社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2006－CSEC－34 (43)
2006／7／21

インシデント分析センタ nicter の可視化技術

中尾康二† 松本文子† 井上大介†

馬場俊輔†† 鈴木和也†† 衛藤将史† 吉岡克成† 力武健次† 堀良彰‡

† 独立行政法人 情報通信研究機構 〒184-8795 東京都小金井市貫井北町 4-2-1
†† 横河電機株式会社 セキュリティプロジェクトセンタ 〒180-8750 東京都武蔵野市中町 2-9-32
‡ 九州大学大学院 システム情報科学研究院 〒812-8581 福岡県福岡市東区箱崎 6-10-1
E-mail: † {ko-nakao, fumi, dai, eto, katsunari_yoshioka, rikitake}@nict.go.jp,
†† {Shunsuke.Baba, Kazuya.S}@jp.yokogawa.com, ‡ hori@csce.kyushu-u.ac.jp

あらまし 筆者らで推進しているインシデント分析センタ nicter プロジェクトでは，広域なインターネット上で発生するネットワークインシデントに関する総合的な対策技術の研究開発を行っている．本稿では，nicter プロジェクトにおけるインシデント分析・運用作業のための可視化技術に焦点を当て，可視化手法の適用領域，具体的な可視化手法について述べ，今後の nicter における可視化技術に関する検討課題等について考察する．
キーワード インシデント分析，可視化，ネットワークセキュリティ

Visualization Technologies of nicter Incident Analysis System

Koji NAKAO†, Fumiko MATSUMOTO†, Daisuke INOUE†,
Shunsuke BABA††, Kazuya SUZUKI††, Masashi ETO†, Katsunari YOSHIIOKA†, Kenji RIKITAKE†,
and Yoshiaki HORI‡

† National Institute of Information and Communications Technology (NICT)
4-2-1 Nukui-Kitamachi, Koganei, Tokyo, 184-8795, Japan
†† Security Project Dept., Business Development Div., Yokogawa Electric Corporation
2-9-32 Nakacho, Musashino-shi, Tokyo, 180-8750, Japan
‡ Faculty of Information Science and Electrical Engineering, Kyushu University
6-10-1 Hakozaki, Higashi-ku, Fukuoka, 812-8581, Japan
E-mail: † {ko-nakao, fumi, dai, eto, katsunari_yoshioka, rikitake}@nict.go.jp,
†† {Shunsuke.Baba, Kazuya.S}@jp.yokogawa.com, ‡ hori@csce.kyushu-u.ac.jp

Abstract The authors have been working on the R&D activities of nicter, an Internet security incident analysis center investigating overall countermeasures against security incidents detected over the wide area Internet. In this paper, focusing on visualization technologies for the purpose of the incident analysis and operation in the nicter, we describe the technologies currently implemented and planned to be developed in the nicter, based on the visualization requirements. Further, some issues for the extended visualization technologies required in the nicter are also mentioned.
Keyword incident analysis, visualization, network security

1. はじめに

筆者らは，社会的に重要性を増すネットワークの安心・安全を保つため，ネットワークインシデントの早期検知を行い，迅速に原因を究明する方法について研究開発を推進している．

本推進の第1段階として，収集したイベント[1]の傾向分析[1][2]，および確保したマルウェア[2]の静的/動的解析を，相関を取りながら実施することで，ネットワークにおいて発生しているインシデントの検知・対策導出をし，その結果を関連機関に配布することを目的とした「インシデント分析センタ nicter」[3]の構築を進めている．nicter（Network Incident analysis Center for Tactical Emergency Response）では，インシデントの分析・運用作業を支援する目的で，多数の可視化技術を採用している．

本稿では，nicter におけるインシデント分析・運用作業のための可視化技術に焦点を当て，可視化手法の適用領域，具体的な可視化手法について述べ，今後の nicter における可視化技術に関する検討課題等について考察する．

2. 可視化技術の研究動向

現在，複数の機関でインシデント分析システムに関わる研究開発および実用化がなされているが，それらの活動においても可視化技術が採用されている．いずれの提案も，ネットワーク内で発生している事象を，インシデント分析システムの分析運用者が直感的に把握することを目的としている．

