Vol.2013-CSEC-61 No.18
Vol.2013-IOT-21 No.18
2013/5/10

# トラフィック情報表示システムによるscan攻撃の可視化

小刀稱 知哉[1]　松井 一乃[1]　池部 実[2]　吉田 和幸[3]

**概要**：大分大学のインバウンドトラフィックのパケットを取得し，送信元 IP アドレスの第 1 オクテットと第 2 オクテット，宛先 IP アドレスの第 3 オクテットと第 4 オクテットをそれぞれ軸にした 2 次元マトリックスで表示した．また，IP アドレスの対応する場所に，パケット数に応じて配色することで，ネットワーク管理者が一目で学内ネットワークの各ホストのトラフィック状況を把握可能なトラフィック情報表示システムを構築した．本論文では，トラフィック情報表示システムを用いて，一定間隔で現在のトラフィック状況を確認し，水平型の scan 攻撃の可視化を試みた．その結果，攻撃者からの送信パケットが少なく，IDS や tcpdump 等の出力データを確認するだけでは気づきにくい水平 scan 攻撃を把握できた．また，22 番ポートに関するパケットデータを取得するよう設定し，本システムと同時に運用している不正通信検知システム・SSH パスワードクラッキング検知システムが共に検知した攻撃者の挙動を可視化した．その結果，水平 scan 攻撃後に SSH パスワードクラッキング攻撃が仕掛けられている様子が観測できた．また，送信元 IP アドレスの第 1 オクテット，第 2 オクテットをパケット数に対応した色を用い，ヒルベルト空間曲線で表示することで送信元の分布を調査した．その結果，複数の送信元から 1 つの宛先にパケットを送信している様子が観測できた．

# Visualization for scan attacks with Network Traffic Viewing System

Tomoya Kotone[1]　Kazuno Matsui[1]　Minoru Ikebe[2]　Kazuyuki Yoshida[3]

***Abstract:*** We have developed a Network Traffic Viewing System that network administrators can easily grasp the traffic status for each host. Our system collects the number of packets from inbound traffic of Oita University. And, our system shows two-dimensional matrix that the horizontal and vertical axis were assigned the third and fourth octet of destination IP addresses. Moreover, the system shows the matrix with the first and second octet of source IP addresses. In this paper, we attempted to visualize the horizontal scan attack using traffic status obtained at intervals. As a result, we could grasped the indiscernible horizontal scan attacks that sent a few packet, just looking at the log outputted by IDS or tcpdump. Also, we collect packet data with port 22 and examine the attackers attempt to SSH password cracking attack after horizontal scan attack. And, we visualized its behavior with our system. As a result, we could grasp the SSH password cracking attacks after the horizontal scan attacks. And, we investigated a distribution of the source IP addresses using the Hilbert curve. This visualization method mapped the first and second octets of the source IP addresses to two-dimentional matrix. As a result, we could grasp attacks from various attackers to a specific host.

## 1. はじめに

インターネットの普及に伴い，ネットワークを通して様々な情報がやり取りされている．Web ページの閲覧や電子メールなどのコミュニケーション手段に留まらず，インターネット上での行政手続やクレジットカード番号を利用した電子決済など公共性の高いサービスも提供されてい

[1] 大分大学大学院工学研究科知能情報システム工学専攻
Course of Computer Science and Intelligent Systems, Graduate School of Engineering, Oita University
[2] 大分大学工学部知能情報システム工学科
Department of Computer Science and Intelligent Systems, Faculty of Engineering, Oita University
[3] 大分大学学術情報拠点情報基盤センター
Center for Academic Information and Library Services, Oita University

る．そのため現在では，ネットワークは社会的基盤の一つとして生活に不可欠な存在になっている．しかし，ネットワークを利用した不正通信も多く存在する．それは，システムの脆弱性を突くものや，ネットワークやホストの存在を探索 (スキャン）するものなど様々な脅威が存在する．

ネットワーク管理者がこれらの脅威を発見する手段として，IDS(Intrusion Detection System) や OS の各プロセスや tcpdump[1] 等が出力するログを解析する手法がある．

我々は scan 攻撃や DoS(Denial of Service) 攻撃等の不正通信を検知する「不正通信検知システム [2]」や，SSH サーバへのパスワードクラッキング攻撃を検知する「SSH パスワードクラッキング攻撃検知システム [3]」を開発・運用してきた．しかし，各システムが出力するログはテキスト形式であり，ネットワーク管理者が分析するには負担が大きい．また，ログに出力されたそれぞれの行の関連性が分かりにくいという問題点がある．そのため，効率良いネットワーク監視の実現や，異常検知の容易さなどネットワーク管理者の負担軽減につながるネットワーク監視手法が重要である．

