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

2005－DPS－122 (16)
2005－CSEC－ 28 (16)
2005／3／22

ネットワーク間プロファイル比較による攻撃異常検知

竹森 敬祐† 三宅 優† 田中 俊昭†

† (株) KDDI 研究所 〒356-8502 埼玉県上福岡市大原 2-1-15

E-mail: † {ke-takemori, yu-miyake, tl-tanaka}@kddi.com

あらまし 昨今，各地のネットワークに攻撃監視用のプローブを設置して，そこから出力されるログを統合解析するセキュリティ監視センタの構築が進められている．セキュリティ監視センタでは，収集されたログの時間的な頻度の変動に注目した解析を行なっており，個々のネットワークの異常を把握することができる．しかしながら，異なる規模のネットワークのログを定量的に比較する手法がないために，検知された異常が他のネットワークのログと比べてどの程度偏っているのか把握するに至っていない．そこで本研究では，個々のネットワークの長期的な頻度を基準に正規化することで，ネットワーク間の攻撃の偏りの程度を定量的に算出する手法を提案する．インターネット上に設置したプローブのログを用いて評価を行い，正規化処理によって誤検知を抑えつつ適切な検知を達成していることを確認する．

キーワード セキュリティ監視センタ，ログ解析，正規化，ネットワークプロファイル

An Anomaly Detection Technique using Network Profiles

Keisuke TAKEMORI† Yutaka MIYAKE† Toshiaki TANAKA†

† KDDI R&D Laboratories Inc. 2-1-15 Ohara, Kamifukuoka-shi, Saitama, 356-8502 Japan

E-mail: † {ke-takemori, yu-miyake, tl-tanaka}@kddi.com

Abstract Recently, a security operation center (SOC) is established against network attacks, which monitors global area networks. Based on computing techniques of time-axis, the SOC evaluates a deviation of mean attack ratio of overall networks, and detects anomaly events. However, there are no comparing techniques of the attack ratio on a space-axis (network-axis). It is hard to evaluate the deviation of mean attack ratio on each network. In this research, we propose a standardizing technique of the mean attack ratio considering with a trend of the network profile. Experimental results with some real audit data show that the objective alarms effect with more reliable response for SOC operators.

Keyword Security Operation Center, Log Analyzer, Standardizing Technique, Network Profile

1. はじめに

近年，サイバーテロに関する脅威が高まる中，ネットワークシステムに対する攻撃を監視するセキュリティ監視センタ（SOC: Security Operation Center）の構築が進められている[1]-[3]．SOC では，各地のネットワークに設置した攻撃監視用のプローブから出力されるログの頻度に注目して，時間軸上での平均値からの乖離を評価することで，個々のネットワークもしくは全てのネットワークを纏めた単位で異常を監視しており[4]，ネットワークの安定運用に支障を及ぼす DDoS（Distributed Denial of Service）攻撃や未知ウィルスの拡大など，ネットワーク運用者が連携して対応するための情報源として期待されている．

ここで，攻撃頻度の規模や影響の範囲を的確に把握するためには，時間軸上での評価のみならず，空間軸（ネットワーク軸）上での偏りの程度を把握する必要がある．これまで攻撃の空間的な拡がりを評価するために，ログの視覚化システムに関する研究が行われてきた[5]．また，攻撃トラヒックの流れを追跡するためにトラヒックの相関分析に関する研究がなされてきた[6]．しかし，異なる特徴を持つネットワーク間のログを定量的に比較することは難しく，ログの正規化手法が必要とされている．

そこで本研究では，個々のネットワークの長期的なログの頻度を基準に正規化することで，ネットワーク間の攻撃の偏りの程度を定量的に評価する手法を提案する．その際，ネットワークが提供しているサービスに依存しない比較を行なうために，各々のネットワークに特徴的なログを除外する．提案手法について，インターネット上に設置した8つのプローブのログを用いて評価を行い，異常な偏りについて，誤検知を抑えつつ確実に検出できることを示す．また，擬似的な未知ウィルスの感染を模擬した実験を行い，攻撃の拡がりを推定できることを確認する．

