TreemapとEdge Bundlingを用いたネットワークトラフィック可視化システムの機能拡張

秋吉 亮[1]　岡田 義広[1,2]

概要：近年では，インターネット社会の発展に伴い，インターネットが国民の身近なものとなる一方で，サイバー犯罪が年々増加傾向にあり，犯罪手口についても高度化・多様化している．特に，脆弱性が発見されてから対策が周知されるまでに受ける攻撃はゼロデイ攻撃と呼ばれ，ウイルス対策ソフトだけでは防ぐことができないため問題となっている．本研究では Treemap と Edge Bundling を利用したダークネットのトラフィックを可視化することで攻撃と考えられるトラフィックの発見を補助するシステムである PacketVisualization の機能拡張を行った．各種フィルタの追加や表示機能の拡張により，膨大なデータの可視化解析を効率的に行うことが可能となる．

キーワード：サイバー攻撃, ネットワークデータ, 可視化, Treemap, Edge Bundling

Function Enhancement of Visualization System with Edge Bundling and Treemap for Network Traffic

Ryo Akiyoshi[1]　Yoshihiro Okada[1,2]

Abstract: The Internet is becoming familiar with people as the development of Internet Society; however, cyber crime is growing, and moreover that criminal technique is becoming more sophisticated and diverse. Especially, zero-day attack, which is an exploit by the attacker before the treatment against the vulnerability, is a serious problem because that cannot be prevented only by anti-virus software. In this paper, the authors extended functionalities of a PacketVisualization system of network traffic data using Treemap and Edge Bundling for analysis of such attacks. As the extension, the authors added some filtering and visualyzing functions that enable us to visually analyze a vast of network traffic data efficiently.

Keywords: Cyber attacks, Network data, Visualization, Treemap, Edge Bundling

1. はじめに

1.1 研究背景

近年では，インターネット社会の発展に伴い，インターネットが国民の身近なものとなる一方で，不正アクセス，システム妨害，オンライン詐欺などのサイバー犯罪が年々増加傾向にある．また，犯罪手口についても高度化多様化しており，ウイルス対策ソフトだけではゼロデイ攻撃のような新たな脆弱性を悪用した攻撃を防ぐことが出来ず，対処が難しくなってきている．したがって，新たな攻撃を検知し，被害を防止もしくは被害の拡大を最小限に留めることが求められている．

1.2 情報可視化

情報可視化 (Information visualization) とは，抽象的情報の特徴を人間が発見もしくは理解するのを助けるため，

[1] 九州大学, 福岡県福岡市西区元岡 744 番地
Kyushu University, Motooka 744, Nishi-Ku, Fukuoka, 819-0395, Japan
[2] 九州先端科学技術研究所, 福岡県福岡市早良区百道浜 2 丁目 1 番 22 号福岡 SRP センタービル 7 階
Institute of Systems, Information Technologies and Nanotechnologies (ISIT), Fukuoka SRP Center Building 7F, Momochihama 2-1-22, Sawara-ku, Fukuoka, 814-0001, JAPAN

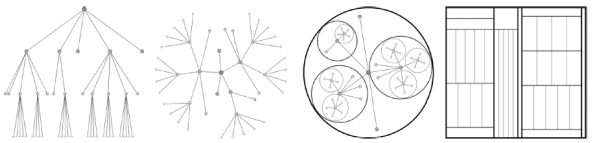

図 1　階層構造を表すグラフの例

画像やアニメーションのような視覚的表現に変換することである．情報可視化に関する研究が始められた頃は，情報可視化を行うことができる計算機が非常に高価であったため，情報可視化の研究をできる機関は限られていたが，近年は安価なコンピュータでもリアルタイムでの 3 次元表示などの高度な描画が十分可能になったため，情報視覚化は極めて身近な技術となってきている．

1.3　研究概要

1.3.1　Treemap

Treemap[1] は，B.Shneiderman によって考案された，階層構造データの可視化手法の一つである．階層構造の可視化手法とそれらの特徴は以下のようにまとめることができる．

表形式 (listing)
表形式は，詳細な情報を提供できるが，一般に構造的な情報を表しにくいという特徴がある．また，大規模な情報を表現するのには向いていない．

箇条書き形式 (outline)
箇条書き形式は，構造的な情報およびデータの内容を表すことができるが，構造的な情報を表すインデントは数行しか表現することができないので不十分であるという特徴がある．また，表形式と同様に，大規模な構造を表現するのに向いていない．

根付き木 (Rooted Tree)
根付き木は，ノードの隣接を直感的に表現する手法の一つであり，親ノードと子ノードに線を引くことで階層構造のデータを可視化する手法である．この手法では，大規模な階層データに対してはノードが密集してしまい，また，ディスプレイ領域を有効に活用することができないという特徴がある．

