6A　IPS・IDS 2

座長　山井成良（岡山大）

STARMINE：サイバー攻撃の統合的視覚化システム

秀島　裕介　　小池　英樹
電気通信大学大学院　情報システム研究科

STARMINE : A Visualization System for Cyber Attacks

HIDESHIMA Yusuke　　KOIKE Hideki
Graduate School of Information System, The University of Electro-Communications

1. はじめに

近年、コンピュータネットワークの普及に伴い、不正侵入、コンピュータウィルス、コンピュータワームなどのサイバー攻撃に関する問題が多く取り上げられている。このようなサイバー攻撃を事前に予知、予測、あるいは早期発見を行うことができたらコンピュータネットワークセキュリティの向上に大きく寄与することは間違いない。現在、このようなシステムを実現するために、様々な研究がなされている。

サイバー攻撃の増加などにより、インターネット定点観測に関する研究が進められている[1][2][3][4]。これはインターネット上に侵入検知システムなどのセンサーを設置し、ネットワーク上で起こる様々なサイバー攻撃に関する情報を収集するものである。これを利用してサイバー攻撃への対処を迅速に行うことが可能である。現在行われているインターネット定点観測では、得られたデータを解析し、国別の攻撃、または個々の攻撃の時間変化のグラフなど web サイトなどで公開している。しかし、これらは攻撃の分布や利用者との関係がわかりづらいという欠点がある。

本研究では、2 章で説明するネットワーク広域監視システムを用いて、インターネット上のサイバー攻撃の天気予報システムの構築を最終目標とし、それを実現するための一手法としてサイバー攻撃情報の地図上への視覚化を行った。また、地理的位置関係と論理的位置関係(IP 空間)の統合的視覚化システム「STARMINE」を作成した。

本稿では、まずネットワーク広域監視システムについて説明を行い、次に地理的位置関係の視覚化について説明する。次に地理的位置関係と論理的位置関係の統合的視覚化システム「STARMINE」についての説明を行う。考察、まとめを行う。

2. ネットワーク広域監視システム

2.1 システムの構成

筆者らの研究グループでは 2003 年 5 月よりインターネット広域観測システムを立ち上げ、インターネット上で発生する攻撃状況の調査を行っている。観測点の内訳は大学内ネットワークが 3 つ、企業内ネットワークが 2 つである。監視を行う計算機の OS は RedHat Linux9.0、MacOS 10.2 を使用している。

各観測点の計算機には攻撃情報を取得するためにネットワーク型侵入検知システム(NIDS)として Snort[5]を使用し、すべてのルールが有効な設定にしている。各観測点で観測されたデータは 1 時間毎にログサーバと呼ばれるアラートログ収集用サーバへ転送する。これは各観測点の計算機上で cron デーモンを稼働させ、ssh、rsync コマンドによって行われている。

2.2 既存の視覚化手法

インターネット定点観測システムでは、インターネット上に設置した観測点からの情報を解析し視覚化を行っている。主に行われている視覚化手法は大別して、時間推移グラフと世界地図にマップされた円グラフという 2 種類がある。時間推移グラフは警視庁[2]、JPCERT/CC[3][6]が採用している。また、世界地図へのマッピングは DShield[1]などが採用している。これらが表示する情報には攻撃手法(ワーム、スキャン、バックドアなど)、宛先ポート番号、国名などがある。時間推移のグラフは攻撃の概要を把握することができるが、システムの利用者がこれを具体的に直接利用することは困難である。これは複数の監視センサーの情報を統合した結果を視覚化しているため利用者との関係がわからないためである。また、世界地図へのマッピングは、現在主にインターネット上で蔓延しているコンピュータウィルスやスキャンの概要を知ることができる。しかし、この手法では巨視的すぎて攻撃の詳細がわからないという欠点がある。

3. 地理的位置関係の視覚化

3.1 地理的位置関係の視覚化の必要性

2.2 で挙げた既存の視覚化は、攻撃の概要を知ることができる。しかし、詳細な情報、とくに利用者と攻撃の関係についての情報はこれら既存の視覚化からは読み取ることはできない。

