# 自己組織化マップを用いたハニーポット送信元地理情報の特徴抽出と分類

沖野浩二 †　　安藤類央 ‡　　片山昌樹 §

† 富山大学
総合情報基盤センター
okino@itc.u-toyama.ac.jp

‡ 情報通信研究機構
ネットワークセキュリティ研究所
ruo@nict.go.jp

§ 有限会社 マギシステム
katayama@magi.co.jp

**あらまし**　本論文では、自己組織化マップを用いたハニーポットの送信元の国や都市などの地理情報の特徴抽出を分類手法を提案する。従来、悪意のある通信パケットの送信元の国などの情報を元にフィルタリングする手法は提案されているが、本研究では攻撃手法の解析から送信元の国や年の情報を抽出する手法により、新たな観点からマルウェアの分類を行うことが可能になる。これにより送信元の国や都市の解析から、新しい分類軸を提供する。評価実験では、評価実験では、３日間で取得した 22,168,821 の悪意のあるパケットに地理情報を付加し、ペイロード、ポート番号などを送信元地理情報の集計を行い、自己組織化マップにより可視化を行った。

# Geographical classification of malicious packets using self-organization map

Koji Okino †　　Ruo Ando ‡　　Masaki Katayama §

†Koji Okino
University of Toyama,Infomation Technology Center, 3190 Gofuku,Toyama,Toayama, JAPAN
okino@itc.u-toyama.ac.jp

‡Ruo Ando
National Institute of Information and Communications Technology, Network security institute
ruo@nict.go.jp

§Katayama Masaki
Magi System Co., Ltd.
katayam@magi.co.jp

**Abstract**　In this paper, we propose a method for geographical classification of malicious packets which is captured by our honey pot using SOM (Self Organization Map). There have been previous efforts for filtering some countries. However, detailed geographical analysis of malicious packets has not been proposed. In our method, geographical information (city, country and latlong) is appended to tokenized data of malicious packets. Then, a newly generated data is classified and visualized by SOM (Self Organization Map). In experiment, we have captured 22,168,821 packets in 3 days and classified these according to countries and cities.

# 1　はじめに

サイバー攻撃の高度化に伴い、攻撃元の詳細な分析が求められている。特に攻撃の動機や技術の多様化によって、防御方法を細かく変更する必要がある。本論文では、攻撃元の地理情報を解析し、国や都市単位で攻撃についての特徴を抽出するための手法を提案する。

従来、攻撃手法や攻撃元の個別ホストについての詳細な分析は多く行われてきたが、攻撃主体について国や都市などの特定の属性に基づいてグループ化し、それらのグループから特徴抽出などを行う研究は少ない。

現況ではサイバー戦争の脅威の顕在化などが議論されるにつれ、元来は不明な点が多かった攻撃元の集団の解析の重要が増している。本論文では、短期間で大量に取得された PCAP データに国と都市の属性を付与し、ポート番号などの頻度別集計可能な項目でデータ処理を行い、自己組織化マップによりクラスタリングを行い、PCAP 分析に新たな観点を提供する。

# 2　提案手法

## 2.1　自己組織化マップ

本論文では、PCAP データに含まれる IP アドレスを地理データに変換することにより、地域ごとの攻撃特徴を抽出することを考え、地域ごとのデータを自己組織化マップを用いて可視化を行った。自己組織化マップは、教師なし学習アルゴリズムの 1 つであり、K 平均法等と異なりクラスタ数を所与としないところに特徴がある。また、自己組織化マップの特長に、データ間のトポロジーを変えずに学習を行うことが可能という点がある。競争層を 2 次元に設置すると、多次元の入力データ間の位相関係を保持しつつ、可視化を行うことが可能である。動作式は下記になり、その他のニューラルネットワークのアルゴリズムと同じくニューロン間の重みを、入力ベクトルと加重ベクトルの差分により修正する

```
Wv(t + 1) = Wv(t)
+ £(v; t)a(t)(D(t) !Wv(t))
```