Treemap
Treemap は，二次元平面上の領域を入れ子状に分割することによって，階層構造のデータを可視化する手法である．空間充填によるレイアウトであるため，ディスプレイスペースを有効に利用することができる．また，階層構造データ全体を表示することができ，各葉ノードの大きさを容易に比較することができる．Treemap の詳しい特徴およびアルゴリズムは第 3 章で詳しく説明する．

1.3.2　Edge Bundling

Edge Bundling[2] とは，Danny Holeton によって考案された 2006 年から始まる比較的新しい技術であり，図 1 のような階層構造を表すグラフにおいて，関係があるノード間にエッジを引くことを指す．Edge Bundling の詳細については第 3 章で説明する．

1.3.3　ダークネット

ダークネットとは，インターネット上で到達可能な IP アドレスのうち，ホストが割り振られておらず，未使用の IP アドレス空間のことを指す．[3] 通常のインターネットの利用では未使用の IP アドレス空間に対してパケットが送信される可能性は低いが，実際には相当数のパケットがダークネットに到達している．観測させる全てのパケットは，設定ミス，送信元 IP アドレスの偽装によるバックスキャッタ，ワームによるスキャンや，その他のネットワークの調査によるものである．したがって，ダークネットに到達するパケットを観測することは，インターネット上での不正な活動を検知および調査するために非常に重要であり，DDos 攻撃，ワームによるスキャン，ボットネットのようなインターネット上の脅威についての情報を得ることが出来る．

1.4　論文構成

本論文は以下の構成をとる．第 1 章では，本研究の背景と概要について述べた．第 2 章では，関連研究を紹介する．第 3 章では，本研究で使用した Treemap のアルゴリズムと EdgeBundling，および，サイバー攻撃に付いて述べる．第 4 章では PacketVisualization の機能拡張について述べる．第 5 章では，本論文のまとめを述べる．

2.　関連研究

2.1　階層構造の可視化に関する研究

階層構造の可視化に関しては，現在までに様々な研究がなされている．ノードの親子関係を線で表現した手法であるものとしては，それぞれのノードがそのノードの深さによってルートノードを中心とする同心円上に位置する Radial Tree[7]，各兄弟ノードがその親ノードを中心とする円の内側に位置する Balloon Tree[8] 等がある．また，画面へのマッピングの研究として，注目しているノードを中央に置き，その親ノードと子ノードをその周囲に配置する Hyperbolic Tree[9] が挙げられる．Hyperbolic Tree は，表示の際に中央から遠くなるほどノードを小さく描画することによって，大きな構造であっても画面内に収まるようにしている．

3 次元空間に階層構造データを可視化するものとしては，親ノードを頂点とする円錐の底面円周上に配置する Cone Trees[6] や，階層情報を立方体の入れ子として可視化する Information Cube[10] がある．また，Treemap に関連するものとして，Treemap の 3 次元拡張版である Treecube[5] がある．

2.2 ネットワーク情報の可視化に関する研究

複雑かつ大規模なインターネットの構造や，インターネットを流れる大量の情報を視覚化する試みが近年多数行われている．独立行政法人 情報通信研究機構（NICT）が公開している nicterWEB[11] では，インシデント分析センター（nicter：ニクター）が観測したダークネットのトラフィックの一部をリアルタイムに可視化している．nicterWEB では，ダークネット宛のトラフィックの送信元 IP，宛先 IP およびポート番号に関する情報を立方体にマッピングして可視化する「Cube」や，世界地図上でトラフィックを表現し，国別のトラフィックに関する情報を可視化する「Atlas」を提供している．

2.3 サイバー攻撃の検知に関する研究

近年、多様化・高度化しているサイバー攻撃の被害を最小限に抑えるために、攻撃を早期に検知して迅速に対処することが求められており、サイバー攻撃を検知する試みが数多くなされている。サイバー攻撃を検知するツールは、IDS（侵入検知システム：Intrusion Detection System）と呼ばれ、リアルタイムで通信を分析し、定義されたパターンと比較することで不正アクセスによりパケットを検知し、管理者に通知する。[14] IDS は、その監視方式によってネットワーク型 IDS（NIDS）とホスト型 IDS（HIDS）に分類することができる。ネットワーク型 IDS はネットワークを流れるパケットを全て監視するものであるが、通信が暗号化されている場合は検知できないという特徴がある。一方ホスト型 IDS は特定のコンピュータの通信を監視するものである。また、分析方式によってシグネチャ型とアノマリ型に分類することができる。シグネチャ型はネットワーク攻撃に関する情報（シグネチャ）と分析するパケットを比較することで不正アクセスを検知する方式である。一方アノマリ型では定義された通常の通信パターンと比較し、ある閾値を超えたときに不正アクセスとして検知する方式である。ネットワーク型 IDS として最も有名なものとしては、フリーのソフトウェアである SNORT®[13] がある。また、ホスト型 IDS としては、Tripwire 社による Tripwire[15] がある。また、IDS の拡張型であり、侵入検知だけでなく接続の遮断などの防御を行う機能をもつものは IPS（侵入防止システム：Intrusion Prevention System）と呼ばれる。

