, S.Suri and M.Bhutani: Comparative Study of Intrusion Detection System, *International Journal of Computer Sciences and Engineering* (JCSE), Vol.2, No.4, pp.197-200 (2014).

[11] J. Gadge,J and A. A. Patil: Port scan detection, *Proc. 16th IEEE International Conference on Networks* (ICON 2008), pp. 1-6 (2008).

[12] C.Wang, Y.Feng and J.Kawamoto, et al: A Parameterless Learning Algorithm for Behavior-Based Detection, *Proc. The 9th Asia Joint Conference on Information Security* (AsiaJCIS2014) (2014)

[13] Nmap: Intro, Nmap (oline), available from 〈http://nmap.org/〉 (accessed 2014-12-15)