サイバーリスクの可視化に関する調査

石川尚樹　緒方悠人　北島暢曜　韓海燕
アドバイザー教員　金岡晃

1　はじめに

インターネットの急速な発展に伴い，社会の情報化が目覚ましく進んでいる．しかし情報化社会はコンピュータウイルスや不正アクセスに代表されるように様々なサイバーリスクを孕んでいる．アンチウイルスソフトやファイアウォールなど，サイバーリスクにおける技術的な対策は多岐に亘るが，その中に**サイバーリスクの可視化**という一分野が存在する．リスクを可視化し解析することはユーザが対策を施す上での支援となる有効な手法であるため，サイバーリスクの可視化は近年非常に注目されている．また，提案された可視化ツールも商用製品やインターネット上で無料でダウンロードできるもの（オープンソースツール）など多岐に亘る．

このような多種多様な可視化ツールはユーザの目的に応じて分類される必要があり，実際に可視化対象を大きく 5 つに分類する手法が既存研究において提案されている．しかしこの 5 分類だけでは，ユーザは可視化自体の表現や必要な知識量の違いにより自らが理解できるツールを選択しにくいという問題が生じるため，新たな分類法が必要であると考えられる．本調査では現存する可視化ツールを調査し，5 分類にユーザの知識レベルという独自の指標を加えることで，ユーザが適切な可視化ツールを選択できる新たな分類法を提案する．また本来サイバーリスクとは，アプリ権限の付与やマルウェア対策，プライバシ情報の保護や機器の故障など広い範囲のリスクを意味するが，本調査ではこの内のネットワークセキュリティの可視化についての調査を行うものとする．

2　既存研究

2.1　5 つのクラス

Shiravi ら [1] の調査によると，サイバーリスクの可視化には 5 つの可視化対象（クラス）が存在する．以下にそれらをまとめる．

1. **Host/Sever Monitoring** : ネットワーク内のホスト・サーバーの状態を可視化しモニタリングするクラスが Host/Sever Monitoring である．図 1 は“鼓”[2] による不正侵入の可視化である．
2. **Internal/External Monitoring** : ネットワークの内部ホストと繋がりのある外部ホストの状態を可視化しモニタリングするクラスが Internal/External Monitoring である．図 2 は“ NFlowVis ”[6] による内部ホストと外部ホストのコネクションの可視化である．
3. **Port Activity** : 管理者が意図していない通信を防ぐために，通信ポートの動きを可視化しモニタリングするクラスが Port Acivity である．図 3 は“Cube of Doom ”[7] による通信ポートの動きの可視化である．
4. **Attack Patterns** : 標的のコンピュータやネットワークに不正に侵入してデータの破壊・改竄などを行うことをサイバー攻撃と呼び，その種類は多岐に亘る．それらの攻撃を可視化しモニタリングするクラスが Attack Patterns である．図 4 は“ Visual Firewall ”[3] による DDoS 攻撃の可視化である．
5. **Routing Behavior** : 通信において不正なルーティングが行われていないかを可視化し，モニタリングするクラスが Routing Behavior である．図 5 は“BGP Eye ”[8] によるルーティングの可視化である．

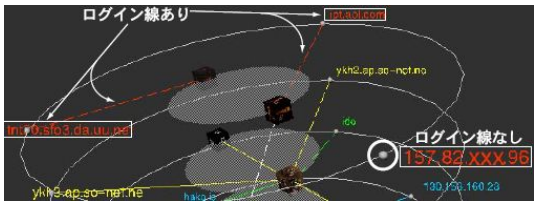

図 1　鼓 [2]

2.2　既存研究の問題点

Shiravi らは数ある可視化ツールを 2.1 節で示した 5 つのクラスに分類し，表にまとめた．これによりユーザが目的のクラスに応じたツールを選択しやすくなるように考えられるが，各クラスに含まれるツールには個々の特徴が存在する．また同じクラスに属するツールであってもユーザに要求される知識はそれぞれ異なるため，場合によってはツールが意味を成さない場合もある．よって Shiravi らの表から得られる情報のみではユーザは適切なツールを選びにくいと考えられる．