これらの問題点をふまえ大野らによって IP マトリクスという視覚化手法が提案された[7]。IP マトリクスとは、A.B.C.D として表される IPv4 アドレスの上位 8bit(A)を縦軸に、次の 8bit(B)を横軸に表したもので、この 2 次元マトリクス上に攻撃情報をマップしていくというものである。これは論理的位置関係の視覚化手法として優れており、IP アドレス空間上でのコンピュータワームの伝播の様子を直感的に知ることができる。IP マトリクスを用いることによって、どういったアドレスでどのような攻撃が流行しているのかといったことを知ることができる。しかし、IP マトリクスではコンピュータワームの地理的な拡散状況を知ることはできない。

小泉[8]らによると IP アドレスの上位 16bit ごとの集合(以下、サイトと呼ぶ)に含まれる国数は平均して 1.4 ヶ国、最大で 79 ヶ国である。つまり、IP マトリクス上では一つの点としか表示されないが、地理的に見ると非常に広域にわたりコンピュータワームに感染している可能性がある。このような地理的な感染状況を知る為に、攻撃情報の地理的位置関係の視覚化が必要であると考えられる。

3.2 システムの処理の流れ

本システムでは、まず視覚化の対象となるアラートログをユーザーが選択する。選択されたアラートログから 1)攻撃の

名前（シグネチャ）、2)日付、3)時間、4)攻撃元 IP アドレス(ソース IP アドレス)、5)攻撃先 IP アドレス(デスティネーション IP アドレス)を取得する。このとき、IP アドレスから地理情報を取得する(3.3 で後述)。また、同時に攻撃の種類ごとに攻撃量の統計をとる。次に視覚化する攻撃を選択し(図 1)、実際に視覚化を行う。またこのとき、選択された攻撃の 1 分毎の攻撃量の統計をとっている。視覚化手法は数種類の中から選択することができ、デフォルトでは globe view となっている。

選択されたアラートログを一定時間毎に監視し、アラートログに変更があれば再読込を行い、再描画を行う。

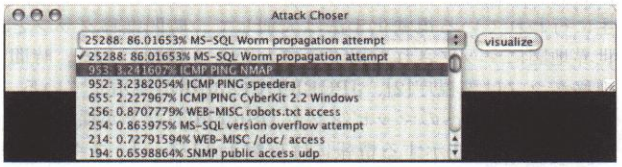

図 1：攻撃の選択画面 – 左から攻撃量、アラートログ全体に占める攻撃の割合(%)、攻撃名が表示されている

3.3 地理情報の取得

地理情報の取得には GeoIP[9]を用いている。GeoIP は MaxMind 社が提供している地理情報のデータベースである。GeoIP を用いることにより、IP アドレスから対応する緯度、経度、国名、国コードなどの情報を得ることができる。本システムでは GeoIP から緯度、経度を取得している。

3.4 視覚化画面

地理的位置関係の視覚化として 2 種類の表示方法を実装した。以下でそれぞれの視覚化について説明する。図 2、図 3 は同じデータを元に視覚化を行った結果である。

3.4.1 globe view

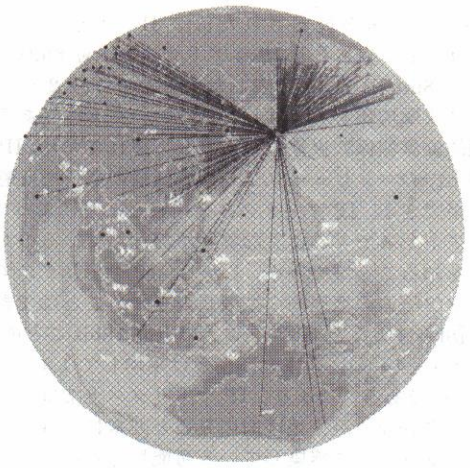

図 2：globe view

globe view(図 2)は地球儀状の視覚化で、攻撃がどこから来ているのかという情報がわかる。攻撃先と攻撃元が地球儀の内部を貫く線で結ばれており、攻撃元側は緑、攻撃先側は白で表している。また、各攻撃元の地球儀上での位置をよりわかりやすく表示するために、各攻撃元には赤い球を配置している。

