複数拠点におけるサイバー攻撃監視のための IPMatrix

秀島 裕介 †　　小池 英樹 ‡

電気通信大学大学院情報システム学研究科
182-8585 東京都調布市調布ヶ丘 1-5-1

†hidesuke@vogue.is.uec.ac.jp, ‡koike@acm.org

あらまし 従来の IPMatrix では複数の情報の比較が困難である. そのため,IPMatrix を用いてインターネット広域監視システムの情報を解析する場合, 攻撃の概要を知る事は出来るが, 詳細情報を参照したり, 観測点毎の比較を行う事ができない. 本研究では従来の IPMatrix の問題点を改善し, 複数の観測点のデータの比較を行うことができる視覚的監視システムの提案を行う. これにより, 攻撃の概要, 詳細を直感的に把握でき, さらに個々の観測点の攻撃状況を視覚的に把握することが可能である.

IPMatrix for Cyber Threat Monitoring Using Multiple Senssors

Yusuke Hideshima†　　Hideki Koike‡

Graduate School of Information System
The University of Electro-Communications
1-5-1, Chofugaoka, Chofu, Tokyo 182-8585, Japan

†hidesuke@vogue.is.uec.ac.jp, ‡koike@acm.org

Abstract It is difficult to compare information using former IPMatrix. Therefore, when analyzing Cyber Threat Monitoring System's information, user can know overview of the attacks, however user cannot know detail of the attacks or cannot compare information between each senssor. In this paper, we propose a visual monitoring system which improved the former IPMatrix's problems. Consquently, the user can know the overview of attack and detail of attack intuitively, furthermore, the user can know the situation of attack on each senssor.

1　はじめに

コンピュータワームやコンピュータウィルス, ボット等のサイバー攻撃が増加している. インターネット上のこれらの攻撃を監視することにより, 攻撃の早期発見や攻撃の予知に役立てようという研究が行われている [1],[2]. これらの研究では複数の拠点からデータを集め, これらのデータを統合して解析を行う. しかし, 全体の傾向は知る事ができるが, 個々の観測点毎での傾向を知ることが難しい. そのためユーザと攻撃の関係を知ることが困難である.

本研究では個々の観測点でのデータの比較を行い, 観測点毎の特徴を明らかにする. 特に本研究では情報視覚化の技術を利用し, 視覚的・直感的に観測データの比較を行う. これによってユーザと攻撃の関係を明らかにし, ユーザがセキュリティ対策を取るために有用な情報の提供を行う.

2 インターネット広域監視システム

本研究グループでは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4つ, 企業内ネットワークが2つである. 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) である Snort[3] を使用し, 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よばれる警告ログ収集用サーバへ転送している.

3 IPMatrix

3.1 IPMatrix の概要

IPMatrix[4][5][6] は IP アドレス空間 (IPv4) の2次元マトリクス表現による視覚化手法である. 図1に概念図を示す.

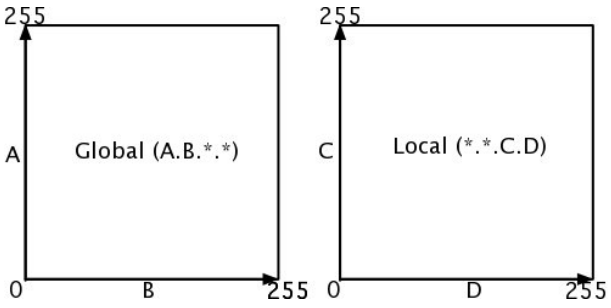

図 1: IPMatrix の概念図

IPMatrix は不正アクセスを行ってきた計算機の IP アドレス (A.B.C.D) の上位 16 ビット (A.B) の値, もしくは下位 16 ビット (C.D) の値を, 正方形の縦と横の辺に対応させた視覚化手法である. 上位 16 ビットの値を用いたものは広域ネットワークの視覚化に [4], 下位 16 ビットの値を用いたものはローカルエリアネットワークの視覚化に用いられる [5]. これにより, あるサイトに届く不正アクセスの IP アドレスから見た近接関係が直感的に理解できる. 本研究では広域ネットワーク監視を想定しているため, 上位 16 ビットの値を用いたものを利用する.

3.2 広域ネットワーク監視のための IPMatrix

利点

IP アドレスの上位16ビットを用いた広域ネットワーク監視のための IPMatrix はインターネット上でのコンピュータワームの感染状況やネットワークスキャン等を概観するのに有用である.