以下2章において，SOCで用いられる広域モニタリングシステムの機能について説明し，3章でその課題をまとめる．4章でログの正規化手法と攻撃範囲の特定手法について提案し，5章で，実運用されているIDSログを用いて妥当性を評価する．そして最後に6章でまとめる．

2. 広域モニタリングシステム

ここでは，ISP（Internet Service Provider）をまたがる広域ネットワークに設置したプローブからのログを統合管理して，ネットワークの安定運用に支障を及ぼす多量の攻撃を監視するシステムについて説明する．図1に，システムモデルを示す．

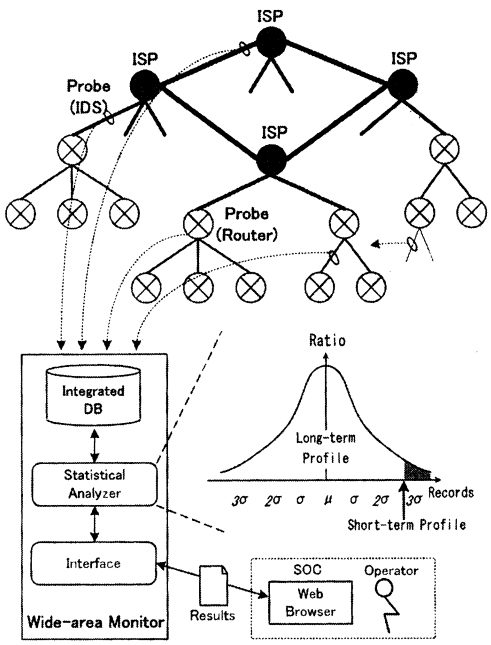

図1. 広域モニタリングシステム

プローブは，ISP間を接続する基幹回線や末端ネットワークを繋ぐ回線など，速度やIP規模がまちまちなポイントに設置される．このプローブには，Routerなどのトラヒック制御機器やIDS（Intrusion Detection System）やFirewallなどのセキュリティ機器が該当し，それぞれトラヒックログやセキュリティログを出力する[7][8]．SOCでは多量に出力される各種ログを効率的に解析するために，単位時間ごとの統計値に注目した解析を行なう．この統計パラメータの例を表1に示す．統計値として10分毎や1時間毎のトラヒック量の平均値や攻撃イベント数が該当する．SOCでは，この統計値に対して，ネットワークごとの時間軸上での偏差を解析し，SOC運用者にWebブラウザやメールを通じて異常を通知する．

表1. 異常検知のための統計パラメータ

パラメータ種別	トラヒックログ	セキュリティログ
トラヒック量(bps)	○	-
パケット数(pps)	○	-
パケットサイズ(～64, 128:～256, ～512, ～1024, ～1512)	○	-
ICMP, TCP, UDP, Other	○	-
ICMP-Unreachable, TCP-RST, UDP-Unreachable	○	○
Source IP, Destination IP	○	○
TCP Port, UDP Port	○	○
攻撃イベント	-	○

3. 解析における課題

ここでは，ログの異常検知に関する従来研究とISPが連携するための多地点監視における要件を整理する．

3.1. 既存の異常解析

これまで，攻撃頻度の時間軸上での偏差に注目した異常検知に関する研究が行なわれてきた[4]．これは，個々のネットワークにおける攻撃頻度の推移を定量的に評価することができ，ネットワーク単位での異常検知に適している．

3.2. 問題点

SOCの運用者は，検知された異常な攻撃について，他のネットワークの状況と比較したい．

しかしながら，個々のネットワークから出力されるログの頻度は，設置されているネットワークのIP規模や提供されている通信サービスによってまちまちである．特に，Webサービスや FTPサービスなど，アクセスが集中するサー

