2006－DSM－43（6）
2006／9／15

IPアドレスとポートによる二次元平面を用いた通信トラフィックの可視化について

新川拓也，山之上卓
鹿児島大学大学院理工学研究科

ネットワーク内の通信トラフィックを,IPアドレスとポートを軸とした二次元平面上に表現する通信可視化手法により，通信状況の概要を視覚的に把握するアプリケーションツールの開発を試みた．従来から様々な方法で通信を可視化する工夫がなされてきたが，ここではIPv4 アドレス 32bit の下位 8bit を取り出したもの(256 点)を横軸とし，port 番号 16bit のうち下位 8bit を取り出したもの(256 点)を縦軸とした．それぞれの点では単位時間あたりの流量を色で表す．この点をクリックすると，詳しいトラフィック状況が確認できるようになっている．すべてのトラフィックのおおまかな概要を人間が一目で確認できるようになったと同時に，その点をクリックして詳しい状況が確認できる．このツールによってポートスキャンなどの異常なトラフィックを簡単に認識することができた．

A Visualization of Network Traffic by a 2D Plane of IP address and Port

Takuya Shinkawa, Takashi Yamanoue
Graduate School of Kagoshima University

A visualization tool, which shows network traffic by a 2D plane of IP address and port, is shown. We use the least significant 8 bits(256 points) of the IPv4 address(32bit) as the X axis and the least significant 8 bits(256 points) of the port(16bit) as the Y axis. The amount of the network traffic during the specified time is shown by the color of each point on the plane. The detail of the traffic can be viewed by clicking each point. We can monitor the over view of the network traffic by the 2D plane of this tool and we also can confirm the detail traffic by clicking the point on the 2D plane of this tool. We could recognize the abnormal traffics such like a port scanning by this tool.

1 はじめに

今日，企業や教育機関などのさまざまな団体，組織においてLAN(Local Area Network）が構築され，重要な活動基盤として利用されている．このようなネットワークの普及により，ネットワークを利用するエンドユーザはもちろんのこと，家庭内のような数台のコンピュータLAN から，ある程度の大きさを持ったLAN を構築したり，管理したりする人間も増加し，管理者の能力の差にも広がりが生じている．

しかし，ネットワーク内には重要な情報が存在することには変わりは無い．そして，その情報を狙った外部からの不正アクセス，またはバックドアやスパイウェアのようにコンピュータ内部に組み込まれ，内部から情報が漏洩するといった脅威が多く存在している．

ネットワーク管理者の仕事にネットワーク上の通信トラフィックの監視作業がある．ネットワーワーク全体およびネットワーク内のホストマシーンの通信状況を監視することにより，身に覚えの無い通信や，異常な通信量を把握することができる．これにより，ネットワーク内のシステムの稼動状況の確認，さらに外部からの不正アクセス等の検知，バックドアやスパイウェアなどの起こす身に覚えの無い不正な通信，もしくはユーザの不正なコンピュータ利用を検知することに繋がる．このように，ネットワークの通信トラフィックの監視は重要度が高い．

通信トラフィックの監視システムで得られる情報は文字中心のログ情報である場合が多く，単位時間当たりの量も膨大である．ログ情報を見て人間が全体や重要な部分を把握することは困難である．そのためアプリケーションツールを利用することにより，通信トラフィックの情報の可視化を行い，監視することがよく行われる．

しかしながら，従来のMRTG[1] 等による通信トラフィック量の監視のみでは詳細な現状を把握するのは困難である．Snort[2] 等のIDS は大量の情報を出力する場合が多く，有効に利用するには困難な場合がある．

このような従来の手法では，始めから可視化する情報を侵入検知に特化した可視化手法になっていることや，可視化対象がIP アドレス毎の表示方式となっている．このためLAN内の現状の通信状況を一目で瞬時に把握することは困難である．

我々はネットワーク内のホストの通信トラフィックをIP アドレスとポート毎に可視化を行うことにより，より効果的に可視化し，現在の通信状況を瞬時に把握することのできるツールの開発を行っている．

本論文は，以下のような構成となっている．第２章では，本研究で用いた可視化手法について述べる．第３章では，本研究で作成した可視化ツールについて述べる．第４章では，可視化例を提示する．最後に，第５章で本論文の結論を述べる．