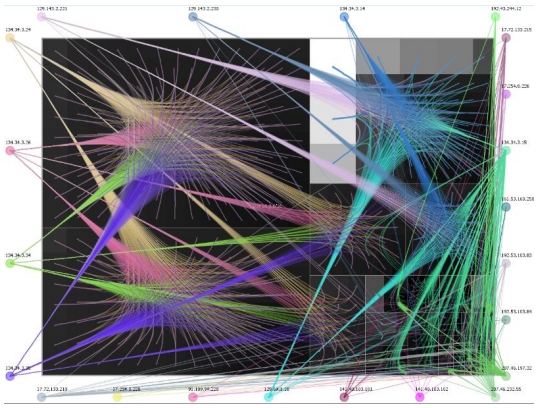

図 2 NFlowVis[6]

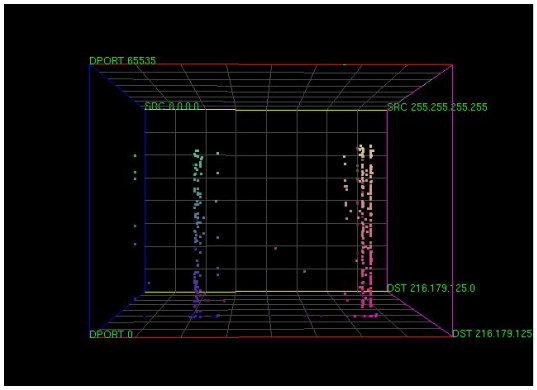

図 3 Cube of Doom[7]

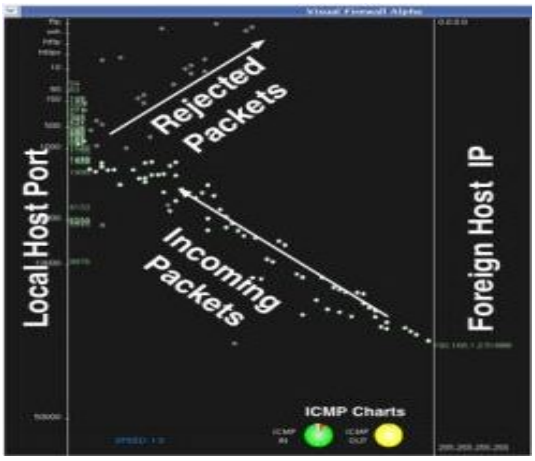

図 4 Visual Firewall[3]

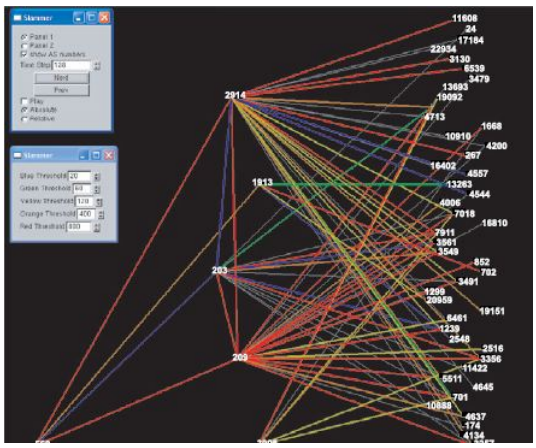

図 5 BGP Eye[8]

3 本調査の目的

本調査では Shiravi らの 5 分類に，ユーザの知識レベルという視点を加え，可視化ツールの分類をより効率的に行う手法を提案する．既存研究の問題点から，可視化ツールをユーザの知識量に応じて分類し，Shiravi らの表を拡張することは非常に有効な手法といえる．

4 調査について

4.1 調査対象

以下の対象について調査を実施する．

- 研究論文で発表されている可視化ツール
- 商用に販売されている可視化ツール
- オープンソースの可視化ツール

4.2 調査項目

本調査では以下の項目について各ツールを調査する．

- 5 つのクラスのいずれに該当するか．
- 可視化を理解するためにユーザに要求される知識は何であり，どの程度か．

これらをグループ内で議論し可視化全体に対する知識レベルを定義する．

5 調査結果

5.1 ツールの二分類

サイバーリスクを可視化するツールは“可視化のみを行うツール”と，“可視化に加え問題点も表示し，ユーザを支援するツール”の二種類に大別される．これらを比較した場合，リスクに対するユーザの理解度は明らかに後者の方が上となる．また，そのようなツールは主に企業が販売している製品に多く見られる．そのため，本調査では各ツールをまず以下の二種類に分類する．

- **研究論文上の可視化ツール/ オープンソースツール**: 端末上のある目的に応じたポイントを可視化するものが多く，ツールを使いこなせるかどうかは各ユーザの知識量に依存する傾向がある．可視化の目的に応じてユーザが自らの知識で問題点を認識したり，ツールの提案者が新しいポイントを可視化しその有用性を示すといった場合の可視化ツールを指す．よって専門的知識を有するユーザを対象としたツールが多く見られる．また，使いこなすことができるか否かは一意にユーザの知識レベルに委ねられる．

