LK-003

内部ネットワーク監視のための視覚化方法の提案

Proposal of a Visualization Method for Local Area Network Monitoring

浅沼 格† 大野 一広† 小池 英樹†
Kaku Asanuma Kazuhiro Ohno Hideki Koike

1．はじめに

近年インターネットの普及に伴い，ワームやウイルスによる被害や不正アクセスなどが社会的な問題となっている．これらの対策としてアンチウイルスソフトやファイアウォールの導入が一般的であるが，ファイアウォールはDoS(DDoS)攻撃や，内部からの不正アクセスなどに対処する事が出来ない．そこで，さらなる対策として不正侵入検知システム(IDS)によりネットワークを監視する方法が重要視されている．IDSは攻撃の予兆となる通信を検知し，異常時に管理者に警告を発信することができるので，迅速に対応すれば，被害を最小限に抑えることができる．また，ネットワークの監視データの分析は，ワームやウイルスの流行や特性の発見材料となる．

それらを目的としたインターネットの定点観測が，世界各国の様々な機関によって行われている[1][2][3][4][5]．各機関は，観測地点で得られたデータを視覚化したものをサイト上で公開している．それらは主に攻撃の時間推移[1][2]や，攻撃と地理的情報の関係[3][4][5]などを表現しているものがほとんどである．

以上に挙げた，インターネット定点観測を行っている機関による視覚化システムの多くは，外部ネットワーク監視のためのものである．一方，本研究では論理的なIPアドレスの位置関係を視覚化した広域監視システム，IPMatrix[6]の表示方法を利用し，ネットワーク管理者が内部ネットワークの監視する負担を軽減出来るような視覚化手法を目的としている．

2．内部ネットワーク監視について

内部ネットワークとは，企業や学校，ビルの中など，特定の団体のネットワークを指す．以下は内部ネットワーク監視における監視ポイントと，その重要性の例である．

1．特定のホストの警告量の変化
短時間の間に特定のホストの警告量が多くなった場合，一つの原因として特定の外部ホストからの攻撃を受けていることが考えられる．また，ワームやウイルスに感染したホストが存在し，それらが攻撃を発信している可能性もある．内部ネットワーク内で１台のホストがワームやウイルスに感染した場合，内部ネットワーク全体に蔓延するスピードは非常に速い．いずれの場合も早期に検知する事が出来れば，即座に攻撃者に対するアクセスの拒否や，感染ホストをネットワークから切り離すなどの対応を取る事ができる．

2．内部ネットワークからの通信状況
内部から外部，また内部から内部への不正アクセスが発見された場合もまた，ワームやウイルスに感染したホストが存在する可能性が考えられる．また，特定のホストからのトラフィック量が極端な場合には，P2Pや何らかのダウンロードソフトが使われている可能性もあり，必要があればこれを制限する事が出来る．

3．OS，ポート，サービスなどに着目した監視
警告のあったホストのOS，ポート，サービス，ホストの起動経過時間などを監視する事により，個々のホストの脆弱性を調べる事が出来る．また，ウイルスに感染してしまった場合に，データを見比べ原因を探る事によって，その後のセキュリティ対策の役に立つ．

†電気通信大学大学院情報システム学研究科

3．IPMatrix

IPMatrix[6]は，IPアドレス(A.B.C.D)の上位16bit(A.B)と下位16bit(C.D)を，２つの正方形にマトリックス表示する手法である(図１)．前者は攻撃元の上位アドレスを表し，後者は攻撃先の内部ネットワークの下位アドレスを表している．これによりIPアドレスの論理的な位置関係が分かり，上位ビットを固定し下位ビットをシフトするような感染経路をもつワームに対しては，ワームが感染し蔓延していくパターンを視覚的に表現することが可能である．ワームの伝搬を視覚化するという観点から見ると，この手法は攻撃とIPアドレスの関係を地理的情報に視覚化した[3][4][5]よりも有効である．なお，攻撃元のアドレスが上位16ビットしか表現されていないのは，この種のウイルスのローカルエリアでの感染速度は非常に早いため，あるサイトから攻撃があった場合，そのサイトに含まれる以下16ビットのアドレスを持ったホストは，すでにウイルスが蔓延している可能性があると考えられるからである．

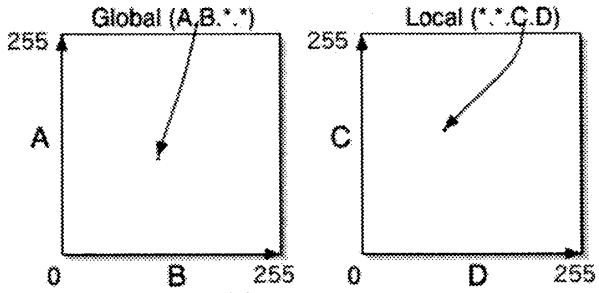

図 1: IPMatrix

4．内部ネットワークの調査データの視覚化

本研究では，内部ネットワークのIPアドレス空間(下位16bit)をマトリックス表示し，そこにネットワークアナライザツールにより得られるポートやサービスの状況，OSの種類などの情報を表し，侵入検知システムがネットワークの異常を検出した時に内部ネットワーク全体の状況を見ることが出来るような手法を目指している．