多くのコンピュータワームはローカルスキャンという伝播アルゴリズムを使用している. ローカルスキャンとは IP アドレスの上位 8 ビットもしくは上位 16 ビットを固定し以下をランダムに変化させ, 感染を試みる伝播方法である. そのため IPMatrix 上では図 2 のように横一列に攻撃が並ぶ特徴的な攻撃の分布となる.

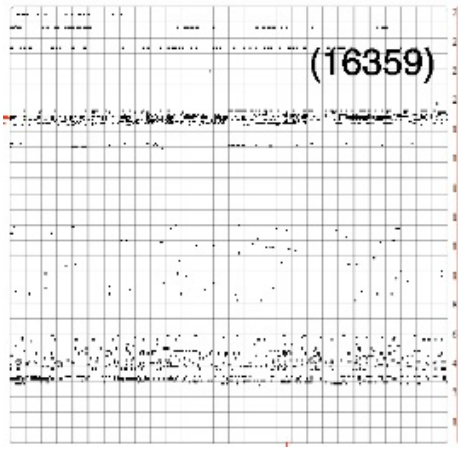

図 2: ローカルスキャンの例

IPMatrix を用いることで攻撃の空間的な分布を直感的に知る事ができ, 攻撃の早期発見や予測に有用である.

問題点

従来の IPMatrix では表現力の問題がある. IPMatrix では1サイトを1ピクセルで表現している. そのため, あるサイトに対して攻撃があるか, ないかという情報しか知る事ができない. そのため, アクセス数が1回のサイトも1万回のサ

イトも同じ点として表示される. ネットワークの管理者にとってアクセス数の違いは重要な情報であるため, これを判別する事が重要である. また, 攻撃の有無以上の情報を表示することが難しいため, 攻撃が使用しているポートや攻撃の種類といった情報を表示する事ができない. また, 従来の IPMatrix では複数の情報を同時に表示する事が困難であるという問題がある. これらの問題を解決する方法として 2 次元の IPMatrix を 3 次元に拡張した IPMatrix-3D[6] があるが,3 次元表示であるためオクルージョン (隠れ) の問題があり, 全体像を適切に把握することが難しい.

また, 複数の観測点毎の比較が困難である. 1 つの IPMatrix に対して 1 つの観測点の情報, もしくは全ての観測点のデータを統合した情報しか表示することができない. これにより観測点毎のデータの比較が困難である.

4 複数拠点監視のための IPMatrix

4.1 概要

従来の IPMatrix の問題点を踏まえ, 本研究では複数拠点監視のための IPMatrix を実装した.

従来の IPMatrix では主に表現力の問題のため, 観測点毎のデータの比較が困難であった. また, 攻撃の多少に関わらず全ての攻撃は 1 ピクセルの点で表されたため, ユーザは攻撃量を知る事ができなかった.

本研究では IPMatrix の表現力の向上のために高解像度表示可能なディスプレイを用いた. 高解像度ディスプレイを用いる事により, 単純に表示領域が大きくなりその分表示する事のできる情報が多くなるという利点がある. また, 高解像度ディスプレイを用いることにより従来の IPMatrix では 1 ピクセルのドットとしてしか表現することの出来なかったサイトを複数のドットを利用して描画することが可能となる. これによって, 一つのサイトで表現する事の出来る情報を増やす事ができるという利点がある. 今回, 高解像度ディスプレイとして FullHD(1920x1080) 解像度表示可能な液晶ディスプレイを用いた.

高解像度ディスプレイを用いて表現力を向上させることによって複数の観測点のデータの比較を行うことが出来る IPMatrix を作成した.

4.2 実装

図 3 は複数拠点監視のための IPMatrix である. 視覚化画面は概要表示部と詳細情報表示部に別れている. 詳細表示部には個々のセンサーの詳細情報について示してある. 概要表示部では個々のセンサーの情報を統合した情報が示してある. 以下でこれらの詳細について説明する.

