内部ネットワーク監視へのIP Matrixの応用

大野 一広† 浅沼 格† 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

{ohno, kaku}@vogue.is.uec.ac.jp, koike@acm.org

あらまし 従来のセキュリティ管理では，外部ネットワークから内部ネットワーク (LAN) への攻撃を監視することに力点が置かれてきた．しかしLANの内側での許可されていない行為もしくは不正な行為を監視する重要性がより高まっている．本論文ではIPアドレス空間の2次元マトリクス表現による，内部ネットワーク監視のための視覚化手法について提案する．LAN上に接続された計算機の複数の情報を視覚化し比較することで，セキュリティポリシーに違反した計算機の発見やネットワークのぜい弱性の検出をより容易にすることができるようになる．

Local Area Network Monitoring Using IP Matrix

Kazuhiro Ono† Kaku Asanuma† Hideki Koike†

†The Graduate School of Information Systems University of Electoro-Communications
1-5-1, Chofugaoka, Chofu-shi, Tokyo 182-8585, Japan

{ohno, kaku}@vogue.is.uec.ac.jp, koike@acm.org

Abstract Traditionally, security administration has been focusing on monitoring attacks from outside to their local area network (LAN). It is, however, getting more an more important to monitor unauthorized or illegal activity inside the LAN. This paper proposed a visualization method for the local area network monitoring using 2-D matrix representation of IP address space. By visualizing and compareing several information of hosts connected to the LAN, it becomes much easier to find the hosts violating their security policy or to find vulnerabilities of their network.

1 はじめに

企業などの組織のセキュリティ対策として組織内ネットワークの監視が重要視されている．これらの監視の主流は，インターネットなどの外部ネットワークから組織のネットワークへ送られる不正アクセスを検知するものである．その例として，ネットワークの入口に設置されるゲートウェイや，ネットワーク内部のそれぞれの計算機へ導入されているアンチウイルスソフトなどがある．

外部からの不正アクセスを検知するために，ネットワーク型不正侵入検知システム (NIDS) の利用が進んでいる．NIDSは組織内ネッワークへの不正アクセスを実時間で検知するシステムであるが，ログ情報は非常に膨大で管理者の負担が大きい．それらを解決するために，監視結果を地図や表で表すもの[1][2][3]や，ログ情報を計算機画面に視覚化する手法が提案されている[4][5][6].

一方，組織のポリシー違反や内部情報の漏洩など，組織内ネットワーク特有の不正アクセスが増加している．これらについては2.1節で詳しく述べる．従来提案されてきたシステムは，外部のネットワーク情報の監視に力点を置いたものであり，特有の不正アクセスが存在する内部ネットワークにそのまま適用することはできない．

本論文では我々の提案してきたIPアドレスの2次元マトリクス表現による視覚化手法 IP Matrix[6][7][8]の応用について述べる．さらに実際のネッ

トワークで観測した結果を提示し，本監視方式の利用方法に関して考察を行う．

2　内部ネットワーク監視

2.1　内部ネットワーク監視のポイント

内部ネットワークとは企業や教育機関など特定の組織内のネットワークを指す．これらはファイアウォールなどの機器を通じて外部ネットワーク (インターネットなど) へ接続されていて，内部ネットワークと外部ネットワークとの間で通信が行われているとする．内部ネットワークを監視するためには，以下のポイントに注意する必要がある．

第 1 点は外部からの不正アクセスである．外部からの不正アクセスを監視することで，アクセス元の計算機の IP アドレスや不正アクセスの手法を得ることが可能である．得られた情報から内部ネットワークとの通信を切断するなどの対処を行うことが可能になる．

第 2 点は内部からの不正アクセスである．内部ネットワークの計算機から同じネットワークの別の計算機への不正アクセスや，内部ネットワークの計算機から外部ネットワークの計算機への不正アクセスが検知される場合がある．これは内部ネットワークでウイルスに感染した計算機が存在している可能性を示している．

第 3 点は内部ネットワークのぜい弱性である．内部ネットワークには，不必要なサービスが稼働していたり，認証を掛けずに内部のリソースへアクセス可能になっている計算機が多く存在する．内部ネットワークのぜい弱性を把握することで，これらの計算機に対する不要なサービスの停止やパスワードの設置などの対処を行うことが可能になる．

