大規模LAN監視における統合的視覚化システム

向坂　真一†　　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

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

あらまし
現在企業や大学等のネットワークは大規模化しており，管理が行き届かなくなっている．内部ネットワーク監視では踏み台となった計算機の内部から外部への攻撃や違法ダウンロードを防ぐ必要がある．さらにこれらの計算機を直ちに止めるために地理情報が必要である．また，ログなどの情報は何種類もあり，これらを統合することで素早く判断することが出来る．本研究ではこれらの問題を解決する視覚化システムを開発した．また，実際に大学で運用し，ボットネットの検出に役立ったことを例に挙げた．

Integrated Visualization System for Monitoring Security in Large-Scale Local Area Network

Shinichi Mukosaka†　　Hideki Koike‡

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

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

Abstract　In monitoring security of enterprise or campus networks, detecting attacks from internal network to external network is becoming more and more important. After detecting such attacks, finding the location of the target PC is sometimes needed. This paper describes a visual security monitoring system for large-scale local area network. The system integrates three information, logical, temporal, and geographical information, in one 3-D visualization. IDS logs obtained at the computer center of our university were visualized, and typical examples such as botnet activities was discussed.

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，内部ネットワークも大規模化している．この傾向は無線 LAN のアクセスポイントの普及やユビキタス化など，現在でも進行していると言える．その一方で，ボットネットやウィルス，ワームなどによる被害や情報漏洩が社会問題となっている．このような状況でローカルエリアネットワークのセキュリティ対策は重要になっており，各計算機へファイアウォールやウィルス対策ソフトの導入が進んでいる．しかしながら，定義ファイルの更新が正しく行われなかったり，セキュリティ対策のとれていない計算機がネットワークに混ざっていたり，zero day attack と呼ばれる未知の攻撃を受けるといった可能性がある．

内部ネットワーク監視ではネットワーク型侵入検知システム (NIDS) や通信量，TCP コネクションのログを見ることが多い．しかしこれらのデータは膨大で，文字データによる目視での監視は事実上不可能である．さらに，他のデータとの対応関係を考慮して解析を行わなければ，本当の危険性を判断することができない．これらの解決方法の一つとして計算機画面に視覚化する手法が数多く提案されている．

さらに，内部ネットワーク監視は広域監視やホストベースの監視とは異なる点がある．そこで本研究では大規模 LAN の監視システムにおける有効な視覚化手法を検討した．管理者は攻撃を全体的に把握し，どこで問題が生じているかを知ることが重要である．これらを満たす視覚化システムを開発し，実際のログを用いて有用性を確認した．

2　内部ネットワーク監視の特徴

内部ネットワークの監視は広域監視やホストベースの監視とは異なる．広域監視とは異なり，監視の結果から直ちに対応しなければならない．ホストベースの監視とは異なり，利用者と管理者が異なる．ここではその特徴について述べた．

2.1　攻撃の分類

内部ネットワーク監視では，攻撃を以下の三種類に分けることができる．

一つ目は外部から内部への攻撃である．組織の外部からの不正アクセスは直接的に組織に被害を与える．業務に支障が出るため，ファイアウォールや IPS などを設置して対策する．

二つ目は内部から外部への攻撃である．これは踏み台になったことによる外部への攻撃や P2P による不正ダウンロード，情報漏洩などである．組織は社会的な責任を問われるため，内部ネットワーク監視において最も重要である．発見次第，直ちに対応する必要がある．

そして三つ目は内部から内部への攻撃である．外部からの攻撃によって感染した計算機による二次感染だけでなく，組織の外部から持ち込んだ機器による感染もある．また，十分に十分に防衛していないホストが多いために比較的容易に被害を受ける．

しかし内部から内部への攻撃を全て監視するためには大量に IDS や IPS を設置しなければならず費用がかかりすぎる．そのため，管理者は内部から外部，外部から内部への攻撃に重点を置いて監視している．

2.2　地理情報

組織の中の計算機は使用者と管理者が異なるため，問題を発見した場合に管理者は傷害のある計算機のところに直ちに向かう必要がある．しかし IP アドレスは実際の計算機の位置を示していない．どこで使われているかは管理者の判断基準の一つとして使う重要な情報でもある．

