IP アドレスの履歴が攻撃に与える影響に関する考察

沖野　浩二†　　片山　昌樹‡　　占部 優希§

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

‡株式会社アズジェント
セキュリティ・プラス　ラボ
mkatayama@asgent.co.jp

§有限会社マギシステム
urabe@forensic.jp

あらまし　ハニーポットで観測されるデータは、そのハニーポットの応答設定により、観測されるデータに変化があることが知られている。本稿では、ハニーポットの応答ではなく、ハニーポットに利用している IP アドレスの利用履歴が、観測データにどのように影響をあたえるのかを調べる。実験として、利用歴が異なる複数の IP アドレスでハニーポットを運用し、観測されたデータを基に、攻撃者は事前情報を有しているか否かを検討する。また、送信元 IP アドレスの国情報や AS 情報を用い、それらの攻撃パターンの特徴分類手法を提案する。

A study on the influence of the attack given by the history of IP address.

Koji Okino†　　Masaki Katayama‡　　Yuki Urabe§

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

‡SecurityPlus Lab, Asgent, Inc.
6-4 Akashicho, Chuo-ku, Tokyo, Japan.
mkatayama@asgent.co.jp

§Magisystem Co., Ltd.
1-13-1 Nihonbashi-Muromachi, Chuo-ku, Tokyo, Japan.
urabe@forensic.jp

Abstract　We know the data observed on a honeypot is changed by its response setting. In this note, we examine how the usage history of IP address influences a honeypot, not by the response of one. As an experiment, to operate a honeypot in IP addresses of a plurality of usage history are different, based on the observed data, the attacker will be examined whether it has a priori information. In addition, by using the AS information and country information for the source IP address, we propose a feature classification method of attack patterns of them.

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。そのためには、攻撃者がどのような情報を元に攻撃を行っているのか。また、事前情報によりその攻撃パターンにどのような差が生じるかを検討する。加えて、攻撃元の IP 情報を解析し、国や AS 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、攻撃主体がどのような情報に基づき攻撃を行っているのかを、国や AS 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、利用歴が異なる複数の IP アドレスでハニーポットを運用することにより、その攻撃パターンにどのような差が生じるかを検討する。

そのため、同時刻で観測された PCAP データに対して、国と BGP4 の AS 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 データ取得環境

2.1 ハニーポット

ハニーポットとしてデータを取得するために、Ubuntu14.04Desktop を準備し以下のサービスを起動した。このサーバへの通信を PCAP による取得し、分析データとする。

- Apache(HTTP)
- Samba
- SSH
- BIND

ハニーポットが応答を行うと、その応答内容により攻撃パターが変更することが知られている [1]。本実験環境では、実際のサーバをおとりとして利用することにより現実の攻撃を観測することできる。また、観測環境には、FW や NAT の設置はなく、ポート変換やポート遮断はないので、攻撃者がこのサーバがハニーポットであることを確認するコストは、限りなく高くなっている。

2.2 比較データ

処理対象データについては、3 つのセグメントを準備を準備し、3 つのセグメントに対して、表 1 の 4 つのハニーポットを設置した。

- FTP セグメント
- 新設セグメント A
- 新設セグメント B

ここで、FTP セグメントは、サービスを行っているセグメントであり、新設セグメントは、過去に利用されたことがないアドレス空間である。

表 1: ハニーポット一覧

ホスト名	目的
FTP_O	過去 FTP 利用 IP
FTP_S	FTP セグメント新設置
New_A	新セグメント A 設置
New_B	新セグメント B 設置

FTP_O は過去の FTP サーバとして利用していたアドレスであり、FTP_S は FTP_O と同一のセグメントにあるサービスに利用したことがないアドレス、New_A および New_B は新設したアドレスとなっている。

2.3 取得データ

2014 年のある 1 週間で取得されたフレーム数は、以下の通りである。

表 2: 観測フレーム数

ホスト名	フレーム数
FTP_O	474,745
FTP_S	237,881
New_A	266,312
New_B	272,099

フレーム数は、FTP_O が多く、他のハニーポットへのほぼ同数のフレーム数となった。

3 基礎解析

4 つのハニーポットに対する攻撃ポートへの変化の分析を行う。

3.1 攻撃先ポート数

表 3 はデータ内に頻出した攻撃先ポート番号の頻度のトップ 10 を示したものである。

表 3: 攻撃先ポート番号のトップ 10

	FTP_O	FTP_S	New_A	New_B
ICMP	20120	215	204	220
21	39409	22	20	18
22	287970	235090	266042	261039
23	222	267	181	219
80	115045	548	786	692
139	189	10	113	117
161	9747	15	15	16
445	791	108	3271	2819
1433	155	150	91	102
3389	69	88	83	81

