利用者の知識レベルに応じたリスクの可視化に関する考察

金岡 晃[1] 石川 尚樹[2] 緒方 悠人[2] 北島 暢曜[2] 韓 海燕[2,]

概要：本研究では、ネットワーク上のリスクに対する可視化手法の分類と、可視化された手法やツールに求められるユーザの知識レベルを 4 段階提案し、それぞれの手法を分類と知識レベルに合わせてマッピングを行った。既存研究が可視化分類を拡張し、ネットワークやサービスプロバイダによる監視を主な視点とした分類研究であったものをユーザ側の端末における可視化とアプリケーションやマルウェアなどのソフトウェア自身の可視化について分類を含むものとした。知識レベルについては経験のない利用者から高い知識を持ったエキスパートまで、4 段階にレベルを分けた。マッピングの結果、ユーザ側端末の可視化においてはユーザ側という特性から比較的ユーザが必要とされる知識レベルが低い可視化が研究されており、反対にネットワーク・サービスプロバイダ側の可視化においてはレベル 2 から 4 までの広範にわたり可視化が研究されてきることがわかった。またそれらの結果から今後可視化の研究が発展していく分野についても検討を行った。

A Study on Risk Visualization based on User Knowledge Level

Akria Kanaoka[1] Naoki Ishikawa[2] Yuto Ogata[2] Nobuaki Kitajima[2] Haiyan HAN[2,]

1. はじめに

ネットワーク上のリスクに対し、可視化を行うことでリスクを認知させる手法が存在する。それらの手法は多岐にわたり、学術研究のみならず、すでに製品化された手法も多い。Shiravi らはネットワークセキュリティ分野の可視化をまとめ分類を行った [1]。しかしネットワーク上のリスクは Shiravi らが挙げたリスクにとどまらず広範に存在する。Shiravi らの調査に置いてもっとも特徴的なものは、ユーザ側のリスク可視化手法についての調査がされておらず、ネットワークの運用者が暗黙的に対象とされている。現在のネットワークでは、スマートフォンに代表されるモバイル端末の充実により高機能かつシーンを選ばない端末の利用形態が広まり、端末を扱うユーザ側もリスクを認知することが重要となってきている。ユーザ側のリスク認知手法もすでにさまざまな手法がフィッシング対策やマルウェア対策として提案され実装・展開されてきているが、なお学術的にも発展途上にある分野である。

本論文では、これらの可視化について以下を示す。

- 既存のリスク可視化手法の整理と分類
- ユーザ知識レベルの定義
- 各可視化手法が対象としているユーザ知識レベルを検討し可視化対象の特徴や不足点を考察

まず既存のリスク可視化手法の整理と分類では、Shiravi らの調査対象をさらに拡大し手法の調査を充実化させる。特に Shiravi らの調査では対象とされていなかったユーザ側の可視化手法についても調査を行う。続いて、収集したそれぞれの手法を分類する。

続いてユーザ知識レベルの定義を行う。上記で挙げられる各手法は、データや観測対象は多岐にわたっているが、誰に向けた可視化であるかの議論がされていない。これまでの可視化については多くが運用者を意識したものであったが、複雑化するネットワークやリスク、また上述のようにユーザ側への可視化の重要性も高まっていることから、可視化の恩恵を受けるユーザの区別とそれぞれのユーザのリスクに対する知識レベルを考慮した可視化が今後重要になってくると考えられる。そこで本論文ではユーザの知識レベルを 4 段階で提案を行い、可視化の手法がどの段階の

[1] 東邦大学
274-8510、千葉県船橋市三山 2-2-1
[2] 筑波大学
305-8573、茨城県つくば市天王台 1-1-1
本論文は筑波大学大学院システム情報工学研究科リスク工学専攻におけるグループ演習の成果を発展させたものである。

ユーザの知識レベルを求めているかを議論する。

最後に各可視化手法が対象としているユーザ知識レベルを検討し可視化対象の特徴や不足点を踏まえ、それぞれの可視化手法を上記 4 レベルにマッピングした表を作成する。マッピングした結果から、現在の可視化手法の研究・製品化がどの分野とどのユーザ知識レベルにおいて盛んにおこなわれているかを示す。また特定の可視化分類における特定の知識レベルを対象とした製品の欠如（マッピングした表において空白地帯となっている部分）についての考察を行う。考察ではまずその欠如部分での可視化必要性を議論し、必要性のある部分についてはどういった可視化が今後されていくべきかを示す。

本論文の構成は以下の通りである。まず第 2 章でネットワークなどのサイバー空間での可視化手法に関する研究を紹介する。第 3 章では既存のリスク可視化手法を整理し、分類を試みる。第 4 章で利用者の知識レベルに基づいたユーザの分類手法を提案する。整理された可視化手法と提案されたユーザ分類手法に基づき、第 5 章ではそれらのマッピングを行い、第 6 章でマッピング結果の考察を行う。最後に第 7 章でまとめる。