- **商用製品**: 分かりやすいアイコンを用いたグラフィックや，円グラフや棒グラフといった単純な可視化をベースに問題点を表示し，解決に導く機能を持つツールが多い．これは知識の少ない一般ユーザに対しても，可視化を通しセキュリティの強化を支援するという目的のもと有料で販売している可視化ツールを指す．

5.2 5 クラスの関係・枠組み

我々は今回，ユーザレベルという可視化ツールの理解に必要な知識レベルの難易度を図 6 を用いて表現する．これにより，ユーザは各可視化ツールの上下関係を判断しやすくなると考えられる．図 6 は，横軸を知識レベルとし，右に向かうほどユーザに要求される知識のレベルが高くなっていくことを表している．さらに既存研究の 5 クラスには，レベルに対し包含関係が見られたのでクラスごとに境界を設けている．この配置の意図として，一番低いレベルにはネットワーク内部のホストとサーバーの状況を見るだけで特別な知識を要求されない Host/Sever Monitoring を，同じモニタリングではあるが内部のホストと繋がりのある外部ホストを見るという意味で Internal/External Monitoring を次のレベルへ，そしてポートの知識も必要となる Port Activity，最後に以上全ての知識をもつことで攻撃を分析することができるという意味で Attack Patterns を最上位のクラスとする．Routing Behavior をこの並びから外して配置したのは，Routing Behavior は各ネットワーク単位で可視化をしており，個々の端末から可視化している他のクラスとは性質が異なるためである．

5.3 可視化ツールのレベル

5.2 節で述べた手法で実際に各ツールを分類する．図 6 において，通常は 1 点のみで可視化レベルを表現するが，例外としてひとつのツールで多種類の可視化を見ることもできるものもあり，そのようなツールはツール名にグラデーションをかけた表現にする．濃い部分は主要な機能であることを示し，薄い部分は主要な機能ではないということを示す．

また表 1 には各ツールの詳細として，主な機能と可視化テクニック，ユーザに要求される知識をまとめた．商用製品において括弧内に含まれる知識は，必ずしも必要とは限らないが知識としてもっているとユーザの理解がより深まると考えられるものである．

具体的なツールの調査例を 2 例付録とする．

6 考察

本調査では 5 つのクラスの難易度は並列関係ではなく，包含関係があると結論付けた．ホスト同士の繋がりの可視化より，ポートやプロトコルといったさらに細部の可視化を理解する方が難しいと考えるのは妥当であると考えられる．

しかし，これは今回の調査で扱った可視化ツールを分類することで導いた可視化レベルの定義であるので，今後の調査で新たに可視化ツールを分類することにより定義自体を変更する可能性も大いにある．

また，目的とユーザのレベルに合った可視化ツールが必ず存在するということは断言できない．例えば，Port Activity は通信ポートの動きを見るというレベルの高い可視化だが，Host/Sever Monitoring と同等レベルまで理解しやすくした可視化も存在するかもしれないことを考え，図 6 のような範囲とした．しかし，誰もが理解できるレベルの Port Activity の可視化ツールが実際に存在するかは現在の調査では見つかっておらず，不明確である．

さらに，ネットワークセキュリティの知識以外の専門的知識を持たなければ理解できない可視化も存在する．例えば火力発電システムを可視化するツールが存在する場合，ユーザはタービンやボイラーなど特別な機器に対する知識を持たなければ理解できなく，エラーが起きた時に適切な対処できない．よって今回のレベルの定義では当てはまらないケースも存在する．

本調査ではこういった特別な知識を考慮せず，ネットワークセキュリティの知識だけでの分類となっているが，最も大きなリスクとなるサイバー攻撃はネットワークを経由することが多い．また非常に多くの可視化ツールが存在し，その分類方法も多岐に亘る中，我々のアプローチは本調査独自のものであり，その最初の結果として今後の研究を促進させることに大いに貢献すると考えられる．

7 まとめと今後の課題

今回の調査では現存する可視化技術やツールを調査し，グループ内でレベルを決め分類した．これらの結果からサイバーリスクの可視化のレベルを図 6 の形で定義することより，ユーザは可視化ツールを扱う際に必要な知識を把握しやすくなった．

