不正侵入調査を目的とした複数ログの時系列視覚化システム

江端真行[†] 小池英樹[†]

不正侵入検知において最も基本的なタスクとして “ログの調査” がある．近年では，計算機やセキュリティ機器の増加にともない，複数のログを対象とし多面的に不正侵入の調査を行うことが必要となってきている．しかし，依然としてログの調査手法はテキストベースで行われていることが多く，複数のログの調査手法としては非効率であるといえる．我々は，複数のログに対して事象の出現頻度を基に時系列に視覚化し，調査支援を行うシステムを構築した．また，本システムをハニーポットのログの調査に適用し，その有効性を示した．

A Visualization System of Multiple Logs with Timelines for Intrusion Analysis

Masayuki Ebata[†] and Hideki Koike[†]

Log analysis is one of the most fundamental task of intrusion detection. In recent years, since a number of computers and network security devices increases, it is required to analyze multiple logs produced by them. However, log analysis is done with text-based techniques and it is inefficient for analyzing of multiple logs. We developed a visualization system for analysis of multiple logs which visualizes the frequency of events by timeline. We analysed logs produced by a honeypot by using the system, and showed its effectiveness.

1. はじめに

近年では，コンピュータネットワークの普及にともない，コンピュータシステムは複雑になり，またセキュリティの問題は非常に重大なものとなった．そして，不正侵入検知，すなわち，不正または異常な活動における兆候を見つけるためのシステムとネットワークの監視は，多くの組織のセキュリティ基盤にとって重大な要素になってきている．

不正侵入検知システムは自動的に成功，不成功だった攻撃やコンピュータシステムの異常を識別しようとするが，誤検知や未遂に終わった攻撃，また他に起因したものによる不正確な警告によって報告されるため，それのみで効果的に運用することはできない．そのため，それら警告に対してより詳細に調査を行い，その警告に対しての判断を人間が行うことが必要であると考えられる．その際，不正侵入検知システムの警告以外にもファイアウォールやシステムのログなども重要な手がかりとなるため，それらのログも含め統合的に調査することが必要である．

† 電気通信大学大学院情報システム学研究科
Graduate School of Information Systems, University of Electro-Communications

このような複数ログの調査作業では，各ログの流れ，またログ間の関連性を把握しての調査が必要となるが，従来からのログ調査手法は非常に煩雑で多くの手間を必要としている．これに対し，ログの概要をつかみ，詳細な調査を容易にするために有効な手法として情報視覚化を用いることがあげられる．

本稿では，不正侵入検知の手法，情報視覚化による支援の重要性について説明し，それらに基づいて構築した複数ログの時系列視覚化システムの概要，使用例，考察について述べる．

2. 不正侵入調査とその手法

不正侵入対策は，監視，調査，対応という 3 つのタスクによるモデルで表されるということを Goodall はセキュリティの専門家へのインタビューによって示した[1]（**図 1**）．

監視のタスクでは，不正侵入検知システムやそれ以外の多くの情報を監視し，監視から調査へは，不正侵入検知システムの警告だけでなく，たとえば，高負荷なネットワークトラフィックや他からの異常の報告などがあった場合など様々な事象によって移行する．その際，ただちに，さらなる調査が必要であるか，またその情報の重要度，信頼性などが判断される．そして，

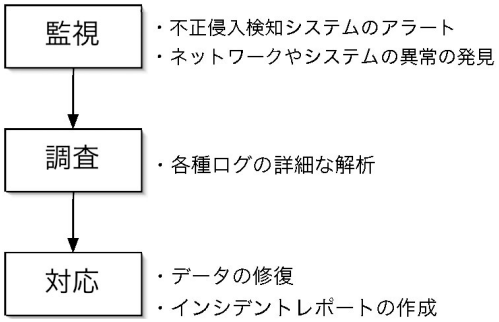

図 1 不正侵入検知のタスクモデル
Fig. 1 A task model of intrusion detection.

図 2 テキストベースによる調査手法
Fig. 2 A typical text-based analysis method.

調査のタスクでは，その事象をより詳細に調査し，調査から対応への移行においては，事象に対する調査とその対策の結果がまとめられる．もし警告が実際の攻撃や他の不正な活動を表していると判断されるならば，適切な対策を考えなければならない．そして，対応のタスクでは，たとえば法的処置を求めるインシデントレポートを作成したりバックアップからシステムを修復したりといったことを行うのである．

調査のタスクにおいて，調査者は監視で発見した事象に対して，何らかの推測を持って行われる．このような推測は，調査者個人のネットワークやシステムのプロトコル，または OS に対する知識，またこれまでに起こった事象に対しての経験によって得られるものであり，個人の能力に依存し，得られる情報によっては不正確にしか判断できないこともある．また，一般的に共通して調査の対象とする情報源としては，以下のようなログがあげられる．