そこで我々は，ネットワーク管理者に学内ホストの現在のトラフィック状態を表示する「トラフィック情報表示システム」を構築する．

本論文では，トラフィック情報表示システムの構築と本システムの有効性を述べる．まず，第 2 章では，トラフィック可視化技術に関する関連技術・関連研究について述べる．第 3 章では，我々が開発しているトラフィック情報表示システムについて述べる．第 4 章では，実際に本システムを運用して得られた水平 scan 攻撃の可視化例を示す．さらに，水平 scan 攻撃後の攻撃を可視化した例を示す．第 5 章では，送信元の分布をヒルベルト空間曲線で表示した例を示す．第 6 章では本論文の結論と今後の課題を述べる．

## 2. 関連研究

トラフィックの可視化には，SNMP(Simple Network Management Protocol) を用いる手法や tcpdump で収集したパケットを解析する方法がある．

SNMP を用いてトラフィックの流量の可視化するには，Tobias Oetiker 氏が開発した MRTG(Multi Router Traffic Gragher)[4] がある．MRTG は SNMP マネージャとして動作し，エージェントからネットワーク・トラフィック情報を取得し，PNG 形式のグラフ画像を生成する．高い柔軟性を持ち，ネットワーク・トラフィック情報のみではなく，SNMP で取得可能な他の情報 (CPU Load Average、Disk 使用率、メモリ空き容量等) や、外部コマンドの実行結果を利用することが可能である．MRTG が取得したデータは過去 2 年間分保存され，過去 1 日間，7 日間，4 週間，12 ヵ月間のグラフを生成する．しかし，SNMP ではスイッチのポート単位でのトラフィック量しか観測できず，学内ネットワークのホスト別トラフィック量を表示する必要がある場合，MRTG では困難である．

また，tcpdump で収集したパケットを解析して可視化する手法が存在する．大野ら [5] は広域ネットワーク監視のための視覚化フレームワークとして”IP Matrix” を提案している．これは，2 次元マトリックスを 2 つ用いて，送信元 IP アドレスの上位 16bit の状況と宛先 IP アドレスの下位 16bit の状況を表示するシステムである．また，攻撃を詳細に分析するため，1 ヵ月，1 日，1 時間の時間間隔を指定し，通信の変化をアニメーションで表示できる．IP Matrix を用いることで IP アドレスの論理的な近接関係を表現できる．しかし，IP Matrix ではすべての通信を単一の 2 次元マトリックスに表示するため，特定の送信元 IP アドレスやネットワークの通信に焦点を当てることができず，それぞれの通信がどの送信元から送信されたものか判断できない．この問題を解決するため，清野ら [6] は，IP Matrix を拡張し，複数の送信元 IP アドレスやネットワークの通信を視覚化する解析ツールを開発した．解析ツールでは，IP Matrix を用いて，複数の送信元の通信をそれぞれの 2 次元マトリックスに色分けして表示する．その後，それらのマップを透過的に重ね合わせることで，複数の送信元の通信を比較可能にする”Layered IP Matrix” を実装し，通信の変化をアニメーションで表現する．清野らはこの他にも，通信の変化を視覚化する機能として，WIV(Worm Infection Visualizer) を開発している．これは，IP アドレスの各オクテットの値を，それぞれ対応した枠の X 座標に縦線で表現し，合計 4 本の縦線で 1 つの IP アドレスを表す．さらに，表示した IP アドレスの縦線を時間の経過と共に減色することで通信時間の経過を表現している．上記のシステムでは，視覚化する対象がコンピュータワームの拡散であり，中長期の攻撃の可視化を目的としているため，収集する間隔が長い．

また，新川ら [7] は送信されたパケットの宛先 IP アドレス 32bit のうち，下位 8bit を横軸に，宛先ポート番号 16bit のうち，下位 8bit を縦軸に設定し，単位時間あたりのトラフィックの流量を色で表現する通信可視化ツールを構築している．2 次元マトリックス上にポート番号を加えることで，水平 scan 攻撃だけでなく，垂直 scan 攻撃も観測できる．しかし，宛先 IP アドレスの下位 8bit が重複した通信があった場合，別々の宛先ホストの通信が重複して表示される．

## 3. トラフィック情報表示システム

### 3.1 システム構成

我々が開発しているトラフィック情報表示システムは，インターネットから学内ネットワークへ送信されたパケットを取得し，トラフィック情報を表示する (図 1).