2.3　ネットワーク調査

内部ネットワークでは細かい調査が可能である．たとえば，稼働している計算機の IP や OS，稼働しているサービスとポートなどを調査できる．Nmap を用いたポートスキャンによる方法がある [8]．

3　提案する監視システム

内部ネットワークの監視システムには外部から内部，内部から外部への攻撃を十分に監視することが必要である．また，以前との比較によっても異常を発見しやすくなるので，時間情報も必要である．このように，IP アドレスを示す論理情報に加えて，地理情報と時間情報も統合して視覚化した監視システムが有効である．これらの三つの情報の関連性を十分に視覚化することが望ましい．

4　関連研究

- Starmine [3] は世界規模での監視システムである．IDS の snort のログを読み取り，選択した攻撃の攻撃元 IP アドレス

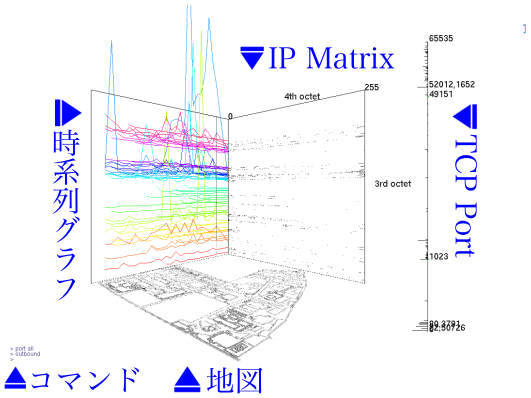

図 1: abstract

と地球上の座標の対応を表示する．論理情報と時間情報と地理情報が統合されている．

- IP Matrix [5] は IP アドレスの上位 16 bit または下位 16 bit を二次元マトリックス上に配置した視覚化手法である．それぞれの 8 bit は縦軸と横軸に配置され，ウィルスやワームの伝播の様子が視覚化された [8]．また，内部ネットワーク監視における有効な IP アドレスの表現方法としても用いられた．

- Secure Decisions [2] では計算機のある建物のフロアと計算機の種類によって分類した二次元マトリックスと，攻撃の危険性を関連づけて視覚化している．

- IDS RainStorm [1] では大規模 LAN として大学のネットワークが視覚化された．この大学のネットワークはクラス B のネットワーク 2.5 個分の大きさがある．縦軸に IP アドレス，横軸に時間をとって表示している．縦軸の IP アドレスは 20 アドレスを 1 ピクセルで表示しており，プロットされた色は緑，黄，赤の順に危険度が高くなる．

5 実装

5.1 対象

本研究では大規模 LAN の具体例として本学のネットワークを管理する情報基盤センターのネットワーク管理者を対象にした．本学はクラス B の IP アドレス空間を所有している．

5.2 システム概要

本システムは論理情報・時間情報・地図情報を各面に視覚化し，それを図 1 のように箱庭型に配置して対応を示したものである．さらにどのサービスへの攻撃があるかを示すために，宛先ポートの視覚化も行った．これには nmap によるネットワーク調査の結果を用いた．本システムでは外部から内部，内部から外部への攻撃を切り替えて視覚化する．また，ネットワーク管理者といったコンピュータのエキスパートはテキスト操作に慣れているため，GUI だけでなく CUI でも視点切り替え (図 2, 3, 4, 5) やフィルタリングの操作を可能にした．

5.3 ログの取得

侵入検知システム (IDS) のログを使用した．視覚化に使用した IDS は proventia [4] もしくは snort [7] である．これらはどちらも本学情報基盤センターで実際に運用しているものである．二つの IDS はどちらも内部ネットワークと外部ネットワークの境界に設置してある．snort のログは毎日約 500MB 出力されている．proventia のログは毎日 20MB から 100MB 程度出力されている．今回は出力し終えたログを読み込んで視覚化したが，リアルタイムで読み込むことも出来る．