第 4 点は違反ソフトウェアの稼働である．実際の内部ネットワークでは，ライセンス違反のソフトウェアや P2P などの組織のポリシーに適合しないソフトウェアを稼働させているユーザが多く存在している．これらは計算機のトラフィック量の増加や，特定のポートでの通信などを監視することで発見できる場合がある．

第 5 点は情報の漏洩である．内部ネットワーク監視の重要なポイントに情報漏洩の抑止がある．近年組織内部の人間によって組織内の機密データを持ち去られる事件が多く報告されている．また外部からネットワーク経由でデータの流出の被害を受けた例も存在する．そのため許可されていない計算機から組織内のデータベースへのアクセスや特定の外部ホストへの不正なアクセスに注意する必要がある．

2.2　IP Matrix の適用による内部ネットワーク監視

我々の研究グループでは，広域ネットワークでの不正アクセス監視を目的とした IP Matrix システムの提案を行っている [7][8]．図 1 に IP Matrix の概念図を示す．

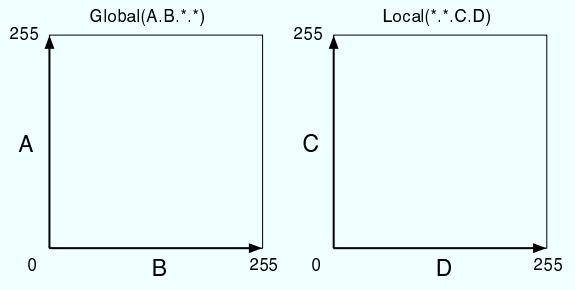

図 1: IP Matrix の概念図

IP Matrix は，不正アクセスを行ってきた計算機の IP アドレス (A.B.*.*) の上位 16 ビット (A.B) 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．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観的に理解でき，かつ IP アドレス空間を経済的に視覚化することが可能である．

本研究では IP Matrix の手法を内部ネットワークへ適用した．内部ネットワークに存在する計算機の IP アドレス (*.*.C.D) の下位 16 ビットの値を正方形の縦横へ割り当てる．これは多くの組織で内部ネットワークの計算機に対する IP アドレスの割り当てが下位のビットに集中しているためである．

3　調査

3.1　ネットワークの概要

本研究では，IP Matrix の視覚化手法を内部ネットワークの監視に適用するため，表 1，2 の環境で調査を行った．

表 1: 調査環境 (1)

ネットワーク名	ネットワーク 1
ネットワーク種別	クラス B グローバル
ネットワーク範囲	A.B.0.0〜A.B.255.255
調査日	2005 年 3 月 23 日〜3 月 24 日
計算機数	1545 台
調査情報	OS 種別, 稼働時間，サービス

表 2: 調査環境 (2)

ネットワーク名	ネットワーク 2
ネットワーク種別	クラス B プライベート
ネットワーク範囲	172.21.0.0〜172.21.255.255
調査日	2005 年 6 月 13 日〜6 月 14 日
計算機数	513 台
調査情報	OS 種別, 稼働時間，サービス

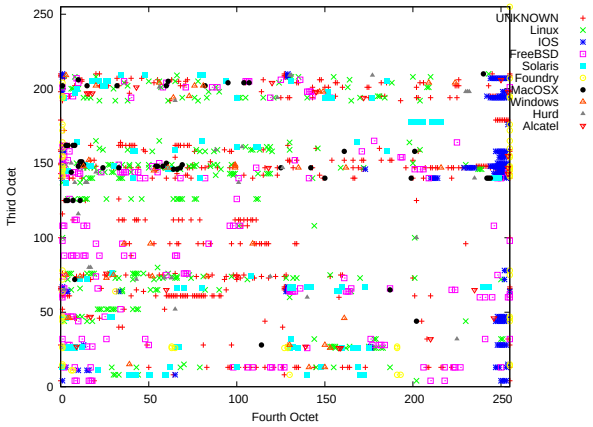

図 2: ネットワーク 1 での OS 分布

ネットワーク 1 は，クラス B に割り当てられているグローバルネットワークである．IP アドレスの第 1，第 2 オクテットをそれぞれ A, B とすると，調査を行った範囲は A.B.0.0 から A.B.255.255 までの範囲である．このネットワークに接続されている計算機は，インターネット側から特定のプロトコルを除いて相互にアクセスが可能である．このネットワークには，対外的に情報を公開するためのサーバが他数接続されている．