本システムは図 2 に示す 3 つのコンポーネント「収集部」

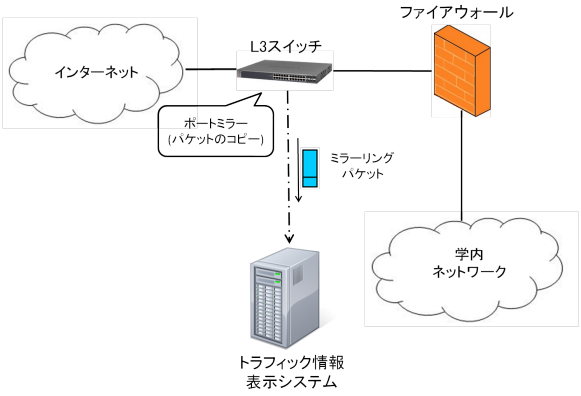



**図 1** システムの構成図

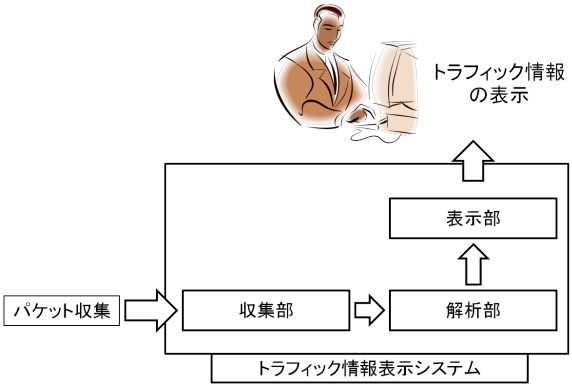



**図 2** システムの内部構成図

「解析部」」「表示部」から構成されている．

次節以降，それぞれのコンポーネントについて述べる．

### 3.2 収集部

収集部ではインターネットから学内ネットワークへ流れるパケットを tcpdump を用いて収集する．

本システムでは，インターネットと学内ネットワークの間に存在し，ファイアウォールの外側にある L3 スイッチからポートミラーしたパケットを収集している (図 1)．

また，tcpdump の機能を利用することで，特定のネットワークやホストからのパケットや，特定の TCP フラグが有効になっているパケット，特定のポート番号に関するパケットのみを収集できる．

### 3.3 解析部

解析部では収集部で得たパケットのバイナリデータから送信元 IP アドレス (外部ホスト) の第 1 オクテット・第 2 オクテット (図 3 の下線の部分)，宛先 IP アドレス (学内ホスト) の第 3 オクテット・第 4 オクテット (図 3 の二重下線の部分) を抽出・分類する．

また，一定時間ごとに収集したパケットを各分類別に集計し，収集結果を表示部へ渡す．

2013-02-21 09:20:21.627660 IP 78.188.X.Y.32949 > 133.37.Z.156.23: Flags [S], seq 1269122910, win 5808, options [mss 1452,sackOK,TS val 312931275 ecr 0,nop,wscale 2], length 0

**図 3** tcpdump から抽出した情報

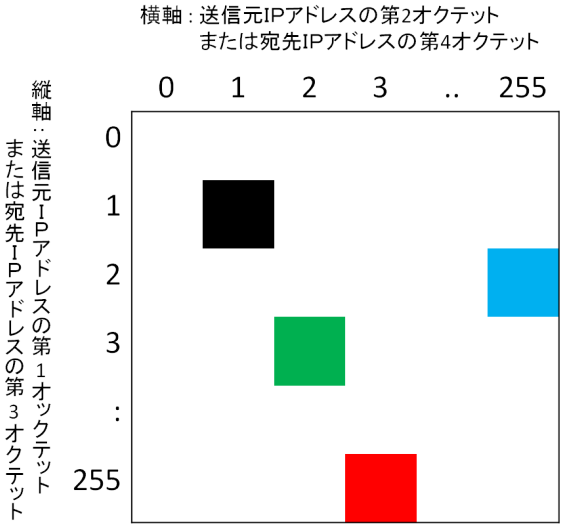



**図 4** 本システムの可視化のモデル図

| 色 | | パケット数 基準1 | パケット数 基準2 |
|---|---|---|---|
| | 赤 | 33~ | 244~ |
| | 紫 | 17~32 | 82~243 |
| | 青 | 9~16 | 28~81 |
| | 緑 | 5~8 | 10~27 |
| | 黄緑 | 3~4 | 4~9 |
| | 水色 | 2 | 2~3 |
| | 黒 | 1 | 1 |
| | 白 | 0 | 0 |