2 関連研究

可視化ツールの一つとして，通信トラフィック量の推移をグラフで表すMRTG[1]が広く用いられている．これは対象のネットワークのトラフィックの量を表したグラフィカルイメージを含んだHTML ページを作成するもので日，週，月，年のような一定の時間毎の表示を行うことができる．

ネットワーク侵入検知データの統計的傾向を，ネットワーク内の計算機群をIP アドレスで階層化した「平安京ビュー」という情報可視化技術を用いて表示する研究がある[3]．また，サイバー攻撃の一つであるワームに焦点を絞ったIPアドレスの二次元マトリックス表示を利用した広域ネットワーク監視のための視覚化手法の研究がある[4]．Quadtree mapping 法を使用し，4000を越えるIPアドレス空間における多数のホストを一目で表示できる情報視覚の研究もある[5]．これらは通信トラフィックのIP アドレスに基づいて視覚化するものである．

このような従来の手法と本ツールが大きく異なる点は，本システムはIP アドレスだけでなく，ポートの情報も使用していることである．従来の手法はネットワーク全体のトラフィック量の視覚化であったり，IP アドレス毎の視覚化であったりするのに対

して，本研究の手法はIP アドレスとポートを縦軸と横軸にとり，二次元マトリックス上にトラフィックを視覚化することで，ポートも含めた通信のパターンの概略を一目で把握することが可能となる．

3 本システムの概要

Maryland のBen Shneiderman は ”overview first, zoom and filter, then details on demand”という表現で，まず情報の全体を見渡し，そこから情報を絞り込み詳細を見ていくことが，情報視覚化の効果的な手法だと示唆している[6]．

この手法を通信トラフィックの情報に適用することにより，通信が活発なまたは特異なホストやポートの存在を確認した後，それらの詳細を見ていくことが可能になり，ネットワーク上のホストさらにはポートの通信全体を人間が効果的に把握することが可能となる．

本システムの可視化手法は，ネットワーク内のホストのIP アドレスに加え，ポート毎の通信トラフィックを一画面に空間的に表示するにより，利用者はトラフィックの概要を一目で把握することができ，さらに，その画面の一部をマウスでクリックすることで，より詳細な通信を知ることができるように作られている．

図2.1 に，本研究で用いた可視化のモデルを示す．このように横軸にIP アドレスをマッピングし，縦軸にポート番号をマッピングした二次元マトリックス表示となっている．その対応するタイルにトラフィック量の度合いを示す色情報を表示する．図2.2 にそのモデルを示す．これにより，管理者はネットワーク内のホスト及びポートの通信トラフィックをパターン的に把握することができ，そこから必要であればタイルをクリックすることにより，詳細情報を表示させる．

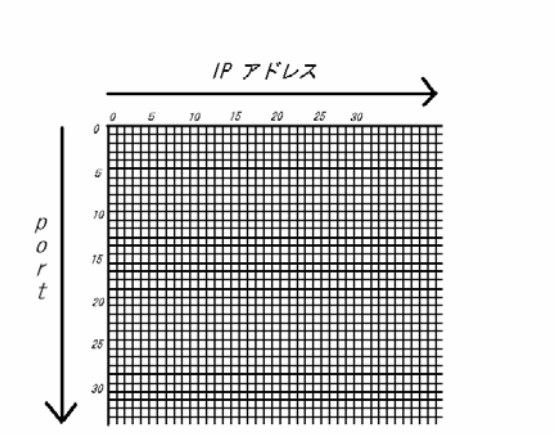

図2.1: 可視化手法のモデル図

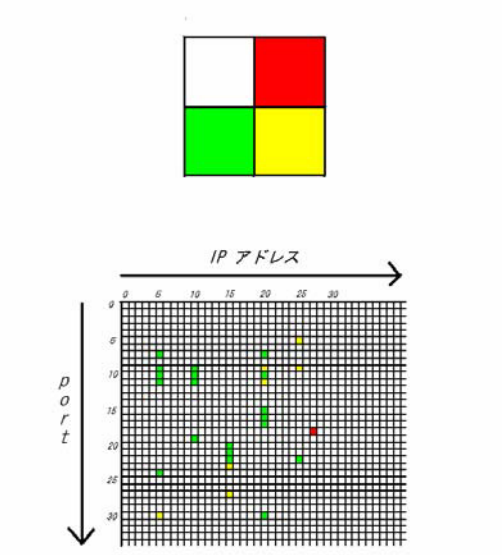

図2.2: 可視化手法のモデル図（トラフィック量表示）

本研究で作成した通信可視化ツールは，開発言語にはJava を使用し，GUI はJava Swing で実装した．ネットワークパケットキャプチャツールのtcpdump により出力されたログ情報を入力情報として，可視化処理を加えている．