2. 関連研究

2.1 ネットワークセキュリティの可視化

リスクそのものではないが、ネットワークセキュリティに関する可視化としては Shiravi らが広範にサーベイをしており、38 種類のシステムに対して、5 つの分類を与えている [1]。Shiravi らによる分類は以下の 5 つとなっている

Host/Server Monitoring
ネットワーク内のホスト・サーバの状態を可視化しモニタリングするクラス [2], [3], [4], [5], [6], [7], [8], [9], [10], [11]

Internal/External Monitoring
ネットワークの内部ホストとつな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 [12], [13], [14], [15]

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 [16], [17], [18], [19], [20], [21]

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・改ざんを行う攻撃を可視化しモニタリングするクラス [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42]

Routing Behavior
不正な経路制御がされていないかを可視化しモニタリングするクラス [43], [44], [45], [46], [47], [48], [49]

それぞれの分類のクラスで 38 種類（48 の文献）を参照している。本論文ではこれらのシステムを改めて分類しなおすためそれぞれの文献についての参照を入れている。

Shiravi らのサーベイには含まれていないが、まだ多くの可視化技術が研究されている。Mansmann らは複雑なファイアウォールのルールを可視化する技術を提案している [50]。また Horn らはネットワークの防御手法を決定するための意志決定を補助する可視化手法を提案している [51]。

Boschetti らの研究ではネットワークの監視に際し、状況の変化を表す可視化を行うことで異常検知を行うシステムを提案している [52]。Kintzel らは広範な IP アドレス群に対する監視を ClockView を利用する可視化手法を提案している [53]。井上らは同じく広範なダークネットの IP アドレス群を監視する DAEDALUS-VIZ を提案している [54]。同じくネットワーク監視ではあるが、Best[56] らの手法では、状況に従ったネットワークの挙動の可視化を行っている。一報、Fischer らは対象を絞り経路制御の様子を可視化する手法を提案している [57]。これらはさまざまな通信をまとめて可視化する手法が主な機能であるが、Lian らの手法では通信の種類を絞った可視化方式が提案されている [58]。

ネットワークの監視・観測ではなく、攻撃そのものの可視化に焦点を当てた研究もまだ多く存在する。たとえば Rasmussen らが提案する可視化手法では侵入検知システム（IDS）の警告情報をもとに可視化を行っている [55]。Roveta らはネットワーク自信が攻撃やその準備などの不穏な動作をしていることを検出した場合にネットワークの表現ごと変えていく可視化手法を提案している [59]。Erbacher の手法 [60] は攻撃などの行為の履歴を可視化することで傾向を把握し、Tsigkas らの手法 [61] ではスパムメールの活動を可視化している。Layman らの手法 [62] では、Microsoft 社の IIS に焦点を当てリアルタイムにイベントを可視化し、履歴と合わせて表示することで攻撃の可視化を行っている。Chu らの手法 [63] はサブネット内のホストと攻撃者の関係性を可視化している。

2.2 ユーザ側のリスク可視化手法

Shiravi らが調査をしたネットワークセキュリティの可視化手法は、その利用者となる層がサーバ管理者、ネットワーク管理者、など様々な利用者が想定され不明瞭な部分はあるが、少なくともネットワークにアクセスをしているエンドユーザに対するものではないことがわかる。

しかしエンドユーザ側のリスク可視化も実用化されているものや、研究として行われているものも多い。たとえば鍵のマークや URL 周辺の色使いなどを利用した Web ブラウザにおける SSL 通信の状況表示は実用化されているエンドユーザ側のリスク可視化の代表的なものであろう。また

各種アンチウイルスソフトも検出時に警告を出すがそれも1つの可視化手法である。

研究でもさまざまな可視化対象に対するアプローチがされている。Raja らは、ブラウザの警告画面を効率的にユーザに伝える研究 [64] や、パーソナルファイアウォールの設定画面での脅威の表示を研究を行っている [65]。Felt らの手法では、Android アプリケーションのパーミッションに関する脅威を可視化している [66]。Kay らは、契約に関する画面表示に関する可視化を研究している [67]。

松尾らの手法 [68] では、ユーザが利用するサービスや環境などのリスクを可視化し、Glatz らの手法 [69] ではホストのトラフィックを可視化している。

Maurer らはブラウザで入力するデータタイプに応じて警告画面を挿入する手法を提案している [70]。Soitirakopoulos らは SSL/TLS 利用時の警告画面についての研究を行っている [71]。Goeks らはこれまでの入力に応じたプライバシやセキュリティのリスクの可視化を提案している [72]。Fahl らはより対象を絞り、Facebook のメッセージに対する暗号化とその可視化を行っている [73]。同じく Shehab らは Facebook で利用される認証連携について、サービスに付与される権限に対する適切性を可視化している [74]。

2.3 その他のリスク可視化手法

ネットワークやホスト自身の可視化、攻撃の可視化とは違ったアプローチとして、ソフトウェアそのものに対するセキュリティの可視化の研究もおこなわれている。Fang らの手法 [75] や Goodall らの手法 [76] では、ソフトウェアの脆弱性などを解析するために可視化手法を取り入れている。