**図 5** パケット数と色の対応

### 3.4 表示部

表示部では解析部から得た情報をもとに，パケット数に応じて色分けする．今回用いた可視化のモデルを図 4 に示す．本システムでは外部ホストと学内ホストをそれぞれ表示させるため，縦 256 ×横 256 の 2 次元マトリックスを 2 つ作成する．1 つは縦軸と横軸に外部ホストの IP アドレスの第 1 オクテットと，第 2 オクテットをそれぞれ配置する．もう 1 つは縦軸と横軸に学内ホストの IP アドレスの第 3 オクテットと，第 4 オクテットをそれぞれ配置する．他にも，ヒルベルト空間曲線 [8][9] でも表示可能である．ヒルベルト空間曲線を用いることで，IP アドレスの隣接関係を比較的近い位置で表現できる．クラスフル IP アドレス (クラス A~E) をヒルベルト空間曲線で表現すると図 6 のようになる．

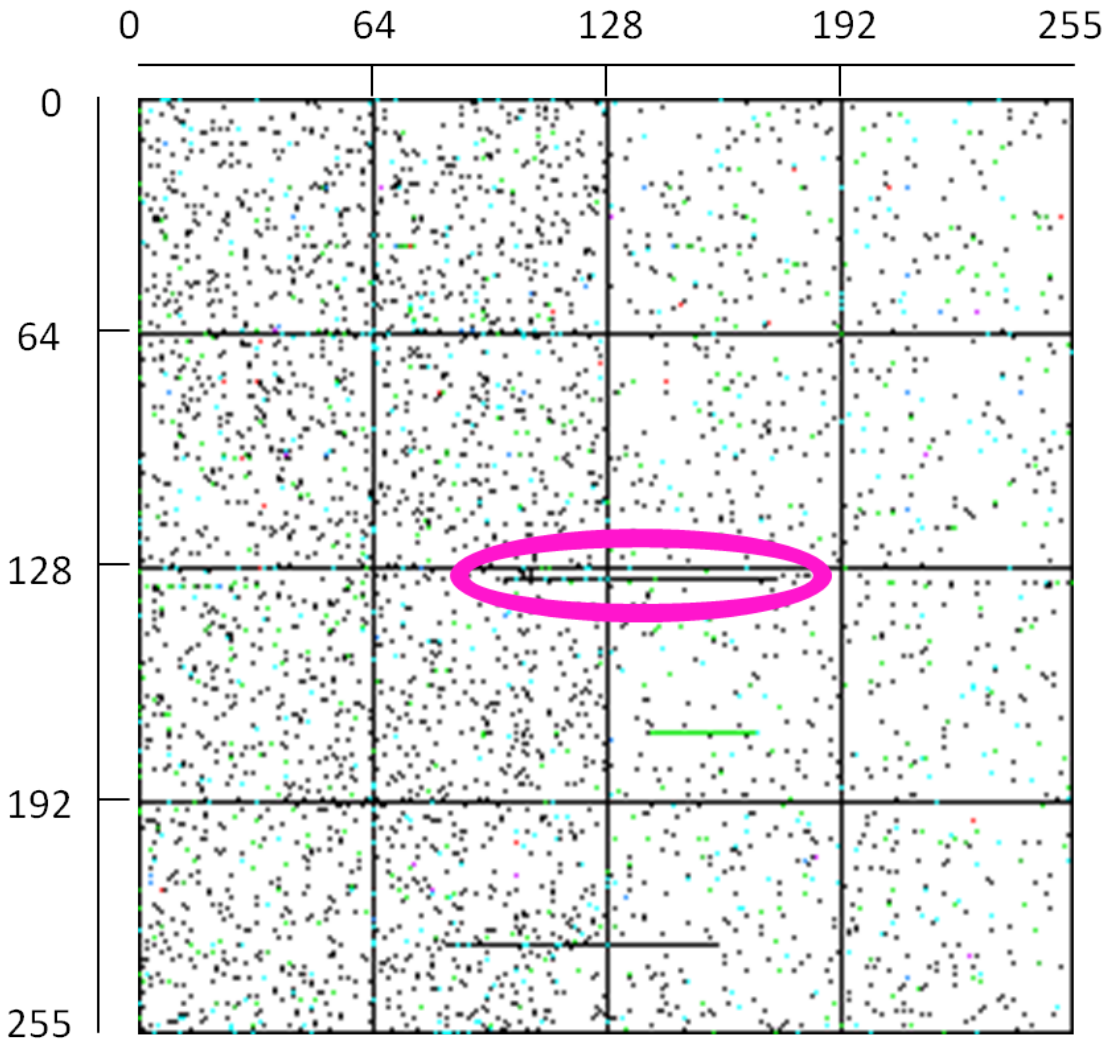



**図 7** 水平 scan 攻撃の可視化 (2013/02/14 04:45:00)

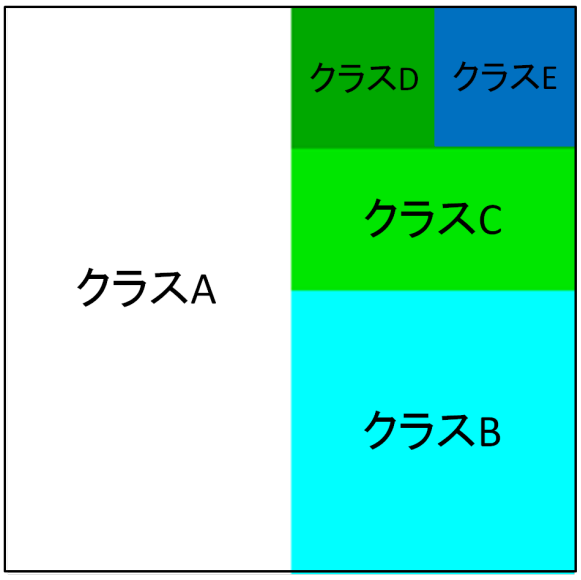



**図 6** ヒルベルト空間曲線を用いたクラスフル IP アドレスの表現

さらに，IP アドレスの対応する場所に，パケット数に応じて配色する．通信がない (パケット数が 0) 場合は白色で表す．一方，通信が観測された (パケット数が 1 以上) 場合にはパケット数に応じて黒，水色，黄緑，緑，青，紫，赤の順で表す．図 5 にパケット数と色の対応を示す．図 5 の配色の理由として，我々が開発・運用している不正通信検知システムの結果から，scan 攻撃者が対象の宛先ホストへ送信するパケット数は通常 1〜2 パケット程度であることが判明している．よって，背景を白に設定し，1 つのパケットを観測した場合には黒を設定し，scan 攻撃を受けているのが把握しやすい色に設定した．

また，外部ホストを表現する際，IP アドレスの第 1 オクテットと第 2 オクテットのみを利用しているのは，上位 2 オクテット (16bit) で地域を区別可能なためである．

さらに，学内ホストを表現する際，IP アドレスの第 3 オクテットと第 4 オクテットのみを利用している理由として，大分大学では学内 LAN をクラス B で運用しており，第 3 オクテットと第 4 オクテットのみを監視すれば，すべ