ネットワーク 2 は，ネットワーク 1 と同じ場所にあるクラス B プライベートネットワークである．ネットワーク 1 の計算機とは相互に接続可能であるが，それ以外の外部ネットワークの計算機にはアクセスができない．対外的なサービスを立ち上げる必要のない計算機がこちらに接続されている．ネットワーク 1，ネットワーク 2 の両方で，計算機情報の調査には nmap[9] プログラムバージョン 3.70 を使用した．調査時間はネットワーク当たり 13 時間程度を要した．また調査した計算機の情報は，OS 種別，計算機の稼働時間 (uptime)，稼働サービス (空きポート) である．

3.2 視覚化例

3.2.1 OS の分布

図 2 にネットワーク 1 に存在している計算機 OS の分布状況を示す．ネットワーク上に存在している OS の発生順に第 1 位から第 10 位までを視覚化している．

ネットワーク 1 では，OS 名を特定できなかったもの (UNKNOWN)，ルータやスイッチなどのネットワーク機器 (Cisco IOS, Foundry FastIron Edge Switch) などを除く OS の分布は，上位 5 件で Linux (263 台)，FreeBSD (178 台)，Solaris (121 台)，MacOS X (47 台)，Windows (39 台) であった．

計算機の OS はランダムに存在しているのではなく，同じ OS がいくつか図の横方法に密集していることが分かる．これは基本的に IP アドレス第 4 オクテットの一定領域を複数の組織が分割して使用しているためである．図を見ることでそれぞれの組織が主に用いている OS の種別が把握できる．

また IP アドレス第 4 オクテットの前半にスイッチ (0，1)，後半 (240〜255) にルータなどのネットワーク機器が多い．このようにネットワーク内の機器の配置ポリシーを把握できる．

図 3 に内部ネットワーク 2 に存在している計算機 OS の分布状況を示す．これも同様にネットワーク上に存在している OS の発生数が多いものの視覚化を行っている．

ネットワーク 2 の計算機では，ネットワーク 1 よりも特定種類の OS の連続性が顕著である．これはネットワーク 2 が外部と直接接続を行う必要のない研究専門の計算機群によって利用されているためであると考えられる．

3.2.2 サービスの分布

図 4，5 にネットワーク 1 に存在する計算機が提供しているサービスの種別を示す．提供サービスは待

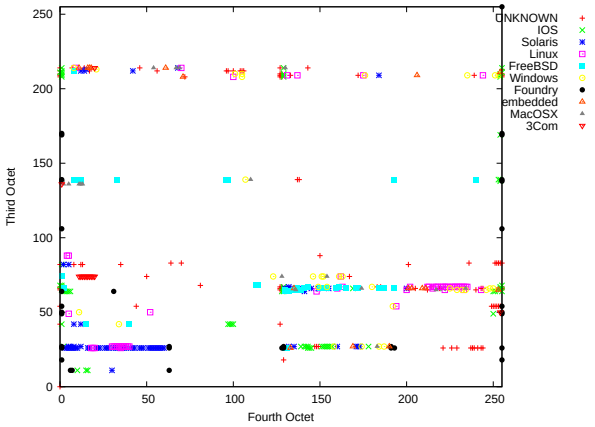

図 3: ネットワーク 2 での OS 分布

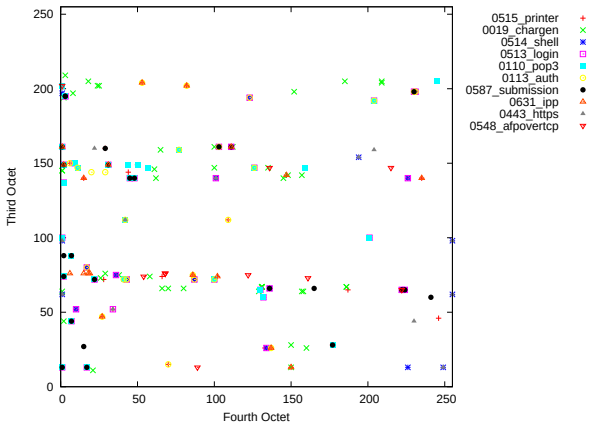

図 5: ネットワーク 1 でのサービス種別 (2)

