攻撃の規則性認識を支援する攻撃量時系列変化比較対照表示システム

三鑰達真*, 大野泰宏*, 吉田和幸**
*大分大学工学部, **大分大学総合情報処理センター

近年インターネットが普及し、通信の安全性を確保するため、アクセス制御や各種暗号化技術などが従来の代表的な対策として講じられている。それと同時に、不正侵入を早い段階で検知し、早期に対策を講じることを可能とすることの重要性も高まってきており、ネットワーク侵入検知システム(IDS: Intrusion Detection System)が注目されている。

我々は、snortが検知したアラートをIPアドレスごとにrrdtoolを用いて時系列グラフ化して，不正パケットの監視を行うIDSを作成している。本論文では、このグラフを検知時刻順にソートしてグラフを比較対照することによって、複数の対象に対する攻撃の規則性の認識向上及び攻撃量と端末全体の状況把握の支援を目的とするシステムについて述べる。

A system for Comparing Amount of Attacks in Time Series that Supports Recognition of Regularity of Attacks

Tatsuma Mikagi*, Yasuhiro Ohno *, Kazuyuki Yoshida**
*Department of Computer Science and Intelligent Systems, Oita University
**Information Processing Center, Oita University

Recently, as the Internet spreads, various information is exchanged through the Internet. An access control, various cryptographic technologies, etc. are taken as a typical measures to the safe and secure communication. It is also important to detect an intrusion at an early stage. Intrusion Detection System (IDS) is paid to attention in recent years.

We are developing IDS using Snort and RRDtool. In this paper, we describe this IDS, and the packets we observed that goes into the LAN of Oita University illegally. By sorting the graphs in order of detection time, and comparison contrast of that graphs, it is easy to grasp the attack on two or more objects, and the whole amount of attacks and a whole terminal.describes the system.

1 はじめに

近年、ネットワークに接続された計算機に対する不正アクセスが増加している。その対策としてIDS（ネットワーク不正侵入検知システム：Intrusion Detection System）が注目されてきている。IDSはネットワークトラフィックの監視を行い、インシデント（不正アクセスに関連した事象）を検知した場合にアラート（警告）を発生する。これにより不正アクセス被害の早期発見が可能となる。IDSはシグネチャと呼ばれるあらかじめ登録された不正アクセス手口のデータベースとのパターンマッチングを行い、インシデントを検出する。しかしながら、特に大規模で開放性の高いネットワーク環境においてIDSを実際に運用してみると、以下のような問題点が挙げられることがわかった。

- インシデント1件ごとにアラートを発生しているため、アラートログの量が膨大になる。
- その膨大さゆえに、インシデントを事後分析するためのアラートログデータベースの管理が容易でない。
- 不正アクセスの手口が複雑化した現在、複数のインシデントによって一連の不正アクセスを構成するケースも多く、その全貌や関連性を把握するためには機械的処理だけでは不十分である。
- 従来の探索的なアラートログ閲覧システムでは、重要なインシデントを探索することが難しい。それは運用者の知識に依存しており、多数の管理者間の知識共有に向かない。また閲覧に多大な時間が必要である。

これらの問題点を解決し、より円滑なIDS運用を行うためには、いくつかの方法がある。我々は、「情報の視覚化」を適用した手法を提示した[9]。これはアラートログを視覚的に表示、解析することで、管理者のアラート調査における事後分析の時間を短縮することを目的としている。

本論文では、これまでの研究利点を引き継ぐと共に、事後分析の時間短縮だけでなく、被害状況をより具体的に把握し易いシステムを作成した。

2 システムの設計

本稿ではIDS警告ログの視覚化による警告発生傾向を表現するシステムを提案する。IDSであるsnort[1]はインシデントを検出しアラートとしてログに残すシステムである。そのため、ログを見れば一目で、どのような脅威が発生したのかわかることが望ましい。しかし、現実にはそのログをそのまま閲覧することは難しい。その理由の一つとして、1章でも述べたようにログが膨大な量になることがあげられる。そこで、ログを視覚化することで、管理者が状況を把握しやすくすることが必須となってくる。