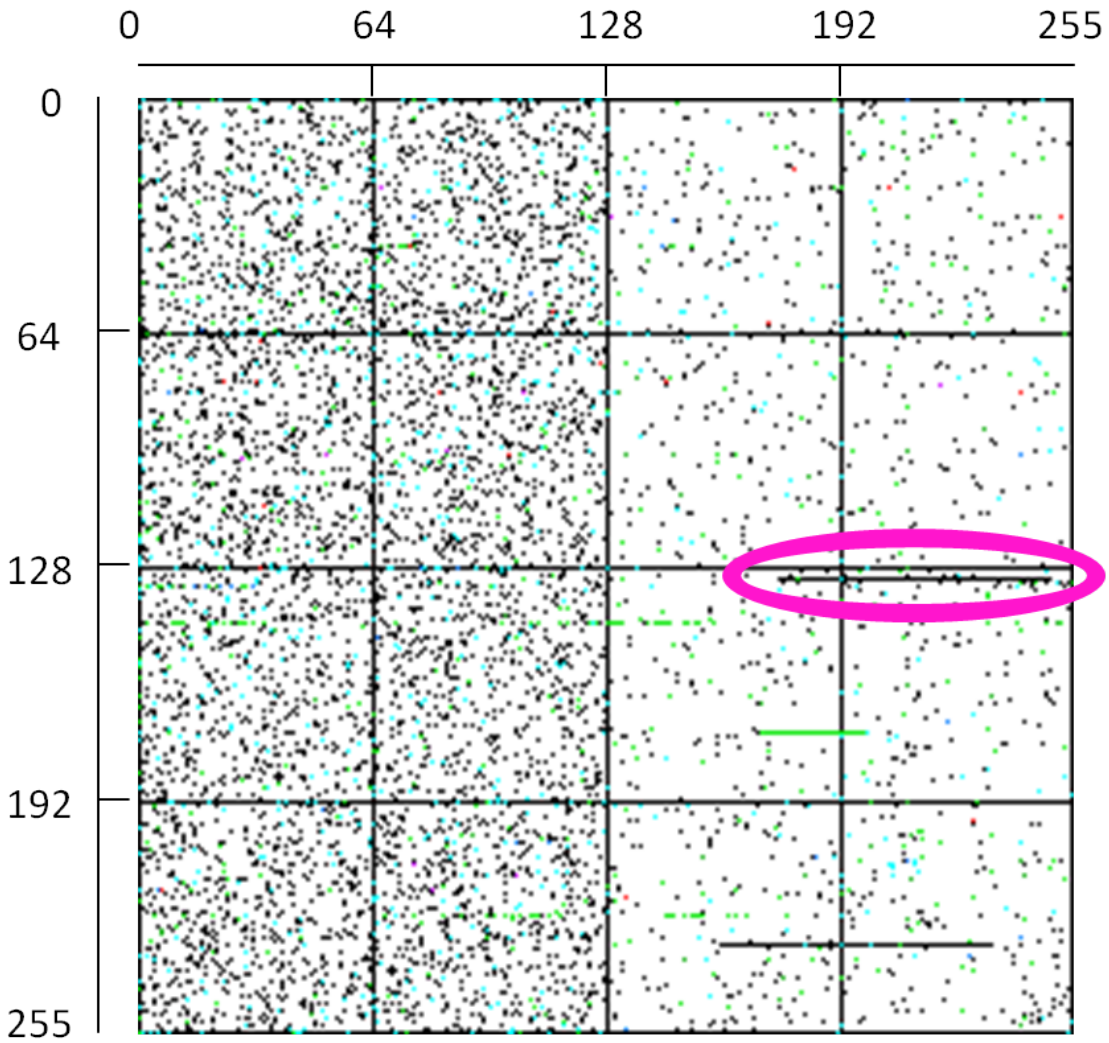



**図 8** 水平 scan 攻撃の可視化 2(2013/02/14 04:50:00)

ての学内ホストを表現可能なためである．

現在は，tcpdump を用いて作成したパケットデータを読み込み，各 png ファイルを作成し，web ブラウザから参照している．

## 4. 攻撃の可視化

今回は短期的な水平 scan 攻撃をリアルタイムに可視化することが目的であるため，300 秒毎にトラフィック情報を表示する設定にした．また，パケット数と色の対応には，図 5 の基準 1 を利用した．

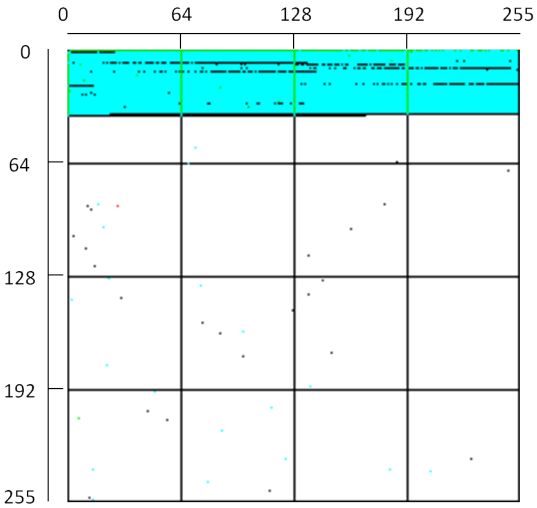
本システムの動作中，tcpdump にて本システムの入力と同じパケットデータを収集した．

### 4.1 水平 scan 攻撃の可視化

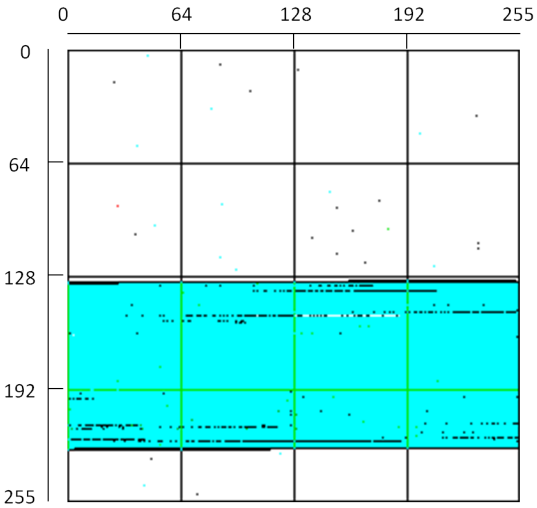
システム運用中に水平 scan 攻撃と思われる挙動を示した送信元ホストが存在した．水平 scan 攻撃の様子を図 7 と図 8 に示す．2 月 14 日 4:42 から 4:54 までに黒の帯域が図の右側から左側へと遷移していた．図 7 では，ピンク色の丸で囲まれた黒の帯域部分は図の左側に位置している．その 5 分後の図 8 では，右側に遷移していた．

同時刻のパケットデータを詳細に調査したところ，上記の送信元ホストは，宛先ポート番号を 8080 番ポート (Webcache) に設定し，学内ネットワークの 133.37.131.0/24 の範囲に 1 つずつ SYN パケットを送信していた．図 7 では，攻撃者が学内 IP アドレスの 133.37.131.25〜133.37.131.99 に 1 つずつ SYN パケットを送信していた．また，パケット送信割合は 300 秒間で 75 パケットであった．正規ユーザがこのような挙動をするとは考えにくく，これは，学内に 8080 番ポートのサービスが動作しているホストを探索する水平 scan 攻撃であると判断した．