広域ネットワークのトラフィックを観測し，時間的な傾向を把握するために，JPCERT/CC の ISDAS[4]，警察庁のセキュリティポータルサイト@police[5]，およびインターネット早期広域攻撃警戒システム WCLSCAN[6]では，広域センサからの情報を収集し，ポート番号ごとの統計データをグラフとして可視化している．具体的には，時系列に沿った攻撃パケット数の変動や，攻撃元の国ごとの攻撃パケット数などをグラフ表示している．分析運用者はこれらの結果から，広域におけるインシデントの傾向を大局的に把握することができる．

また，ネットワークのトラヒックを観測し，リアルタイムに状況を把握するための可視化研究には，NVisionIP[7]や VisFlowConnect[8]などがある．これらはホスト間の通信に対して，プロトコルやポート番号ごとに統計解析を行い，その結果を可視化している．また，送信元/宛先間の情報を線分と時間的変化で可視化しており，リアルタイムのトラヒックの傾向を知ることができる．

さらに，侵入検知システムのログデータを統合して，攻撃の状況を把握するための可視化研究には，IP Matrix[9]や Spinning Cube[10]などがある．これらは，IP アドレス空間における，アラート情報やポート番号など複数の情報を統合して可視化する研究であり，画面を動的に変化させ，不正アクセスの状況を視覚的に把握することができる．

その他にも，複数の手法を連携させることで，状況を把握するための可視化研究として，IDS RainStorm[11]や Visual Firewall[12]などがある．IDS RainStorm では，時間軸に沿った可視化がなされ，ズーム領域を指定し，段階的に詳細化することができる．これにより，送信元/宛先の IP アドレスの関係を把握できるようになっている．また，Visual Firewall では，リアルタイムのトラフィックの入出力，シグネチャ，時間軸でのトラフィック統計値および IDS アラームの4つの分析結果を同一画面上で表示し，統合的に状況を知ることができる．

分析運用者は，それぞれのツールを使用し必要な情報を収集，可視化しているが，最終的な原因と現象の関連付けは，未だ外部情報などを駆使して行っているのが現状である．

3. インシデント分析センタ nicter

本章では，筆者らのグループが研究開発を推進しているインシデント分析センタ nicter の概要を述べ，次いで nicter における可視化技術の適応領域を述べる．

3.1. nicter の概要

nicter は，我が国の情報通信基盤の安定運用に資することを目標に掲げ，インターネット上で生起する多種多様なイベント[1]の収集・分析を定常的に実施することで，ネットワークに大局的な悪影響を及ぼすインシデントの発生を早期に検出し，迅速かつ実効的な対策導出を可能とするシステムである．

nicter は，広域のネットワークモニタリングによって収集したイベントを解析し，その中からインシデントを検出するマクロ解析と，マルウェアの検体を収集・解析して，それらの挙動を抽出するミクロ解析という2つの解析パスを持つ（図 1）．これら自動化された2つの解析パスは，マクロ-ミクロの相関分析によって融合し，インシデントの「現象」と「原因」を対応付けることが可能となる．換言すると，マクロ解析で

[1] トラヒックデータや IDS，ファイアウォールのログなど，ネットワーク上で起こった事象の記録の総称．
[2] ウィルス，ワーム，ボットなど悪意のあるソフトウェアの総称．

はネットワーク上で発生しているインシデントの現象を捉えることができ，一方，ミクロ解析ではインシデントの原因と考えられるマルウェアの挙動を把握できるため，双方の解析結果を照合することで，発生中のインシデントの原因特定が可能となり，さらに，特定されたマルウェアに応じた対策導出も可能となる．その結果，ネットワークモニタリングによって観測された統計データ等の提示に留まらず，インシデントの原因とその対策にまで踏み込んだ実効性・即時性の高いインシデントレポートを，政府・官公庁や一般ユーザに向けて発行できる．

マクロ/ミクロ解析ならびにマクロ-ミクロの相関分析は機械的に処理されることを前提に研究開発を進めている．これら解析の結果，自動検出されたインシデントの候補群は nicter の分析運用者に対してタスクリストとして逐次提示される．分析運用者は定められたワークフローに沿って各インシデントの候補に対してインシデントの重要性の判定を行い，最終的にインシデントレポートの発行を行う．これら分析運用者による一連の処理はインシデントハンドリングシステム（IHS）と呼ばれる統合的な GUI フレームワークの上で行われる．