ログを視覚化する方法は様々で、個別のアラートの全体での割合や時間単位の量、IPアドレスの地理的把握など、表現は多々ある。そんな中、本研究では攻撃量の時間単位での量を把握しやすい時系列のグラフに着目した。

アラートを認識する際に重要な要素は複数存在する。一つは、時間単位での攻撃量である。これは、攻撃量を時間単位で分けることで、その攻撃の発生日時を分析し、発生傾向を推測するのに適している。また、グラフの内容を把握する際に、単に一つのグラフを表示するよりは比較する対象が存在する方がより把握を行いやすいといえる。

また、攻撃対象となっている端末のIPアドレスも重要である。これは単に攻撃量を把握することと異なり、被害状況を把握する際に最も重要な要素の一つとなる。例えばBACKDOORを検知した際、その検知数を把握することも大事であるが、攻撃対象となっている端末の把握が重要であり、必要ならばその端末のユーザに対して状況の通知を行うことや、対策を講じる必要性が出てくる。また、一つの端末だけではなく、侵入を検知した際に他の端末の状況と比較することも、状況把握の鍵を握るといえる。

そして、作成したグラフをソートして、いかに見やすく、管理者が状況を把握しやすいかである。上記を踏まえ、IPアドレスごとにグラフを作成すると、その数が多くなることで逆に見難くなってしまうという危険性が出てくるので考慮する必要がある。また、従来はグラフを検知した順に並べて表示していたが、複数の端末に対しての規則性の高い攻撃を考慮し、より規則性が認識しやすいように並べる必要がある。

以上のことを踏まえ、従来の視覚化表現の問題点を論じ、その上でIDSに必要なログ視覚化要件について論じる。そして既存のログ情報化システムではどのようになっているのかを説明し、新たに提案するログ視覚化システムについて検証する。

2.1 従来の視覚化表現における問題点

ログ視覚化についての研究は以前から行われており、主に既存のデータ視覚化表現であるグラフによって視覚化が行われている。それは量的な割合や変化を見ることを主たる目的としている表現手法であり、攻撃ごとのグラフを作成し一日や一週間などのスタンスでの攻撃量を時系列に表示するものがある。また、グラフを並べて表示することで、日ごとの攻撃量を表すシステムも存在する。しかし、不正アクセスを検知した際に、その攻撃の対象となっているIPアドレスごとにグラフを作成し、並べて表示するシステムは少ない。つまり、他の攻撃や端末のIPアドレスといった他の要素との比較を行うのに適する表示システムが少ない。仮に同一時刻に複数の端末に対して攻撃があったとすると、管理者に同攻撃の対象となった端末ごとのグラフを比較対照したいというニーズがある場合、従来のシステムではその要求に応えることが出来ない可能性がある。

2.2 既存のログ視覚化システム

既存のログ視覚化システムにおけるログ視覚化要件について説明する。ログ情報の「情報視覚化」という手法について関連が深いシステムやツール、研究については以下のようなものが挙げられる。

- ACID（BASE）[2][3]

snortのログをグラフィカルにブラウジングできるツール。様々な条件でアラートを検索できる。

- BIONS[4]

snortのログをグラフ化し、ブラウジングするツール。

- SnortSnarf[5]

snortのログをHTML化し、一覧するツール。

- Snort ALog[6]

Snortのアラートを解析し、HTML／PDF／Plain Textで出力することができるツール。

- 見えログ[7]

情報視覚化とテキストマイニング技術を用いたログ情報ブラウザ。

- 平安京ビュー[8]