Nataraj らの手法 [77] は、マルウェアのバイナリデータの分類を可視化を通じて行うものとなっている。

3. 既存のリスク可視化手法の可視化対象による分類

Shiravi らの調査では、その分類を Host/Server Monitoring、Internal/External Monitoring、Port Activity、Attack Patterns、Routing Behavior の 5 種類に分けられていたが、今回の我々の調査では Shiravi らの調査では行われていなかったユーザ側やアプリケーション自身のセキュリティに関する可視化も対象としており、Shiravi らの分類では不十分である。そこで我々は、可視化の対象をネットワークとユーザ側、ソフトウェアと大別した後、さらに細分化を行う分類を行う。提案する分類は以下の通りである。

1 ユーザ端末における可視化
- **1-1** ユーザ端末設定の可視化
- **1-2** ユーザが利用するネットワークの可視化
- **1-3** ユーザの動きの可視化

2 ネットワーク・サービスプロバイダ側における可視化
- **2-1** ホスト/サーバ内部の可視化
- **2-2** ネットワークの通信の可視化
- **2-3** 通信ポートの動きの可視化
- **2-4** 攻撃パターンの可視化

3 ソフトウェアの可視化
- **3-1** アプリケーションの可視化
- **3-2** マルウェアの可視化

運用者側における可視化の細分化項目は、Shiravi らと類似するものではあるが、Routing Behavior として分類されていたものが「ネットワークの通信の可視化」に分類され、より単純化されている。

4. ユーザ知識レベルの定義

2 章で挙げられる各手法はデータや観測対象は多岐にわたっているが、誰に向けた可視化であるかの議論がされていない。これまでの可視化については多くが運用者を意識したものであったが、複雑化するネットワークやリスク、またユーザ側への可視化の重要性も高まっていることから、可視化の恩恵を受けるユーザの区別とそれぞれのユーザのリスクに対する知識レベルを考慮した可視化が今後重要になってくると考えられる。そこで本論文ではユーザの知識レベルを下記の 4 段階に分けて各可視化を議論する

レベル 1 知識がない、または経験がない利用者。

レベル 2 ある程度の知識を持った利用者。専門ではないがある程度の技術を知っている。

レベル 3 十分な知識を持った利用者。実務に従事している技術者など。

レベル 4 高い知識を持った利用者。実務を通じ高い実践経験を持つエキスパート。

上記 4 レベルは、情報処理推進機構（IPA）の IPA 情報セキュリティスキルマップ [78] における 4 レベルや、経済産業省におる IT スキル標準 [79] の 7 レベルを参照にし、技術者でない一般消費者のレベルと可視化の分野の成熟度を加味し設定した。

5. 可視化手法分類とユーザ知識レベルによる各手法のマッピング

第 2 章の関連研究で取り上げた各手法を、第 3 章による可視化対象による分類と第 4 章によるユーザ知識レベルに基づき、マッピングを行う。マッピングにあたっては、Shiravi らの研究で参照されている各論文に関してはその分類対象は Shiravi らのものを踏襲している。あらたに本論文で参照した論文については筆者らによりその対象がどこにあるかを検討してマッピングした。

ユーザ知識レベルのマッピングに関しては、そもそもの可視化対象が必要とする技術的な知識の深さは考慮にいれず、単に可視化された結果を扱うことや可視化情報をもとに物事を判断するためにはどの程度の知識が必要かという

点を第 1 に据え、知識のレベルを踏まえ、可視化自体がその知識レベルの引き下げに貢献しているかを考慮した。

マッピングの結果を表 1 に示す。なお、表内の数字は本論文における各手法の参考文献番号となっている。また各分類は各番号が 3 章で提案したものを示し、図の表示領域の面から名称は略称が示されている。

マッピングの結果を見ると、ユーザ端末における可視化については、いずれの小分類（1-1 ユーザ端末設定の可視化、1-2 ユーザが利用するネットワークの可視化、1-3 ユーザの動きの可視化）についてもユーザに求められる知識レベルが低く集まっていることがわかる。

ネットワーク・サービスプロバイダ側における可視化では、いずれもレベル 1 の知識レベルのユーザが扱える可視化とはなっていない。他のレベルでは広く可視化が行われているものの、レベル 4 はレベル 2、3 と比較して少ない結果となった。

一報、ソフトウェアの可視化では、そもそも研究の数自体が少ないが、いずれもレベル 4 の知識を必要とするものとなっている。これは運用や監視、あるいは日常的なサービス利用といったものではなく、アプリケーションの開発やマルウェアの解析に用いられる特殊な可視化であることから、その可視化を求める対象がそもそも高い知識レベルにあることからこの傾向が表れていることと思われる。