赤い球とは別に黄色い球も配置してある。これは攻撃元と IP アドレスの上位 16bit が同じ IP アドレスを持つ国に配置してある。多くのコンピュータワームは IP アドレスの上位 8bit、もしくは 16bit を固定し残りの bit をランダムに変化させ感染するコンピュータを探す。そのためワームに感染しているコンピュータと IP アドレスの上位 bit が同じ場合、コンピュータワームに感染している可能性が高い。黄色い球はコンピュータワームに感染している可能性のある場所を表している。

また、globe view は地球の地軸を軸としてゆっくりと回転している。また、マウス操作によって任意の方向に回すことができる。

3.4.2 map view

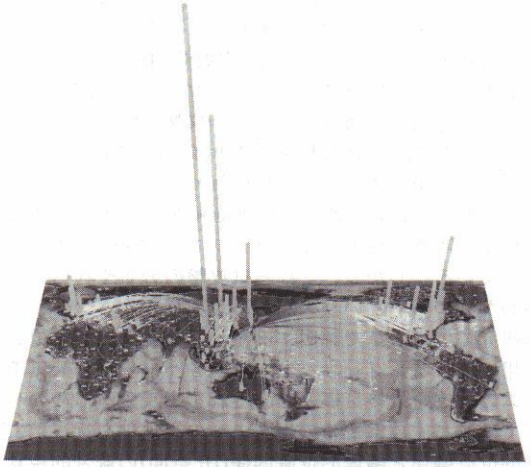

図 3：map view

map view(図 3)は平面の世界地図を用いた視覚化で、どこからどれだけの攻撃が来ているのかという情報がわかる。攻撃先と攻撃元が弧で結ばれており、攻撃先側が黄色、攻撃元側が赤くなっている。また、図中の緑色の柱は、各攻撃元の攻撃量を表していおり、高さが高いほど攻撃量が多いということを表している。

3.5 地理的位置関係の視覚化の考察

globe view は攻撃がどこから来ているか、どういう地域で流行しているかという情報を直感的に知ることができる。しかし、globe view では攻撃の“量”に関する情報がない。これは、globe view は球体への視覚化であるため、map view のように柱の高さで攻撃量を表現することが難しい。これは柱の見かけの高さが場所によって変わるため相対的に比較することができないからである。

map view も globe view と同様に攻撃がどこから来ているか、どういう地域で流行しているかという情報を直感的に知ることができる。更に攻撃量に関する情報も得ることができるため、どの地域からの攻撃が多いかと言った情報を得ることができる。しかし、globe view にあるような“ワームに感染している可能性のある場所”を知ることはできない。globe