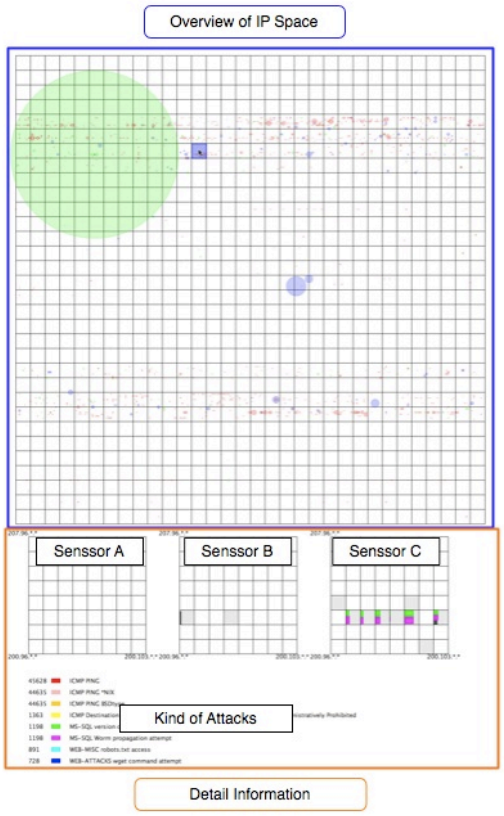

図 3: 複数拠点監視のための IPMatrix

4.2.1 データ処理

本視覚化システムのデータは 2 章で述べたインターネット広域監視システムによって収集された侵入検知システム Snort[3] の警告ログを利用している. 収集された警告ログをデータベー

スに格納し, これを利用して視覚化を行っている. 警告ログからデータベースに格納する情報は, 1) シグネチャ(攻撃名), 2) 日付, 時刻, 3) 攻撃元 IP アドレス, 4) 攻撃元ポート番号, 5) 攻撃元国名, 6) 攻撃元緯度, 経度, 7) 攻撃先 IP アドレス, 8) 攻撃先ポート番号, 9) 攻撃先国名, 10) 攻撃先緯度, 経度である. 5), 6), 9), 10) 等の地理情報は GeoIP[7] を利用して取得している. 地理情報の利用については 5 章で述べる.

4.2.2 概要の表示

視覚化画面上部は概要表示部となっている (図 4). これは A.B.C.D で表される IP アドレスの上位 8 ビット (A) を縦軸に, 次の 8 ビット (B) を横軸に取ったマトリクスである. 概要表示部では詳細表示部で表示してある観測点の情報を統合した情報が示されている. 図 4 では 3 つの観測点の情報を一度に表示している. マトリクス上の円は攻撃量を表しており, 円が大きいほど攻撃量が多い. 円の中心の点が攻撃を受けているサイトである. 円の色は観測点毎に別けてあり, 図 4 では 3 つの観測点のデータをそれぞれ緑, 青, 赤に色分けしている.

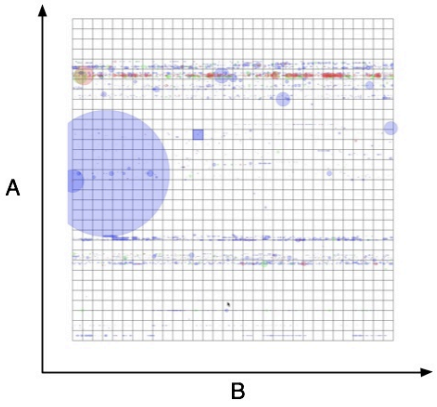

図 4: 概要表示部

概要表示部は 32x32 の格子に別けられている. 一つの格子には 8x8 のサイトが含まれている. 図 5 のように格子を選択する事によって, その格子の詳細情報が視覚化画面下部の詳細情報表示部に表示される.

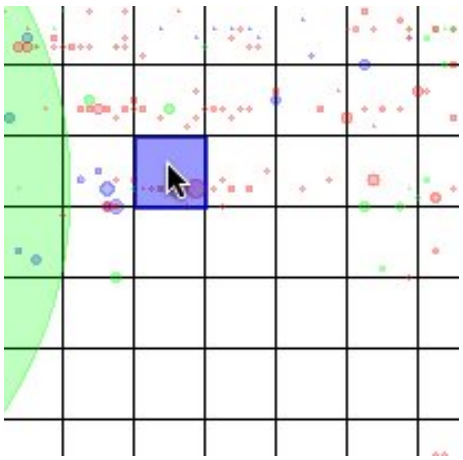

図 5: 格子の選択

4.2.3 詳細情報の表示

図 6 は詳細情報表示部である. 詳細情報表示部は, 概要表示部で選択した格子の部分の詳細情報が表示される. 概要表示部では全ての観測点のデータを一つのマトリクス上に表示していたが, 詳細表示部では観測点毎にそれぞれマトリクスを用意してある. 詳細表示部のマトリクスは概要表示部で選択した格子の拡大表示になっており,8x8 サイトが表示されている.