- ファイアウォールや他のネットワーク機器
- 不正侵入検知システムの警告
- ネットワークスニッファツール
- システムとアプリケーションのログ
- システム構成とネットワークパフォーマンスに関するデータ
- セキュリティスキャナの結果
- ファイルの完全性チェックツール

そして，調査者は，これらのログを基に頭の中で事象に対する重要な情報を抜き出し，どのような事象が，どのような経緯によって起こったのかを検証していく．このため，調査は，複数のログに対して統合的に行われることが求められる．

また調査では，事象系列を基にした調査と時系列を基にした調査がある．事象系列を基にした調査とは，事象名を基に行われるものであり，ある事象に対して，ログにどのように記録されるか把握しているなど，事象に対する知識が十分にある場合などに有効である．その場合，ある事象さえ抜き出すことができれば，それに付随してその前後の事象では何があったのか推測していくことができる．しかし，複数のログの調査においては，あるログの事象名と他のログの事象名が一致しないため，あるログで具体的に起こった事象が分かっても他のログではそれがどのように関連しているのか分からないといった場合がある．この場合，事象が起こった時刻において，他のログでどのような事象があったかを見る時系列を基にした調査が必要となる．

従来から行われている調査手法は，テキストベースで less や grep などを駆使したものである．これらは，すでに事象が明らかに分かっている事象系列を基にした調査においては手っ取り早く調査を行うことができる．しかし，この手法において，時系列を基にした調査を行いたい場合には，**図 2** に見られるように複数の調査対象のログをそれぞれを別々のターミナルで表示させ，ターミナルを切り替えながら調査するということが要求され，非常に煩雑な操作をともなう．

このような調査のタスクに対し，その支援を行うために有効な手法としては，複数のログに対して時系列を基にした情報視覚化を行うことが考えられる．時系列を基にした情報視覚化によって，複数のログの時刻に基づく概要を知ることができ，ログ間の関連や前後の事象を把握することが容易となり，詳細な調査を支援することができると考えられるためである．

3. 関 連 研 究

これまでにも不正侵入検知における視覚化の研究はいろいろと行われている．これらの多くは，ネットワークの状況を表示するためにリンクや階層化，または散布図による視覚化を行い，時間的なデータ属性の表示のためにアニメーションを用いており，刻々と変化する状況の認識を支援している．

VisFlowConnect [2] では，ホスト間のリンクを見せ

るため座標を並列に表示している．また平安京ビュー[3]ではIDSの警告ログを用いてIPアドレスを基に階層化し，各ネットワークの警告を種別ごとにヒストグラム表示する．

NVisionIP[4]はNetflowデータを用いて，現在のクラスBネットワークの状態を示すために，IPアドレスの散布図を用い，各IPアドレスにおける特定のポートの活動を色別表示している．またPortVis[5]は1時間間隔でのポートの活動を表示するために，メインの視覚化に散布図を使用している．

ただし，これらの視覚化は主として調査者が現在の状況を知る，状況認識を行う際に用いられるものであり，不正侵入検知における監視のタスクを支援するために使用することを目的としていると考えられる．それは，これらの視覚化は，異常かどうかの判断には優れるが，調査のタスクにおいて調査者が一番必要とする，どのように異常なのか，またなぜそのような状況になったのかといった詳細な情報を知ることには向いていないためである．

また，調査を支援するという点に着目したログの視覚化を行う研究もすでにいくつか存在する．

SeeLog[6]は，コマンド履歴を記録したpacctログを視覚化するツールであり，抽象化，色，集合化，フィルタリング，対話機能を使用して，ログから得られる異常なパターンを発見しやすくするものである．また，見えログ[7]は，システムのログを記録する際に汎用的に用いられるsyslogログに対し，頻度情報やログのアウトラインなどを用いて1画面上に比較的長期のログを表示させることを可能とし，概要と詳細を把握しつつ調査を行うことができる．

しかし，これら調査の支援を目的としたログの視覚化であっても，単一のログを視覚化することに焦点が当てられている．実際の不正侵入調査では，複数のログを対象とした支援が行われなければならない．もし，これらを使用し調査を行う場合には，それぞれのログごとに視覚化を表示する必要があり，複数のログを統一して調査を行うことが困難であるといえる．

4. 複数ログの時系列視覚化システム

本システムでは，不正侵入検知における調査支援を目的に，複数ログに対して時系列に着目して視覚化する手法を適用する．複数のログを調査する際には，あるログの注目する事象に対して，他のログでの関連した情報や同時刻帯での他のログの出力状況を知るということが非常に重要であり，そのためログの時系列を視覚化することによってログの時間的な流れに対する概要の把握を容易にし，また複数のログをその時間軸を一致させて並べることにより，他のログにおいて同時刻で起こった事象を把握しやすくし，その関連を意識できるようにするためである．また，視覚化に対して対話的な操作することで，詳細情報の表示時刻を変更することを可能にし，視覚化と詳細なログ情報とが関連付けられ一貫した調査が行えることを考慮して，システムの構築を行った．

