4W-03

# DBSCANによるクラスタ出現確率を用いたマルウェア感染由来のHTTPトラフィック検知

小川 秀貴† 山口 由紀子†† 嶋田 創†† 高倉 弘喜††† 秋山 満昭†††† 八木 毅††††

†名古屋大学情報科学研究科 ††名古屋大学情報基盤センター †††国立情報学研究所 ††††NTTセキュアプラットフォーム研究所

## 1 はじめに

昨今，サイバー攻撃が深刻化しており，以前のような愉快犯による攻撃と異なり，特定の個人や組織を標的とした標的型攻撃が増加している．独立行政法人情報処理推進機構（IPA）によると高度標的型攻撃は主に，計画立案，攻撃準備，初期侵入，基盤構築，内部侵入・調査，目的遂行，再侵入の7つの段階で構成されている[1]．特に初期侵入は巧妙化しており，従来対策でマルウェア感染を完全に防ぐことが困難な状況となっている．そこで，初期侵入後の段階におけるマルウェア感染検知技術が求められている．

## 2 提案手法

**概要** 我々はこれまでk-means++によるクラスタ出現確率を用いて基盤構築段階後のマルウェアが発するHTTPトラフィックを検知する手法を提案してきた[2]．しかし，従来手法では最適なクラスタ数を指定する必要があり，最適なクラスタ数の探索コストが大きいという課題点がある．

そこで，本論文ではクラスタリングの際に，クラスタ数を自動で決定することのできるDBSCANを用いることで，クラスタ数の探索コストを軽減したマルウェア感染由来のHTTPトラフィック検知を実現する．提案手法は図1に示す通り，以下の段階で構成される．

**HTTPリクエスト/レスポンスペア構成および通信ホストペアごとの分割** 1つのHTTPリクエストに対応するレスポンスを1つ（以降，HTTPリクエスト/レスポンスペア）にまとめる．また，通信ホストのペア（以降，通信ホストペア）ごとにHTTPリクエスト/レスポンスペアを分割する．

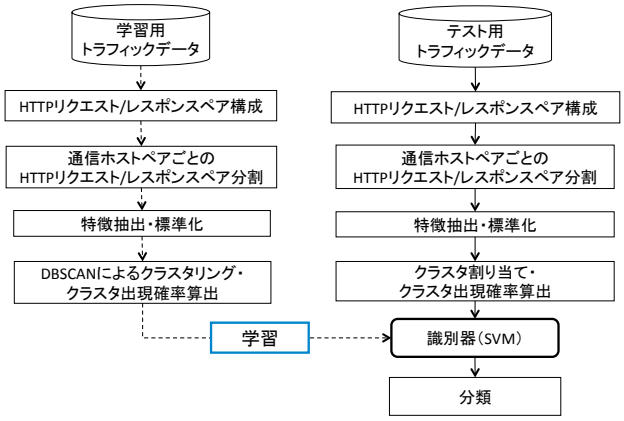


図1: 提案手法

表1: 抽出する特徴量

| | |
|---|---|
| リクエスト間隔 | リクエストボディサイズ |
| レスポンスボディサイズ | GETリクエストフラグ |
| POSTリクエストフラグ | その他のリクエストメソッドフラグ |
| リクエストヘッダのbag-of-words | レスポンスヘッダのbag-of-words |

**特徴ベクトル抽出・標準化** 学習データおよびテストデータについて通信ホストペアごとに分割したHTTPリクエスト/レスポンスペアから表1に示す特徴量を抽出する．なお，リクエストヘッダおよびレスポンスヘッダのbag-of-wordsという特徴量は，学習データに出現したヘッダの数に依存するため，可変長である．

特徴量毎にスケールが大きく異なるので，学習データについて抽出した各特徴量ごとに平均が0，分散が1となるように，標準化を行う．テストデータについては，学習データで算出した各特徴量ごとの平均および標準偏差を用いて学習データと同様に特徴ベクトルの標準化を行う．

**クラスタリング・クラスタ出現確率算出** 学習データについて，標準化した特徴ベクトルをDBSCANによってクラスタリングする．DBSCANにおける2つのパラメータEpsは0.5，MinPtsは1と設定した．

---

Malware Originated HTTP Traffic Detection Utilizing Cluster Appearance Ratio with DBSCAN

Hideki OGAWA† Yukiko YAMAGUCHI†† Hajime SHIMADA†† Hiroki TAKAKURA††† Mitsuaki AKIYAMA†††† Takeshi YAGI††††