3. 準備

3.1 Treemap アルゴリズム

Treemap は階層構造をもつ情報を，2 次元平面上の領域を入れ子状に分割することによって可視化する手法である．木構造では大きな階層構造を表現しようとすると深さが大きくなっていくにつれて大きさが広がるという性質があるが，Treemap では空間充填によるレイアウトとなっているため，大きな構造でもディスプレイ領域を有効利用できるという性質がある．それぞれのノードは長方形で表され，その面積は設定された特徴量の値に比例する．加えて，色のパラメータを変化させることで，より多くの情報を表現することもできる．Treemap アルゴリズムは多くの提案がなされているが，本節では，Slice-and-dice Treemap[1]，Squarified Treemap[4] について紹介する．

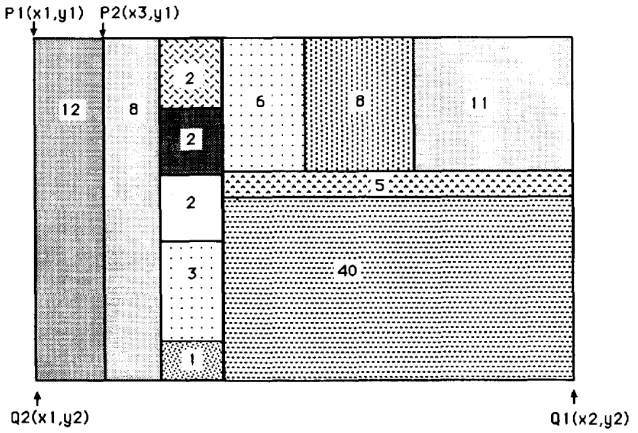

図 2 Slice-and-dice Treemap

Slice-and-dice Treemap

Slice-and-diceTreemap は，まず，木構造のルートおよび，左上と右下の座標を表す $P1(x1, y1)$, $Q1(x2, y2)$ で定義される正方形領域が入力として与えられる．次に，ルートノードからの出力辺を $[x1, x2)$ の範囲の区画で定義する．ルートノードが持つ子のうち，最も左の子はルートノードのサイズの $Size(child[1])/Size(root)$ 倍のサイズを持っているため，以下の式に従って 1 つ目のの垂直な区切り線を描く．

$$x3 = x1 + \frac{Size(child[1])}{Size(root)} \times (x2 - x1)$$

以下，このアルゴリズムは長方形 $P2(x3, y1)$，$Q2(x1, y2)$ を 90°回転させて再帰的に分割・マッピングを行う．

Squarified Treemap

Squarified Treemap は，簡単なアルゴリズムで各ノードがマッピングされる長方形領域のアスペクト比を 1:1 に近づけた Treemap である．また，入力として長方形領域 R と順序付きノードのリスト L を入力とする．以下にアルゴリズムを示す．

(1) 順序付きノードのリスト L を各ノードの重みで降順にソートする．
(2) 長方形領域 R の短い方の辺に沿ってノードをマッピングする．
(3) 2 でノードマッピングした際に，各ノードのアスペクト比の最大値がマッピングする前の各ノードのアスペクト比の最大値よりも高くなる場合はマッピングしない．アスペクト比が高くならない場合は 2 を再帰的に繰り返す．