| 16: standard find query | | 6:random ID choice | |
|---|---|---|---|
| NA | 4592822 | ms-sql | 1782 |
| ssh | 2414321 | telnet | 807 |
| netbios-ssh | 406387 | http-alt | 463 |
| domain | 393338 | mysql | 420 |
| microsoft-ns | 143160 | sip | 385 |
| netbios-ns | 112523 | bgp | 208 |
| http | 81747 | loc-srv | 196 |
| ntp | 25123 | fido | 189 |
| netbios-dgm | 22212 | tfido | 169 |
| smtp | 16328 | dircproxy | 161 |
| pop3 | 9080 | https | 156 |
| imap2 | 5680 | ms-sql-m | 130 |
| pop3s | 3032 | epmd | 113 |
| imaps | 2792 | icpv2 | 78 |
| x11 | 2758 | - | - |

表 1: 攻撃先ポート番号の頻度トップ 29

ここで W はノード間の加重係数行列、D は入力ベクトル、アルファは学習係数である。自己組織化マップでは、各ノードに対して BMU(best matching unit) を決定する。上式のシータは BMU からの距離によって変化する。学習過程を終了させる敷居値は、学習回数に応じて決定する。

## 2.2　ハニーポットと PCAP データ

処理対象データについては、3 日間で取得した 22,168,821 の悪意のあるパケットに地理情報を付加し、ペイロード、ポート番号などを送信元地理情報の集計を行い、自己組織化マップにより可視化を行った。表 1 はデータ内に頻出した攻撃先ポートの番号の頻度をソーティングしたものである。評価実験では、このデータを国と都市別に分割した後にクラスタリングを行った。

# 3　評価実験

3 日間で取得した 22,168,821 の悪意のあるパケットに地理情報を付加し、ペイロード、ポート番号などを送信元地理情報で集計を行い、自己

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1798978 | 1775218 | 2039 | 651 | 2137 | 1187 | 11124 | 0 | 529 | CN |
| 486907 | 420268 | 0 | 0 | 4 | 6 | 1262 | 1 | 0 | PL |
| 274890 | 220553 | 8908 | 1749 | 7718 | 377 | 29462 | 26 | 297 | US |
| 111750 | 104353 | 0 | 22 | 51 | 3425 | 912 | 0 | 80 | DE |
| 437 | 0 | 0 | 324 | 0 | 0 | 30 | 0 | 0 | AL |
| 5656164 | 87831 | 390284 | 390674 | 5832 | 3537 | 10078 | 112458 | 79051 | JP |
| 76279 | 4133 | 0 | 4 | 8 | 0 | 577 | 0 | 12 | GB |
| 157293 | 28697 | 0 | 0 | 27 | 0 | 414 | 112521 | 43 | CA |
| 50481 | 47429 | 0 | 1 | 4 | 0 | 2462 | 0 | 132 | KR |
| 34568 | 34542 | 0 | 0 | 0 | 0 | 14 | 0 | 0 | NZ |
| 9750 | 9462 | 0 | 0 | 0 | 0 | 264 | 0 | 0 | CL |
| 13760 | 8795 | 145 | 17 | 4 | 0 | 4461 | 2 | 175 | IN |
| 11598 | 6059 | 95 | 0 | 0 | 200 | 4802 | 3 | 18 | RU |
| 15036 | 5932 | 635 | 0 | 400 | 0 | 7765 | 0 | 158 | TW |
| 320136 | 13141 | 0 | 230564 | 14 | 0 | 610 | 100 | 31 | TR |
| 115662 | 7499 | 28 | 0 | 0 | 0 | 11746 | 80880 | 30 | IT |
| 11466 | 75 | 379 | 0 | 0 | 0 | 11002 | 0 | 0 | SA |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | AP |
| 1714 | 0 | 8 | 1134 | 0 | 0 | 471 | 0 | 0 | CO |
| 8218 | 3382 | 1490 | 1 | 0 | 0 | 3189 | 0 | 0 | TH |
| 279511 | 0 | 0 | 2 | 0 | 0 | 64495 | 112521 | 0 | PA |
| 3719 | 0 | 668 | 0 | 0 | 0 | 3044 | 0 | 0 | IE |
| 5019 | 3134 | 0 | 1 | 0 | 0 | 18 | 0 | 0 | ME |
| 35988 | 368 | 0 | 29 | 3 | 0 | 4576 | 30920 | 14 | RO |
| 5818 | 5138 | 0 | 155 | 4 | 0 | 89 | 0 | 123 | NL |
| 34465 | 235 | 36 | 0 | 0 | 0 | 3033 | 30920 | 49 | BR |
| 194071 | 366 | 184 | 0 | 0 | 0 | 65539 | 112521 | 0 | ES |
| 2210 | 2136 | 0 | 0 | 0 | 0 | 72 | 0 | 0 | NG |
| 3135 | 2158 | 9 | 0 | 0 | 0 | 935 | 0 | 18 | PK |
| 98645 | 0 | 7 | 40 | 0 | 0 | 2270 | 80878 | 0 | VE |