22（SSH) ポートに関しては、どのホストでも同じ攻撃回数であると思われる。FTP_S と New_A,B は同様な傾向がみられる。FTP_O に関するアクセスでは、80(HTTP), 21(FTP) は、過去のサービスに応じた攻撃となる。SSH への攻撃を除けば、攻撃先ポートに対しては、サービスを行っていたポートに関してのアクセスが頻発していることが見受けられる。

3.2 国別の分析

図 1 は、国別の攻撃元トップ 10 である。国ごとに各ハニーポットへのアクセス頻度に大きな差があることがわかる。

攻撃元の国別の分析では、大きく分けて

- すべての IP に関して、アクセスがある国（China,Mexico)
- FTP_O に対するアクセスが多い国（Russia,Japan）
- 上記二つを合わせたもの (United States)

に分類できる。

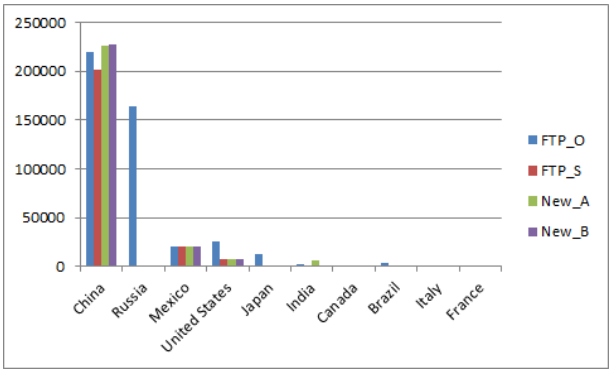

図 1: 攻撃元国別のトップ 10

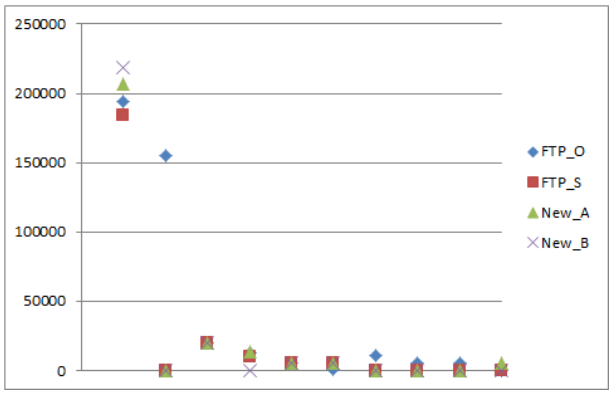

図 2: AS 別のトップ 10

3.3 AS 別解析

AS 毎にフレームを集計した結果を示す。AS 毎の集計では top10(図 2) までと 11-50 位 (図 3) までに分割して表示する。

トップ 10 を確認したところ、

- すべてのポートに対する攻撃グループ (1,3)
- 過去にサーバがあった IP のみに対するグループ (2,7)
- その他

に分類できる。トップ 50 には、FTP_S に対してのアクセス数に差があるものも見える。このことから、一部の攻撃者は、過去にサーバのあったアドレスやその周辺セグメントに攻撃を行っている可能性が見える。