空間的に分布された計算機群に侵入検知データの統計量をマッピングできる。

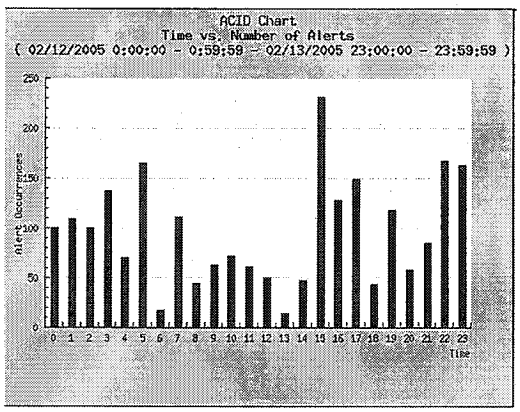

図 1 特定のシグネチャの時間ごとのアラート数：ACID

このようにログ情報の「情報視覚化」に関しては様々な研究がなされている。今回は有名な snort のログの解析、視覚化ツールである ACID（BASE）を元に説明する。ACID では特定のシグネチャの年、月、日、時間ごとのアラート数を表現できる（図 1）。しかしアラート全体の量や個々のシグネイチャにおけるインシデントの傾向は把握できるが、他の要素(攻撃名、IP アドレス等)との比較を時系列で行うことが出来ない。また、シグネチャごとのアラート数や、始め及び最後のアラート発生時間の一覧表示などの機能を備えている(図 2)。インシデントの質的表現や量的表現は得られるが、時系列に沿った表現は表されていない。

ACID（BASE）は一つずつシグネチャを特定することにより時系列ごとのアラート発生数が得られる。しかしこれは一つの画面で一つのシグネチャのみ表示すので、複数のパラメータを表示するには複数回画面を切り替えなければならず、すべてのインシデントを調べるには何度もグラフを作成し直さねばならない。そのため作業に非常に手間がかかり、日常で運用するには面倒な作業といえる。つまり、部分的にログ視覚化における要求を満たしてはいるが、管理者の問う回答を得るためにはいくつかのステップを踏む必要があり、時間もかかる。多忙な管理者では手に負えないのである。

3. システムの構築

本研究では検出した攻撃を効果的に視覚化するシステムの構築を行った。本システムの視覚化設計の概要、システムの動作について説明する。本研究で入力データとする IDS のログデータは、IDS である snort が出力する一般的なテキスト形式のログファイルである。検出された 1 回のアラートに対してログファイルに出力されたデータのうち、本システムでは以下のデータを参照する。

- 具体的な不正アクセスの種類を示すメッセージ
- 不正アクセスの snortID
- 受信元 IP アドレス
- 発生時刻
- 危険度を表す優先度レベル

IDS のインシデントの種類数自体は環境に則してシグネチャをメンテナンスすることによって抑えることができる。そこで IDS による警告アラートを種類ごとに各警告発生数の変化をグラフによって表し、一覧するシステムを作成した。それらを調べることで、行われた攻撃の種類、時間、頻度などを容易に比較することができるようになった。また、ターゲットとなっている IP アドレスや、不正パケットを送信してくるホストの IP アドレスごとにグラフを作成し並べて表示することで、攻撃量を比較対照することが可能となり、複数の攻撃対象に対しての一斉攻撃等の状況を把握し易くなった。