ち受けを行っている TCP ポート番号で判断を行っている．提供されているサービスの多い順に，図 4 は 1 位から 10 位まで，図 5 は 11 位から 20 位までのサービスを視覚化している．

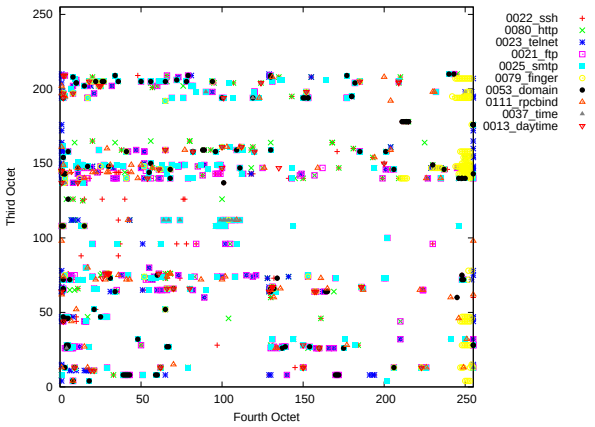

図 4: ネットワーク 1 でのサービス種別 (1)

ネットワーク 1 での提供サービスは，上位 10 件が SSH (428 台)，HTTP (322 台)，FTP (304 台)，SMTP (272 台)，FINGER (202 台)，DOMAIN (140 台)，RPCBIND (79 台)，TIME (69 台)，DAYTIME (62 台) であった．

図 4 と 5 では最大 10 個のサービスをシンボルの重ね合わせで表示を行っている．この重なりをみることで，特定の計算機がどれだけのサービスを立ち上げているかわかる．またシンボルの相関を見ることで，計算機で提供しているサービスの特徴が見られる．ネットワーク 1 ではサービス間で以下のような相関が見られた．1)SMTP サービスと HTTP サービス，2)SMTP サービスと FTP サービス，3)TELNET サービスと FTP サービス，4)SSH のみ．

また OS 分布の場合と同様に，図の横方向で同じアイコンが連続する箇所が多く存在する．これは負荷分散などを目的として特定のアドレス範囲でまとまって一定のサービスを提供しているものと考えられる．

図 6，7 にネットワーク 2 に存在する計算機が提供しているサービスの種別を示す．

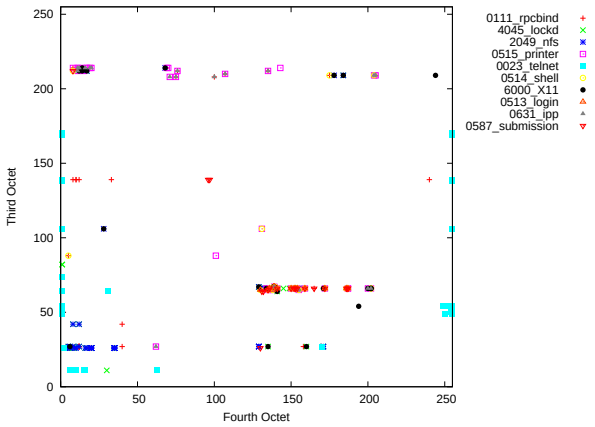

図 6: ネットワーク 2 でのサービス種別 (1)

ネットワーク 2 は外部ネットワークとの直接の接続が出来ないにもかかわらず，HTTP や HTTPS 等の公開サービスが存在している．また rpcbind，printer など通常外部からアクセスを行わないサービスが確認できた．これらの計算機ではファイアウォールなどの防御機構に気を配っていない計算機が数多いと