4.1 システムの概要

本システムはJava SE 1.4で実装しており，様々な環境で使用することが可能である．

本システムでは，**図3**で示すように，多種のログに対応して視覚化を行うため，ログファイルを読み込む際に様々なフォーマットのログを統一的に扱えるように汎用ログ形式のデータへと抽出・変換を行い，その後抽出したデータから頻度解析の処理を行って時系列視覚化と詳細情報の表示を行う．

汎用ログ形式への抽出・変換処理では，**図4**のように，ログメッセージの時刻を秒を基準とした数値に統一し，またIPアドレスやポート番号などの各ログにおいて重要な情報は，特徴情報として文字列から整数値などの型に変換して抽出する．また変換処理では時系列視覚化ではより状況を判断しやすくするため，調査対象に合わせてメッセージ中の不要な情報についてフィルタリングも行う．この抽出・変換された汎用ログ形式のデータは，詳細情報表示で表形式に表示する．

また，そのデータに対し頻度解析処理によって，時系列で視覚化される際の最小単位である“分”でログ

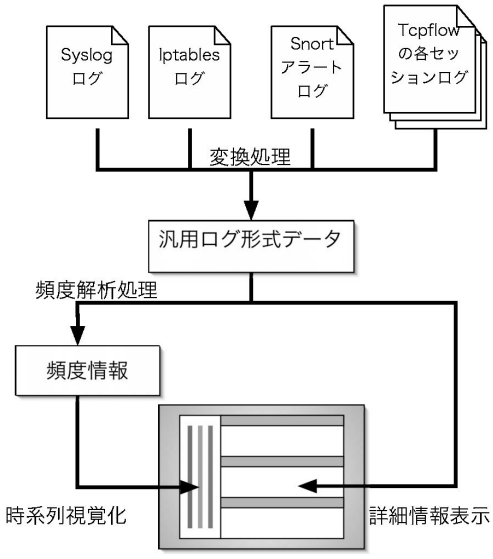

図3 システムの処理概要
Fig. 3 An overview of data processing.

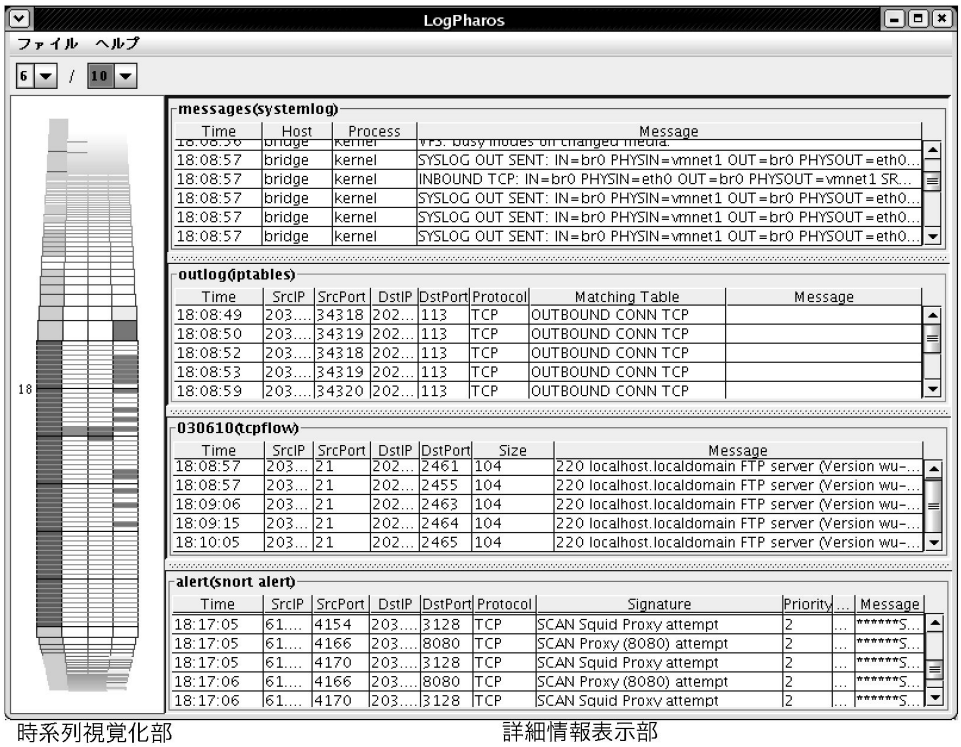

図 5 システム画面
Fig. 5 A screenshot of the system.