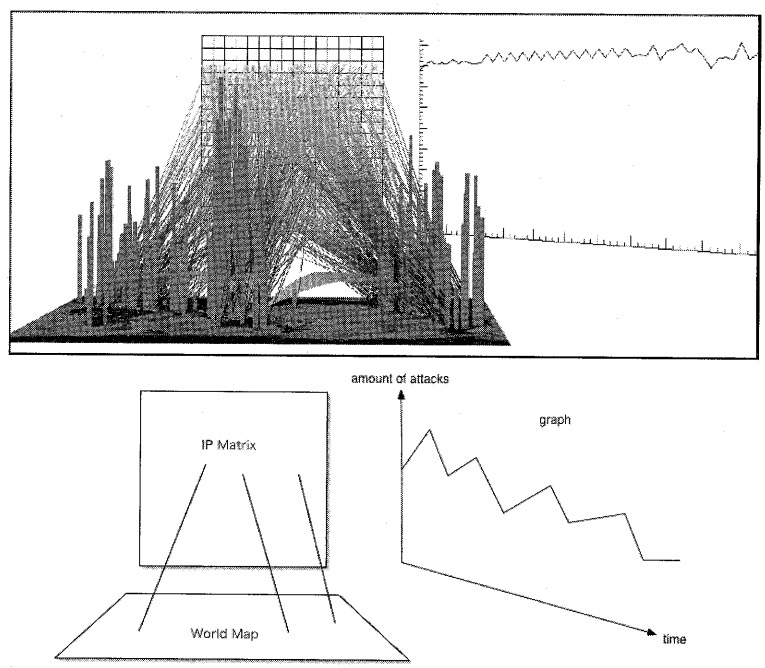

図 4：STARMINE の実行画面

view と同じように球を配置することで表現しようとすると map view に描画されている弧によって隠れてしまうため新たな表現手法を考える必要がある。globe view、map view 共に IP アドレスに関する情報がないという問題点がある。3.4.1 で触れたように現在多くのコンピュータワームは IP アドレスに基づいて感染活動を行う。そのため、ワームの伝播アルゴリズムを考慮すると地理的位置関係の視覚化だけでは不十分であると言える。

4. 統合的視覚化システム

4.1 統合的視覚化

地理的位置関係の視覚化だけでは IP アドレスに関する情報が無いという問題を解決するため、地理的位置関係と論理的位置関係の統合的視覚化のプロトタイプシステム「STARMINE」を作成した。

4.2 視覚化画面

STARMINE の視覚化画面は平面の地図と IP マトリクスから構成されている(図 4)。画面正面に IP マトリクスを配置し、縦軸を IP アドレスの上位 8bit、横軸を次の 8bit としている。画面下方に配置してある地図と IP マトリクスは、IP アドレスと対応する地図上の点を線で結んである。これにより論理的位置と地理的な位置の対応関係を知ることができる。

位置関係に関する視覚化を補佐し、攻撃状況の概要の把握を助ける為に本システムでは“量”に関する情報の表示も行っている。まず、攻撃元毎の攻撃量を表す為に、攻撃元の地図上の点に緑色の円柱を表示してある。これは高さが高いほどその攻撃元からの攻撃量が多いことを表している。次に画面右側に攻撃量の時間推移のグラフを配置している。このグラフは縦軸に攻撃量、横軸に時間をとっている。データの量、観測期間に応じて動的にグラフのスケールを変更することができる。

4.3 実行例

本システムの実行例を図 5、図 6 に示す。

図 5、図 6 は本研究グループの広域監視システムで観測した Sasser ワームを視覚化した結果である。Sasser ワームは 2004 年 5 月に発生したワームであり、Snort のアラートログには“ICMP PING NMAP”として記録されている。図 5 は 2004 年 4 月、図 6 は 2004 年 5 月のアラートログを視覚化した結果である。

図 5 は Sasser ワームが発生する以前のため“ICMP PING NMAP”の警告は少ない。これらの警告はおそらく誤検知(False Positive)であると思われる。一方、図 6 では東アジアを中心に蔓延している様子がわかる。また、IP マトリクスをみると 218.*.*.*という IP アドレス帯で流行している様子がわかる。

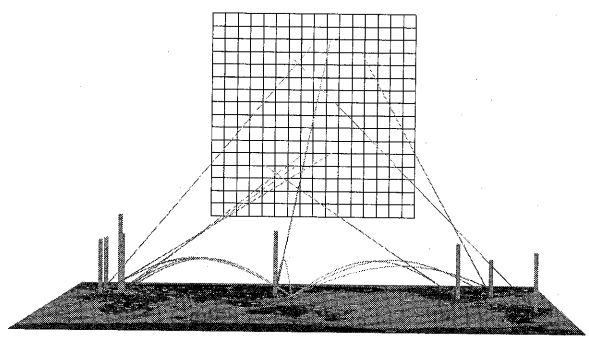

図 5：Sasser ワームの視覚化(2004 年 4 月)