ビスが提供されている場合，そのサービスへのトラヒックや攻撃ログも集中するため，単純にネットワーク間の攻撃数を比較することはできない．異なる組織を横断的に監視するSOCでは，各地のプローブの配下で提供されているサービスや，割り当てられているIP規模を把握する手段はなく，プローブから出力されるログを正規化する手段がない．このため，全てのプローブのログを総合した頻度に注目することになるが，この場合，隠れた異常や攻撃拡大の様子を把握することができない．

3.3. 要件

以上の検討から，ネットワーク間の特徴比較を行なうための要件を纏める．

要件1) 提供サービスによる影響を排除できること

要件2) 異なるIP規模のネットワークのログを正規化できること

要件3) 相対比較で異常な攻撃頻度のネットワークを検出できること

要件4) 隠れた異常や攻撃拡散の程度を把握できること

4. ネットワーク間比較手法の提案

ここでは，提供しているサービスの影響を排除しつつ異なる規模のログを定量的に比較する手法について提案する．以下，説明の簡素化のために，攻撃イベント数に注目して説明する．

図2に，提供サービスの影響をフィルタリングした後に，攻撃頻度による正規化を行い，ネットワーク間を比較することで異常検知する処理の流れを示す．

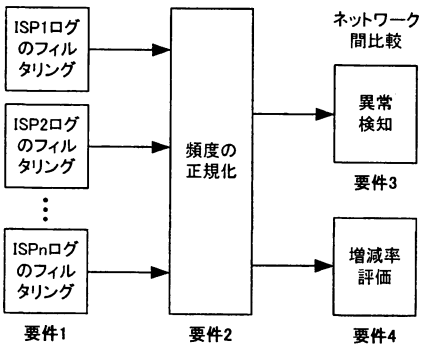

図2. ネットワーク間比較のための処理手順

4.1. TOP-Mイベントのフィルタリング

ここでは要件1を考慮して，提供しているサービスにより発生する攻撃イベントの偏りを排除する手法を提案する．

例えば，Webサービスが提供されているサイトの手前にプローブを設置した場合，Webサービス関連の攻撃イベントが頻繁に検知される．勿論，Webサービスに関する基本的なパッチやセキュリティ対策は図られているはずで，SOC運用者は日頃から頻繁に検知され続けている冗長な攻撃イベントに対して，特に注意を払う必要はない．このようなプローブからのログを他のプローブと比較するためには，過去の長期間における頻度が高い特有の攻撃イベントを排除した攻撃イベント数を比較することが有効である．そこで，ある時点のログを比較する場合，過去の出力頻度の高い上位 M 個分の攻撃イベントを排除した残りの攻撃イベントの総和に対して正規化を行なうことにする．

4.2. 攻撃頻度の長期的傾向からの正規化

ここでは要件2を考慮して，プローブが設置されているネットワーク規模やIPの利用密度によってばらつきが生じる攻撃イベント数の正規化手法を提案する．

例として，図3にN個のプローブから出力される攻撃イベント数の時間的な推移を○印の大きさで表した様子を示す．横軸をプローブ番号として，縦軸を単位時間（タイムスロット）の経過を表わしており，1番目のプローブは定常的に大きな頻度であり，N番目のプローブは定常的に小さな頻度となっている．

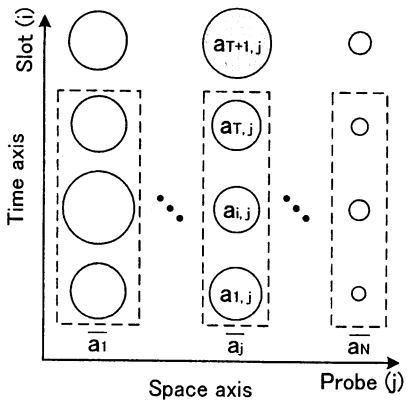

図3. 時間軸と空間軸におけるログの頻度

時間軸上でのi番目のタイムスロットにおける空間軸上でのj番目のプローブから出力される攻撃イベント数を $a_{i,j}$ と表すことにする．プローブがN個，タイムスロットがT個あるとき，j番目のプローブの攻撃イベント数の平均値と，N個全てのプローブの平均値は，