5.4 論理情報

IP Matrix を用いて IP アドレスを視覚化した．クラス B のネットワークの全てのホストを視覚化できるように，縦軸に IP アドレスを第 3 オクテットを，横軸に第 4 オクテットをとっ

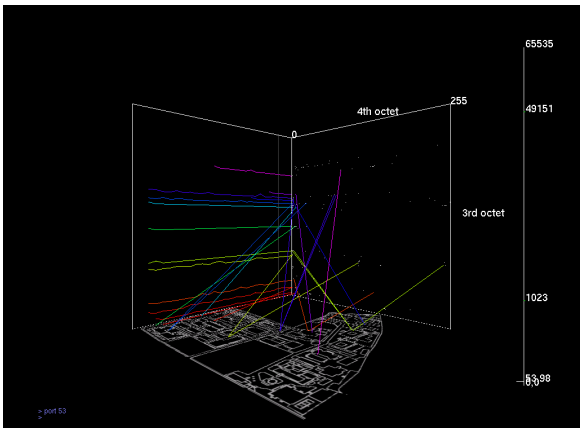

図 2: 俯瞰図

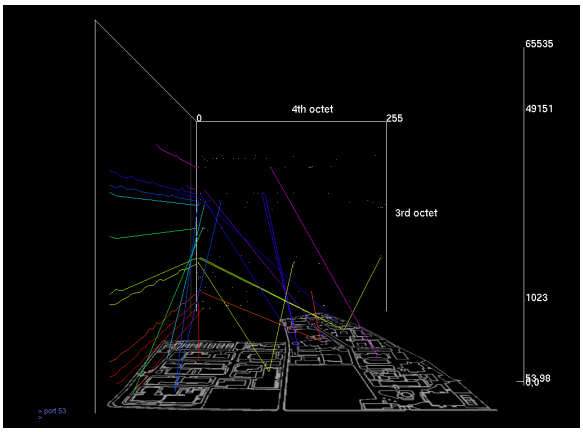

図 3: IP Matrix 用の視点

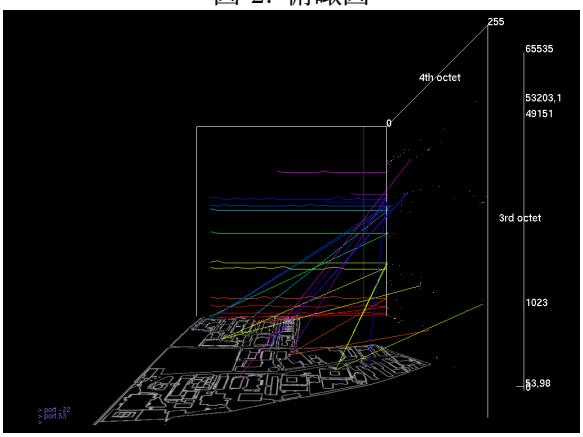

図 4: 時系列グラフ用の視点

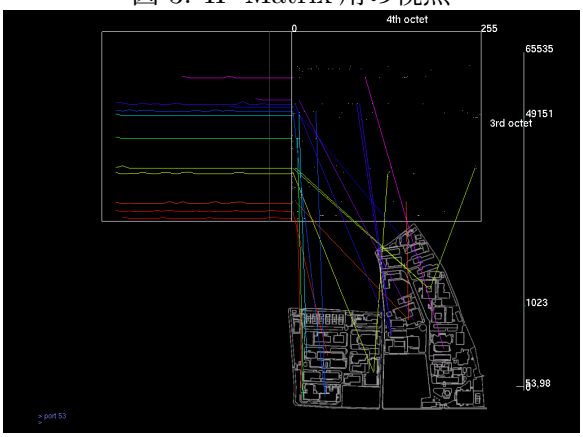

図 5: 展開図

た．ポートが空いていれば外部から攻撃される可能性があるので，プロットした．組織の保有する IP アドレスの全てが使われているわけではないので，これによってどの IP アドレスで計算機が稼働しているかがわかる．また，ネットワーク調査の結果よりホストの OS の種類を色で表した．