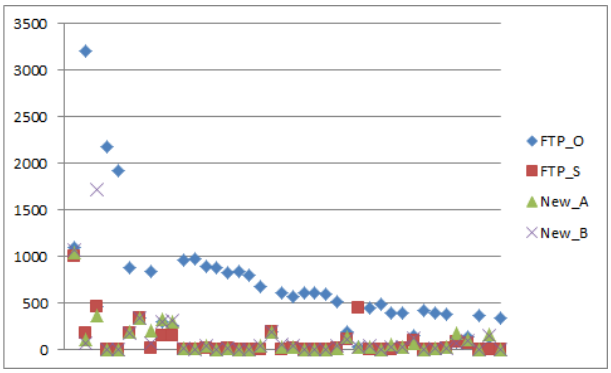

図 3: AS 別のトップ 50

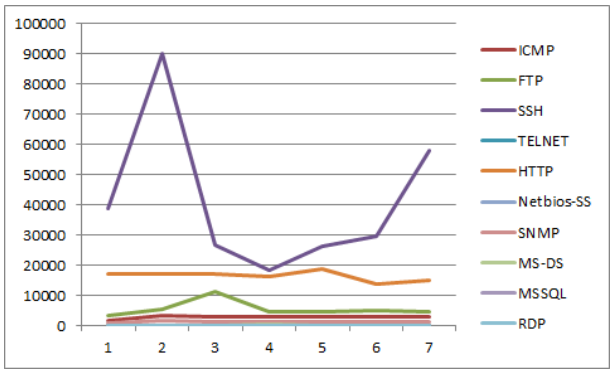

図 4: FTP_O への攻撃先 Port 時間変化

3.4 攻撃 Port の時間変化

実験には、過去に FTP サーバとして運用してから 1 か月程度の時間を置いている。しかしながら、DNSCache が残留している可能性や Mirror などの設定変更し忘れなどユーザ側が意識せずにアクセスする可能性も否定できない。そこで、1 週間のポートへのアクセス変化を確認する。

ここでは、FTP_O サーバへの主要ポートへのアクセス変化 (図 4) および比較のために New_A へのアクセス変化 (図 5) を示す。

FTP_O および New_A の両方に対して、攻撃に対する大きな変動はなく、ほぼ一定の水準で変わらない。FTP_O および New_A の攻撃の差は、過去の IP 利用履歴が攻撃に対して影響を与えていると考えられる。

3.5 基礎解析のまとめ

New_A,B に関しては、アクセスに関して、ポートおよび国に関して差はないが、過去に FTP

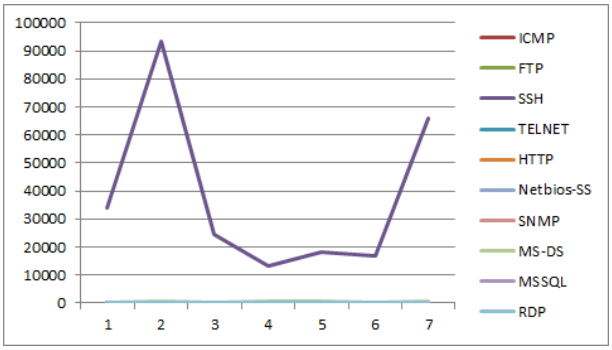

図 5: New_A への攻撃先 Port 時間変化

サービス（HTTP,FTP）を運用していた IP に対しては、顕著な差が見られた。DNS のキャッシュデータは、長くとも 1 週間程度しかもたないこと、また、サービス以外へのポートにも攻撃数が増えており、一部の攻撃者はランダムではなく、過去の IP アドレス利用実績を保存し、サービスに対して意図的な攻撃を行っている可能性を示している。ただし、過去のサービス利用者の設定等が残っているためにアクセスしてきている可能性も否定はできない。

4 提案手法

4.1 既存解析の問題点

今回の実験では、複数の観測点でデータ比較であるため、時間、国、AS 番号等による解析軸や攻撃先 Port に対するデータ集合となり、多次元データとなる。そのため、それぞれのデータの関連性を分析することはできない。特に国間や AS 間の差をそのままでは分析することができない。

4.2 自己組織化マップによる解析

本論文では、PCAP データに含まれる IP アドレスを国および AS データに変換することにより、国ごとおよび AS ごとの攻撃特徴を抽出することを考え、国または AS ごとのデータを自己組織化マップ (以下 SOM という) を用いて可視化を行った。SOM 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、SOM 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。

$$\mathbf{Wv}(t+1) = \mathbf{Wv}(t) + \theta(t)\alpha(t)(\mathbf{D}(t) - \mathbf{Wv}(t))$$

ここで $\mathbf{Wv}$ はノード間の加重係数行列、$\mathbf{D}$ は入力ベクトル、α は時間によって変化する学習係数である。SOM では、各ノードに対して BMU(best matching unit) を決定する。上式の θ 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。