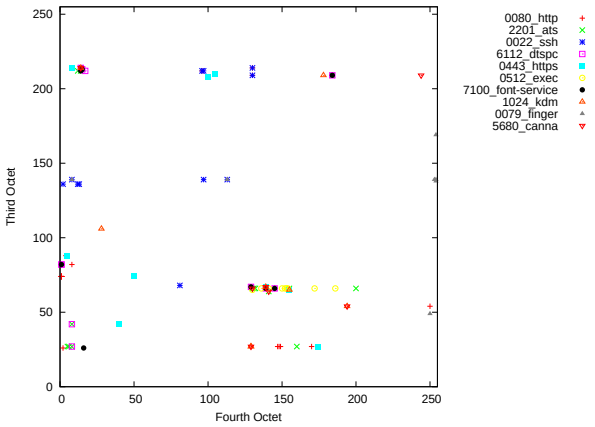

図 7: ネットワーク 2 でのサービス種別 (2)

推測される．

3.2.3 稼働時間

図 8 にネットワーク 1 に存在する計算機のシステム稼働時間 (uptime) を示す．

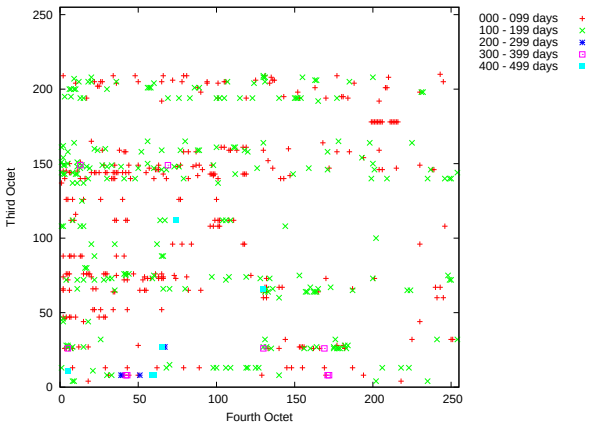

図 8: ネットワーク 1 でのシステム稼働時間

ネットワーク 1 での計算機の稼働時間は 0〜99 日が 320 台，100〜199 日が 244 台，200〜299 日が 5 台，300〜399 日が 9 台，400〜499 日が 6 台であった．なお，稼働時間は UNIX 系 OS を対象としているため，ネットワーク 1 の総計算機数とは異なる．

通常ネットワーク 1 では建物の停電などで定期的に計算機を再起動するため，稼働時間が 200 日以内のものがほとんどであるが，いくつか例外となる計算機が存在した．調査を行ったところ，稼働時間が 400 日を超えているものは全てネットワーク 1 の DNS を担当している計算機であった．また 200〜299 日，300〜399 日稼働している計算機については OS のバージョンが古く提供サービスも多い計算機であった．ネットワークに接続したまま管理をしていない計算機などは，外部の不正アクセスの対象になりやすいため，詳しい調査が必要である．

図 9 にネットワーク 2 に存在する計算機のシステム稼働時間 (uptime) を示す．

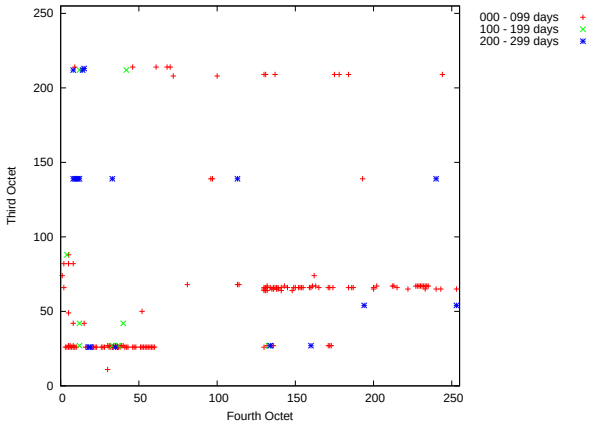

図 9: ネットワーク 2 でのシステム稼働時間

ネットワーク 2 では，300 日以上起動している計算機は存在していない．このネットワークでは組織内でのみ利用する計算機が所属しており，建物の定期点検に伴う停電などと周期が一致している．