視覚化した通信の表示画面の二次元マト

リックスには，１つのタイルを4 × 4 ピクセルで表し，横軸にIP アドレスの下位８ビット，縦軸にポート番号の下位８ビットをとっている．つまり4 × 4 ピクセルのタイルの256 × 256 のマトリックス表示となる．

本システムは他に次に挙げるような機能を持つ

○ 特定のネットワークインターフェースの指定
○ 特定のホスト指定，サブネットを指定した表示
○ TCP，UDP によるプロトコルを指定した表示

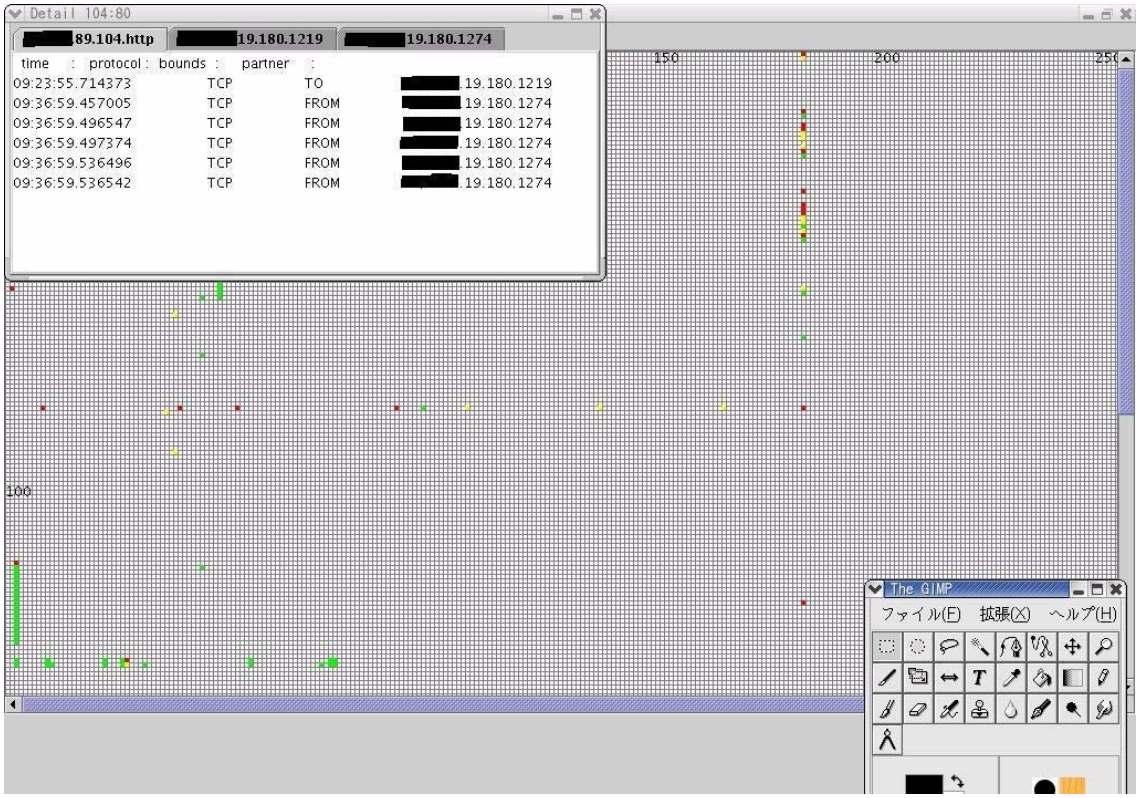

図4.1:通常時のトラフィックの視覚化

4 表示例

本研究で作成した通信可視化ツールを用いて，実際に通信の可視化を行った．ルータサーバーとして稼動しているRedHat Linux，FedoraCore3 上で動作させている．

4.1 通常の状態の表示例

通常は図4.1のような表示が行われている．ここでは，*.*.19.180で本ソフトを動作させている．横軸180に縦の線が見えるのは，このホストがルータとWebサーバの役割を果たしているためである．縦軸80に横線が見えるのは，Webア

クセスが多いことを表している．縦軸137，138付近の横線はnetbios-nsとnetbios-dgmである．

左上の詳細表示は(104,80)をクリックして表示したものである．

タブのラベルはクリックしたタイルのアドレス－ポートを持つパケットのIPアドレスである．それぞれのアドレスのパケットについて左から時間，プロトコル，方向，あて先を示している．