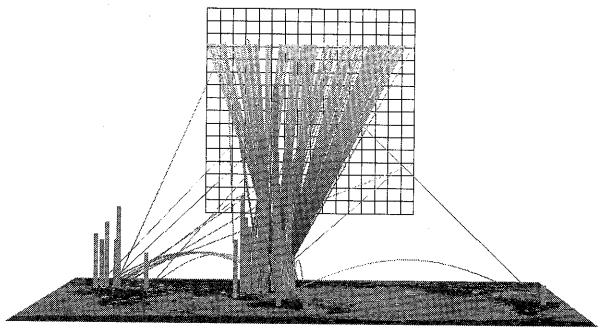

図 6：Sasser ワームの視覚化(2004 年 5 月)

5. 考察

5.1 システムの考察

3.4.1 で述べたように、現在流行している多くのコンピュータワームは IP アドレスをもとに感染活動を行っている。そのためワームの拡散には地理的要因は無関係であると言われている。しかし、図 6 を見ると IP アドレスの上位 8bit が同じ場所が東アジアに集中している様子がわかる。このように IP アドレスと地理的位置関係は無関係であるとは言い切れない。また、現在自分のノートパソコンを職場や自宅、インターネットカフェなどに気軽に持ち運ぶことが可能である。このように簡単に持ち運ぶことができるノートパソコンがワームに感染している場合、例えば職場や自宅のような IP アドレス上では離れていても地理的には近接したネットワークにある計算機はワーム感染の驚異にさらされることとなる。このように物理的な移動によってワームに感染する可能性もあるため、地理的な情報は重要であると考えられる。

5.2 今後の課題

STARMINE の今後の課題としては、まずさらなる情報の付加が挙げられる。現在、STARMINE では IP アドレスの情報、地理的位置関係の情報、攻撃量に関する情報が含まれている。これにくわえ、例えば情報エントロピー[10]の手法を用いて解析した情報を付加したいと考えている。次に、アニメーションによる時間的変化の表示機能の実装が必要であると考えられる。現在のシステムでは一定時間毎にアラートログの再読込および再描画を行っているが、これだけでは最新の状態がわかるだけで、時間的な変化は見えない。また、詳細情報の表示機能が必要であると考えられる。

6. まとめ

本研究ではネットワーク広域監視システムを用いて、地理的位置関係の視覚化システムを作成した。さらに、論理的位置関係と地理的位置関係の統合的視覚化システム「STARMINE」を作成した。今後アニメーション機能の追加、表示する情報の追加などを行いサイバー攻撃の統合的視覚化システムの完成を目指す。

参考文献

[1] DShield, http://www.dshield.org/
[2] 警視庁セキュリティポータルサイト @Police, http://www.cyberpolice.go.jp/detect/observation.html
[3] JPCERT/CC Internet Scan Data Acquisition System (ISDAS), http://www.jpcert.or.jp/isdas/
[4] SANS Internet Storm Center, http://www.incidents.org/
[5] Snort NIDS, http://www.snort.org/
[6]戸田洋三, 松本直人, 宮川雄一, ISDAS: Internet Data Acquisition System, コンピュータセキュリティシンポジウム(CSS2004), 情報処理学会, 2004
[7] Kazuhiro OHNO, Hideaki KOIKE, Kanba KOIZUMI, IPMatrix : An Effective Visualization Framework for Cyber Threat Monitoring, Proc. on 9th International Conference on Infomation Visualization (IV05), 2005
[8] 小泉芳, 小池英樹, 安村通晃, ウィルスの拡散過程と感染国数の関係について, 第 27 会コンピュータセキュリティ(CSEC)研究発表会, 情報処理学会, 2004
[9]GeoIP, MaxMind 社, http://www.maxmind.com/
[10] 小泉芳, 小池英樹, 高田哲司, 安村通晃, 石井威望, 情報エントロピーを用いたネットワーク侵入検知解析手法の提案, コンピュータセキュリティシンポジウム(CSS2003), 情報処理学会, 2003