図 1: 自己組織化マップに用いた国別のポート番号の集計表

組織化マップにより可視化を行った。今回は、下記の 8 種類のポート番号についての集計を行った。

```
34          if($p[4]==22){$ssh++;}
35          if($p[4]==139){$samba++;}
36          if($p[4]==53){$dns++;}
37          if($p[4]==25){$smtp++;}
38          if($p[4]==110){$pop++;}
39          if($p[4]==445){$https++;}
40          if($p[4]==137){$netbios++;}
41          if($p[4]==80){$http++;}
```

手順としては、まずPCAP データのそれぞのパケットデータに地理情報を付与し、攻撃頻度別にソーティングした国と都市ごとにフィルタリングを行い、上記8項目ごとに集計を行った。

図1は、自己組織化マップに用いた国別のポート番号の集計表である。集計の結果、国ごとに攻撃先についての特徴があることが明らかになった。図2は自己組織化マップのクラスタリングの結果である。この場合、クラスタ数は所与ではないが、概ね３～６のグループに分類され、それぞれ識別可能な特徴があることが示されている。

図３は、自己組織化マップに用いた都市別のポート番号の集計表である。ポート番号については、攻撃種別に加えて都市別のランキングの変化の度合いが大きいことが明らかになった。今回は２０１３年６月時点でのデータを処理したが、攻撃元の都市については攻撃手法によっては、アドレス詐称も含めて、長期的に観測解析を行うことが重要であると考えられる。図４は自己組織化マップの都市別のクラスタリングの結果である。この場合、クラスタ数は所与ではないが、概ね３～６のグループに分類され、それぞれ識別可能な特徴があることが示されている。この場合、概ね４～６のグループに分類されていることが示されている。