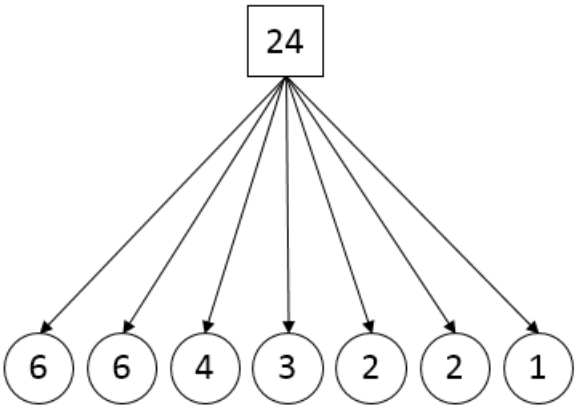

図 3　(a) 木構造

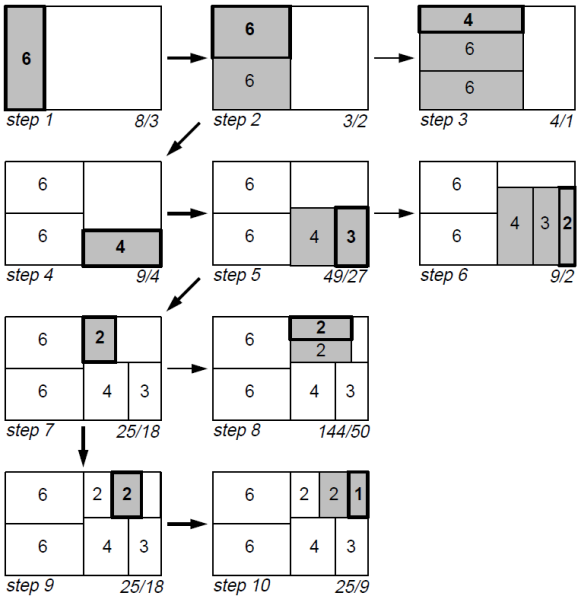

図 4　(b)Squarified Treemap

(4) 3. で追加しなかった場合は，残りの部分を新たな長方形領域 R，残りのノードを新たな順序付きノードのリスト L として，2,3,4 を再帰的に繰り返す．すべてのノードがマッピングされるとアルゴリズムは終了する．

図 3 の (a) で表される木構造データがこのアルゴリズムによってマッピングされる例を，図 4 の (b) に示す．Squarified Treemap は最終的な各ノードを表す正方形のアスペクト比を 1:1 に近づけるため，各ノードを比較，および，選択することが簡単になる．しかし，ノードを重みの大きい順にソートした配置であるため，レイアウト上での順序が損なわれ，特定のノードを探すのが困難である．

3.2　Edge Bundling

Edge Bundling は，階層構造を表すグラフにおいて，関係があるノード間に線（Edge）を引くことを指す．単純な直線，または，曲線でエッジを引いただけでは図 5 の (a)，(b) のように，Visual Clutter と呼ばれるグラフの可視性の低下が発生する．そこで，図 6 の (c) ようにエッジを引くノード間の経路上のノードを制御点として，スプライン曲線でエッジを描くことで，エッジが束ねられ，Visual Clutter を低減することができる．Edge Bundling によって図 5 の (b) で表されるグラフの Visual Clutter が低減されたものを図 7 に示す．

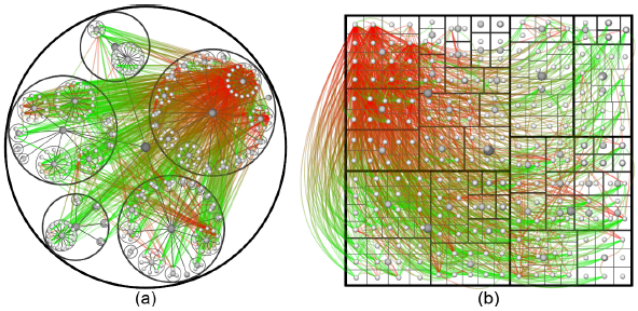

図 5　(a) 単純な直線，(b) 単純な曲線でエッジを引いた図（緑から赤への向き）

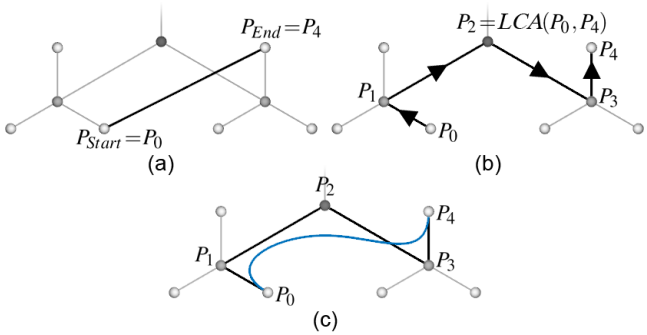

図 6　(a) 直線によるエッジ，(b) 始点から終点までの道，(c) スプライン曲線によるエッジ

3.3　サイバー攻撃

サイバー攻撃は，コンピュータやネットワークへの不正アクセスによって，データの不正な取得，破壊，改ざん等を行ったり，特定のサービスの機能を停止させるような攻撃のことを指す．本節では，ポートスキャン，ゼロデイ攻撃，DoS 攻撃/DDoS 攻撃について説明する．

3.3.1　ポートスキャン

インターネットの通信で一般的に使用される TCP あるいは UDP では，ポート番号と呼ばれる 16 ビットの符号なし整数 (0〜65535) で表される識別子によって通信を行うプロセスを区別している．ポートスキャンは，このポートに順番にアクセスし，脆弱なポートがないかどうかを調べる行為である．