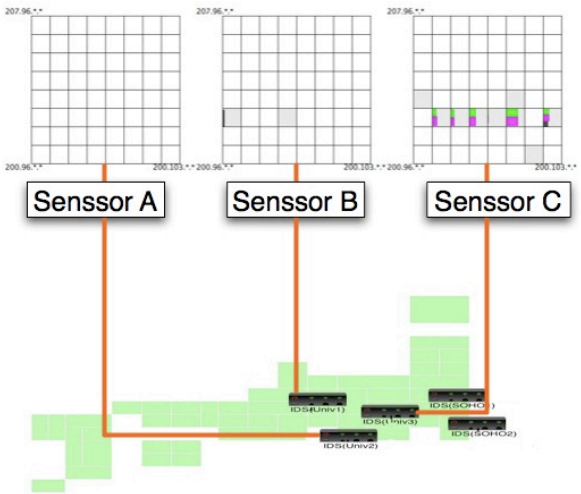

図 6: 詳細情報表示部

詳細情報表示部では一つのサイトを 32x32 ピ

クセルの格子で表現している．攻撃情報がある格子には灰色で色がついている．図 7 のように格子中に色分けされた棒グラフが表示されている．これは攻撃の種類とそのサイト中でのそれぞれの攻撃の量を表している．概要表示部で表示されている攻撃の量が多いもの上位 10 件をそれぞれ色分けされている．色分けについては詳細表示部の下部に凡例を表示している．各格子の横軸が攻撃の絶対量を表しており，縦軸はそのサイト中での攻撃の占める割合を示している．

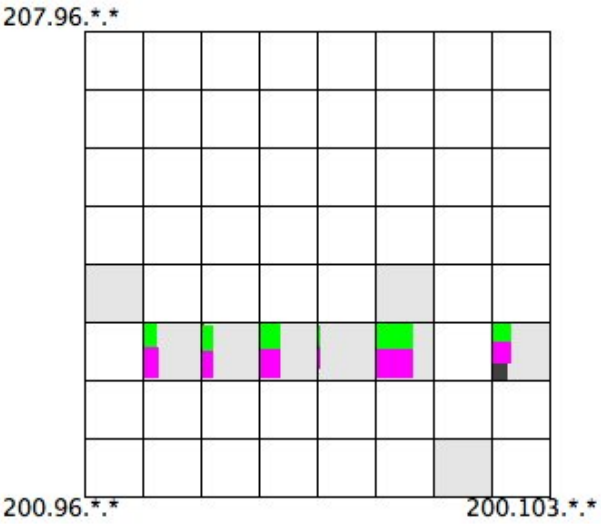

図 7: 攻撃の種類の表示

4.3 実行例

図 8 は複数の観測点で同種類の攻撃が観測された例である． 図 8 の概要表示部を見ると横一列に攻撃が並んでいる様子が分かる．これはワーム等の自動化攻撃によるアクセスであると推定される．概要表示部から攻撃のある部分を選択し，詳細表示を見ると 2 つの観測点でそれぞれ 2 種類の攻撃が行われていることが分かる．従来の IPMatrix では自動化攻撃による攻撃が行われていることは分かったが，攻撃の種類まで知る事は出来なかった．

図 9 は特定のサイトから大量の攻撃が観測された例である．他のサイトのアクセスに比べて明らかに攻撃量が多いことが概要表示部より分かる． これは，この観測点での特徴的なアクセスである．従来の IPMatrix ではこのような特徴的な攻撃もただ一つの点として表現されるため知る事ができない．

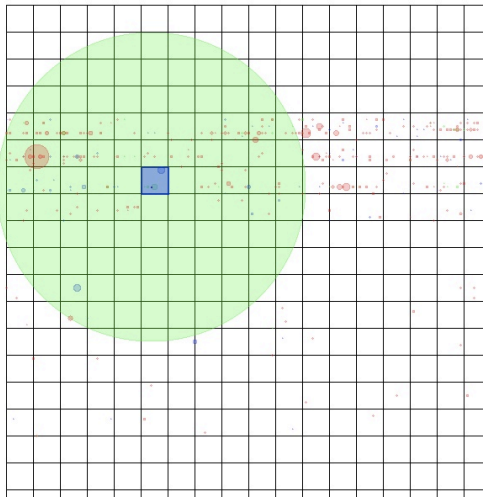

図 9: 特定のサイトから大量の攻撃が観測された例

5 今後の課題

本システムの課題として，以下の事項が挙げられる．

- リアルタイム性
  現在，インターネット広域監視システムでは 1 時間に一度警告ログをログ収集用サーバに転送するようにしている．そのため，視覚化の表示には最低で 1 時間のタイムラグが生じる．何かしらの攻撃があったとき，早期に発見し対策をとることが重要であるため，リアルタイム性は重要である．そのため，警告ログの収集をリアルタイムで行う事ができるよう改良が必要である．