5.5 時間情報

時間情報は図 6 のように時系列グラフによって示した．グラフの原点は前述の論理情報でプロットされた IP アドレスの座標である．セキュリティ監視においては，具体的な攻撃量の数値よりもネットワーク間の比較が重要である．この時系列グラフでは攻撃量の具体的な数値はわかりづらいが，攻撃量の変化がわかりやすい．たとえば複数のホストで同時に攻撃量が増えて

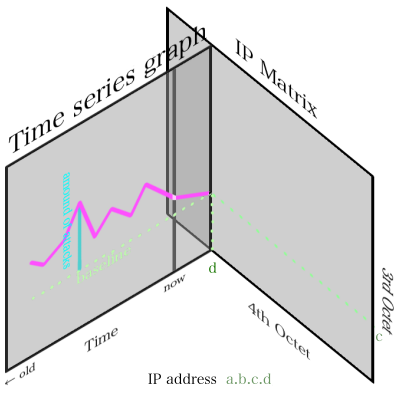

図 6: IP Matrix と時系列グラフの関係

いたり，一つだけ異なる波形をしていると直感的に判断できる．

時系列グラフの面は IP Matrix に垂直なまま横軸の方向に平行移動させることができ，それによって表示する第 4 オクテットを変更することができる．ただし第 4 オクテットが 0 の

ときはサブネットごとの攻撃量の和を示すようにした．なぜなら，まずはホスト一つ一つの情報よりもサブネットごとにまとめられた情報のほうが重要だからである．第 4 オクテットが 0 になるとネットワークアドレスのことになるので，ネットワークの熟練者はこの表現で直感的に分かるのである．これによって管理者は全体的な状況を一目で判断することができる．

5.6 地図情報

一般的に IP アドレス空間と地図上の位置に規則性はない．大規模 LAN では使用する IP アドレスもコンピュータの数も多い．そのため，IP アドレスからどの建物にあるホストかを瞬時に判断することは難しい．一般的に同一の建物や部屋のコンピュータはネットワークアドレスが同一である．また，攻撃されたホストがどのネットワークであるかわかれば，直ちに各サブネットのネットワーク管理者へ通知できる．そこでサブネットと地図上の位置との対応を事前に入力した．このデータを用いて IP アドレスからその計算機がどこにあるのかがわかるように線で示した．

5.7 ポート情報

一般に攻撃の送信先ポートを見ることでどのサービスへ攻撃したかがわかる．それゆえに送信先ポートごとの攻撃量によって攻撃の傾向を見ることができる．本監視システムでは，画面の右側に TCP の送信先ポートを表示した．縦軸はポート番号を示し，横軸は攻撃量の対数をとったものになっている．縦軸の下から 25.0% は well known port と呼ばれる 1024 までのポートを表示し，その上は 65535 までを示している．well known port はウェブやメール，DNS 等の重要なサービスが多く，そのため攻撃の対象にもなりやすい．この軸は表現したい情報量よりピクセル数が圧倒的に少ないため，LensBar [6] のようなズーマブルインタフェースを用いた．

5.8 フィルタリング

大規模 LAN のログは膨大であるため，全てを見ることは難しい．そのため，実際にネットワークを管理する場合には ”grep” コマンドを用いてログをフィルタリングして解析している．同様に大規模 LAN の視覚化システムにはフィルタリングが必要である．このシステムでは IP アドレスやポート番号によるフィルタリングをコマンドやマウス操作によって対話的にできるようにした．