3.3.2　ゼロデイ攻撃（Zero-Day Attack）

ゼロデイ脆弱性（Zero-Day Vulnerability）は，攻撃者が脆弱性を発見してからその脆弱性に対する修正プログラム

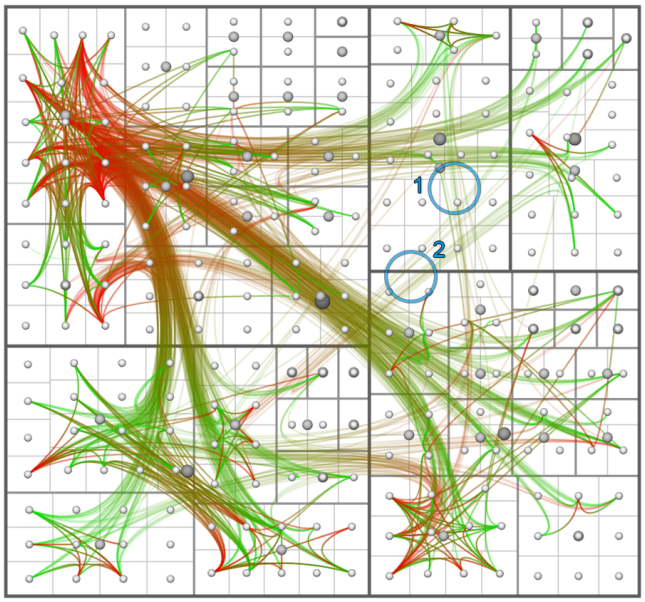

図 7　図 5 の (b) に Edge Bundling を適用した例

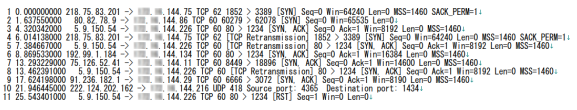

図 8　可視化するダークネットの観測データ

図 9　Treemap で可視化した画面

が公開されるまでの脅威にさらされているセキュリティホールのことを指し，このセキュリティホールが存在する間にその脆弱性を突いて攻撃者が攻撃することをゼロデイ攻撃と呼ぶ．[12]

3.3.3　DoS 攻撃/DDoS 攻撃

DoS 攻撃（Denial of Service attack）は，特定の標的に不正なデータや大量のデータを送信することで標的のコンピュータに負荷をかけ，システムを停止状態にさせたり以上終了させる攻撃のことである．

DDoS 攻撃（Distributed Denial of Service attack）は DoS 攻撃を分散攻撃の手法に進化させたもので，ボットネットによる攻撃が有名である．ボットネットはボットによって構成されるネットワークの事を指し，ボットとは攻撃者が無関係なコンピュータをマルウェアに感染させ，外部からの司令によって操作できる状態にしたコンピュータのことを指す．

DoS 攻撃は，攻撃元が一つであるので，比較的容易に攻撃元を特定し，遮断することで対策を講じることが可能である．一方，DDoS 攻撃は，ボットネットからの攻撃であるため，攻撃が分散しており，攻撃命令を出した攻撃元を特定するのが難しく，また，正常な通信との見分けもつきにくいため，攻撃元を 1 つずつ遮断していくのも容易ではない．

4.　PacketVisualization

4.1　システム構成

PacketVisualization の開発言語は C#であり，Windows 用ソフトウェアである .Net Framework 4.5 以上の環境での動作を前提としている．また，後述する 3D Edge Bundling グラフの描画には Direct X を使用した．読み込むダークネット観測データは，Wireshark の CUI 版である tshark を用いて，パケットキャプチャを行ったデータを図 8 のようなテキストファイルに変換したものを使用した．観測データには様々な情報が含まれているが，本システムでは以下のものを用いた．

- 時間
- 送信元 IP アドレス
- 宛先 IP アドレス
- 宛先ポート番号

4.2　PacketVisualization

PacketVisualization は前章で紹介した Treemap および EdgeBundling を用いてダークネットの観測データを可視化するツールである．観測データは Wireshark の CUI 版である tshark を用いて，ネットワーク観測データを図 8 のようなテキストファイルに変換したものを使用した．

4.2.1　マクロレベル可視化

PacketVisualization は 1 ヶ月のダークネット観測データを図 9 のように Treemap に表示する．階層構造は 1 ヶ月，1 日，1 時間の構造を持つ．各ノードの大きさは当該ノードのパケット数に比例し，色は葉ノードに含まれるパケットの送信元 IP のユニークホスト数についての情報量を表しており，情報量が小さい（葉ノードの色が赤い）とき，そのノードは特定の送信元 IP から大量のパケットが送信されていると判断することができる．また，各ノードをクリックによって選択することで，当該ノードの時間・パケット数・ユニークホスト数を表示し，Edge Bundling を用いたミクロレベル可視化で描画するノードを選択することができる．