- 高解像度ディスプレイの有効活用
  本システムでは従来の IPMatrix の表現力の問題を補うために高解像度ディスプレイを用いた視覚化システムの実装を行った．しかし，現在の視覚化では高解像度を

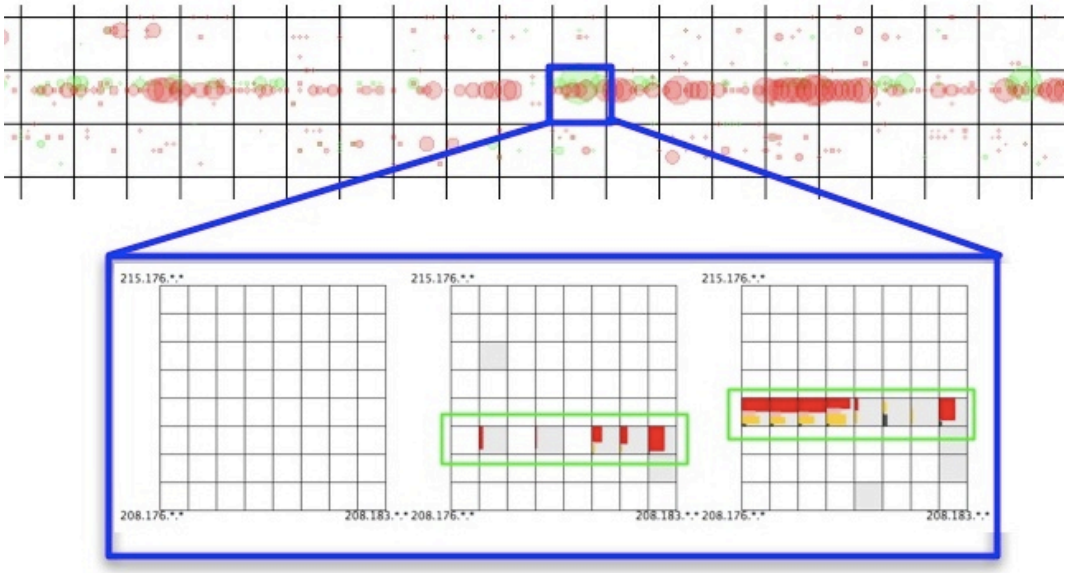

図 8: 複数拠点で同種の攻撃が観測された例

有効に使用できているとは言い難い. 本システムでは 1 サイトにつきせいぜい 3 つの情報しか与えることができていない. 高解像度ディスプレイを用いることによって, さらに多くの情報を効果的に 1 サイトに与える事が可能であると考えられる. また, 従来の IPMatrix を大量に並べて情報の比較を行うといった方法も考えられる.

- 他の情報との連携本視覚化システムでは IP アドレス空間での攻撃の概況, 攻撃量, 攻撃の種類といった主に 3 種類の情報について表示している. しかし, 実際の解析にはさらに多くの事項について調べる必要が有る. 本システムでは上記の 3 つの事項に加え, ポート番号, 地理情報といった情報も利用できる. 今後, ポート番号によるフィルタリング機能や地理情報を表示することによって, 様々な角度からの解析が可能となる.

6 まとめ

本研究では複数拠点監視のための IPMatrix の作成を行った. また, 本研究グループが行っているインターネット広域監視システムで集められたデータを元に視覚化システムの効果について示した. 今後はシステムの改良を進めシステムの完成を目指す.

参考文献

[1] Distributed Intrusion Detection System DShield, http://www.dshield.org/

[2] LEURRE.COM Honeypot Project , http://www.leurrecom.org/

[3] Snort, The Open Source Network Intrusion Detection System, http://www.snort.org/

[4] Hideki Koike, Kazuhiro Ohno, Kanba Koizumi, Visualizaing Cyber Attacks using IP Matrix, Visualization for Computer Security 2005 (VizSEC 2005), IEEE, 2005

[5] 大野 一広, 浅沼 格, 小池 英樹, 内部ネットワーク監視への IP Matrix の応用, コンピュータセキュリティシンポジウム (CSS2005), 情報処理学会, 2005

[6] 大野 一広, 小池 英樹, ワームの伝播アルゴリズムを考慮した広域ネットワーク視覚化システムの提案, 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] MaxMind LLC., GeoIP, Geolocation IP Address to Country, http://www.maxmind.com/