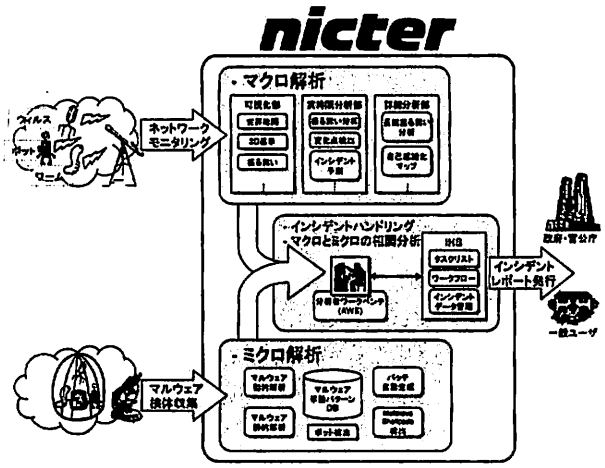

図 1 nicter の全体像

3.2. nicter における可視化技術の適応領域

上述のように，nicter は広域ネットワークにおけるイベントの傾向把握，およびその原因特定を行うことを当面の目標として，実時間で高精度の分析を推進しており，種々の分析手法の高度化が重要な課題である．同時に nicter では分析運用者がそれら複数の分析エンジンを駆使して広域ネットワークの定常的な観測を行っており，分析運用者による迅速なインシデント検知から対策導出までを支援するために，以下の技術領域において可視化手法の適応が必須である．

(1) イベントの傾向把握

実時間で収集するイベントを高速に分析することにより，広域のネットワークがどのような状況に曝されているのかを把握する必要がある．個々のイベントの属性（宛先ポート番号等）から求められる統計量の変化をグラフで示すだけでなく，より高次のデータを実時間で視覚的に表現することによって，分析運用者によるイベントの生起傾向の把握を可能にする．

(2) 攻撃ホストの振る舞い把握

スキャン等の攻撃パケットの送信元ホスト（攻撃ホスト）ごとに振る舞いの特徴を捉え，その分類や急激な攻撃量の変化の検出を行う必要がある．個々の攻撃ホストの振る舞いについて，数値的な特徴による分類も実施するが，さらにそれら振る舞いを可視化することにより，分析運用者が複数の攻撃ホストの振る舞いをイメージとして捉らえ，類似性等の視覚的な把握を可能にする．

(3) 分析手法間の相関性把握

上述のマクロ-ミクロの相関分析に見られるように，2つ以上の分析結果の相関をとる必要がある．その場合，相関性の分析を数値的なモデルに基づいて行うことも必要であるが，分析運用者が可視化された情報から相関を見出すことで，相関性の迅速な把握を可能にする．

(4) 多角的な属性による相関性把握

マクロ解析には，即時的に自動分析を実施する実時間分析部と，分析運用者によってより高精度の分析を行うための詳細分析部が含まれる（図 1）．この詳細分析の過程において，実時間分析では把握できなかった複数属性を用いた詳細な相関性を導出する必要がある

(5) IHS における操作支援

上述の可視化技術とは対象を異にするが，実時間のイベント分析から重要なインシデントを判定し，必要な警告，関連情報を含んだインシデントレポートを発行するためにインシデントハンドリングシステム（IHS）の構築が必要となる．分析運用者が的確なハンドリングを行うために，複数の情報源を視覚的に表示し，直感的な操作によるドリルダウン手法の提供が必要となる．

以上は，nicter の研究開発において必要な可視化技術の適用領域であるが，それぞれの可視化手法は個々の分析手法と強く関係しており，完全に切り離して考察することが難しい場合が多い．

4. nicter の可視化技術

本章では，nicter が現在実現している可視化技術，および将来的に研究開発が必須である可視化技術について述べる．

4.1. イベントの傾向把握のための可視化

nicter ではインシデントとなりうるイベントの傾向を実時間で把握する必要があり，分析運用者にとって可視化されたイベントは重要な情報源となる．そこで nicter のマクロ解析では，収集したイベント（トラヒック）を，1) イベントの発生対地，2) イベントの挙動形状，3) イベント量，のそれぞれの傾向が実時間で把握できるよう可視化を行っている．その際，トラヒックを構成する各パケットの送信元 IP アドレス/ポート番号，宛先 IP アドレス/ポート番号，プロトコル種別の 5 つの属性を用いている．