4.2.2　ミクロレベル可視化

前述したマクロ解析の画面で選択したノードを，図 10 のように，2 つの Treemap と Edge Bundling を用いた可視

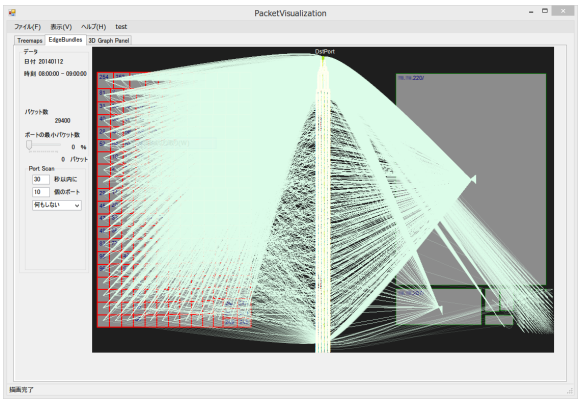

図 10　EdgeBundling でトラフィックを可視化した画面

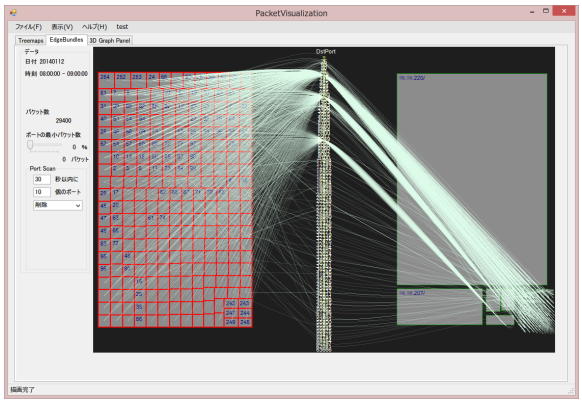

図 12　ポートスキャンを削除した図

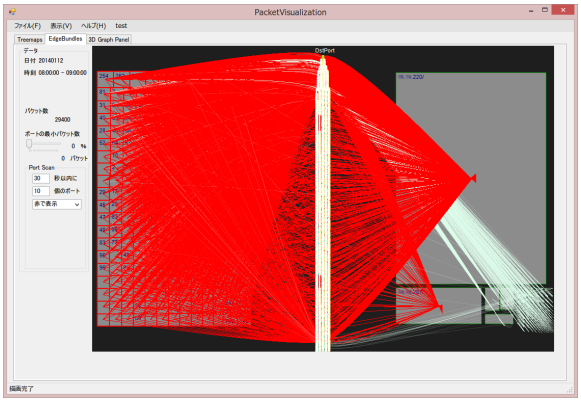

図 11　ポートスキャンを赤で表示した図

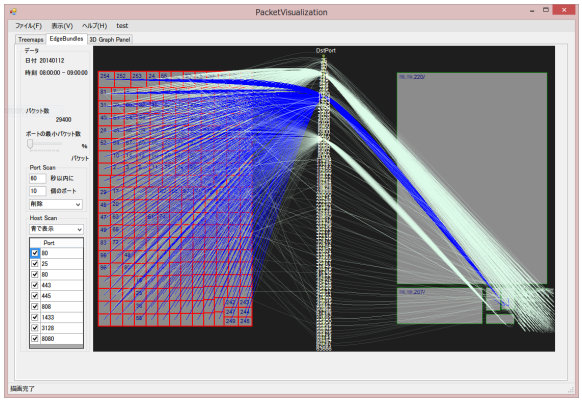

図 13　ホストスキャンを赤で表示した図

化により詳細に表すことができる．左の Treemap が宛先 IP，中央の点が宛先ポート，右の Treemap が送信元 IP を表しており，それらを繋いでいるエッジそれぞれがパケットを表している．

4.3　PacketVisualization の拡張

本節では、前述した PacketVisualization に追加した機能について述べる。

4.3.1　ポートスキャンの検知

第 3 章で紹介したポートスキャンを検知する機能を追加した．ポートスキャンを検知する手法として，Snort[13] と呼ばれるフリーの侵入検知システムの手法を使用した．この手法では，特定のホストから t 秒以内に p 以上のポートに対してパケットが観測されたときにポートスキャンとして検知する．この手法によって図 10 で表されるトラフィックからポートスキャンを検知したものを図 11 に示す．ここでは，閾値は t=30，p=10 とし，ポートスキャンとして検知したパケットを赤のエッジで表示した．

また，ポートスキャンとして検知されたパケットを削除することにより，Visual Clutter を改善することができた．図 10 および図 11 で表されるトラフィックからポートスキャンとして検知されたパケットを削除したグラフを図 12 に示す．これらの図を比較すると，図 10 および図 11 でポート番号を表す文字やパケットを表すエッジが重なって表示され，Visual Clutter の問題が発生していたが，図 12 ではそれらがある程度は解消されていることが分かる．