$$\overline{a_j} = \frac{1}{T}\sum_{i=1}^{T} a_{i,j} \qquad (1)$$

$$\overline{A} = \frac{1}{T}\frac{1}{N}\sum_{i=1}^{T}\sum_{j=1}^{N} a_{i,j} \qquad (2)$$

と表される．これより，j 番目のプローブの T+1 番目のタイムスロットのログを，同じ T+1 番目のタイムスロットにおける他のプローブのログと比較する場合，(3)式のように正規化できる．

$$\frac{\overline{A}}{\overline{a_j}} \cdot a_{T+1,j} \qquad (3)$$

この正規化手法では，j 番目のプローブの攻撃イベント数の平均値が他のプローブに比べて大きな場合，(3)式の分母が大きくなり，T+1 番目のタイムスロットの攻撃イベント数は小さく評価される．反対に，他のプローブに比べて小さな場合，(3)式の分母が小さくなり，T+1 番目のタイムスロットの攻撃イベント数は大きく評価される．

4.3. 異常検知

ここでは要件 3 を考慮して，ネットワーク間の比較により異常な頻度のプローブを抽出する手法を提案する．

個々のプローブから出力されるログについて，4.2 節の正規化後の頻度が正規分布に従うものと仮定して，その平均値と標準偏差を用いて信頼区間から外れる場合を異常と判定する．例えば，上側 95%信頼区間から外れる頻度の攻撃イベントが検知されたネットワークを異常と判定する．

4.4. 攻撃拡散の状況把握

ここでは要件 4 を考慮して，攻撃の拡散の状況を把握する手法を提案する．

例えば，j 番目のプローブが監視するネットワーク内のホストに対して活発な攻撃が検知された場合，$a_{T+1,j}$ の値が集中的に大きくなる．未知のウィルスが発生して各地のネットワークのホストに感染が拡大した場合，SOC で統合管理されるログの総量 A_{T+1} が大きくなる．攻撃の増減率を相互比較することで，拡散の程度を把握する手法について検討する．

ここでウィルスの中には，10 分程度でインターネット全体に拡散するものや数時間掛かるものがある．拡散の状況を把握するには，複数タイムスロットに及び検知される攻撃イベント数でネットワーク間比較を行う必要がある．そこで比較対象のタイムスロット長を L としたとき，プローブ j のタイムスロット T 個分の攻撃イベント数の平均値に対して，タイムスロット T+1 から T+L 番目の平均値の増減率 $g_{T+1\sim L,j}$ は，

$$g_{T+1\sim L,j} = \frac{\frac{1}{L}\sum_{k=1}^{L} a_{T+k,j}}{\overline{a_j}} \qquad (4)$$

と表される．同様に，SOC で統合管理される総攻撃イベント数の増減率 $G_{T+1\sim L}$ は，

$$G_{T+1\sim L} = \frac{\frac{1}{L}\sum_{k=1}^{L} A_{T+k}}{\overline{A}} \qquad (5)$$

となる．これより，総攻撃イベント数の増減率に対する j 番目のプローブの相対増減率 r_j は，

$$r_j = \frac{g_{T+1\sim L,j}}{G_{T+1\sim L}} \qquad (6)$$

と表される．

【r_j<1.0 の場合】

他のプローブの平均増減率より低く，ウィルス感染や DDoS 攻撃などの集中的な攻撃は，発生していない．

【$r_j \fallingdotseq 1.0$ の場合】

SOC が監視する広域ネットワークの平均的な攻撃イベントの増減率と同じ程度であり，プローブ j で検知されている攻撃は，広くインターネット上で拡散している攻撃である．