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer4 Proto >
#0-(1-3261107)	[snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2006-05-07 07:24:34	64.251.71.68	133.37.8.63	ICMP
#1-(1-3261106)	[arachNIDS] [snort] SCAN FIN	2006-05-07 06:31:29	86.143.201.31:53356	133.37.204.45:1591	TCP
#2-(1-3261105)	[arachNIDS] [snort] SCAN FIN	2006-05-07 06:31:29	86.143.201.31:53356	133.37.204.45:1591	TCP
#3-(1-3261104)	[snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2006-05-07 02:17:26	203.81.48.185	133.37.144.96	ICMP
#4-(1-3261103)	[snort] ICMP Destination Unreachable Communication with Destination Network is Administratively Prohibited	2006-05-06 22:03:45	62.36.214.22	133.37.144.141	ICMP
#5-(1-3261102)	[snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2006-05-06 19:23:10	129.132.235.48	133.37.204.13	ICMP
#6-(1-3261101)	[snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2006-05-06 19:22:29	129.132.235.48	133.37.204.13	ICMP
#7-(1-3261100)	[snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2006-05-06 19:15:40	63.247.74.2	133.37.204.123	ICMP
#8-(1-3261099)	[snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2006-05-06 19:15:15	129.132.235.48	133.37.204.13	ICMP
#9-(1-3261098)	[McAfee] [snort] BACKDOOR typot trojan traffic	2006-05-06 12:51:06	38.31.213.115:3076	133.37.8.54:65221	TCP
#10-(1-3261097)	[snort] ICMP Destination Unreachable Communication with Destination Network is Administratively Prohibited	2006-05-06 12:09:31	62.36.214.17	133.37.144.237	ICMP
#11-(1-3261096)	[McAfee] [snort] BACKDOOR typot trojan traffic	2006-05-06 11:48:52	125.114.15.20:4849	133.37.145.197:34144	TCP
#12-(1-3261095)	[McAfee] [snort] BACKDOOR typot trojan traffic	2006-05-06 06:39:11	7.231.106.40:37314	133.37.146.165:582	TCP

図 2 シグネチャの一覧表示：ACID

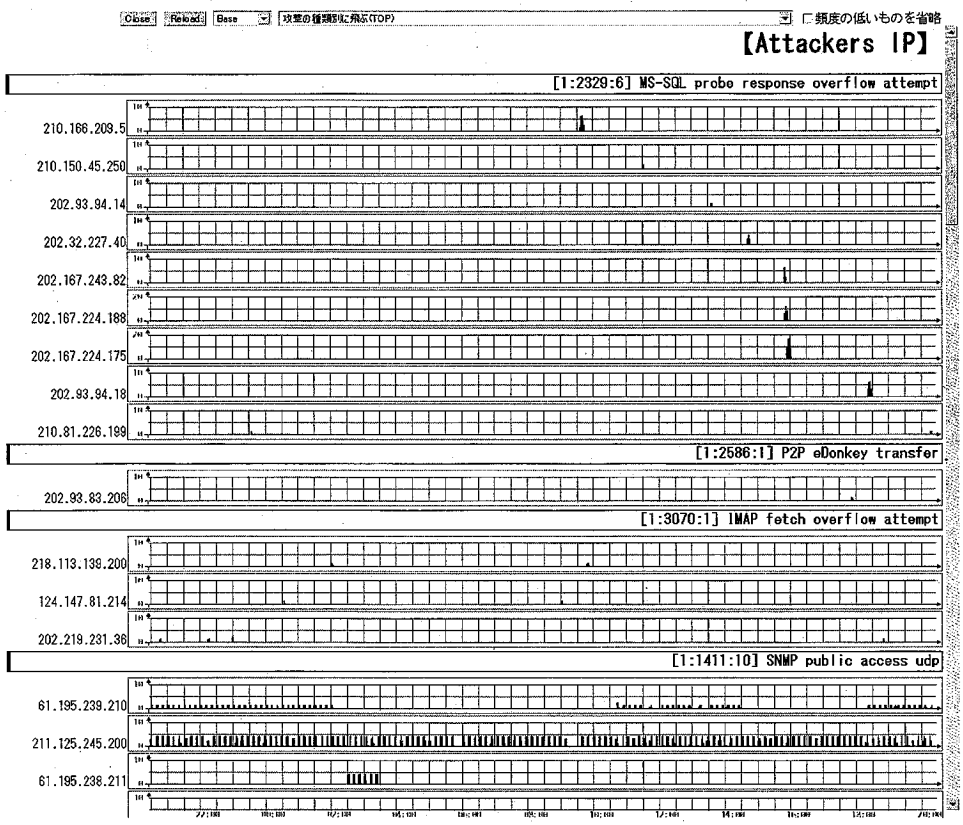

図3 提案する視覚化モデル

グラフ作成においては RRDtool(Round Robin Database Tool) [10]を用いた。RRDtool とはデータベースを定義し、アップロードすることで値を記録し、そのデータベースの内容を描画することで時系列のグラフを作成するツールである。ログ視覚化システムの問題点の一つにログの膨大さがあり、ログの処理をいかに効率よく行うかという問題が存在する。それは、膨大なログをもとにリクエストがあるたびにグラフを作成していては反応速度が遅くなるからだ。例えば ACID(BASE)は様々な要求に対応したために、反応速度に問題がある。