4.3.2　ホストスキャンの検知

4.3.1 で述べたポートスキャンの検知方法とほぼ同様の手法でホストスキャンを検知する機能を追加した。この手法では、特定のホストから事前に指定したポートへ t 秒以内に p 以上のホストに対してパケットが観測されたときにホストスキャンとして検知する。この手法によって図 10 で表されるトラフィックからホストスキャンを検知したものを図 13 に示す。ここでは、閾値は t=60、p=10 とし、ホストスキャンとして検知したパケットを青のエッジで表示した。

4.3.3　画像出力機能

4.2 で述べた PacketVisualization では、特徴のあるノードを探すためには Treemap の画面からノードを一つ選択し、Edge Bundling グラフを表示する必要があり、それぞれのノードの Edge Bundling グラフを比較するのが困難であった。そこで各ノードの Edge Bundling グラフを最大で 1 ヶ月分まとめて画像に出力する機能を追加することでこの問題を対処した。これにより、ユーザが使い慣れた画像閲覧ソフトを使用して、容易に各グラフを比較、および、特徴のあるグラフを探すことができる。

図 14　出力画像選択画面

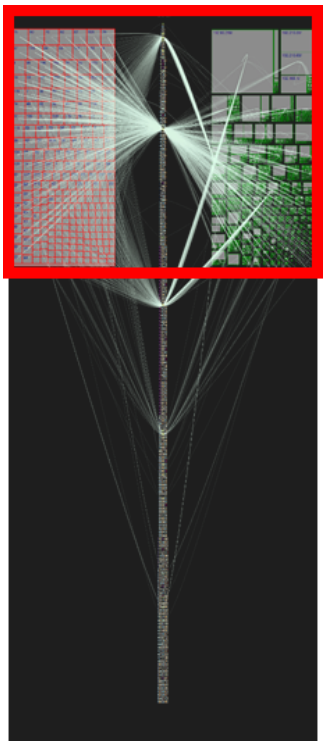

図 15　3D Edge Bundling 用のグラフ

4.3.4　3D Edge Bundling グラフ

前節で述べた画像出力機能で出力したそれぞれのグラフでは、それぞれ左右の Treemap のレイアウトが異なるだけでなく、描画されているポートの位置も異なるため、それぞれのグラフを比較するには不十分な点があった。そこで、それぞれの 1 時間分のグラフを 1 日分（24 枚）3 次元的に縦に重ねることで、より容易に各グラフを比較するための機能を追加した。

描画方法

3D Edge Bundling グラフでは、各ポートの時間的変化を解析することが目的であるため、1 度に全てのパケットをディスプレイ領域に描画することよりも、それぞれのエッジが重ならないよう描画することが求められる。そこで中央の各ポートを等間隔に描画し、図 15 のように縦に長いグラフを描画し、その赤で囲った部分で示されるような一部を画面に表示するという手法をとった。また、グラフを重ねるにあたって、それぞれのグラフの中央のポート番号の位置と左右の Treemap を統一した。

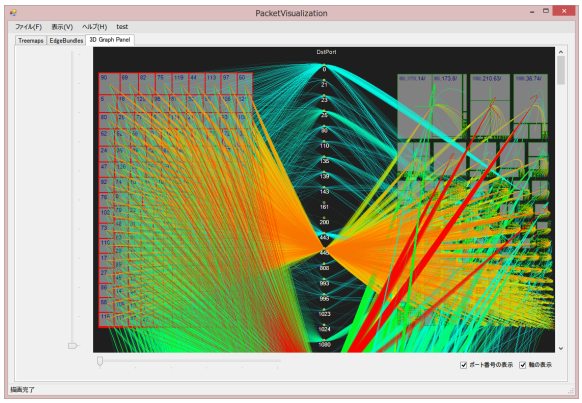

図 16　真上から見た図

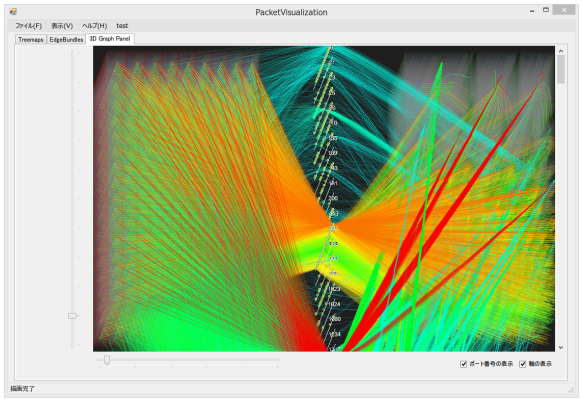

図 17　斜めから見た図

色追加

Edge Bundling グラフを単純に重ねるだけでは、エッジが全て同じ色となり、Visual Clutter が発生した。そこで、エッジに色を付けることでこれに対処した。各時間・各ポートごとのパケット数に比例して水色→緑→赤と変化するように色付きのエッジで描画した。