6. 可視化手法マップの考察

マッピングの結果、大項目「ユーザ端末における可視化」では「ユーザ知識レベル 0 あるいは 1」に多くの手法がマッピングされ、ユーザ知識レベル 2 や 3 での手法が多くは存在しなかった。これはユーザ端末における可視化、という分類が示すとおり、ユーザになんらかのリスクを示すものであり、ユーザ端末を利用するユーザの知識レベルに合さなければならないという可視化要件が働き、一般ユーザのような比較的知識レベルの低いユーザを対象に可視化が研究されていることを示すものと言える。ユーザ端末という特性を考慮すれば、これは現在可視化の対象として不足になっている部分とはいえず、今後必要になっていく可能性は低いと考える。しかし、1-2 ユーザが利用するネットワークの可視化については、組織内の端末を外部に持ち出した際に組織内接続をするような環境など、用途としては一定の利用が求められる分野であり、今後の研究が必要であるものと考えられる。

一方で「ネットワーク・サービスプロバイダ側の可視化」についてはレベル 2 からレベル 4 まで広範にわたり可視化が行われているが、その分布には偏りがあり、レベル 1 を対象とした可視化については無く、またレベル 4 についてもレベル 2 とレベル 3 に比べて少ないことがわかる。これは、通信データやログデータなどのデータを直接提示するのではなくなんらかの加工をして可視化をするという可視化自体の性質がエキスパートの作業には決して必要ではなく、データの直接提示が最も良い効率で作業ができる点が考えられる。レベル 4 に対する研究の少なさもうかがえるが、昨今の APT（Advanced Persisitent Threat）といった高度の攻撃に対しては、エキスパートであってもデータを直接監視して複合的に判断するのは困難であることから、研究に対する要求は存在すると考えられる。

7. まとめ

本研究では、ネットワーク上のリスクに対する可視化手法の分類と、可視化された手法やツールに求められるユーザの知識レベルを 4 段階提案し、それぞれの手法を分類と知識レベルに合わせてマッピングした。可視化の分類については既存研究があったものの、ネットワークやサービスプロバイダによる監視を主な視点とした分類研究であり、本研究ではそれらをさらに拡大しユーザ側の端末における可視化とアプリケーションやマルウェアなどのソフトウェア自身の可視化について分類を行った。知識レベルについては 4 段階にレベルを分けた。

マッピングの結果、ユーザ側端末の可視化においてはユーザ側という特性から比較的ユーザが必要とされる知識レベルが低い可視化が研究されており、反対にネットワーク・サービスプロバイダ側の可視化においてはレベル 2 から 4 までの広範にわたり可視化が研究されてきることがわかり、それらの結果から今後可視化の研究が発展していく分野についても検討を行った。

参考文献

[1] H. Shiravi, A. Shiravi, A. A. Ghorbani, ”A Survey of Visualization System for Network Security”, IEEE Trans. on Visualization and Computer Graphics, Vol.18, No.8, pp.1313-1329, Aug. 2012.

[2] R. Erbacher, K. Walker, and D. Frincke, “Intrusion and Misuse Detection in Large-Scale Systems,” IEEE Computer Graphics and Applications, vol. 22, no. 1, pp. 38-48, Jan./Feb. 2002.

[3] R. Erbacher, “Intrusion Behavior Detection through Visualiza-tion,” Proc. IEEE Int’ l Conf. Systems, Man and Cybernetics, pp. 2507-2513, 2003.

[4] T. Takada and H. Koike, “Tudumi: Information Visualization System for Monitoring and Auditing Computer Logs,” Proc. Sixth Int’ l Conf. Information Visualisation, pp. 570-576, 2002.

[5] K. Lakkaraju, W. Yurcik, and A. Lee, “NVisionIP: Netflow Visualizations of System State for Security Situational Aware-ness,” Proc. ACM Workshop Visualization and Data Mining for Computer Security, vol. 29, pp. 65-72, 2004.

[6] K. Lakkaraju, R. Bearavolu, A. Slagell, W. Yurcik, and S. North, “Closing-the-Loop in Nvisionip: Integrating Discovery and Search in Security Visualizations,” Proc. IEEE Workshop Visualization for Computer Security (VizSEC ’ 05), pp. 75-82, 2005.

[7] G. Fink, P. Muessig, and C. North, “Visual Correlation of Host Processes and Network Traffic,” Proc. IEEE