そこで、以上の点を考慮したシステムの作成を行った。システムは C 言語を用いて作成した。Snort のアラートを抽出後、RRDtool に渡してグラフを作成し、ソートした後に加工を施し、グラフの中にある不要な部分を切り取ることで縦の長さを短縮し、グラフを並べて HTML 形式で表示するプログラムを crontab により定期的に実行することでこのシステムを実現している。定期的に実行することで、リアルタイムでの処理は出来ないが、ページを定期的に作成するのでリクエストに対しての反応が比較的早く行えるという利点がある。

4 視覚化方法の構築

2.2 で述べた要求を踏まえ、攻撃対象となっている端末の IP アドレスとそのアラート名及び ID を示したグラフを並べ、比較対照を行えるログの視覚化システム[11]を作成した。次に、図 3 の各行における視覚化方法について述べる。前回までのシステムのグラフ(図 4)と新たに作成中のシステムのグラフ(図 5)に図 3 の各行における表示例を示す。前回までのシステムは、従来のシステムの表示に対し、攻撃 ID、危険度、攻撃対象及びホスト側の IP アドレスとポート番号などの、重要と位置づけた要素を盛り込んだグラフを表示するものであった。それにより、単に時間単位の攻撃量だけでなく攻撃対象となっている端末の状況や、複数の端末の状況及び、その攻撃パターンを認識し、把握する上で非常に有効であると思われたが、IP アドレスと攻撃名ごとに作成したグラフを縦に並べて表示するというこのシステムでは、アラートが沢山生成されるにつれてグラフの数も多くなるという観点から、見易さを保ちつつもサイズの縮小をする必要性を痛感した。また、snort の生成するアラートをもとに RRD を生成し、攻撃名ごとにソートするという前回のシステムでは、規則性の