4.2 ポートスキャンを行ったときの表示例

本論文では，ポートスキャンを行うツール，nmap[7] を使用して筆者の一人が管理しているホストにポートスキャンを実行した．その様子を図4.2に示す．*.*.*.102 のホストにはTCP ハーフスキャンを，*.*.*.200 のホストにはUDPスキャンをかけた．この画面から２台のホストのポートを走査的にスキャンしている様子がわかる．また，プロトコル別に表示を行った様子を図4.3，図4.4に示す．

ポートスキャンを行った場合，縦方向に上から下まで均等に線が見えるので他と区別がつきやすい．

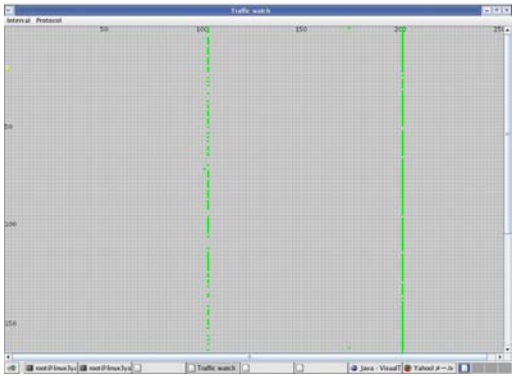

図4.2: ポートスキャン時の通信可視化

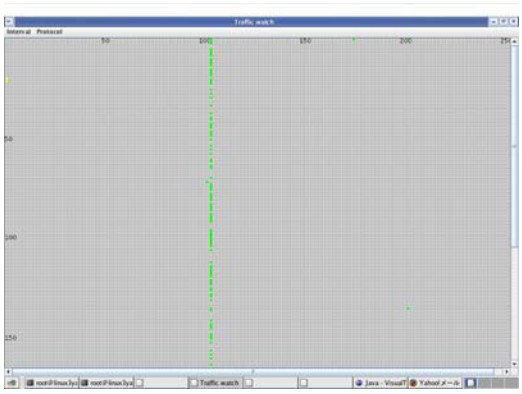

図4.3: TCP のみの視覚化

図4.4: UDP のみの視覚化

5 おわりに

本研究では，IP アドレスとポートによる二次元マトリックス表示を用いた手法を提案し，それに基づいた通信可視化ツールを作成し，ネットワーク内の通信トラフィックの可視化を行った．ネットワーク内の通信の状況をある程度，一目で把握することができた．オプションでIP アドレス指定や，プロトコル指定で照準を合わせることができ，効率よく通信を可視化することができた．

しかしながら，本システムではIP アドレス，ポート共に下位８ビットのみに対応した表示を行うため，下位８ビットが重複するような場合，別のホストの通信が１つの表示タイルに重複してしま

う.現段階では通信量の度合いによるタイルの色の変化というハイライトしか行っていない.また，詳細情報に統計的な情報を含んでいないため,リアルタイムの詳細でしか判断できない.これらの問題を解決する手法を現在検討している．また，ajax のような技術を使って web で表示できるようにすることも検討している.

本システムは
http://yama-linux.cc.kagoshima-u.ac.jp/security-research/
でダウンロードし,設定することにより利用できる.

参考文献

[1] MRTG(Murti Router Traffic Grapher) http://www.mrtg.jp/

[2] Snort http://www.snort.org/

[3] 伊藤貴之，高倉弘喜，沢田篤史，小山田耕二：ネットワーク不正侵入監視のための視覚化の一手法，情報処理学会分散ネットワーク/ インターネット運用技術シンポジウム，pp63-68，2004.

[4] 小池英樹，大野一広，小泉芳：広域ネットワーク監視のための視覚化手法の提案と実装，pp319-323，日本ソフトウェア科学会第21 回大会，2004.

[5] 堀良彰，櫻井幸一：ネットワークセキュリティのためのQuadtree mapping 法を使用した情報可視化，電気関係学会九州支部連合大会研究報告，10-2A-10，pp539.

[6] Ben Shneiderman，”The Eyes Have It: A Task by Data Type Taxonomy for Information Visualizations，” Proceedings of the 1996 IEEE Symposium on Visual Language(VL96), pp.336-343,1996.

[7] Nmap http://www.insecure.org/nmap/