【$r_j >> 1.0$ の場合】

SOC が監視する広域ネットワークの平均的な攻撃イベントの増減率に対して大きく増加しており，j 番目のネットワーク上で集中的な攻撃が発生している．

5. 評価

ここでは，インターネット上に設置したプローブを用いて，正規化手法の妥当性と攻撃範囲を特定する手法の有効性を確認する．

5.1. 評価環境

8 社の ISP からドメインを取得して，それぞれ 4 つのグローバル IP へアクセスしてくる通信情報を収集した(以下，ISP1 から ISP8 と表す)．この 4 つの IP アドレスにはホストを設置しておらず，ここへのアクセスを探索や攻撃を目的とした通信とみなす．ウィルスや攻撃ツールの中には，ICMP Echo Request パケット送信して，ホ

ストの存在を確認した後に攻撃を仕掛けてくるものや，TCP の 3Way ハンドシェイクを確立した後に攻撃を仕掛けてくるものが多い．そこで我々は，ICMP Echo Request に対して ICMP Echo Reply パケットを返信する機能と，TCP-SYN パケットに対して TCP-SYNACK パケットを返信する機能を持った，未割り当て IP アドレス用のおとりプローブを設置して，ICMP，TCP，UDP アクセスに関する情報を収集した．

5.2. ネットワーク間比較による異常検知

8 箇所のプローブから 2005 年 2 月 1 日と 2 月 6 日に収集したログについて，タイムスロット長を 1 時間，長期間のタイムスロット T を 1 日としたものを検証用ログとして用いる．図 4 に，左斜め方向を時間軸に，右斜め方向を空間軸に，縦軸を攻撃イベント数として表すインタフェースを示す．図 4-a は 2 月 1 日のログの推移であり，ISP 1 に注目すると小さな頻度のイベントが出力され続けている中，22 時台に小さなピークが観測されている．図 4-b は 2 月 6 日のログ頻度の推移であり，12 時台に ISP 5 において集中的な攻撃が検知されているが，11 時台までは安定した数のログが出力されている．よって，下記の 3 つのタイムスロットにおいてネットワーク間の比較を行い，ISP1 と ISP5 で異常と判定される場合を正しい検知とみなすことにする．

- ﾀｲﾑｽﾛｯﾄⅰ） 2 月 1 日 22 時台　異常 ISP1
- ﾀｲﾑｽﾛｯﾄⅱ） 2 月 6 日 11 時台　異常なし
- ﾀｲﾑｽﾛｯﾄⅲ） 2 月 6 日 12 時台　異常 ISP5

表 2 に，ISP1 から ISP8 の正規化前後の攻撃イベント数を示す．ここでは，各 ISP で特にサービスを提供していないため，4.1 節のフィルタリングは実施していない．灰色で塗られている枠は上側 95%信頼区間を超えて異常と判定された箇所を表している．

図 4 や表 2 より，ISP1 から ISP8 までは監視 IP 規模が等しいにも関わらず攻撃頻度にばらつきがある．ISP の初めの 1 バイトアドレスは，60., 61., 202., 210.を取得しているが，同じ 60. の ISP 間や 210.の ISP 間で攻撃頻度特性は異なる．各 ISP の IP アドレスの割り当て密度が，攻撃頻度特性に影響しているものと考えられ，同一規模のネットワークを監視する場合でも正規化が必要になることがわかる．

表 2 より，ﾀｲﾑｽﾛｯﾄⅰ)でネットワーク間の比較を実施した場合，正規化前では常に頻度の高い ISP 7 が異常と判定されており，正規化後は

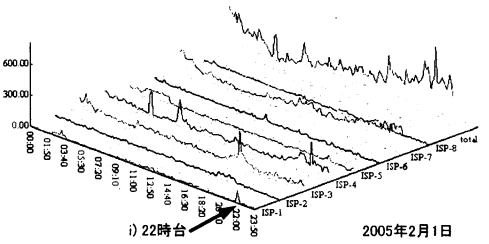

図 4-a. 時間軸と空間軸表示(2005 年 2 月 1 日)