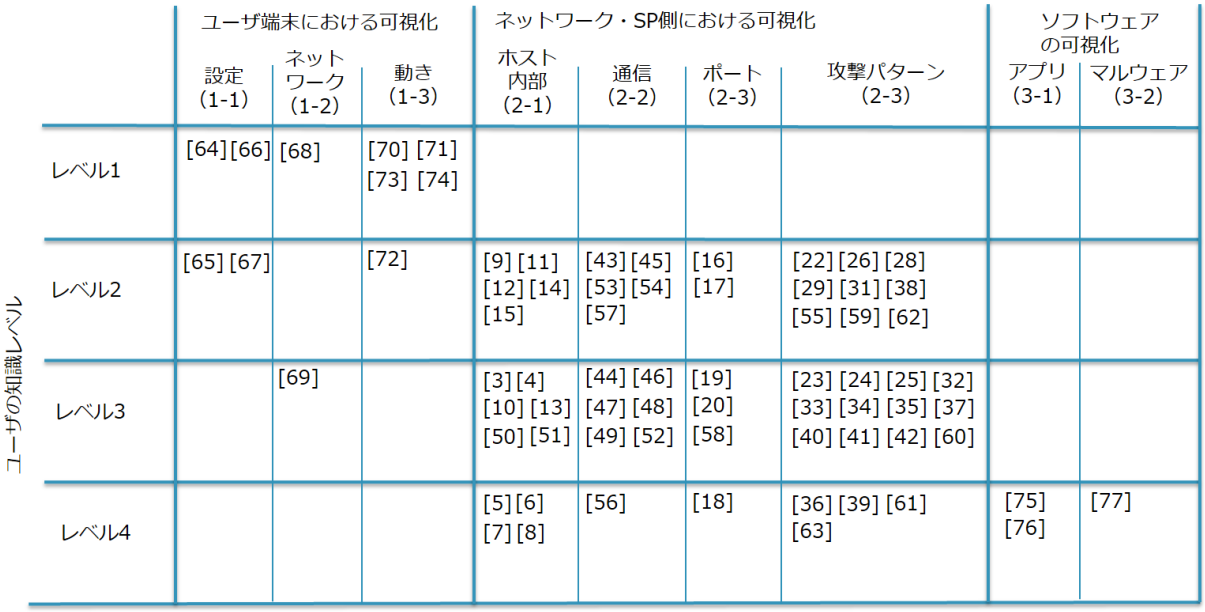

図 1 可視化手法の分類とユーザ知識レベルによる各手法のマッピング

Workshop Visualization for Computer Security (VizSEC 05), pp. 11-19, 2005.

[8] G. Fink, V. Duggirala, R. Correa, and C. North, "Bridging the Host-Network Divide: Survey, Taxonomy, and Solution," Proc. 20th USENIX Conf. Large Installation System Administration, pp. 247-262, 2006.

[9] J. Pearlman and P. Rheingans, "Visualizing Network Security Events Using Compound Glyphs from a Service-oriented Per-spective," Proc. Workshop Visualization for Computer Security (VizSEC ' 07), pp. 131-146, 2008.

[10] D. Keim, F. Mansmann, J. Schneidewind, and T. Schreck, "Monitoring Network Traffic with Radial Traffic Analyzer," Proc. IEEE Symp. Visual Analytics Science and Technology, pp. 123-128, 2006.

[11] F. Mansman, L. Meier, and D.A. Keim, "Visualization of Host Behavior for Network Security," Proc. Workshop Visualization for Computer Security (VizSEC ' 07), pp. 187-202, 2008.

[12] R. Ball, G.A. Fink, and C. North, "Home-Centric Visualization of Network Traffic for Security Administration," Proc. ACM Work-shop Visualization and Data Mining for Computer Security, pp. 55-64, 2004.

[13] X. Yin, W. Yurcik, M. Treaster, Y. Li, and K. Lakkaraju, "Visflowconnect: Netflow Visualizations of Link Relationships for Security Situational Awareness," Proc. ACM Workshop Visua-lization and Data Mining for Computer Security, pp. 26-34, 2004.

[14] R. Erbacher, K. Christensen, and A. Sundberg, "Designing Visualization Capabilities for ids Challenges," Proc. IEEE Work-shop Visualization for Computer Security (VizSEC ' 05), pp. 121-127, 2005.

[15] J. Goodall, W. Lutters, P. Rheingans, and A. Komlodi, "Preserving the Big Picture: Visual Network Traffic Analysis with tnv," Proc. IEEE Workshop Visualization for Computer Security (VizSEC ' 05), pp. 47-54, 2005.

[16] K. Abdullah, C. Lee, G. Conti, and J. Copeland, "Visualizing Network Data for Intrusion Detection," Proc. Sixth Ann. IEEE SMC Information Assurance Workshop (IAW ' 05), pp. 100-108, 2005.

[17] S. Lau, "The Spinning Cube of Potential Doom," Comm. the ACM, vol. 47, no. 6, pp. 25-26, 2004.

[18] J. McPherson, K. Ma, P. Krystosk, T. Bartoletti, and M. Christensen, "PortVis: A Tool for Port-Based Detection of Security Events," Proc. the ACM Workshop Visualization and Data Mining for Computer Security, pp. 73-81, 2004.

[19] T. Taylor, S. Brooks, and J. McHugh, "Netbytes Viewer: An Entity-based Netflow Visualization Utility for Identifying Intrusive Behavior," Proc. Workshop Visualization for Computer Security (VizSEC ' 07), pp. 101-114, 2008.

[20] J. Janies, "Existence Plots: A Low-Resolution Time Series for Port Behavior Analysis," Proc. Fifth Int' l Workshop Visualization for Computer Security (VizSec ' 08), pp. 161-168, 2008.

[21] (2011) Re-Inventing Network Security. Palo Alto Networks. http://www.paloaltonetworks.com/literature/whitepapers/Re-inventing-Net work-Security.pdf, 2011.

[22] L. Girardin, "An Eye on Network Intruder-Administrator Shoot-outs," Proc. First Conf. Workshop Intrusion Detection and Network Monitoring, vol. 1, pp. 3-13, 1999.