3D Edge Bundling の表示結果

前述した点を踏まえて描画したグラフを図 16 と図 17 に示す。また、ここでは、前述した手法によりポートスキャンおよびホストスキャンを除去している。

また、この可視化方法によって、2014 年 4 月 10 日のある時間から 993 番ポートへのパケットが増加していることが確認できた。そして、それ以前のトラフィックでは 993 番ポートへのパケットが集中することはほとんどないことも確認できた。993 番ポートは SSL/TLS を使用した IMAPS の通信に利用されているポートであり、これは 2014 年の 4 月に発見された OpenSSL の脆弱性である Heartbleed を狙った攻撃であると推定される。

5. おわりに

5.1 結論

本論文は Treemap と Edge Bundling を用いて階層的な構造としてネットワークトラフィックを可視化するツール PacetVisualization を紹介し，各種フィルタ機能の追加，および，マクロな視点でのネットワークトラフィックの解析を助ける手法を提案した．ネットワーク攻撃のフィルタ機能の追加によって既知の攻撃を除去することにより，その他の未知の攻撃を発見し易くなった．また，複数の Edge Bundling グラフを比較することができるシステムによってネットワークトラフィックの大まかな特徴をとらえることができるようになった．3D Edge Bundling グラフでは，それぞれのグラフを重ねるだけでなく色情報を追加することによって，それぞれのグラフの時間的変化を直感的に把握することが可能となった．

5.2 今後の課題

本システムはダークネットトラフィックの解析を前提としており，ハニーポットや通常のインターネットなどの利用によるトラフィック等のネットワークデータを対象としておらず限定的であるため，さらに検討する必要がある．また，本論文で提案した 3D Edge Bundling においては，各ポート番号を等間隔で表示しているため，解析するネットワークデータによっては，ポートスキャン・ホストスキャンの検出および除去だけでは十分にポート数を削減できずアスペクト比が非常に高いグラフが作成されてしまい，特徴のあるポートの発見に手間がかかるという点が今後の課題である．

謝辞 本研究の一部は，総務省による「国際連携によるサイバー攻撃の予知技術の研究開発」プロジェクトの支援を受けたものである．

参考文献

[1] Shneiderman, Ben. "Tree visualization with tree-maps: 2-d space-filling approach." ACM Transactions on graphics (TOG) 11.1 (1992): 92-99.
[2] Holten, Danny. "Hierarchical edge bundles: Visualization of adjacency relations in hierarchical data." Visualization and Computer Graphics, IEEE Transactions on 12.5 (2006): 741-748.
[3] Bailey, Michael, et al. "Practical darknet measurement." Information Sciences and Systems, 2006 40th Annual Conference on. IEEE, 2006: 1496-1501.
[4] Bruls, Mark, Kees Huizing, and Jarke J. Van Wijk. Squarified treemaps. Springer Vienna, 2000.
[5] Tanaka, Yoichi, Yoshihiro Okada, and Koichi Niijima. "Treecube: Visualization tool for browsing 3d multimedia data." Information Visualization, 2003. IV 2003. Proceedings. Seventh International Conference on. IEEE, 2003: 427-432.
[6] Robertson, George G., Jock D. Mackinlay, and Stuart K. Card. "Cone trees: animated 3D visualizations of hierarchical information." Proceedings of the SIGCHI conference on Human factors in computing systems. ACM, 1991: 189-194.
[7] Yee, Ka-Ping, et al. "Animated exploration of dynamic graphs with radial layout." infovis. IEEE, 2001: 43-50.
[8] Lin, Chun-Cheng, and Hsu-Chun Yen. "On balloon drawings of rooted trees." Graph Drawing. Springer Berlin Heidelberg, 2006: 285-296.
[9] Lamping, John, Ramana Rao, and Peter Pirolli. "A focus+ context technique based on hyperbolic geometry for visualizing large hierarchies." Proceedings of the SIGCHI conference on Human factors in computing systems. ACM Press/Addison-Wesley Publishing Co., 1995: 401-408.
[10] Rekimoto, Jun, and Mark Green. "The information cube: Using transparency in 3d information visualization." Proceedings of the Third Annual Workshop on Information Technologies & Systems (WITS'93). 1993: 125-132.
[11] "nicterWeb"，独立行政法人 情報通信研究機構，http://www.nicter.jp/
[12] "What is a Zero-Day Vulnerability? | Security News"，Symantec，http://www.pctools.com/security-news/zero-day-vulnerability/
[13] "SNORT®Users Manual"，Snort，http://manual.snort.org/
[14] Rowland, Craig H. "Intrusion detection system." U.S. Patent No. 6,405,318. 11 Jun. 2002.
[15] "TripWire"，http://www.tripwire.org/