4 考察

本視覚化手法の利点に，内部ネットワークに存在する計算機の分布を一覧することが可能な点がある．内部ネットワークのアドレス空間に余裕がある箇所や集中している箇所を発見することが容易なため，アドレス空間を効率よく使用するために役立つと考えられる．また複数の IP Matrix を重ね合わせることで情報を総合し，特徴のある箇所を判別することが可能である．例として，OS 情報と計算機の起動時間を重ね合わせることで，内部ネットワークでアップデートの必要な計算機を検出することができる可能性がある．本調査では，サービスの分布について，複数の情報を重ね合わせて表示した．その結果，特定のホストでは起動しているサービスにいくつかの相関関係があった．このことから，内部ネットワー

ク内の計算機の役割や OS のぜい弱性の検出が容易になると考えられる．

本視覚化手法の欠点として，複数の IP Matrix を重ね合わせた場合に，情報の重複の発生している部分が判別しにくくなるという点がある．その対策として，複数の情報が重なっている点に関しては点滅を行うことや，重なりが発生しても判別しやすいシンボルの使用が考えられる．本実験では，実施中いくつかの問題点が発生した．調査を行ったネットワークは計算機の台数が多かったため全ての計算機の調査を終えるまでに半日程度を要した．計算機の IP アドレスを動的に割り振るネットワークでは，以前調査した IP アドレスが別の計算機に割り当てられる可能性がある．ネットワークによっては今回の調査方法では正確に情報を取得できない可能性があった．また計算機の情報を収集する方法は，不正アクセスを行う侵入者が計算機情報を取得する方法に類似している．今回の実験の際，複数の管理者に調査の連絡が届いていなかったため，不正アクセスが発生したのではないかと報告を受けた事例が発生した．計算機の調査に関しては，十分に連絡を徹底しておくことが必要である．

今後の課題には，NIDS の警告情報を実時間で IP Matrix に表示するシステムの構築，内部ネットワークのさらに中に設置されたサブネットワークの表示手法の検討，さらに地理的な情報との連係を考慮したファシリティマネージメントとの統合などがある．

5　おわりに

本論文では従来インターネット状態の観測に用いていた 2 次元マトリクス視覚化手法 IP Matrix を内部ネットワークの監視に適用する提案を行った．従来のネットワーク監視手法は外部からの攻撃を観測するものが主流であったがネットワークの内側の状態を監視する必要性が増している．しかし内部ネットワークには特有の不正アクセスが存在するため，従来手法をそのまま適用できない．そこで内部ネットワークの監視では注意すべきポイントが存在することから，我々はそれらを元に実際のネットワークで調査を行い，結果の視覚化を行った．最後に視覚化手法の効果についての考察を行った．

参考文献

[1] HackerWatch.org - Anti-Hacker Community, http://www.hackerwatch.org/.

[2] DShield,http://www.dshield.org/

[3] Internet Storm Center, SANS http://www.incidents.org/

[4] Gregory Conti, Kulsoom Abdullah, Passive Visual Fingerprinting of Network Attack Tools, Conference on Computer and Communications Security (CCS2004), Proc. of the 2004 ACM workshop on Visualization and data mining for computer security (VizSEC'04), pp.45-54, 2004.

[5] Stephen Lau, The Spinning Cube of Potential Doom, Communications of the ACM, Vol.47, Issue 6, pp.25-26, 2004.

[6] Hideki Koike, Kazuhiro Ohno, Kanba Koizumi, Visualizing Cyber Attacks using IP Matrix, Internet Proceedings of the 2005 Workshop on Visualization for Computer Security (VizSEC 2005), 2005. to appear

[7] 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.

[8] Kazuhiro Ohno, Hideki Koike, Kanba Koizumi, IP Matrix : An Effective Visualization Framework for Cyber Threat Monitoring, Proc. on 9th International Conference on Information Visualization (IV05), IEEE Computer Society, pp.678-685, 2005.

[9] Nmap security scanner, http://www.insecure.org/nmap/.