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 186902 | 93421 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | Hefei |
| 113948 | 56949 | 0 | 0 | 0 | 0 | 18 | 0 | 0 | Atlanta |
| 110886 | 55417 | 0 | 0 | 0 | 0 | 6 | 0 | 6 | Chaoyang |
| 107806 | 52564 | 0 | 579 | 0 | 0 | 236 | 0 | 325 | Beijing |
| 93954 | 46977 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Buga |
| 31366 | 0 | 0 | 0 | 0 | 0 | 6 | 0 | 0 | Douglas |
| 27214 | 13525 | 0 | 0 | 0 | 0 | 53 | 0 | 0 | Shanghai |
| 16858 | 8429 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Fairport |
| 15092 | 1 | 0 | 0 | 0 | 0 | 74 | 0 | 0 | Tokyo |
| 14866 | 0 | 1560 | 0 | 0 | 0 | 5872 | 0 | 0 | Rome |
| 13028 | 0 | 1636 | 0 | 0 | 0 | 4876 | 2 | 0 | Lynn |
| 12106 | 0 | 1124 | 0 | 0 | 0 | 4929 | 0 | 0 | Shelbyville |
| 11772 | 5862 | 0 | 0 | 0 | 0 | 18 | 0 | 0 | Houston |
| 9680 | 0 | 0 | 0 | 0 | 0 | 12 | 0 | 0 | Osaka |
| 8476 | 4238 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Schwerin |
| 6350 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Kyoto |
| 5766 | 0 | 646 | 0 | 0 | 0 | 2235 | 0 | 0 | Warsaw |
| 5302 | 2168 | 2 | 0 | 0 | 0 | 433 | 0 | 8 | Seoul |
| 4052 | 0 | 0 | 0 | 0 | 0 | 2003 | 0 | 0 | Hanoi |
| 3772 | 1873 | 0 | 0 | 0 | 0 | 0 | 0 | 13 | Yamato |
| 3704 | 1762 | 0 | 0 | 7 | 0 | 28 | 0 | 0 | Guangzhou |
| 3588 | 1794 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Zhongji |
| 3416 | 1683 | 0 | 0 | 0 | 0 | 25 | 0 | 0 | Novosibirsk |
| 2812 | 976 | 0 | 0 | 0 | 0 | 399 | 0 | 6 | Moscow |
| 2272 | 1102 | 0 | 0 | 0 | 0 | 19 | 0 | 0 | Hangzhou |
| 1772 | 0 | 0 | 0 | 16 | 0 | 798 | 0 | 0 | Taipei |
| 1550 | 0 | 0 | 4 | 0 | 0 | 18 | 0 | 0 | Hsinchu |
| 1446 | 0 | 0 | 289 | 0 | 0 | 0 | 0 | 0 | Tianjin |
| 1418 | 700 | 0 | 0 | 0 | 0 | 6 | 0 | 0 | Milan |
| 1300 | 623 | 0 | 0 | 0 | 0 | 18 | 0 | 0 | Jakarta |

図 2: 自己組織化マップに用いた都市別のポート番号の集計表

## 4 関連研究

Honeypot をはじめとする deception system の研究の歴史は長く、システム仮想化を用いたものからネットワークトラフィックの大規模な処理まで多岐にわたる。攻撃トラフィックや関連情報の分類や特徴抽出は [1][2] で行われている。[2] は、ハニーポットの運用から一歩進めて、抽出した特徴をもとに攻撃のシグニチャを新たに生成する手法を提案している。インターネットの Darknet や Background radiation、マルウェアの可視化の研究には [4][5][6] がある。攻撃トラフィックを大規模データをとして捉え分析を行ったものに [7] がある。ハニーポットの運用管理の新しいアーキテクチャを提示したものに [8] がある。また、２０１２年には NSA が従来の侵入検知システムの改良として、SQL に関数型言語のフレームワークを導入し、主にアプリケーションレイヤでの解析を可能にしたシステムを提案している [9]。また、最近盛んに研究されているネットワーク観測項目として、DNS がある。[10] は、多地点の６００のリゾルバから、260 億の DNS クエリを解析し、無効な TLD などを発見している。[11] は、DNS への悪意のある行為への早期発見と対策のための観測手法を提案している。

## 5 まとめと今後の課題

サイバー攻撃の高度化に伴い、攻撃元の詳細な分析が求められている。特に攻撃の動機や技術の多様化によって、状況に応じて防御方法を細かく変更する必要がある。本論文では、既存の研究とは異なり、攻撃元の地理情報を解析し、国や都市単位で攻撃についての特徴が抽出するための手法を提案する。従来、攻撃手法や攻撃元の個別ホストについての詳細な分析は多く行われてきたが、攻撃主体について国や都市などの特定の属性に基づいてグループ化し、それらのグループから特徴抽出などを行う研究は少ない。