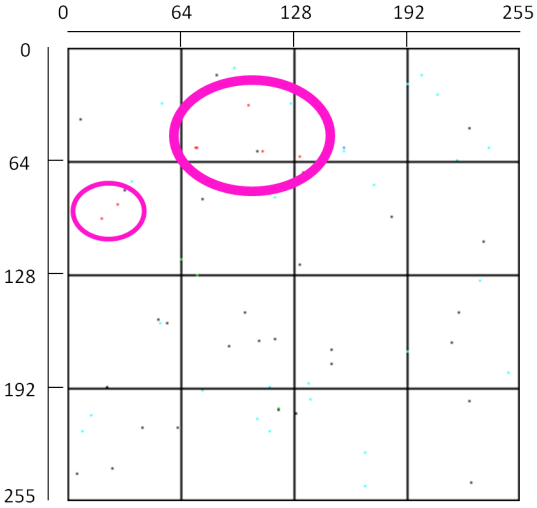
水平 scan 攻撃が観測された期間の 300 秒ごとの全体の受信パケット数は約 35,000 パケットであった．また，この攻撃者の 300 秒間の SYN パケットの送信数は 75 パケット (全体の 0.21%) であり，tcpdump の出力データを確認しただけでは，これが水平 scan 攻撃と判断するのは困難である．しかし，300 秒ごとのトラフィック量を表示する



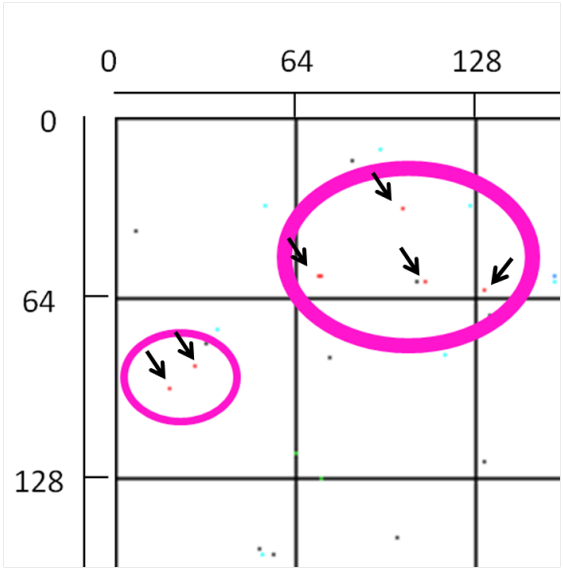

(a) :2013/03/09 04:45:00




(b) :2013/03/09 04:55:00




(c) :2013/03/09 05:05:00




(d) :2013/03/09 05:00:00 を拡大したもの

**図 9** 水平 scan 攻撃後の攻撃の可視化

ことで，黒の帯域の遷移が把握可能になり，通常では気づきにくい水平 scan 攻撃を発見できた．

### 4.2 水平 scan 攻撃後の攻撃の可視化

本システムと同時に運用している「不正通信検知システム [2]」と「SSH パスワードクラッキング攻撃検知システム [3]」が共に検知した攻撃者を調査し，学内ネットワーク内のホストに水平 scan 攻撃を行った後，反応のあったホストに SSH パスワードクラッキング攻撃を試みる挙動を可視化した．パケット取得の際に，tcpdump の機能により 22 番ポート (SSH) に関するパケットを取得する設定にした．可視化の様子を図 9 に示す．図 9 の (a) の段階では水色と黒の帯域が図の上部にある．その 10 分後の (b) の段階では水色と黒の帯域が下方へと遷移している．(b) の 10 分後の (c) の段階で，ピンク色で囲まれた特定の IP アドレスへパケットが多く送信されていた．(c) の段階を拡大したものを (d) に示す．

前節と同様に，tcpdump で収集したトラフィックを詳細に調査した結果，この攻撃者は，学内ネットワークの全ホストの 22 番ポート (SSH) に 2 つずつ SYN パケットを送信する水平 scan 攻撃を仕掛けていた．その際に不正通信検知システムが検知していた．その後，反応のあった学内ホストに SSH パスワードクラッキング攻撃を試みており，同様に SSH パスワードクラッキング攻撃検知システムが検知していた．

以上のことから，本システムにより，22 番ポートに関するパケットデータを取得すると，水平 scan 攻撃から SSH パスワードクラッキング攻撃へ遷移する攻撃者の挙動を把握可能である．