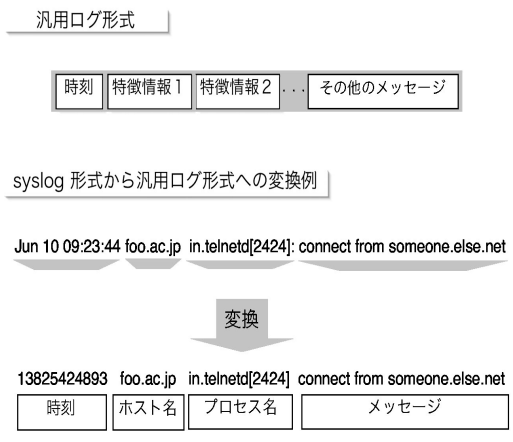

図 4 汎用ログ形式への変換例
Fig. 4 An example of conversion into general log form.

情報の出力頻度を解析し，頻度情報を取得する．この頻度情報を基に，時系列視覚化でログの時系列を視覚化する．

時系列視覚化では，ログの出現頻度を表現したログの時系列を時間軸を一致させてログごとに並列に表示する．ログの視覚化によるイメージと詳細な情報が結びつくことに配慮し，比較的長期を俯瞰するための直線で表現した時系列視覚化，また注目する時間が拡大しそれ以外の時間が縮小する distortion view を用いた時系列視覚化の 2 つを用い，注目する時刻を変更して見ることができる．

また詳細情報表示では，汎用ログ形式データで抽出した特徴情報は各テーブルの列に対応して表示される．また，調査者が時系列視覚化で注目する時間を対話的に選択した際に，それに連動して詳細情報を表示する．これにより，複数のログの時刻を統一して調査することができ，またログ間の関連情報を把握することも容易になる．

図 5 に本システムの画面を示す．

4.2 対象とするログ

本システムでは，汎用ログ形式に変換することにより，どのログでも対応することができる．またログに限らず，定期的に取得することさえできれば CPU 負荷などのシステムリソースの情報にも対応させることも可能である．

現在は，以下の 4 種類を調査対象とした．

- システムログ：syslog ログ
  システムログでは，OS やデバイス，アプリケーションプログラムで起こった事象が記録され，各

コンピュータの異常を発見する際に有効である．本システムではシステムログの中でも多くのオペレーティングシステムで使用されている syslog を対象にした．

- ファイアウォールのログ：iptables ログ
  ファイアウォールはネットワークのゲートウェイなどに置かれ，パケットの通過・ブロックの管理を行う．そのためそのログには，通過またはブロックしたパケットの情報が記録される．通過させたパケットの IP アドレスやポート番号などが有効な手がかりとなるため，不正アクセスなどにおいて外部の犯行か内部の犯行かを示す際に重要なログとなる．本システムでは Linux で一般的に用いられているファイアウォールソフトウェアである iptables [8] のログを対象とした．
- ネットワーク型不正侵入検知システムのログ：snort の警告ログ
  ネットワーク型不正侵入検知システムは，そのシステムが配置されたネットワークに流れているパケットを監視し，不正なものを検知して警告するシステムである．そのため，そのログには警告の内容や IP アドレスやポートなど不正アクセスに関する多くの情報を得ることができる．しかし，誤検知という問題があり，そのログのみを安易に信用することはできない．本システムでは，多くのプラットフォームで動作し広く使用されているネットワーク型不正侵入検知システムである snort [9),10)] の警告ログを対象とした．
- パケットスニファのログ：tcpflow ログ
  パケットスニファは本来プロトコル解析などに使用され，スニファに流れるすべてのパケットを記録する．そのため，そのログはすぐに膨大な量になってしまうため，運用しているコンピュータに使用することはない．しかし，異常が起こった際に短期的に使用するなどすれば，何が起こったのかを詳細に知ることができる．本システムでは，パケットスニファの中でも多くのプラットフォームで動作し，TCP セッションごとに記録することができる tcpflow [11] のログを対象とした．

このようにどのログにも一長一短が存在し，あるログのみを信用して運用しても，異常に気づかなかったり，詳細を調べることができなかったり，またはログの量がすぐに膨大となってしまい，調査が非常に困難をともなったりするため複数の種類のログに対応することが非常に重要である．

4.3 時系列視覚化と対話手法

時系列視覚化では，同時刻帯の比較，そして概要と詳細情報を同時に表示できるということを目的に，時系列を直線としそれぞれのログの時系列を並列に並べる一般的な表示手法と，distortion view を用いた視覚化として代表的な Perspective Wall [12)] を基にした視覚化手法の 2 つの視覚表現を用いた．

時系列視覚化ではどちらも，1 日分の時系列を格子列で表しており，各ログの時系列が並列に表示される．直線表現を用いた時系列視覚化では，1 格子は 10 分を表し，その格子が示す時刻にログが出力されている場合，出現頻度を格子の色の濃淡で表す．濃淡の基準は，その格子が表す時間のログの出力量が 1 日のうち 10%以上あれば濃い色，5%以上ならば通常の色（原色），出力があれば薄い色，なければ着色なしとした 4 段階で表現され，これによって 1 日のログの出力状況のイメージを把握することができる．