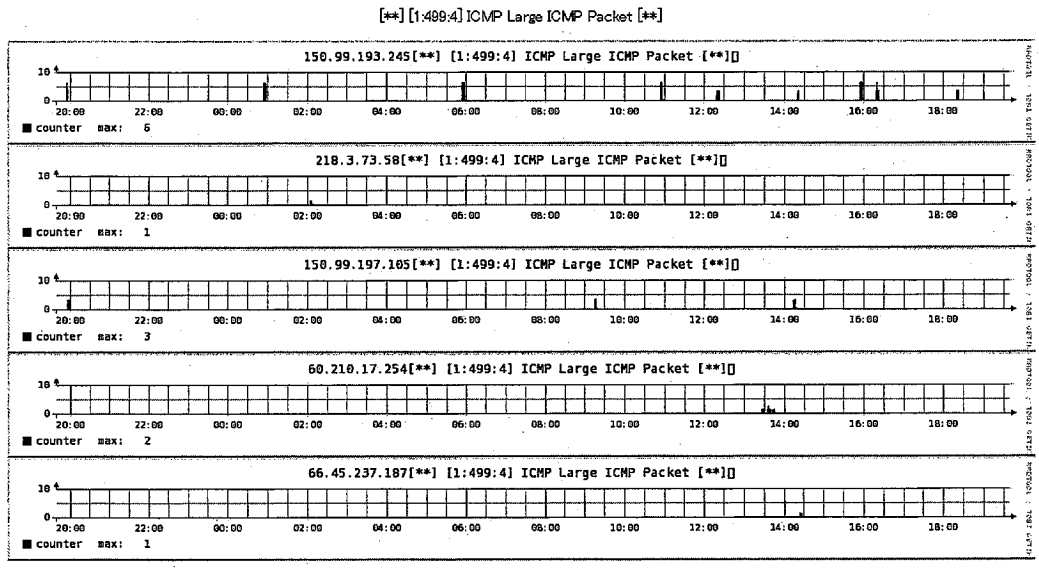

図4　前回までのシステムのグラフの表示例

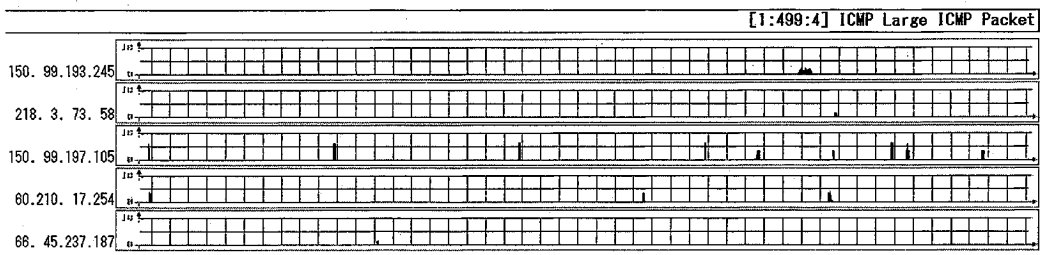

図5　新たに作成中のシステムのグラフの表示例

高い不正通信のパターンを認識するという上ではグラフの並び方が不十分さを痛感した。

以上の点に留意し、システムの改良を行っている。縦にグラフを並べることが最大の特徴であるこのシステムで、グラフ作成に用いている RRDtool のグラフをオリジナルのまま使用するとグラフに不要な領域も存在し、並べることに適していないため、加工を施している。このことによりサイズは約 1/6 に、縦のサイズも半分以下となり、SXGA の画面で表示出来るグラフの数は従来のシステムの数の 2.5 倍の約 23 個を表示できるようになった。このことから、比較対照を行う上で、前回以上に有効なシステムになったと思われる。

5 システムの運用と評価

本システムの運用にあたり,攻撃量を比較対照する上で,ネックとなってくるのが IP アドレスとポート番号,そして攻撃名を 1 セットにグラフを作成するが故のグラフの数の多さであった。それは、比較対照を行う上で攻撃対象となっている IP が多ければ多い程,縦に並ぶグラフの数が多くなってしまう。故に、グラフの見易さを維持しつつ加工することで、一画面中に表示できるグラフの多さを 2 倍以上にすることが可能となった。また、複数の攻撃対象に対しての不正パケットの送信方法には、何らかの規則性があるという見解から、グラフを同じ攻撃において検知時刻の若い順にソートするようにした。現段階では、同じアラートに対し、検知時刻の 24 時間前から若い順にソートすることで、パターンを見出すようにしている。これは、大量のアラートが発生した場合に、各 IP アドレスに対して単発的な攻撃が多いことからこの考えに至った。通常は、規則性の高い攻撃はなかなかあるものではないが、不正パケットを複数の端末に対して単発的に送ってくる場合、何らかの規則性がある場合が多い。特に、このシステムはグラフを並べて表示するものであるので、そのパターンを視認しやすいという特徴を持っているのである。図 6 に示すように、BACKDOOR のパケットを複数の端末に対し、単発的に送信してきていることが伺える。よって、攻撃には規則性が存在するものもあり、これを的確に管理者に対して表示できれば,管理者の負担軽減につながると思われる。そして、

その攻撃パターンの認識を自動化することが本研究の最終目的であり、今後の課題としたい。また、グラフが大量にある場合に、ユーザ側で表示するグラフを任意に選択できるシステムを現在検討中である。