4.3 生成データ

SOM を行うデータを作成するために、国別や AS 毎に下記のデータを作成する。

この時、すべてのポートに関して行うのではなく、基礎解析のポートアクセス数およびその他情報から、ICMP, 21, 22, 23, 25, 53, 80, 110, 161, 445, 1433, 3389, その他のポート合計とその攻撃を行った IP アドレス数とするデータを作成した。(図 6)

5 評価実験

5.1 国別データによる SOM

国別に対して集計を行ったデータによる SOM 解析結果を図 7 に示す。国別の解析結果では、多くの国が右下側に集まり、これらの国が普通の利用における通信パターンに該当する。また、右下から右中央に関しての変化は FTP_O へのアクセス傾向の変化となり、この部分は、過去のユーザの設定が残っている可能性が高いと考えられる。それ以外のグループに関しては、FTP_O, FTP_S, New_A, New_B が同じ位置に配置されるものと FTP_O が別位置に配置されるものに分けられる。これにより、一部の国からの FTP_O へのアクセスは他の国とは異なっていることが示された。

5.2 AS 別データによる SOM

AS 別に対して集計を行ったデータに対する SOM 結果を図 8 に示す。

AS 毎に対する分類を行った場合には、9 個程度に分類でき、多くの場合には、右中央下の普通の利用における通信パターンに該当する。また、右側上下の集団は、FTP_O に対してのみにアクセスを行っている AS の集団となる。それ以外の場所に関しては、それぞれ特徴的なアクセスがあるということになる。

5.3 評価実験のまとめ

基礎解析と比較し、詳細な国または AS 毎に攻撃パターンに特徴があることが算出されている。特に、国と AS 毎の両方ですべてのハニーポットが同一な傾向を持つものと、FTP_O のみが離れているものが見受けられる。とくに AS 分析では、FTP_O のみが距離を離れているものが顕著に確認でき、加えて、FTP_O に対するアクセスも AS 毎に差があることが確認できる。また、国および AS の両方で、基礎解析では確認した FTP_O 以外へのアクセスは、ほぼ同等な傾向を持つことが確認できた。

実験の結果、FTP_O に対するアクセスに関して、いくつかのグループが通常とは異なる傾向をもっており、これらのグループは、設定のミスなどではなく、事前データを用いて攻撃を行っていると考えられる。

6 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 [2][3] で行われている。

17																
#SrcIP Co	ICMP(0)	21	22	23	25	53	80	110	135	137	139	161	445	1433	3389	others
272	6	4	507	10	0	0	2964	0	0	0	0	0	0	0	1	4 Brazil_FTP_0
14	2	0	0	8	0	0	4	0	0	0	0	0	7	0	6	4 Brazil_FTP_S
32	2	0	0	3	0	0	4	0	0	0	4	0	170	0	1	3 Brazil_New_A
37	2	0	0	8	0	0	4	0	0	0	0	0	150	0	3	4 Brazil_New_B
1	0	0	0	0	0	0	15	0	0	0	0	0	0	0	0	0 British Virgin Islands_FTP_0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0 British Virgin Islands_FTP_S
1	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0 British Virgin Islands_New_A
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0 British Virgin Islands_New_B
17	1	9	0	2	0	0	203	0	0	0	0	0	0	0	0	3 Bulgaria_FTP_0
6	0	0	0	4	0	0	37	0	0	0	0	0	0	0	0	0 Bulgaria_FTP_S
15	0	0	0	1	0	0	0	0	0	0	0	0	80	0	0	0 Bulgaria_New_A
15	1	0	0	2	0	0	37	0	0	0	0	0	52	0	0	0 Bulgaria_New_B
71	12	2	984	1	0	0	401	0	0	0	0	0	0	0	0	26 Canada_FTP_0
15	0	0	967	1	0	0	2	0	0	0	0	0	0	0	0	22 Canada_FTP_S
25	3	0	963	0	0	0	2	0	0	0	0	0	6	0	0	41 Canada_New_A
35	11	0	981	0	0	0	2	0	0	0	0	0	27	0	0	45 Canada_New_B