4.1.1. イベントの発生対地

イベントの発生対地（発生したエリア）を，パケットの送信元 IP アドレスから特定し，それを世界地図上にプロットして，パケットの流れをイメージとして捉えられるように，ロケットの形状で送信元から宛先へ飛来するアニメーションで表示する．ロケットが飛び交う様子から，どの対地/国からの攻撃が多いのかを直感的に把握することができる．また，プロトコル種別をロケットの色によって表現することで，対地毎の攻撃の傾向を把握することが可能である．具体的な可視化イメージを図 2に示す．

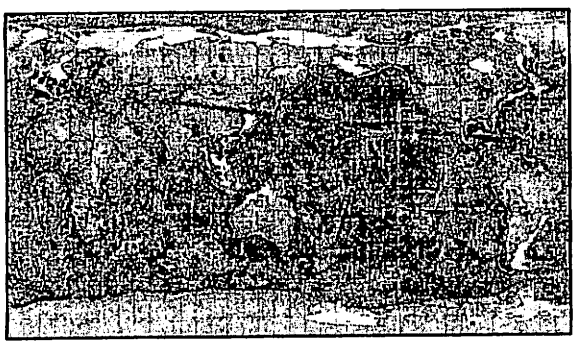

図 2 パケットの世界地図上での可視化

4.1.2. イベントの挙動形状

イベントの挙動形状を視覚的に把握するためには，4.1節で述べた 5 つの属性を 3 次元空間で表現する方法が有効である．送信元 IP アドレスと送信元ポート番号を直交 2 次元平面にプロットし，宛先 IP アドレスと宛先ポート番号についても同様な処理を行う．これら 2 つの 2 次元平面を平行に並べ，小さな線分として表現したパケットを送信元の平面から宛先の平面へと移動させる．線分は上述のロケット同様，プロトコル種別により色分けがなされている．これにより，攻撃の前段で行われるスキャンの挙動が典型的な形状として可視化されるため，インシデントの判定や各種の詳細分析を開始するトリガとなるなど，分析運用者の支援ツールとして非常に有用である．具体的な可視化イメージを図 3に示す．図の左側が送信元，右側が宛先の 2 次元平面であり，それぞれの平面の縦軸に IP アドレス，横軸にポート番号がプロットされている．

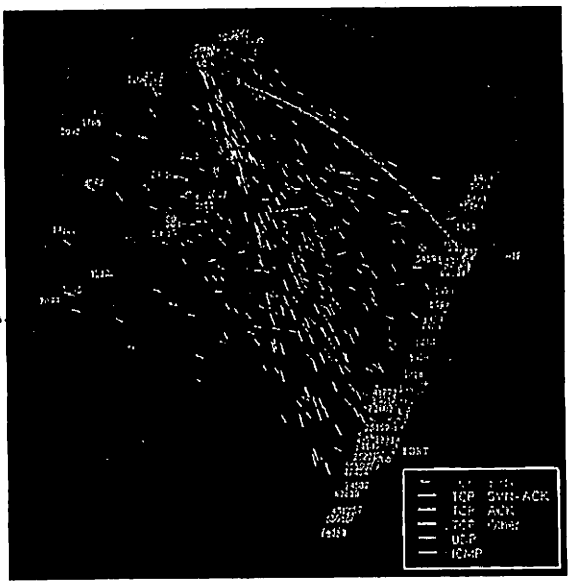

図 3 パケットの 3 次元空間での可視化

4.1.3. イベント量

上述したイベントの発生対地および挙動形状の可視化手法におけるイベント量については，飛来するロケットや線分の多寡によって，量的な視覚情報を与えることができる．

4.2. 攻撃ホストの振る舞い把握のための可視化

4.1節で述べた可視化手法は，広域ネットワークの大局的な傾向を把握するためのものであり，特定の攻撃ホストから何番のポートに対してスキャンが行われ，その攻撃ホストの振る舞いがどのような時間的変化を示すかといった，局所的なイベントを表現するものではない．そこで nicter では，攻撃ホストごとの振る舞いに着目し，それを2次元平面上で表現する可視化手法[13][14]を検討している．図 4はこの可視化手法の概要を示しており，画面の左半分の2次元平面に送信側（攻撃ホスト側），右半分の2次元平面に宛先側を配置している．送信側は縦軸にポート番号，横軸に時刻を，宛先側は縦軸にポート番号，横軸に IP アドレスをそれぞれ取っており，左右の両平面にイベント（パケット）をプロットし，さらにそれらを直線で結んでいる．直線の色は4.1節の可視化手法と同様に，プロトコル種別を表している．これにより，ある単一の攻撃ホストの短中期間の振る舞いが可視化できる．