また，distortion view を用いた視覚化では，注目する 1 時間は引き延ばされ，その格子は 1 分単位となるが，その他の時間は 10 分単位のまま注目時間から離れるほど格子が縮小する．このため，注目時間は詳細に，それ以外の時刻は概要を示すものとする Focus + Context な視覚化となっている．

また，**図 6** で示されるように 1 日の格子列から注目する 1 つの格子をマウスクリックによって選択すると，distortion view を用いた時系列に変更される．また，その注目時間はマウスホイールを動かすことにより 10 分ずつ変更していくことが可能である．このこ

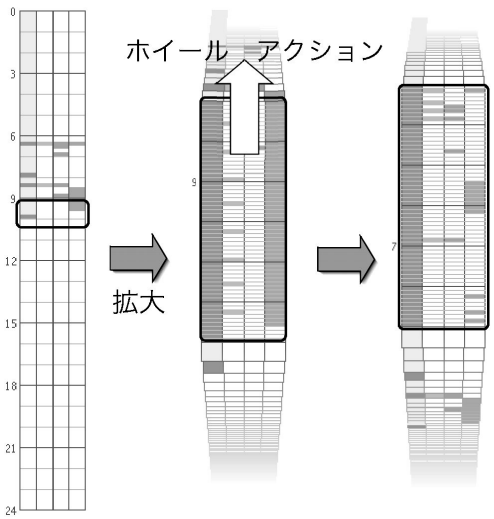

図 6 時系列視覚化での視覚化と対話手法
Fig. 6 Visualization and interaction in timelines visualization.

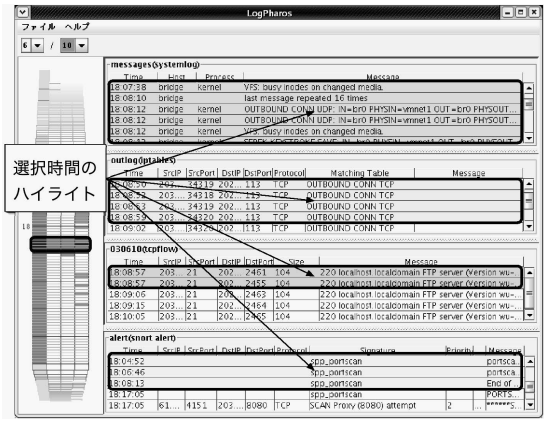

図 7 詳細情報表示のハイライト
Fig. 7 Highlighting detailed information.

とにより 1 日のログから “分” 単位まで 1 画面上でスムーズに調査することができ，1 日という比較的長期間をログの出力イメージから調査者が注目する 1 時間また 1 分単位までイメージが崩れることなく調査することが可能となる．

詳細情報表示では，ログメッセージの出力時刻，各特徴情報，その他のメッセージをそれぞれ列として分け，1 ログメッセージを 1 行で表示する．また，時系列視覚化で行われた対話操作とも連動しており，初めは 1 日のログメッセージすべてがそのテーブルに表示されているが，distortion view を用いた時系列表現に変更されたときに，テーブルに表示されるログメッセージが 1 日から選択した 1 時間へと絞り込みが行われる．さらに，**図 7** のように distortion view を用いた時系列視覚化において，調査者が注目している “分” を選択すると，その “分” のログ情報がハイライトされるという視覚効果を持つ．これにより，注目時刻とそれ以外を区別することが容易になる．

5. システムの使用例

我々は，ハニーポット[13)~15)] を実験的に運用している[16)]．ハニーポットとは，不正侵入の手法や侵入者の意図など知るために設置するおとりのサーバである．不正侵入の痕跡を得るために，ハニーポットでは種々のツールを用いてログを取得する．そのため，ハニーポットでは複数のログを調査することが非常に重要である．ただし，これらに用いられるツール，またログは一般のサーバなどにおいても不正侵入の調査においては重要な手がかりとして用いられるものであり，またその調査の工程はハニーポット，一般のサーバともに大差はない．

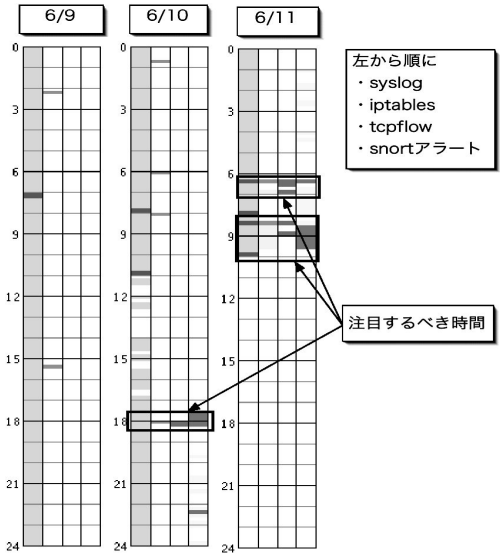

図 8 時系列視覚化による異常検知
Fig. 8 Anomaly detection by timelines visualization.