6 運用例

本学の実際のデータを用いて視覚化した．以下にボットネットの視覚化の例をあげる．

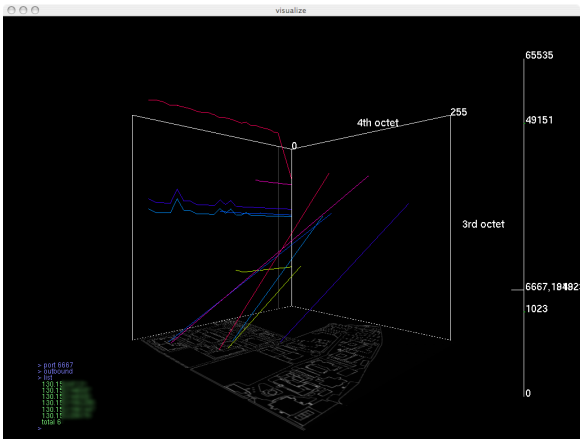

図 7: ボットネットの例

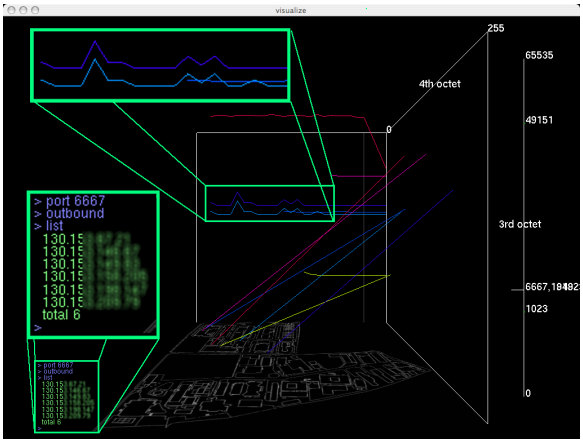

図 8: ボットネットの挙動

図 7 はボットネットと思われる不審な IRC chat の警告が出たときのものである．ボットネットとは外部から不正に遠隔操作できる PC で構成された悪意のあるネットワークのことである．ボットは命令を受けるために IRC サーバに接続し，Herder と呼ばれるボットネットを操る攻撃者の命令を待つ．IRC サーバは一般に 6667 番ポートを使っているため，この図の不審な IP アドレスへの接続はボットネットの疑いが強い．6667 番ポートのみが表示されるようにフィルタリングを行い，outbound の攻撃を選んだ．今回使用したログは snort のものである．

数カ所の IP アドレスから 6667 番ポートへのアクセスでアラートが出ていることがわかる (図 8)．その中で水色と紫色のデータがほぼ同一の攻撃量の変化を示していることがわかる．これによりボットネットに感染したコンピュータが同一の挙動を示すことと本システムの有効性を確認した．

7　今後の課題

実装した監視システムでは全体的な傾向はわかる．さらに実用性を高めるためには，詳細を見えるようにすることが必要である．また，IP やポート以外にもフィルタリングを可能にする．しかし複雑なフィルタリングが可能になると再設定が難しくなる．そのためフィルターの保存と読み込みを実装する．

実際の管理では通信量も監視している．そこで時系列グラフには攻撃量以外に通信量なども視覚化する．最後に，リアルタイムでログを監視して運用し，評価を行う．

8　結論

大規模 LAN のセキュリティ監視システムを開発した．不審な攻撃をしているホストの場所に直ちに駆けつけることができるようになった．実在する IP とポートを識別するためにネットワーク調査の結果を使用した．実際に運用し，その有効性を確認した．

謝辞

有益なご助言と IDS のログを頂いた電気通信大学情報基盤センター土屋英亮助教授に感謝いたします．

参考文献

[1] K. Abdullah, C. Lee, G. J. Conti, J. A. Copeland, and J. T. Stasko. IDS RainStorm: Visualizing IDS Alarms. *IEEE Workshop on Visualization for Computer Security (VizSEC 2005)*, page 1, 2005.

[2] S. Decisions. Secure decisions. http://www.securedecisions.com/.

[3] Y. Hideshima and H. Koike. STARMINE : A Visualization System for Cyber Attacks. *Asia Pacific Symposium on Information Visualisation (APVIS2006)*, 60:131–138, 2006.

[4] ISS. Internet Security Systems http://www.iss.net/.

[5] H. Koike, K. Ohno, and K. Koizumi. Visualizing Cyber Attacks using IP Matrix. *IEEE Workshop on Visualization for Computer Security (VizSEC 2005)*, page 11, 2005.

[6] T. Masui. LensBar - Visualization for Browsing and Filtering Large Lists of Data. In *INFOVIS '98: Proceedings of the 1998 IEEE Symposium on Information Visualization*, pages 113–120, Washington, DC, USA, 1998. IEEE Computer Society.

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

[8] 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. 情報処理学会, 2005.