現況ではサイバー戦争の脅威の顕在化などが議論されるにつれ、元来は不明な点が多かった攻撃元の集団の解析の重要が増している。本論

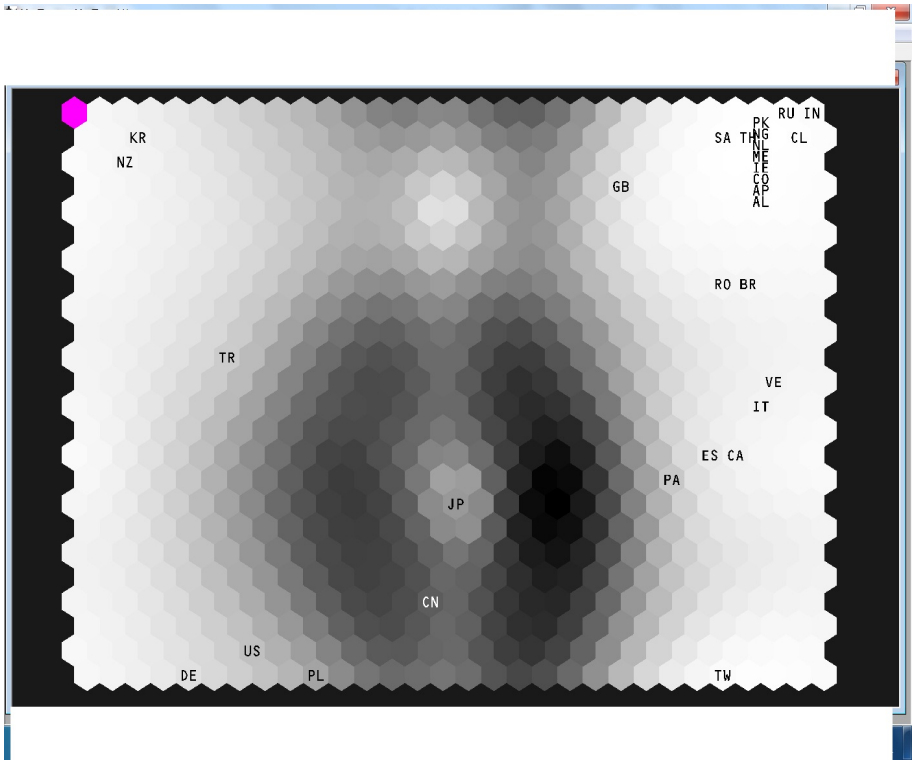


図 3: 自己組織化マップに用いた攻撃元の国のクラスタリング結果

文では、短期間で大量に取得された PCAP データに国と都市の属性を付与し、ポート番号などの頻度別集計可能な項目でデータ処理を行い、自己組織化マップによりクラスタリングを行い、PCAP 分析に新たな観点を提供した。

評価実験により、国の攻撃種別について自己組織化マップのクラスタリングの結果から目視可能な特徴が抽出されることが明らかになった。また、都市については、国ごとの解析と比較して、より識別分離可能な結果が算出された。

今後の課題としては、長期的な観測データから、複数の解析結果を行い、時系列的な推移から含意のある結論を引き出すことである。また、今回はポート番号ごとの集計という比較的単純な処理をおこなったが、クラスタリングの結果から、類似性のある国や都市が、自己組織化マップ上で近隣に配置される原因を、より詳細な攻撃データの解析により調査することで、攻撃元のグループの解析に別観点からの知見を得ることができると想定される。また関連研究で議論したダークネットや DNS の観測結果とあわせることで、早期対策や、防御側のフィルタリングや動的構成の粒度を高度化するための情報が得られる可能性がある。

## 参考文献

[1] An internet protocol address clustering algorithm, Robert Beverly, Karen Sollins, in Proc. SysML'08 Proceedings of the Third conference on Tackling computer systems problems with machine learning techniques

[2] Honeycomb - Creating Intrusion Detection Signatures Using Honeypots, Christian Kreibich, and Jon Crowcroft. Proceedings of the Second Workshop on Hot Topics in Networks Hotnets II

[3] J. M. Agosta, Carlos Diuk, Jaideep Chandrashekar and Carl Livadas, An Adaptive Anomaly Detector For Worm Detection,