ハニーポットで得られた実際のログを用い，本システムを使用した調査手法について説明する．ハニーポットの場合，極力正規のユーザのアクセスがないようにするため，システムに何らかの異常が起こった場合，不正侵入であると考えて調査のタスクに移行する．そのため監視から調査へのタスクの移行は容易である．たとえば，ファイアウォールのログの出力数などを監視して，出力数が極端に増えた場合には不正侵入であるとの疑いを持って，調査のタスクに移行するだろう．

調査を行う際には，手がかりとなる時刻付近におけるログの調査を行う．**図 8** は，本研究室において運用した Linux ハニーポットにおいて 2004 年 6 月 9 日から 11 日の不正侵入に対処するまでのログを本システムで読み込ませたときの時系列視覚化の様子であり，日ごとに左から順に syslog，iptables，tcpflow，snort の警告のログの時系列を示している．iptables の出力数が異常に増えた 6 月 11 日 6 時 20 分付近に着目すると，この付近ではやはり複数のログで出現頻度が高いことが確認できる．このように複数のログで出現頻度が高い時刻では，何らかの異常によって瞬間的に警告などのログ量が増えている可能性が高いためである．これにより何らかの異常があったという確信を深めることができる．

そして，より詳細に調査するために時系列を拡大表示する．**図 9** は，6 時 20 分付近に時刻を絞った際の時系列視覚化と詳細情報表示部の様子である．時系列視覚化では左から，詳細情報表示部では上から，順に syslog，iptables，tcpflow，snort の警告の各ログの

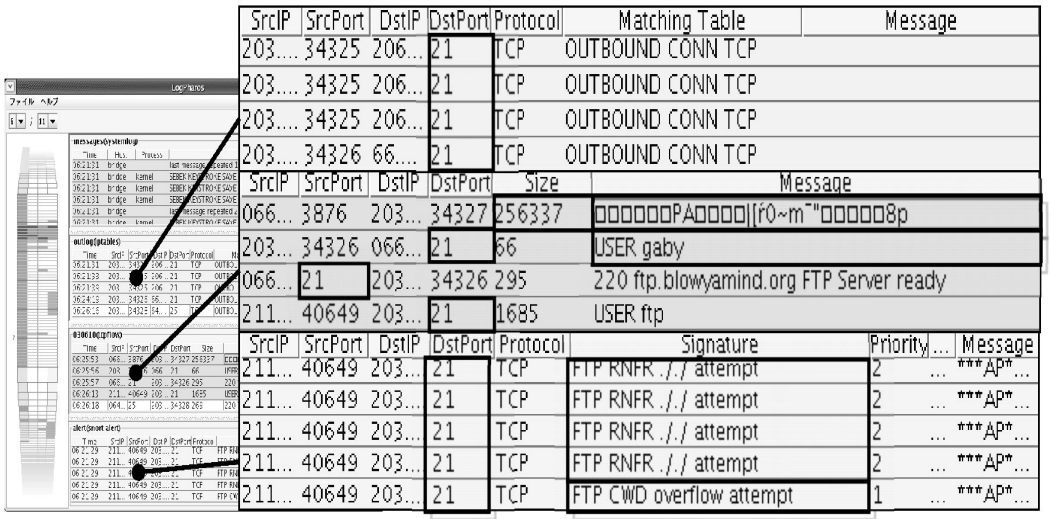

図 9 視覚化と詳細情報表示を用いたログの調査
Fig. 9 Analyzing logs with visualization and detailed information display.

状況を表示している．その時刻付近では iptables のログを確認すると 21 番ポートへのアクセスが増えており，また snort の警告ログでは，ftp サーバのバッファオーバフローの脆弱性を狙った攻撃に対するシグネチャが確認され，tcpflow ログにも同様に同一の IP アドレスからの 21 番ポートへのアクセスが確認された．さらに tcpflow を調査すると正規のユーザではないユーザによる ftp のログインの履歴とバイナリデータのような長いメッセージが残っていることが確認できた．このように同時刻のログを確認することにより ftp サーバの脆弱性を狙った攻撃による不正アクセスを受けたことを確認した．

そして，さらにその時刻の前後の事象について調査を行う．さきほどの調査で ftp サーバに対して攻撃を行った攻撃者の IP アドレスが分かっている．この IP アドレスが出現したログの時刻を基に，そのとき起動していたプロセスやファイルアクセスを他の syslog などを調査することができる．また，得られた手がかりだけではログを絞ることが難しい場合には，さらに図 8 の出現頻度が高い時刻に着目することで前後の以上を示す可能性の高い重要な事象について効率良く調査を行うことができる．例では，11 日 6 時前後で出現頻度が高くなっているのは，10 日の 18 時付近また 11 日の 9 時付近である．実際に調査を進めていくと，攻撃を受ける前日の 6 月 10 日の 18 時付近にポートスキャンを受けた形跡があった．