今後の課題としては，以下のものが挙げられる．

- **調査の拡大**：今回の調査では現存する可視化ツールの全てを調査することはできなかった．よって今後はさらに調査を拡大し，適切なレベルに分類する．

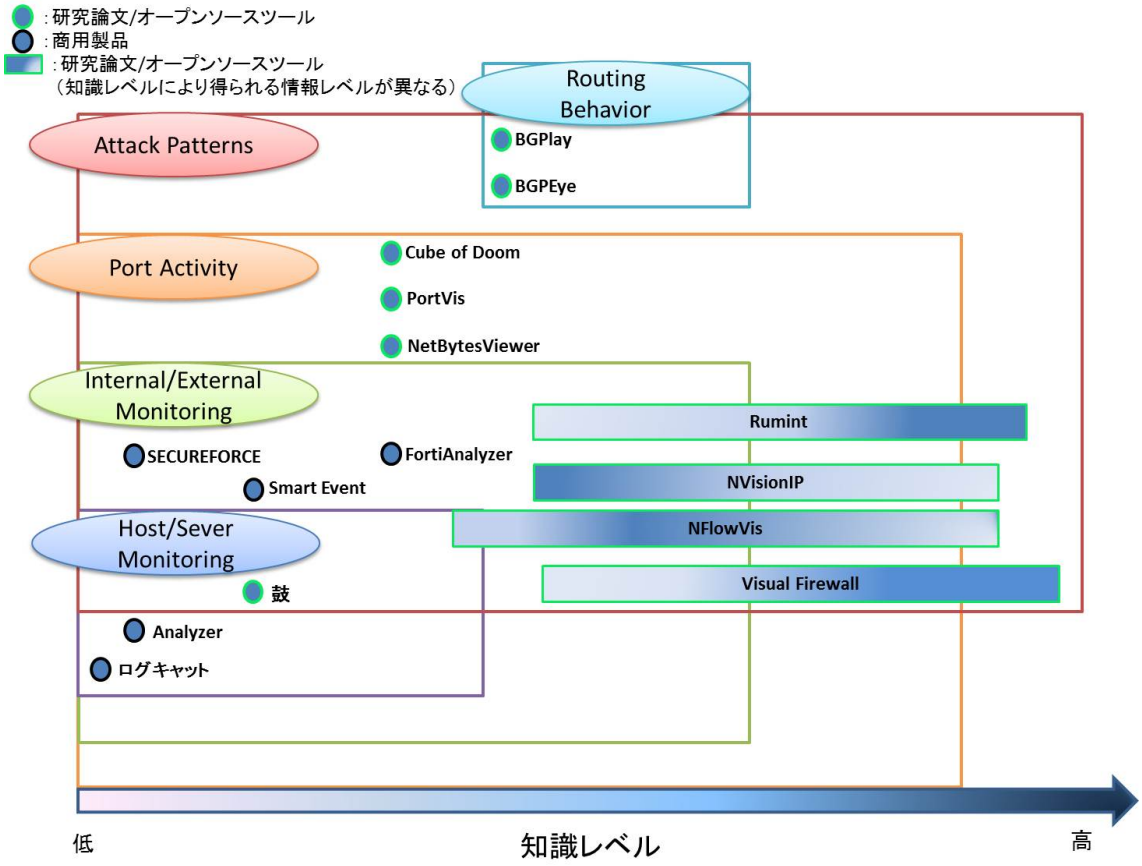

図 6　知識レベルによるツールの分類

表 1　ツールの詳細

ツール名	機能	可視化テクニック	要求される知識	分類
鼓[2]	ログ収集 / IDS	3D Node Link	IPアドレス / DNS / IDS	研究論文
Visual Firewall[3]	トラフィック可視化 / シグネチャ可視化 / 通信ポート可視化 / IDS	Scatter Plot / Line Graph	IPアドレス / ポート / IDS / DoS / ウイルス	研究論文
PortVis[4]	通信ポート可視化	Scatter Plot / 3D Line Graph	IPアドレス / ポート	研究論文
NVisionIP[5]	通信ポート可視化 / トラフィック可視化	Scatter Plot / Bar Graph	IPアドレス / ポート / ウイルス / DoS	オープンソース
NFlowVis[6]	トラフィック可視化 / ネットワーク可視化 通信ポート可視化 / IDS	Tree Map / Line Graph / Node Link / Bar Graph	IPアドレス / ポート / DoS / SSHに対する攻撃 / IDS	研究論文
Cube of Doom[7]	通信ポート可視化	3D Scatter Plot	IPアドレス / ポート	オープンソース
BGPEye[8]	ルーティング可視化	Color Map / Node Link / Bar Graph / Pie Graph	AS / BGP	研究論文
NetBytesViewer[9]	通信ポート可視化	3D Impulse Graph	IPアドレス / ポート	研究論文
BGPlay[10]	ルーティング可視化	Node Link	AS / BGP	オープンソース
Rumint[11]	トラフィック可視化 / 通信ポート可視化 / IDS	Parallel Coordinates	IPアドレス / ポート / IDS / DoS / ウイルス	オープンソース
ログキャット[12]	ログ収集・解析	Bar Graph / Line Graph	ー	商用製品
SECUREFORCE[13]	ログ収集・解析 / ネットワーク可視化 / IPS	Bar Graph / Pie Graph / Line Graph / Color Map	IPアドレス / (ウイルス / DoS)	商用製品
analyzer[14]	ログ収集・解析 / ネットワーク可視化 / 機器故障検知	Bar Graph / Line Graph / Node Link	IPアドレス	商用製品
Smart Event[15]	ログ収集・解析 / IPS	Node Link / Pie Graph / Bar Graph / Color Map	IPアドレス / (DoS / ウイルス)	商用製品
FortiAnalyzer[16]	ログ収集・解析 / ネットワーク可視化 / IDS / その他脆弱性スキャン	Bar Graph / Pie Graph / Line Graph	IPアドレス / (ポート / ウイルス / DoS)	商用製品

- **可視化レベルのより明確な境界を定義**：今回の図 6 では 5 つのクラスの境界を明確に定義できていない．理由としては考察で述べたように，今回の調査では見つかっていないが存在する可能性のあるツールを考慮してレベルの範囲を定義した箇所がいくつか存在するからである．よって調査を拡大すると共に，今回定義したレベルをさらに明確にし，適宜変更する必要がある．

8 謝辞

本調査において，第 2 班のアドバイザー教員である金岡晃助教授には調査に対するアプローチや考察において大変多くのアドバイス，丁寧かつ熱心なご指導を賜りました．ここに感謝の意を表します．

参考文献