図 5は実際に観測された 445 番ポートを狙ったネットワークスキャンの例である（左半面の折れ線グラフはイベント量の推移を示している）．

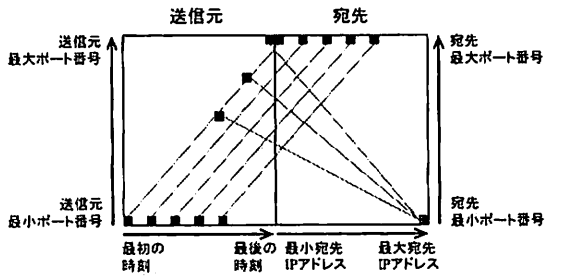

図 4 攻撃ホストの振る舞い可視化の概要

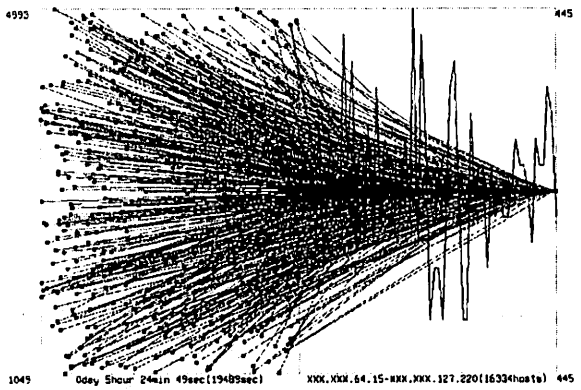

図 5 攻撃ホストの振る舞い可視化の実例

また，このように可視化された攻撃ホストの振る舞いを単位時間（例えば1日）ごとに区切って表示することで，攻撃ホストの長期的な振る舞いの変遷を把握することができる（図 6）．

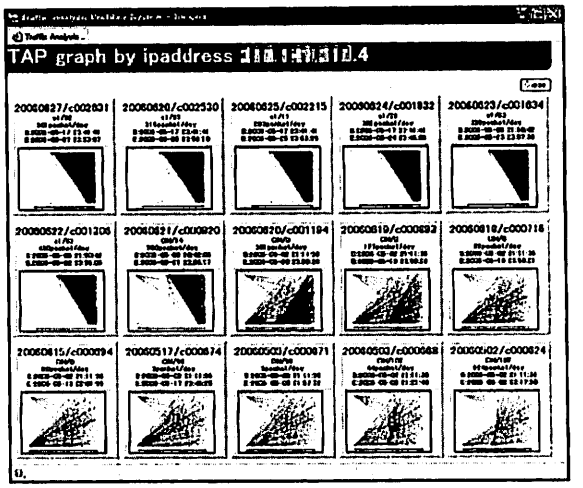

図 6 攻撃ホストの長期的振る舞い

4.3. 分析手法間の相関性把握のための可視化

図 1で示したように，nicter は様々な分析/解析手法を持つ．これらの手法によって導き出される複数の分析結果の相関性を把握するためにも可視化は有用であり，研究開発を推進している段階である．一例を挙げると，ミクロ解析に含まれるマルウェア静的/動的解析によってマルウェアの挙動が抽出できるが，この挙動情報を4.1.2節や4.2節で示した可視化手法の入力とし，マクロ解析で観測されている現象と対比させることで，マクロ-ミクロの相関分析を分析運用者の視覚という観点からも行うことが可能となる．

4.4. 多角的な属性による相関性把握のための可視化

イベントが持つ属性は4.1節で示した 5 つ以外にも，時間的な属性（パケットの到着時刻や到着間隔）や，量的な属性（パケットのペイロード長），内容的な属性（IP 層以上の情報）など様々なものがある．nicter はそれら多角的な属性から攻撃ホストをクラスタリングする手法[2]の研究を実施している．この手法では，観測されたイベントを攻撃ホストごとに集約し，それらイベントの属性群を特徴ベクトルとして自己組織化マップ（SOM: Self-Organization Map）の入力とし，2次元平面に出力して可視化する（図 7）．これにより，相関性の高い攻撃ホストは2次元平面上で近傍に位置す