[23] K. Nyarko, T. Capers, C. Scott, and K. Ladeji-Osias, "Network Intrusion Visualization with niva, an Intrusion Detection Visual Analyzer with Haptic Integration," Proc. 10th Symp. Haptic Interfaces for Virtual Environment and Teleoperator Systems (HAPTICS ' 02), pp. 277 -284, 2002.

[24] H. Koike and K. Ohno, "SnortView: Visualization System of Snort Logs," Proc. ACM Workshop Visualization and Data Mining for Computer Security, vol. 29, pp. 143-147, 2004.

[25] P. Ren, Y. Gao, Z. Li, Y. Chen, and B. Watson, "Idgraphs: Intrusion Detection and Analysis Using Histographs," Proc. IEEE Workshop Visualization for Computer Security (VizSEC ' 05), pp. 39-46, 2005.

[26] H. Koike, K. Ohno, and K. Koizumi, "Visualizing Cyber Attacks Using ip Matrix," Proc. IEEE Workshop Visualization for Computer Security (VizSEC ' 05), pp. 91-98, 2005.

[27] C. Lee, J. Trost, N. Gibbs, R. Beyah, and J. Copeland, "Visual Firewall: Real-Time Network Security Monitor,"

Proc. IEEE Workshop Visualization for Computer Security (VizSEC ' 05), pp. 129-136, 2005.

[28] K. Abdullah, C. Lee, G. Conti, J. Copeland, and J. Stasko, "Ids Rainstorm: Visualizing ids Alarms," Proc. IEEE Workshop Visua-lization for Computer Security (VizSEC ' 05), pp. 1-10, 2005.

[29] Y. Livnat, J. Agutter, S. Moon, R. Erbacher, and S. Foresti, "A Visualization Paradigm for Network Intrusion Detection," Proc. Sixth Ann. IEEE SMC Information Assurance Workshop (IAW ' 05), pp. 92-99, 2005.

[30] Y. Livnat, J. Agutter, S. Moon, and S. Foresti, "Visual Correlation for Situational Awareness," Proc. IEEE Symp. Information Visuali-zation (INFOVIS ' 05), pp. 95-102, 2005.

[31] S. Foresti, J. Agutter, Y. Livnat, S. Moon, and R. Erbacher, "Visual Correlation of Network Alerts," IEEE Computer Graphics and Applications, vol. 26, no. 2, pp. 48-59, Mar./Apr. 2006.

[32] G. Conti, K. Abdullah, J. Grizzard, J. Stasko, J. Copeland, M. Ahamad, H. Owen, and C. Lee, "Countering Security Information Overload through Alert and Packet Visualization," IEEE Computer Graphics and Applications, vol. 26, no. 2, pp. 60-70, Mar./Apr. 2006.

[33] S. Krasser, G. Conti, J. Grizzard, J. Gribschaw, and H. Owen, "Real-Time and Forensic Network Data Analysis Using Animated and Coordinated Visualization," Proc. Sixth Ann. IEEE SMC Information Assurance Workshop (IAW ' 05), pp. 42-49, 2005.

[34] P. Ren, J. Kristoff, and B. Gooch, "Visualizing dns Traffic," Proc. Third Int' l Workshop Visualization for Computer Security (VizSEC ' 06), pp. 23-30, 2006.

[35] L. Xiao, J. Gerth, and P. Hanrahan, "Enhancing Visual Analysis of Network Traffic Using a Knowledge Representation," Proc. IEEE Symp. Visual Analytics Science and Technology, pp. 107-114, 2006.

[36] I.-V. Onut and A.A. Ghorbani, "Svision: A Novel Visual Network-Anomaly Identification Technique," Computers Security, vol. 26, no. 3, pp. 201-212, 2007.

[37] F. Mansmann, D. Keim, S. North, B. Rexroad, and D. Sheleheda, "Visual Analysis of Network Traffic for Resource Planning, Interactive Monitoring, and Interpretation of Security Threats," IEEE Trans. Visualization and Computer Graphics, vol. 13, no. 6, pp. 1105-1112, Nov./Dec. 2007.

[38] E. Bertini, P. Hertzog, and D. Lalanne, "Spiralview: Towards Security Policies Assessment through Visual Correlation of Net-work Resources with Evolution of Alarms," Proc. IEEE Symp. Visual Analytics Science and Technology, pp. 139-146, 2007.

[39] F. Fischer, F. Mansmann, D.A. Keim, S. Pietzko, and M. Waldvogel, "Large-Scale Network Monitoring for Visual Analysis of Attacks," Proc. Fifth Int' l Workshop Visualization for Computer Security (VizSec ' 08), pp. 111-118, 2008.

[40] A. Yelizarov and D. Gamayunov, "Visualization of Complex Attacks and State of Attacked Network," Proc. Sixth Int' l Workshop Visualization for Cyber Security (VizSec ' 09), pp. 1-9, 2009.