このような使用法から，従来からの手法に比べてより早く，異常の発見，原因の究明，他への影響などを時間的なつながりを確認しながら行うことができ，調査を非常に効率的に行うことができる．

6. システムの考察

本システムは，時系列視覚化により，各ログの出現頻度からその概要を把握し時間的な流れをとらえることが容易であり，また時系列視覚化から，ログの詳細情報表示までが対話操作により連動し，時刻に基づいたログ間の関連の把握をスムーズに行うことができる．また，出現頻度を基にした時系列により，時刻や情報があいまいである場合や前後関係の調査を行う際にも効果的に行うことが可能である．

もし，異常が発生した時刻より前の何らかの兆候を示す事象を調査したい場合に，テキストを基にした従来の手法では，ログごとに grep によって異常が発生した時刻より前のログを日時などで大まかに切り出し，さらにログごとに less などでスクロールさせながら関連のありそうな文字列を検索し，もしあるログで兆候と思われる事象を見つけた場合には，その時刻を基に他のログにおいてその兆候について検証するといった操作が必要となったが，本システムでは，複数のログの出現頻度が異常発生の直前で上がっている時刻を 1 クリックして拡大し，その周辺をスクロールして各ログでその詳細を確認するといった操作していくだけでよい．

このため，ハニーポットの調査において非常に効果的に調査を行うことができた．しかし，本システムは，ハニーポットだけではなく，運用しているシステムも

含めた不正侵入調査の支援を行うこと目的としている．ただし，実運用中のシステムではハニーポット以上に検討すべき事項がある．以下では，実運用環境での不正侵入調査への適用と，また本システムの視覚化手法における課題について考察する．

6.1 実運用環境における不正侵入調査への適用

実運用環境では，ハニーポットと違って正規のユーザによるアクセスにより飛躍的にアクセス数があり，環境によってログの出力量は大きく異なる．ハニーポットの場合，使用例で示したような 3 日分のログでは，たとえば snort の警告ログの場合 1,065 警告数（150 KB）しかなく，PowerPC G4 1.25 GHz，メモリ 1 GB の MacOSX の計算機で使用する場合，読み込みと表示ともに 1 秒未満でストレスなく行うことができる．しかし 404,583 警告数（138.8 MB）の snort の警告ログに対しては同一計算機を用いて読み込みに 65 秒，初期描画に 20 秒程度かかる．ただし，その後の描画では，解析したデータはメモリ内に保持しているため，スクロールなどの表示でもたつくことはなかった．そのため，実運用中のシステムの調査においても，ある程度はそのまま行うことができると考えられる．また，ログの量が非常に多い場合にも，調査すべき日時や手がかりが分かっている場合に，事前にその部分のログだけ切り出すなどしておくことで，よりストレスなく調査することが可能である．

また現在，本システムでは，最小単位を分とし，色の濃度を出現頻度によって 4 段階で一意に決めているが，実運用する環境によっては，計算機の台数や，また取得するログの出力傾向が環境に応じて大きく異なることも考えられる．その際には，時間の最小単位を秒などにしたり，また格子の色の定義を変更したりして調査すべきであるため，実運用環境で用いるために，これらの値をその環境に応じて変更できる機能が必要であると考えられる．

6.2 視覚化手法に関する課題

本システムでは，時刻を基にしたログの絞り込みについては支援されていると考えている．しかし，特徴情報を基にその関連によってログを調査したい場合や，調査する環境やログによっては分や秒で時刻の絞り込みを行っても出力が多く調査しにくい場合があるため，特徴情報を用いた絞り込みも重要であると考えられる．そのため，選択した特徴情報によって色などを用いて，徐々に条件を細かくしていくことができる機能も必要であると思われる．

また，調査において，システムの正常時のログの出力状況を知っていれば，異常時に対する状況認識を容易にできると考えられる．このため時系列解析などを用い正常時の傾向を表示して，より異常時を際立たせると視覚化を行うことも重要であると考えられる．

また，ディスプレイの解像度に対する課題も存在する．これは詳細情報表示における表示領域を縦分割しており，読み込むログが増えることによって行数が限られるためである．本システムでは現在 1,024 × 768 のウィンドウサイズで読み込むログ数が 8 個を超えると，詳細情報表示での各ログの表示数が 2 行程度となってしまい，非常に比較しにくくなる．これには，注目しているログ以外の詳細情報は小さいフォントサイズで表示するなどにより対応できると考えている．

7. ま と め

本研究では，不正侵入検知における調査を支援することを目的とした複数ログの時系列視覚化システムの構築を行った．本システムでは，ログの時系列に着目した視覚化を行い，また視覚化とその対話的な操作による詳細情報の表示を行うことにより，ログ間の関連や前後関係を意識し，また概要から詳細までの一貫した調査を支援する．そして，本システムによりハニーポットの不正侵入調査において非常に効果的にその作業を行うことができることを確認した．