[1] Hadi Shiravi, Ali Shiravi, and Ali A. Ghorbani, “A Survey of Visualization Systems for Network Security”, IEEE Transactions on Visualization and Computer Graphics, Vol.1, No.1, pp.1-19, 2011.

[2] 高田哲司, 小池英樹, “鼓：不正侵入検知を目的としたログ情報の視覚化”, コンピュータセキュリティシンポジウム, pp.271-276, 2000.

[3] Chris P. Lee, Jason Trost, Nicholas Gibbs, Raheem Beyah, and John A. Copeland, “Visual Firewall: Real-time Network Security Monitor”, IEEE Workshops Visualization for Computer Security, pp.129-136, 2005.

[4] Jonathan McPherson, Kwan-Liu Ma, Paul Krystosk, Tony Bartoletti, and Marvin Christensen, “PortVis: A Tool for Port-Based Detection of Security Events”, ACM Workshop on Visualization and Data Mining for Computer Security, pp.73-81, 2004.

[5] Kiran Lakkaraju, William Yurcik, and Adam J. Lee, “NVisionIP: NetFlow Visualizations of System State for Security Situational Awareness”, ACM Workshop on Visualization and Data Mining for Computer Security, pp.65-72, 2004.

[6] Florian Mansmann, Fabian Fischer, Daniel A. Keim, and Stephen C. North, “Visual Support for Analyzing Network Traffic and Intrusion Detection Events using TreeMap and Graph Representations”, 3rd ACM Symposium on Computer Human Interaction for Management of Information Technology, pp.19-28, 2009.

[7] Stephen Lau, “The Spinning Cube of Potential Doom”, Communications of the ACM, Vol.47, No.6, 2004.

[8] Soon Tee Teoh, Supranamaya Ranjan, and Chen-Nee Chuah, “BGP Eye: A New Visualization Tool for Real-time Detection and Analysis of BGP Anomalies”, VizSEC’06, pp.81-90, 2006.

[9] Teryl Taylor, Stephen Brooks, and John MeHugh, “NetBytes Viewer: An Entity-based NetFlow Visualization Utility for Identifying Intrusive Behavior”, VizSEC’07, pp.101-114, 2008.

[10] Lorenzo Colitti, Giuseppe Di Battista, Federico Mariani, Maurizio Patrignani, and Maurizio Pizzonia, “Visualizing interdomain Routing Behavior with BGPlay”, Journal of Graph Algorithms and Applications, Vol.9, pp.117-148, 2005.