今回は，ある機関の内部ネットワークに対してネットワークアナライザツール(nmap[8])を利用し，ping応答のあ

るホストを対象にして調査を行った．これによりホストの分布(図２)，OS の種類(図３)，起動継続時間(図４)などの情報を得ることが出来る．図２は内部ネットワーク内のホストの分布(計 1333 台)，図３は WINDOWS のホスト分布，図４は起動してから 200 日以上経過したホストを 100 日ごとに色分けして表示している．

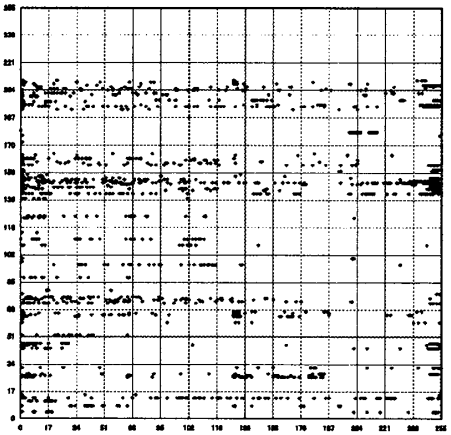

図２：ホスト分布(*.*.C(縦軸).D(横軸))

５．考察

図２のホスト分布図には，ping 応答のないホストは表示されていないので，実際にはもっと多くのホストが存在する．しかし現状でも C クラスの上位部分のように空欄になっている部分では，未使用の IP アドレスの領域がまとまって存在している可能性が高い．このような図は組織内のネットワークを増やす際に，効率的にアドレスを利用するのに有効である．

図３の OS の分布図は，他の情報を表す図と比較してはじめて意味を持つ．例えば，図４の OS の起動経過時間と見比べると長時間再起動されていないホストが確認できる．再起動をしていないということは，古い OS を使用し続けているか，またはセキュリティパッチを適用していないことを意味し，危険度が高い．このようなホストが一台あるだけでも，組織のセキュリティは危うくなってしまう．また特定の OS において，外部に対して開けておくと危険なポートが開いているホストを図示したものと比べれば，脆弱性は一目瞭然となる．

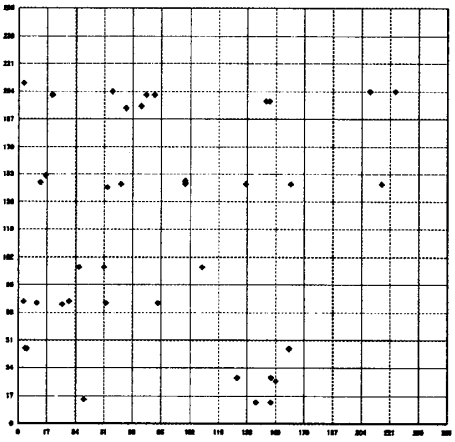

図３：OS の分布(WINDOWS)

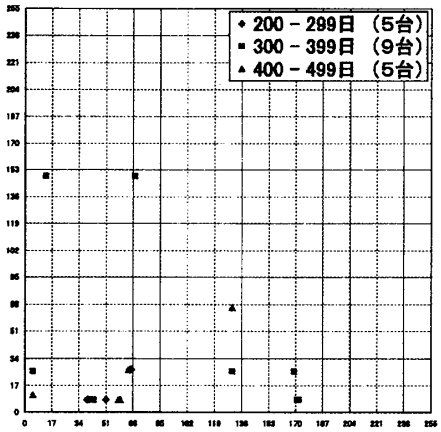

図４：起動経過時間 (単位: 日)

６．今後の課題

・全てのホストを表示する方法の検討

現時点でのホストの分布(図２)は，内部ネットワークに存在する全てのコンピュータを表示することはできない．なぜなら，図２上にプロットされている一つの点は NAT ルータを表すものが多く含まれており，一つの点が複数台のホストを表していることもあるからである．従って，それらを含む全てのコンピュータを調査し，表示できるようにする必要がある．

・侵入検知システムを使ったリアルタイム監視

今回の調査場所と同じ場所に設置した Snort IDS[7]から警告情報を実時間で読み込み，必要な項目をマトリックス表示し，それらと nmap から得られた図３，図４のような図を同時に複数表示させることにより，リアルタイムで内部ネットワークの状況を監視できるようにする．

・警告のあったコンピュータの設置場所の表示

実際にネットワークの管理者が利用することを考えると，異常と思われるホストを発見した場合に，そのコンピュータの IP アドレスだけではなく実際にどこに置かれているのかということが分かれば，より適切な対処を取ることができるはずである．例えば，内部ネットワーク内の地図のようなものを作り，そこに警告のあったホストの場所を表示するなどの方法が考えられる．

参考文献

[1] 警察庁 @police http://www.cyberpolice.go.jp/
[2] JPCERT/CC http://www.jpcert.or.jp/
[3] Internet Storm Center http://isc.sans.org/
[4]Internet Traffic Report http://www.internettrafficreport.com
[5] HackerWatch.org http://www.hackerwatch.org/
[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]Snort.org http://www.snort.org/
[8]nmap "Network Mapper" http://www.insecure.org/nmap/