本システムはセキュリティ管理者にとって有用であると考えており，今後実装を進め，実運用環境などにも適用していきたいと考えている．

参 考 文 献

1) Goodall, J.R.: User Requirements and Design of a Visualization for Intrusion Detection Analysis, *Proc. IEEE SMC Information Assurance Workshop* (*IAW*), New York, IEEE, pp.394–401 (2005).
2) Yin, X., Yurcik, W., Treaster, M., Li, Y. and Lakkaraju, K.: VisFlowConnect: NetFlow Visualizations of Link Relationships for Security Situational Awareness, *Proc. ACM Workshop Visualization and Data Mining for Computer Security* (*VizSEC/DMSEC*), Washington DC, ACM SIGSAC, pp.26–34, ACM Press (2004).
3) 伊藤貴之，高倉弘喜，沢田篤史，小山田耕二：ネットワーク不正侵入監視のための視覚化の一手法，第 9 回分散システム/インターネット運用技術シンポジウム，情報処理学会，pp.63–68 (2004).
4) Lakkaraju, K., Yurcik, W. and Lee, A.J.: NvisionIP: NetFlow Visualizations of System State for Security Situational Awareness, *Proc. ACM Workshop Visualization and Data Mining for Computer Security* (*VizSEC/DMSEC*), Wash-

ington DC, ACM SIGSAC, pp.65–72, ACM Press (2004).
5) McPherson, J., Ma, K.-L., Krystosk, P., Bartoletti, T. and Christensen, M.: PortVis: A Tool for Port-Based Detection of Security Events, *Proc. ACM Workshop Visualization and Data Mining for Computer Security* (*VizSEC/DMSEC*), Washington DC, ACM SIGSAC, pp.73–81, ACM Press (2004).
6) Eick, S.G. and Lucas, P.J.: Displaying trace files, *Software Practice and Experience*, Vol.26, No.4, pp.399–409 (1996).
7) 高田哲司，小池英樹：見えログ：情報視覚化とテキストマイニングを用いたログ情報ブラウザ，情報処理学会論文誌，Vol.41, No.12, pp.3265–3275 (2000).
8) The netfilter/iptables project. http://www.netfilter.org/
9) Roesch, M.: Snort — Lightweight Intrusion Detection for Networks, *Proc. 13th USENIX conference on System administration* (*LISA'99*), Seattle, USENIX, USENIX Association, pp.229–238 (1999).
10) Snort — The de facto standard for intrusion detection/prevention. http://www.snort.org/
11) tcpflow A TCP Flow Recorder. http://www.circlemud.org/~jelson/software/tcpflow/
12) Mackinlay, J.D., Robertson, G.G. and Card, S.K.: The Perspective Wall: Detail and context smoothly integrated, *Proc. SIGCHI conference on Human factors in computing systems: Reaching through technology*, New Orleans, ACM SIGCHI, pp.173–176, ACM Press (1991).
13) Spitzner, L.: *Honeypots: Tracking Hackers*, Addison Wesley (2002). 小池英樹ほか（訳）：Honeypots—ネットワーク・セキュリティのおとりシステム，慶應義塾大学出版会 (2004).
14) The Honeynet Project.: *Know Your Enemy: Learning About Security Threats*, Addison Wesley, 2nd edition (2004). 園田道夫ほか（訳）：ハニーネットプロジェクト—汝の敵を知れ，毎日コミュニケーションズ (2005).
15) The Honeynet Project. http://project.honeynet.org/
16) 澁谷芳洋，小池英樹，高田哲司，安村通晃，石井威望：高対話型おとりシステムの運用経験に関する考察，情報処理学会論文誌，Vol.45, No.8, pp.1921–1930 (2004).

(平成 17 年 7 月 8 日受付)
(平成 18 年 2 月 1 日採録)

江端　真行（学生会員）

2004 年電気通信大学電気通信学部情報工学科卒業．現在，電気通信大学大学院情報システム学研究科情報システム運用学専攻修士課程在学中．情報視覚化の研究に従事．特に情報視覚化，ネットワークセキュリティ，ユビキタスコンピューティングに関心がある．

小池　英樹（正会員）

1991 年東京大学大学院工学系研究科情報工学専攻博士課程修了．工学博士．同年電気通信大学電子情報学科助手．1994 年同大学院情報システム学研究科助教授．現在に至る．1994〜1996 年，1997 年 U.C. Berkeley 客員研究員．2003 年 U. Sydney 客員研究員．情報視覚化の研究に従事．特に視覚化へのフラクタルの応用，Perceptual User Interface，情報セキュリティへの視覚化の応用に興味を持つ．1991 年日本ソフトウェア科学会高橋奨励賞，2000 年情報処理学会 DICOMO 2000 最優秀論文賞，2001 年 IEEE VR2001 Honorable Mention for the Outstanding Paper Award 受賞．ACM，IEEE/CS，日本ソフトウェア科学会各会員．