**図 10** 送信元の表示

## 5. 送信元の可視化

tcpdump の機能により SYN パケットのみを取得し，3,600 秒 (1 時間) ごとに送信元のトラフィック情報を表示する設定にした．

パケット数と色の対応には，図 5 の基準 2 を利用した．

前章と同様に，本システムの動作中，tcpdump にて本システムの入力と同じパケットデータを収集した．

### 5.1 送信元の表示結果

学内にパケットを送信した外部 IP アドレスをヒルベルト空間曲線で表示した．

結果を図 10 に示す．図 10 の赤色とピンク色の枠で示した部分に青色・紫色・赤色に着色された箇所が集団で存在していた．tcpdump で収集したトラフィックを詳細に調査した結果，複数の送信元 IP アドレスから学内で未使用の 2 つの宛先 IP アドレスへ大量の SYN パケット (3,600 秒で 24,000 パケット以上) が送信されていた．正規ユーザがこのような挙動をするとは考えにくく，これは，複数の攻撃者，または送信元を偽装した攻撃者が大量に SYN パケットを送信したと判断できる．

以上のことから，本システムにより，パケットを多く送信した送信元の分布が容易に把握可能である．

## 6. おわりに

### 6.1 まとめ

本論文では，管理者が一目で学内ネットワークの各ホストのトラフィック状況を把握可能なネットワークトラフィック表示システムを開発し，本システムの有効性について検証した．大分大学へ送信されたインバウンドパケットの送信元 IP アドレスの第 1 オクテットと第 2 オクテット，宛先 IP アドレスの第 3 オクテットと第 4 オクテットをそれぞれ 2 次元マトリックスで表示した．また，IP アド

レスの対応した場所にはにパケット数に応じて配色し，トラフィック量を色別で把握可能な表示方法を用いた．

システムの検証結果，少ない送信パケット数でも，時系列別に通信を観測した帯域の遷移が把握可能なため，通常気づきにくい水平 scan 攻撃が仕掛けられていることを発見できた．

この他にも，我々が開発・運用している不正通信検知システムと SSH パスワードクラッキング検知システムが共に検知した攻撃者の挙動を調査した．その結果，水平 scan 攻撃後に SSH パスワードクラッキング攻撃が仕掛けられている様子が観測できた．

また，学内にパケットを送信した外部 IP アドレスをヒルベルト空間曲線で表示した．その結果，複数の送信元から 1 つの宛先にパケットを送信している様子が観測できた．本システムにより，パケットを多く送信した送信元の分布が容易に把握可能である．

### 6.2 今後の課題

水平 scan 攻撃を検知する際，現在の設定は，1 枚の画像につき 300 秒間だけのパケット数を表示している．よって，水平 scan 攻撃者が連続した宛先 IP アドレスにパケットを送信した場合は攻撃の遷移が把握可能であるが，あるセグメントのランダムな宛先 IP アドレスにパケットを送信した場合には把握が困難である．その場合，少し前の状態も表示することで観測できる可能性がある．よって，以前のトラフィック状態を保持する期間について検討する必要がある．

また，トラフィックの表示を目的とする本システムと，実際の攻撃検知を目的とする不正通信検知システムや SSH パスワードクラッキング検知システムとの連携についても検討していく必要がある．

## 参考文献

[1] tcpdump. http://www.tcpdump.org/.
[2] 有馬竜昭, 小埜勇貴, 永山聖希, 吉田和幸：scan 攻撃検知システムの誤検知の調査，インターネットと運用技術シンポジウム 2011 論文集，pp. 45–50 (2011 年 11 月).
[3] 天本 大地, 小刀祢 知哉, 池部 実, 吉田和幸：scan 攻撃検知システムを用いた SSH に対する攻撃についての調査，第 65 回電気関係学会九州支部連合大会論文集，pp. 279–279 (2012 年 9 月).
[4] MRTG: The Multi Router Traffic Grapher. http://oss.oetiker.ch/mrtg/.
[5] 大野一広, 小池英樹, 小泉芳：IP Matrix: 広域ネットワーク監視のための視覚化手法，情報処理学会論文誌，Vol. 47, No. 4, pp. 1077–1086 (2006 年 4 月).
[6] 清野祥之，小池英樹：複数ホストの通信視覚化による比較解析，情報処理学会マルウェア対策研究人材育成ワークショップ (MWS2010) (2010).
[7] 新川拓也，山之上卓：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，情報処理学会研究報告. DSM, [分散システム/インターネット運用技術]，pp. 31–36 (2006 年 9 月).
[8] Irwin, B. and Pilkington, N.: High Level Internet Scale Traffic Visualization Using Hilbert Curve Mapping, VizSEC 2007, Mathematics and Visualization, Springer Berlin Heidelberg, pp. 147–158 (2008).
[9] Munroe, R.: Map of Internet. http://www.xkcd.com/195/.