†Graduate School of Information Science, Nagoya University

††Information Technology Center, Nagoya University

†††National Information Informatics

††††NTT Secure Platform Laboratories

続いて，通信ホストペアごとにクラスタの出現確率を算出する．テストデータについては，各特徴ベクトルと学習データの全特徴ベクトルとのユークリッド距離を算出し，最小の距離であるクラスタを割り当てる．テストデータについても，学習データと同様にクラスタ出現確率を算出する．

**学習・判定**　学習段階では，通信ホストペアごとに算出したクラスタ出現確率を入力ベクトルとして，識別器に学習をさせる．なお，識別器には Support Vector Machine（SVM）を用い，SVM のパラメータはグリッドサーチにより最適値を算出する．判定段階では，学習済みの識別器を用いて，正常もしくは感染由来の HTTP トラフィックの 2 値判定を行う．

## 3　評価実験

**データセット**　1 つのリクエスト/レスポンスペアのみでは正常および感染由来の HTTP トラフィックであるかどうかの識別が困難である点，リクエスト間隔を特徴量とすることから，HTTP リクエストが 5 個以上発生している通信ホストペアをデータセットとして用いた．

正常トラフィックデータは，事前告知を行った上で研究室 LAN 内で 30 分を 1 区切りに 2.5 日分収集を行ったデータを使用した．感染トラフィクデータは NTT セキュアプラットフォーム研究所の動的解析環境である BotnetWatcher でマルウェアを動作させたときに収集されたデータのうち，Kaspersky の検知名のプレフィックスに Urgent Detection System（UDS）もしくは not-a-virus を含まないものを使用した．

**実験方法および評価基準**　評価は，正常データおよび感染データを合わせたデータを 5 分割し，4/5 を学習データ，1/5 をテストデータとして試行を行うことをデータを入れ替えて 5 回繰り返す，5 分割交差検証によって行った．評価基準として正常データおよび感染データの F 値*の平均値を用いる．また，従来手法と比較するために，クラスタリング手法として k-means++を利用し，そのクラスタ数を 100 から 1000 まで 100 刻みで変化させたときの F 値の平均値も同様に算出する．

**結果および考察**　従来手法の各試行において，一番良い F 値が得られたクラスタ数（最適クラスタ数）およびその時の F 値，提案手法での各試行で得られたクラスタ数およびその時の F 値を表 2 に示す．

従来手法では 5 分割交差検証の平均において，最も良い F 値は 0.986 で最適クラスタ数は 600 であったのに対し，DBSCAN を使用した提案手法では，0.972 であった．また，従来手法では交差検証の各回ごとに最適クラスタ数が表 2 のように異なっていることがわかる．提案手法のクラスタ数が従来手法の最適クラスタ数よりも大きい理由は，DBSCAN が密度ベースのクラスタリングである上，今回はノイズクラスタをなしとした点が考えられる．

表 2: 交差検証におけるクラスタ数と F 値

| 交差検証（回） | | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 従来手法 | 最適クラスタ数 | 400 | 600 | 700 | 300 | 300 |
| | F 値 | 0.986 | 0.993 | 0.980 | 0.990 | 1.000 |
| 提案手法 | クラスタ数 | 2920 | 2992 | 2763 | 2660 | 3114 |
| | F 値 | 0.957 | 0.986 | 0.969 | 0.984 | 0.965 |

表 2 に示したとおり，DBSCAN によりクラスタ数を自動決定した場合でも，従来手法と同等の検知精度が得られた．本研究の手法では特徴ベクトルの長さが学習データに依存して異なるため，k-means++による従来手法では学習データを更新する度に最適クラスタ数を探索する必要があった．本手法ではクラスタ数が自動決定されるため，最適クラスタの探索コストを軽減できるという利点がある．

## 4　おわりに

本稿では，DBSCAN によるクラスタ出現確率を用いたマルウェア感染検知手法を提案した．従来手法と比較して，クラスタ数が自動で決定されるため，最適クラスタ数の探索コストを軽減でき，同程度の検知精度であることを示した．今後は抽出する特徴量の見直しや，次元圧縮手法の検討などを行い，クラスタ数爆発の抑止手法について検討する．

## 参考文献

[1] 独立行政法人情報処理推進機構, “「高度標的型攻撃対策」に向けたシステム設計ガイド”, https://www.ipa.go.jp/files/000046236.pdf, 2014 年 9 月.

[2] H. Ogawa et al., “Malware Originated HTTP Traffic Detection Utilizing Cluster Appearance Ratio”, ICOIN2017, Jan. 2017.

*Precision 値と Recall 値の調和平均