ることとなる．図 7で，各円は類似した属性を持つ攻撃ホストのクラスタを示しており，円の大きさがホスト数を表現している．この 2 次元平面の経時変化を視覚的に捉えることで，マルウェアに感染したホスト数の増減や，マルウェアの亜種の出現を把握することが可能となる．また，任意の属性を持つクラスタをハイライトし，そこからさらに詳細な分析へと移ることが可能である（図 8）．

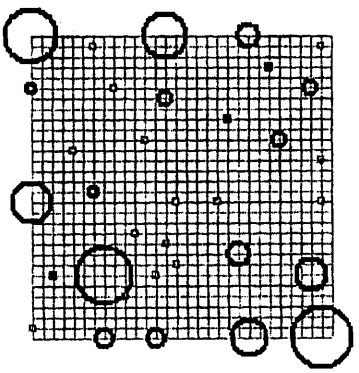

図 7 クラスタリングされた攻撃ホスト群の可視化

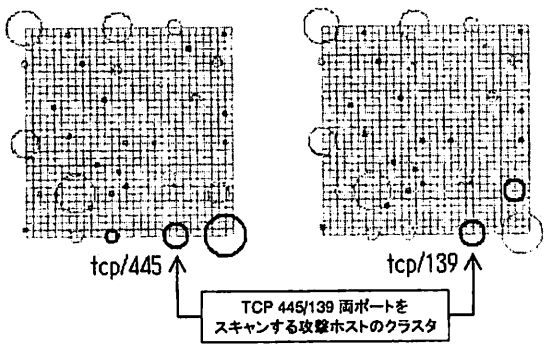

図 8 特定の属性によるクラスタのハイライト

4.5. IHS における操作支援のための可視化

分析運用者が nicter を迅速かつ効率的に操作するために，オペレーションの可視化を司るインシデントハンドリングシステム（IHS）の構築が必須であり，nicter の重要課題として研究開発に取り組んでいる．IHS は，インシデント候補であるイベントの視覚的な通知に始まり，分析運用者がインシデント判定を行うために詳細分析に移った際の各分析手法間のシームレスな連携，さらにはインシデントレポートの GUI による半自動生成など，分析運用者を支援する様々な機能を有する．また，FPR（False Positive Rate）や FNR（False Negative Rate）を低減させるため，インシデント判定結果の自動的なフィードバックや分析運用者による GUI 操作で，各分析手法のチューニングを可能にすることも IHS の重要な機能であり，今後の構築課題となっている．

5. 考察

インシデント分析センタ nicter における可視化技術の適用領域において，現在検討を進めている可視化手法を前章にて紹介した．基本的に可視化処理が特定の分析手法（4.2節の振る舞い分析など）と直接連動する場合は，該分析の結果を視覚的に容易に導出できるが，可視化処理方法が，分析手法に強く依存することとなり，可視化処理を共通利用することはなかなか難しい．

現状の nicter では，ハニーポットなどで確保したマルウェアの静的/動的解析を実施しており，それらの処理は，基本的にシステム構築の面から 3 層構造により体系化されている．すなわち，静的/動的解析に必要な生のログを蓄える DB 部，解析した結果に XML 化処理を施す機能部，および XML 情報を分析運用者にとって理解しやすい形で表示する可視化処理部により構成される．現状の体系化はマルウェア解析部分にのみ適用されているが，本体系を拡張して，ミクロ-マクロの相関分析，インシデント対応，レポート作成などのインシデントハンドリング機能を実現する機能群に対して柔軟に適用できるようにする必要がある．この場合，XML で記述された結果情報を複数の可視化モジュールがそれぞれ処理し，分析運用者にとって利用し易い形で構築することが重要となる．

従って，分析手法に依存した可視化手法も可能な限り利活用できる形でモジュール化し，上述の 3 層の体系にはめ込むことにより，柔軟で拡張性の高いシステム化が達成できるものと考える．4.3節で述べたように，ミクロ解析で得たスキャン系の挙動情報（マルウェアの先頭の挙動ログ等）を，スキャン系イベントの挙動形状可視化モジュールにて動作させ挙動を視覚的に把握する．すなわち，事前にネットワークから直接収集したイベント情報に対して挙動形状可視化モジュールを利用した結果と，ミクロ解析の結果を視覚情報として比較することにより，相関分析の視覚化処理に活用できる．ここで，挙動形状を把握するための可視化モジュールは，複数の分析手法にて共通的に活用でき，上述の体系化に従った，より効果的なシステム化が達成できると言える．

nicter のような実用型システムは，長期的な運用経験による実績を考慮することが必要で，分析運用者自らのフィードバックを繰り返すことで，機能性，運用性，性能の向上を体系的に目指す必要がある．今後の開発においても，nicter 分析運用者，分析手法設計者，