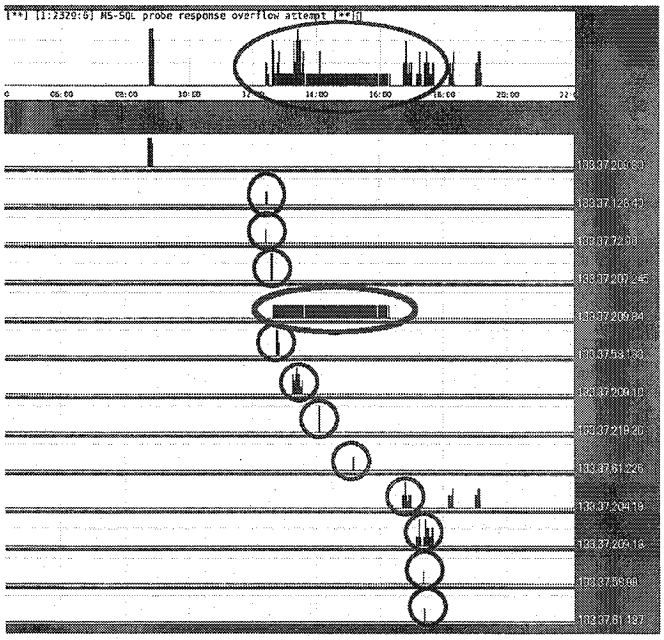

図 6 規則性の高い検知例

6. おわりに

本システムは snort のログを視覚化するだけでなく、危険度の同じ攻撃に対して比較対照を行うこともでき、管理者が不正侵入に対し対策を講じることが出来るよう具体的な要素(IP アドレスやポート番号)も表示することで、管理者が状況を把握しやすいシステムを目指している。

ログの視覚化において重要なことは、その視認性の高さである。一画面中に表示できるグラフの数と一つ一つのグラフの見易さはトレードオフの関係にある。RRDTOOL によるグラフ化に伴う制約は加工することで改善できた。それに攻撃パターンの認識生の向上ソートしてゆく機能とあわせれば、より状況を把握しやすくし、かつ管理者の負担を軽減できるものとなると思われる。

参考文献

[1] snort.org：snort
http://www.snort.org/
[2] Roman Danyliw：
Analysis Console for Intrusion Databases：ACID
http://acidlab.sourceforge.net/
[3] Basic Analysis and Security Engine project：BASE
http://secureideas.sourceforge.net/
[4] Ryo Nakano：
BIONS －believe it or not , snort－
http://bions.ryonkn.com/
[5]Silicon Defense：
SnortSnarf
http://www.snort.org/dl/contrib/data_analysis/snortsnarf/
[6] the Free Software Foundation, Inc.：
Snort ALog －Snort Analyser Logs－
http://jeremy.chartier.free.fr/snortalog/
[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解析支援システム, 情報処理学会論文誌 Vol.41, No.12, pp.3265-3275, (2000).
[8] 伊藤貴之,高倉弘喜,沢田篤史,小山田耕治:ネットワーク不正侵入監視のための一手法, 分散システム/インターネット運用技術シンポジウム 2004 年度論文集、情報処理学会シンポジウムシリーズ IPSJ Symposium Series Vol.2004,No.16 、pp.63-68(2004).
[9] 三原慎仁, 宮部博行, 吉田和幸, 不正侵入検知システム snort の警告ログの視覚化について, マルチメディア, 分散, 協調とモバイル(DICOMO 2005)シンポジウム論文集、情報処理学会シンポジウムシリーズ IPSJ Symposium Series,Vol.2005,No.6,pp.477-480(2005).
[10] Tobi Oetiker：RRDtool
http://people.ee.ethz.ch/~oetiker/webtools
[11] 三鑰達真, 三原慎仁, 吉田和幸, 攻撃量時系列変化の比較対照表示システムとその使用経験, マルチメディア分散, 協調とモバイル(DICOMO 2006)シンポジウム論文集、情報処理学会シンポジウムシリーズ IPSJ Symposium Series,Vol.2005,No.6,pp.901-904(2006)