[41] Q. Liao, A. Striegel, and N. Chawla, "Visualizing Graph Dynamics and Similarity for Enterprise Network Security and Manage-ment," Proc. Seventh Int' l Symp. Visualization for Cyber Security (VizSec ' 10), pp. 34-45, 2010.

[42] H. Shiravi, A. Shiravi, and A. Ghorbani, "Ids Alert Visualization and Monitoring through Heuristic Host Selection," Proc. 12th Int' l Conf. Information and Comm. Security, pp. 445-458, 2010.

[43] L. Colitti, G. Di Battista, F. Mariani, M. Patrignani, and M. Pizzonia, "Visualizing Interdomain Routing with BGPlay," J. Graph Algorithms and Applications, vol. 9, pp. 117-148, 2005.

[44] T. Wong, V. Jacobson, and C. Alaettinoglu, "Internet Routing Anomaly Detection and Visualization," Proc. Int' l Conf. Dependable Systems and Networks (DSN ' 05), pp. 172-181, 2005.

[45] M. Lad, D. Massey, and L. Zhang, "Visualizing Internet Routing Changes," IEEE Trans. Visualization and Computer Graphics, vol. 12, no. 6, pp. 1450-1460, Nov./Dec. 2006.

[46] S.T. Teoh, K.-L. Ma, S. Wu, and X. Zhao, "Case Study: Interactive Visualization for Internet Security," Proc. IEEE Visualization (VIS ' 02), pp. 505-508, 2002.

[47] S.T. Teoh, K. Zhang, S.-M. Tseng, K.-L. Ma, and S.F. Wu, "Combining Visual and Automated Data Mining for Near-Real-Time Anomaly Detection and Analysis in bgp," Proc. ACM Workshop Visualization and Data Mining for Computer Security, pp. 35-44, 2004.

[48] S.T. Teoh, K.-L. Ma, S. Wu, and T. Jankun-Kelly, "Detecting Flaws and Intruders with Visual Data Analysis," IEEE Computer Graphics and Applications, vol. 24, no. 5, pp. 27-35, Sept./Oct. 2004.

[49] S.T. Teoh, S. Ranjan, A. Nucci, and C.-N. Chuah, "Bgp Eye: A New Visualization Tool for Real-Time Detection and Analysis of bgp Anomalies," Proc. Third Int' l Workshop Visualization for Computer Security (VizSEC ' 06), pp. 81-90, 2006.

[50] Florian Mansmann, Timo Gbel, and William Cheswick. Visual analysis of complex firewall configurations. In Proceedings of the Ninth International Symposium on Visualization for Cyber Security (VizSec '12). ACM, New York, NY, USA, 2012

[51] Chris Horn and Anita D'Amico. Visual analysis of goal-directed network defense decisions. In Proceedings of the 8th International Symposium on Visualization for Cyber Security (VizSec '11). ACM, New York, NY, USA, 2011

[52] Alberto Boschetti, Luca Salgarelli, Chris Muelder, and Kwan-Liu Ma. TVi: a visual querying system for network monitoring and anomaly detection. In Proceedings of the 8th International Symposium on Visualization for Cyber Security (VizSec '11). ACM, New York, NY, USA, 2011

[53] Christopher Kintzel, Johannes Fuchs, and Florian Mansmann. Monitoring large IP spaces with ClockView. In Proceedings of the 8th International Symposium on Visualization for Cyber Security (VizSec '11). ACM, New York, NY, USA, 2011

[54] Daisuke Inoue, Masashi Eto, Koei Suzuki, Mio Suzuki, and Koji Nakao. DAEDALUS-VIZ: novel real-time 3D visualization for darknet monitoring-based alert system. In Proceedings of the Ninth International Symposium on Visualization for Cyber Security (VizSec '12). ACM, New York, NY, USA, 72-79, 2012

[55] Jamie Rasmussen, Kate Ehrlich, Steven Ross, Susanna Kirk, Daniel Gruen, and John Patterson. 2010. Nimble cybersecurity incident management through visualization and defensible recommendations. In Proceedings of the Seventh International Symposium on Visualization for Cyber Security (VizSec '10). ACM, New York, NY, USA, 102-113. , 2010

[56] Daniel M. Best, Shawn Bohn, Douglas Love, Adam Wynne, and William A. Pike. Real-time visualization of

network behaviors for situational awareness. In Proceedings of the Seventh International Symposium on Visualization for Cyber Security (VizSec '10). ACM, New York, NY, USA, 79-90, 2010

[57] Fabian Fischer, Johannes Fuchs, Pierre-Antoine Vervier, Florian Mansmann, and Olivier Thonnard. VisTracer: a visual analytics tool to investigate routing anomalies in traceroutes. In Proceedings of the Ninth International Symposium on Visualization for Cyber Security (VizSec '12). ACM, New York, NY, USA, 80-87, 2012

[58] Wilson Lian, Fabian Monrose, and John McHugh. Traffic classification using visual motifs: an empirical evaluation. In Proceedings of the Seventh International Symposium on Visualization for Cyber Security (VizSec '10). ACM, New York, NY, USA, 70-78, 2010