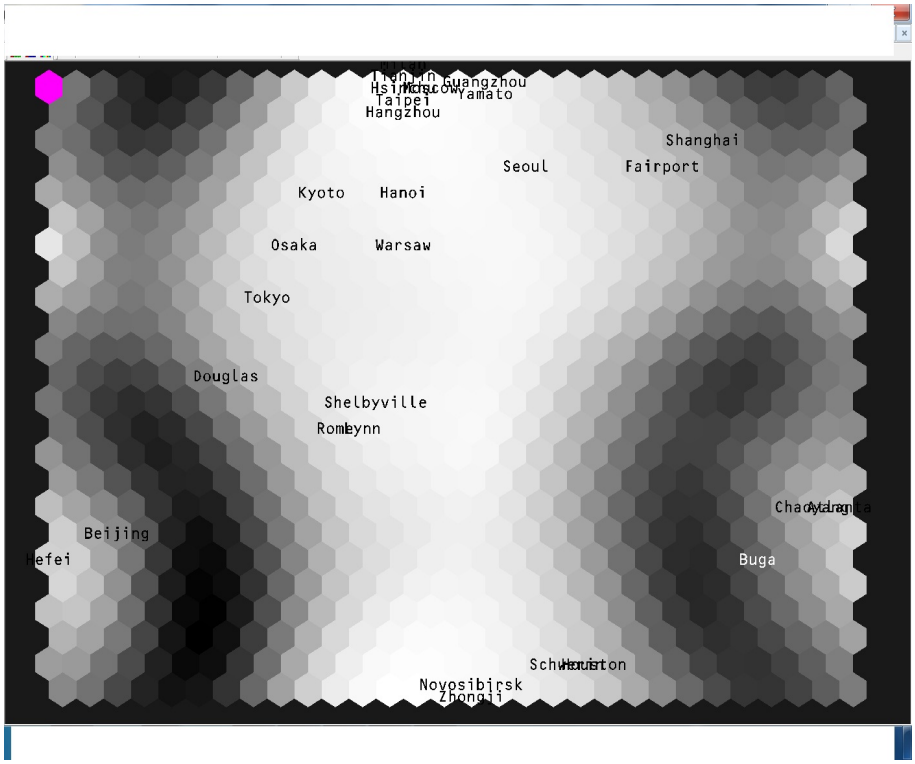


図 4: 自己組織化マップに用いた攻撃元の都市のクラスタリング結果

Workshop on Tackling Computer Systems Problems with Machine Learning Techniques (sysML-07) 2007

[4] Characteristics of Internet Background Radiation, Ruoming Pang, Vinod Yegneswaran, Paul Barford, Vern Paxson, and Larry Peterson Appeared in IMC 2004, Taormina, Sicily, Italy, October 2004

[5] nicter: An Incident Analysis System Toward Binding Network Monitoring with Malware Analysis, Inoue, D. Eto, M. ; Yoshioka, K. ; Baba, S. ; Suzuki, K. ; Nakazato, J. ; Ohtaka, K. ; Nakao, K, WISTDCS '08 Proceedings of the 2008 WOMBAT Workshop on Information Security Threats Data Collection and Sharing

[6] Wei Zhuo, Yacin Nadji "MalwareVis: Entity-based Visualization of Malware Network Traces" Symposium on Visualization for Cyber Security (VizSec) 2012

[7] Guofei Gu, Roberto Perdisci, Junjie Zhang, Wenke Lee. "BotMiner: Clustering Analysis of Network Traffic for Protocol- and Structure-Independent Botnet Detection". USENIX Security Symposium 2008

[8] DarkNOC: Dashboard for Honeypot Management B. Sobesto, M. Cukier, M. Hiltunen, D. Kormann, G. Vesonder, and R. Berthier in Proc. 25th Usenix Large Installation System Administration Conference (LISA ' 11), Boston, MA, December 2011

[9] K. Borders, J. Springer, M. Burnside, Chimera: A Declarative Language For Streaming Network Traffic Analysis, Proc. USENIX Security, 2012

[10] Hongyu Gao, Vinod Yegneswaran, Yan Chen, Phillip Porras, Shalini Ghosh, Jian Jiang, Haixin Duan. An Empirical Reex-

amination of Global DNS Behavior. Proceedings of ACM SIGCOMM, August 2013

[11] Shuang Hao, Nick Feamster and Ramakant Pandrangi. Monitoring the Initial DNS Behavior of Malicious Domains. ACM SIGCOMM Internet Measurement Conference. Berlin, Germany. November 2011.