[11] Gregory Conti, Kulsoom Abdullah, Julian Grizzard, John Stasko, John A. Copeland, Mustaque Ahamad, Henry Owen, and Chris Lee, “Countering Security Analyst and Network Administrator Overload Through Alert and Packet Visualization”, IEEE Computer Graphics and Applications, pp.60-70, 2006.

[12] エムオーテックス株式会社, “LanScope ログキャット”, http://www.motex.co.jp/release10/release10014.html.

[13] 株式会社アイバックス, “SECUREFORCE”, http://www.secureforce.jp/sf-system.aspx.

[14] HITACHI, “analyzer”, http://www.hitachi.co.jp/Prod/comp/soft1/itoperations/analyzer/exp/index.html.

[15] チェック・ポイント・ソフトウェア・テクノロジーズ株式会社, “SmartEvent”, http://www.checkpoint.co.jp/products/smartevent-software-blade/index.html.

[16] フォーティネットジャパン株式会社, “FortiAnalyzer”, http://www.fortinet.co.jp/products/fortianalyzer/feature1.html.

A 可視化ツールの調査例

付録として可視化ツールの調査例を 2 例紹介する．

A.1　Analyzer[14]

1. **分類**：Host/Sever Monitoring
2. **機能**：ログ収集・解析/ネットワーク可視化/機器故障検知
3. **動作概要**：ネットワーク内の全ての PC，サーバ，ストレージの稼働状況をリアルタイムで把握することができるツールである．ネットワーク内に異常が発生した場合，管理者は原因となっている機器を特定することが可能である．また PC のパフォーマンス状況や機器，サーバの詳細な状態も可視化する機能を備えている．図 7 のように各オブジェクトにカーソルを合わせることで，その対象と繋がっているネットワークがピックアップされる．さらにオブジェクトをクリックすることで機器の詳細が表示される．

　このような機能から Analyzer はユーザの問題解決を支援してくれるツールであると言え，ユーザにネットワークセキュリティに関する知識を特に要求しないことから表 1 のように位置づけられる．

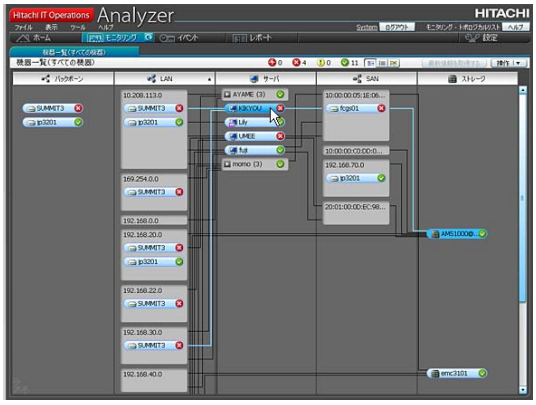

図 7　Analyzer[14]

A.2　Rumint[11]

1. **分類**：Internal/External Monitoring，Port Activity，Attack Patterns
2. **機能**：トラフィック可視化/通信ポート可視化/IDS
3. **動作概要**：Rumint は pcap データセットをロードすることで動作する．ロードされたパケットは 7 種のウィンドウで表現され，それらの組み合わせから計 20 種の可視化手法を選択することができる．その一例として，図 8 ではキャプチャされたパケットとそのトラフィックを同時に可視化している．

　可視化の手法としては多岐に亘るが，一方でユーザに対する問題解決のための支援はなく，異常が発生しているか否かの判断は各ユーザの裁量に一方的に委ねられてしまうことから表 1 のように位置づけられる．

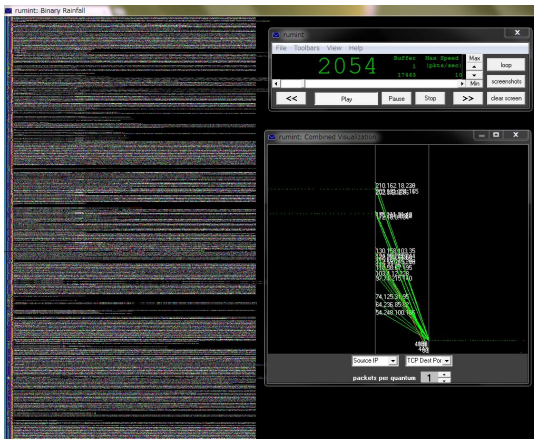

図 8　Rumint[11]