[59] Francesco Roveta, Giorgio Caviglia, Luca Di Mario, Stefano Zanero, Federico Maggi, and Paolo Ciuccarelli. BURN: baring unknown rogue networks. In Proceedings of the 8th International Symposium on Visualization for Cyber Security (VizSec '11). ACM, New York, NY, USA, 2011

[60] Robert F. Erbacher. Visualization design for immediate high-level situational assessment. In Proceedings of the Ninth International Symposium on Visualization for Cyber Security (VizSec '12). ACM, New York, NY, USA, 17-24., 2012

[61] Orestis Tsigkas, Olivier Thonnard, and Dimitrios Tzovaras. Visual spam campaigns analysis using abstract graphs representation. In Proceedings of the Ninth International Symposium on Visualization for Cyber Security (VizSec '12). ACM, New York, NY, USA, 64-71, 2012

[62] Lane Harrison, Xianlin Hu, Xiaowei Ying, Aidong Lu, Weichao Wang, and Xintao Wu. Interactive detection of network anomalies via coordinated multiple views. In Proceedings of the Seventh International Symposium on Visualization for Cyber Security (VizSec '10). ACM, New York, NY, USA, 91-101, 2010

[63] Matthew Chu, Kyle Ingols, Richard Lippmann, Seth Webster, and Stephen Boyer. Visualizing attack graphs, reachability, and trust relationships with NAVIGATOR. In Proceedings of the Seventh International Symposium on Visualization for Cyber Security (VizSec '10). ACM, New York, NY, USA, 22-33, 2010

[64] Fahimeh Raja, Kirstie Hawkey, Steven Hsu, Kai-Le Clement Wang, and Konstantin Beznosov. 2011. A brick wall, a locked door, and a bandit: a physical security metaphor for firewall warnings. In Proceedings of the Seventh Symposium on Usable Privacy and Security (SOUPS '11). ACM, New York, NY, USA, 2011

[65] Fahimeh Raja, Kirstie Hawkey, and Konstantin Beznosov. Revealing hidden context: improving mental models of personal firewall users. In Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS '09). ACM, New York, NY, USA, 2009

[66] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. Android permissions: user attention, comprehension, and behavior. In Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12). ACM, New York, NY, USA, 2012

[67] Matthew Kay and Michael Terry. Textured agreements: re-envisioning electronic consent. In Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10). ACM, New York, NY, USA, 2010

[68] S. Matsuo, A. Kanaoka, T. Takahashi, T. Minowa, "Demo: Prototype System for Visualizing Security Risks on Mobile Devices", the 8th Symposium on Usable Privacy and Security, 2012

[69] Eduard Glatz. Visualizing host traffic through graphs. In Proceedings of the Seventh International Symposium on Visualization for Cyber Security (VizSec '10). ACM, New York, NY, USA, 58-63, 2010

[70] Max-Emanuel Maurer, Alexander De Luca, and Sylvia Kempe. Using data type based security alert dialogs to raise online security awareness. In Proceedings of the Seventh Symposium on Usable Privacy and Security (SOUPS '11). ACM, New York, NY, USA, 2011

[71] Andreas Sotirakopoulos, Kirstie Hawkey, and Konstantin Beznosov. On the challenges in usable security lab studies: lessons learned from replicating a study on SSL warnings. In Proceedings of the Seventh Symposium on Usable Privacy and Security (SOUPS '11). ACM, New York, NY, USA, 2011

[72] Jeremy Goecks, W. Keith Edwards, and Elizabeth D. Mynatt. Challenges in supporting end-user privacy and security management with social navigation. In Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS '09). ACM, New York, NY, USA, 2009

[73] Sascha Fahl, Marian Harbach, Thomas Muders, Matthew Smith, and Uwe Sander. Helping Johnny 2.0 to encrypt his Facebook conversations. In Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12). ACM, New York, NY, USA, 2012

[74] Mohamed Shehab, Said Marouf, and Christopher Hudel. ROAuth: recommendation based open authorization. In Proceedings of the Seventh Symposium on Usable Privacy and Security (SOUPS '11). ACM, New York, NY, USA, 2011

[75] Wenbin Fang, Barton P. Miller, and James A. Kupsch. Automated tracing and visualization of software security structure and properties. In Proceedings of the Ninth International Symposium on Visualization for Cyber Security (VizSec '12). ACM, New York, NY, USA, 2012

[76] John R. Goodall, Hassan Radwan, and Lenny Halseth. Visual analysis of code security. In Proceedings of the Seventh International Symposium on Visualization for Cyber Security (VizSec '10). ACM, New York, NY, USA, 2010

[77] L. Nataraj, S. Karthikeyan, G. Jacob, and B. S. Manjunath. Malware images: visualization and automatic classification. In Proceedings of the 8th International Symposium on Visualization for Cyber Security (VizSec '11). ACM, New York, NY, USA, 2011

[78] 情報処理推進機構、情報セキュリティプロフェッショナル育成に関する調査研究報告書、2003 年 4 月

[79] 情報処理推進機構、IT スキル標準 V3 2011、2012 年 3 月