図 6: SOM データ例

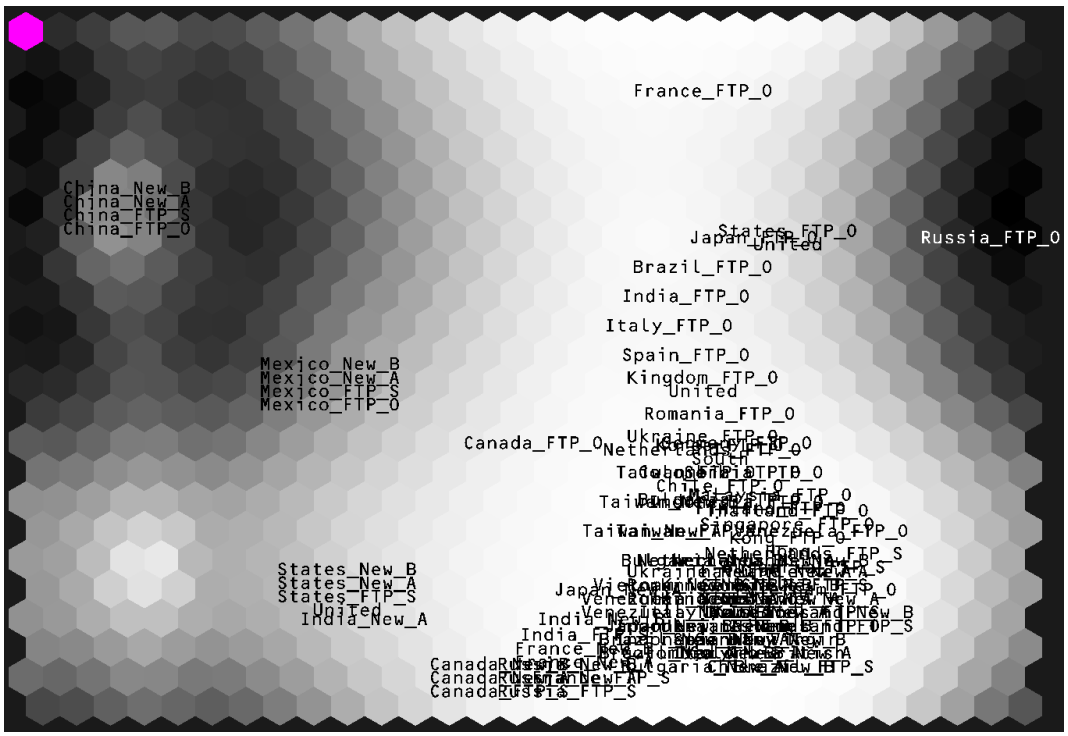

図 7: 国別データによる SOM

[4] 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 [5][6][7] 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 [8] がある。

攻撃データの IP アドレスを地理情報に変化した上で、SOM を適応し、攻撃者を分析したものに [9] がある。本論文では、地理情報だけでなく AS 情報と組み合わせ、加えて、条件の異なる複数のハニーポットと比較することで、攻撃者の分析を行っている。

攻撃者が事前情報を利用していることを示している研究例としては、[10] がある。これは攻撃者が Web 検索エンジンを利用していることを示しているが、本論文では、検索エンジンだけではない情報を有している可能性を示している。

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。[11] 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。[12] 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。