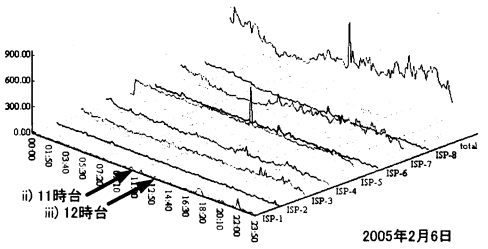

図 4-b. 時間軸と空間軸表示(2005 年 2 月 6 日)

表 2. 正規化前後の攻撃イベント数

ISP番号 先頭IP	i) 1日22時		ii) 6日11時		iii) 6日12時	
	正規化前	正規化後	正規化前	正規化後	正規化前	正規化後
ISP 1 210.b.c.d	未226	正781	61	298	49	236
ISP 2 60.b.c.d	75	158	70	370	41	217
ISP 3 61.b.c.d	340	269	330	301	312	304
ISP 4 210.b.c.d	980	617	273	234	119	101
ISP 5 202.b.c.d	175	263	誤1107	603	正1569	正803
ISP 6 61.b.c.d	17	57	41	89	89	209
ISP 7 60.b.c.d	誤1395	448	誤880	366	951	395
ISP 8 61.b.c.d	70	235	82	128	79	129
平均	410	353	356	299	401	299
標準偏差	471	228	386	150	525	209
上側95% 信頼区間 (閾値)	1186	729	669	620	1268	644

ISP 1 のパルス的な頻度が異常と判定されている．よって，正規化前の ISP 7 は誤検知，ISP 1 は未検知，正規化後の ISP 1 は正しい検知と言える．ﾀｲﾑｽﾛｯﾄⅱ)では，正規化前に ISP 5 と ISP 7 で誤検知が発生しており，正規化後は特に異常と判定される ISP はなかった．ﾀｲﾑｽﾛｯﾄⅲ)では，正規化前と正規化後の両方ともに正しく検知できている．よって，ネットワーク間の攻撃頻度を比較するための提案した正規化手法の妥当性を確認できた．

5.3. 隠れた異常と拡散状況の把握の評価

5.2 節では，単独のネットワークに発生した異常に注目して評価を行なった．本節では，さらに未知のウィルスが拡大する様子を模擬した攻撃データを加えて，隠れた異常の抽出と，拡散する攻撃の把握について評価する．単独ネットワークの異常としてﾀｲﾑｽﾛｯﾄiii)に注目する．拡大する攻撃として 2 月 17 日 14 時台に 8 箇所のネットワークに対してそれぞれ 1000 回の TCP アクセスを行った．この様子を図 5 に示す．- ﾀｲﾑｽﾛｯﾄiv) 2 月 17 日 14 時台 異常 ISP 全て ﾀｲﾑｽﾛｯﾄiii)とﾀｲﾑｽﾛｯﾄiv)の単独増減率(4)式の結果と相対増減率(5)式の結果を，表 3 に示す．ここで，(4)(5)式の"L"は，"L=1"とする．

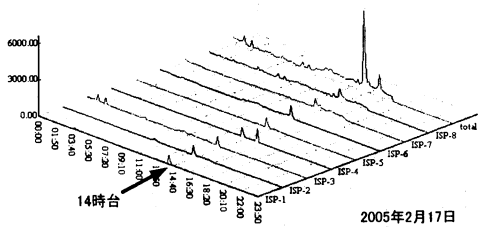

図 5. 時間軸と空間軸表示(2005 年 2 月 17 日)