インシデントハンドリング処理設計者などと強い連携をとりながら，より効果的な成果物が得られるものと期待している．

6. おわりに

本稿では，開発過程にあるインシデント分析センタ nicter における可視化技術について報告した．本検討では，従来の可視化技法をより高度化し，nicter に適合した可視化技術について具体的に概観した．これら可視化技術は，個々の分析手法と大きく依存し，共通的なシステム構築が難しいといった課題があるが，広域のネットワークを対象とする nicter においては，可能な限り可視化技術をそれぞれの分析手法などで有効活用し，分析運用者が簡易かつ迅速に対応処理のできるよう，これからも検討を加速化していく予定である．

最後に，当研究を進めるに当たり，ご助言やご支援を頂いた関係者一同に，深く感謝の意を表する．

文　献

[1] 竹内純一，佐藤靖士，力武健次，中尾康二，“変化点検出エンジンを利用したインシデント検知システムの構築，” 電子情報通信学会，2006年暗号と情報セキュリティシンポジウム (SCIS2006), 2E2-2, Jan. 2006.

[2] 大河内一弥，力武健次，中尾康二，“自己組織化マップを用いたネットワークインシデント分析の研究，” 電子情報通信学会，2006年暗号と情報セキュリティシンポジウム (SCIS2006), 2E2-3, Jan. 2006.

[3] 中尾康二，力武健次，竹内純一，大河内一弥，吉岡克成，衛藤将史，守山栄松，松本文子，“インターネットにおける実時間イベント分析の研究開発，” 電子情報通信学会，2006年暗号と情報セキュリティシンポジウム (SCIS2006), 3B4-5, Jan. 2006.

[4] JPCERT/CC Internet Scan Data Acquisition System (ISDAS), http://www.jpcert.or.jp/isdas/.

[5] 警察庁セキュリティポータルサイト@police, http://www.cyberpolice.go.jp/detect/observation.html.

[6] インターネット早期広域攻撃警戒システム WCLSCAN, http://www.wclscan.org/.

[7] K. Lakkaraju, W. Yurcik, A. J. Lee, R. Bearavolu, Y. Li, X.Yin, “NVisionIP: NetFlow Visualizations of System State for Security Situational Awareness,” Proc. 2004 ACM workshop on Visualization and data mining for computer security (VizSEC04), pp. 65-72, Oct. 2004.

[8] X. Yin, W. Yurcik, M. Treaster, “VisFlowConnect: NetFlow Visualizations of Link Relationships for Security Situational Awareness,” Proc. 2004 ACM workshop on Visualization and data mining for computer security (VizSEC04), pp. 26-34, Oct. 2004.

[9] 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，” 情報処理学会論誌，Vol.47, No.4, pp. 1077-1085, Apr. 2006.

[10] S. Lau, “The Spinning Cube of Potential Doom,” Communications of the ACM, Volume 47, Issue 6, pp. 25-26, Jun. 2004.

[11] K. Abdullah, C. Lee, G. Conti, J. A. Copeland, J. Stasko, “IDS RainStorm: Visualizing IDS Alarms,” IEEE Workshop on Visualization for Computer Security 2005 (VizSEC05), pp. 1-10, Oct. 2005.

[12] C. P. Lee, J. Trost, N. Gibbs, R. Beyah, J. A. Copeland, “Visual Firewall: Real-time Network Security Monitor,” IEEE Workshop on Visualization for Computer Security2005 (VizSEC05), pp. 129-136, Oct. 2005.

[13] 鈴木和也，馬場俊輔，田中貴志，“未利用アドレスブロック監視型モニタリングシステムの開発，” 第4回情報科学技術フォーラム (FIT2005), L-021, Sep. 2005.

[14] 鈴木和也，馬場俊輔，高倉弘喜，“未利用アドレスブロックに到達するトラフィックの解析，” 信学技報，vol. 105, no. 530, IA2005-23, pp. 25-30, Jan. 2006.