このようにサーバへのアクセス記録等を利用し、攻撃者の動向を把握し、対策を行う研究が

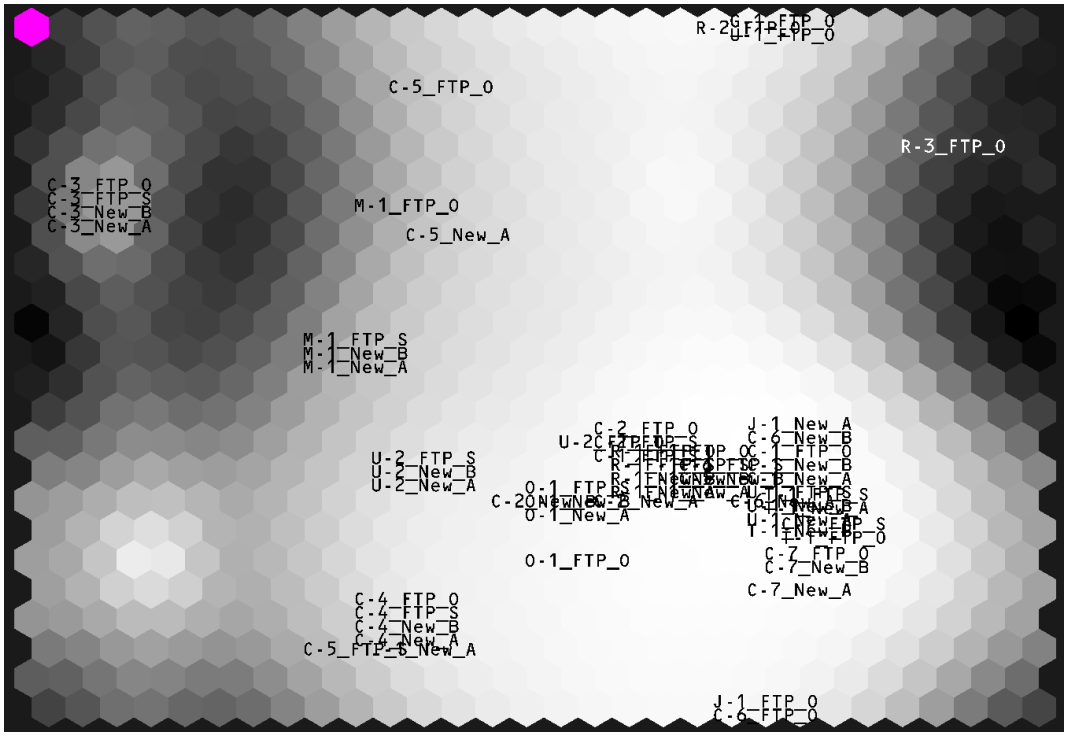

図 8: AS データによる SOM

進んでいる現状がある。

7　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、防御方法を細かく変更する必要がある。本論文では、利用履歴の異なる IP アドレスを有した複数のハニーポットにおいて同時刻に観測されたデータ間の差に着目することにより、攻撃者が事前情報を利用し、その攻撃パターンにどのような差が生じるかを、観測データの攻撃元 IP アドレスではなく、攻撃元の国または AS 番号に変換することにより、管理組織ごとの攻撃パターンの特徴として抽出するための手法を提案した。

今回の実証実験では、提案手法を適応した結果、一部の攻撃者が事前情報を利用した攻撃を行っている可能性が算出でき、また、国の攻撃種別について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、AS 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。

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、ハニーポットに利用する IP アドレスがどのように観測データに影響を及ぼすか、また、攻撃者が過去の情報をどのくらい利用しているのかを検討している研究は少ない。

元来は不明な点が多かった攻撃元解析の重要性が増しているなか、本論文では、利用履歴が異なる IP アドレスのハニーポットを利用することで、攻撃者がどのような攻撃を行っているかを、取得された PCAP データに国と AS 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、SOM によりクラスタリングを行うことで、攻撃分析に新たな観点を提供した。

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 AS 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] 横田凌一, 大久保諒, 曽根直人, 森井昌克,” ダークネット観測に対してハニーポットが与える影響 (その 2)”, 信学技報 113(43), 97-100, 2013-05-16, 電子情報通信学会 ,2013.

[2] 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, 2008.

[3] Honeycomb - Creating Intrusion Detection Signatures Using Honeypots, Christian Kreibich, and Jon Crowcroft. Proceedings of the Second Workshop on Hot Topics in Networks Hotnets II,2007.

[4] J. M. Agosta, Carlos Diuk, Jaideep Chandrashekar and Carl Livadas, An Adaptive Anomaly Detector For Worm Detection, Workshop on Tackling Computer Systems Problems with Machine Learning Techniques (sysML-07) 2007

[5] 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

[6] 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

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

[8] 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

[9] 沖野 浩二 , 安藤 類央 , 片山 昌樹," 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",CSS2013 論文集,2013(4),716-722, 情報処理学会,2013.

[10] 谷本 直人 , 八木 毅 , 針生 剛男 [他] , 伊藤 光恭," 複数のドメインに配置されたハニーポットを用いたWebサイトへの攻撃の実態調査 ", 信報学技. ICSS, 情報通信システムセキュリティ 109(476), 25-28, 2010-03-19, 電子情報通信学会,2010.

[11] Hongyu Gao, Vinod Yegneswaran, Yan Chen, Phillip Porras, Shalini Ghosh, Jian Jiang, Haixin Duan. An Empirical Reexamination of Global DNS Behavior. Proceedings of ACM SIGCOMM, August 2013

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