表 3. 攻撃イベント数の増減率

	iii) 6日12時		iv) 17日14時	
	単体増減率(4)式	相対増減率(5)式	単体増減率(4)式	相対増減率(5)式
ISP 1	0.7	0.6	12.0	3.4
ISP 2	0.7	0.5	10.7	3.1
ISP 3	0.9	0.8	2.7	0.8
ISP 4	0.3	0.3	5.0	1.4
ISP 5	2.5	2.0	16.2	4.6
ISP 6	0.6	0.5	2.1	0.6
ISP 7	1.2	1.0	2.5	0.7
ISP 8	0.4	0.3	3.1	0.9
平均	1.2	1.0	3.5	1.0

表 3 のﾀｲﾑｽﾛｯﾄiii)に注目すると，全体の頻度が 1.2 倍に増加している中，個々のネットワークの単体増減率に分離すると，ISP5 が 2.5 倍，ISP7 が 1.2 倍に増加し，特に相対増減率に注目すると ISP5 のみが 2.0 倍になっており，総合頻度の増減では捉え難い異常が，個々のネットワークに分離すると異常な箇所を抽出し易くなる様子がわかる．

次にﾀｲﾑｽﾛｯﾄiv)に注目すると，全てのネットワークの単体増減率が増加しており，広く攻撃が拡大している様子がわかる．また，ISP3, ISP6～ISP8 では，単体増減率が 2 倍以上に増加しているにも関らず，相対的増減率は減少しており，周囲のネットワークでさらに大きな異常が発生している広く拡散した攻撃である様子を把握できる．今回は，通常時の攻撃頻度を考慮することなく同じ 1000 回のアクセスを実施しているため，増減率が ISP ごとに異なっている．

6. おわりに

本研究では，各ネットワークで検知された攻撃頻度の程度を他のネットワークと比較するために，ネットワークごとの長期的なログの頻度を基に正規化を行い，その値から異常を判定する手法を提案した．インターネット上で収集されたログを用いて評価を行なった結果，誤検知を低く抑えて，的確に異常を抽出できることを確認した．総合的な攻撃頻度を個々のネットワークの頻度に分離することで，発見し難い隠れた異常を検出できること，攻撃の拡散の状況を把握できることがわかった．今後の課題として，さらに広くプローブを設置して評価用ログを収集する．また，特有の攻撃イベントをフィルタリングする手法の有効性についても確認する．

謝　辞

本研究は，独立行政法人情報通信研究機構（NICT）から「広域モニタリングシステムに関する基盤技術の研究開発」の成果である．ここに深謝する．

文　献

[1] Internet Storm Center, http://isc.incident.org/

[2] インターネット定点観測システム(ISDAS), JPCERT/CC, http://www.jpcert.or.jp/isdas/

[3] 戸田洋三, 松本直人, 宮川雄一, "ISDAS: Internet Scan Data Acquisition System", 情処, ｺﾝﾋﾟｭｰﾀｾｷｭﾘﾃｨｼﾝﾎﾟｼﾞｳﾑ（CSS2004), pp.199-203, 2004 年 10 月.

[4] 竹森敬祐, 三宅優, 中尾康二, 菅谷史昭, 笹瀬巌, "Security Operation Center のための IDS ログ解析支援システム", 信学, 論文誌, Vol.J87-A, No.6, pp.816-825, 2004 年 6 月.

[5] 大野一広, 小池英樹, "ワームの伝播アルゴリズムを考慮した広域ネットワーク視覚化システムの提案", 情処, ｺﾝﾋﾟｭｰﾀｾｷｭﾘﾃｨｼﾝﾎﾟｼﾞｳﾑ（CSS2004), pp.187-192, 2004 年 10 月.

[6] 佐藤徹, 和泉勇治, 根元義章, "独立成分分析を用いたトラヒックパターン解析による DoS 攻撃経路追跡手法の提案", 信学, 技報, NS2004-101, pp.1-6, 2004 年 9 月.

[7] sFlow, http://www.sflow.org/

[8] Snort, http://www.snort.org/