2007－OS－106 (6)
2007／8／3

断片アドレスを用いた分散協調インターネット監視に関する一考察

廣津 登志夫[†1] 福田 健介[†2] 栗原 聡[†3]
明石 修[†4] 菅原 俊治[†5]

インターネットでは常に多量の攻撃性のパケットが流れている。これらを観測・モデル化することは，防御の基盤を構築する際にも非常に重要である。本稿では，分散した複数の小規模ネットワークの協調監視により，効率良く攻撃性情報を収集・モデル化する分散協調型監視アーキテクチャの検討について述べ，収集データの初期的な解析結果について報告する。

A Study on Distributed Cooperative Attack Monitoring using Fragmented Network Addresses

Toshio Hirotsu,[†1] Kensuke Fukuda ,[†2] Osamu Akashi ,[†4]
Satoshi Kurihara [?] and Toshiharu Sugawara [†5]

In the Internet, the illegal attack packets are always falling to our network. It is very important to observe and model the those attacking traffic for constructing the protection system from the attacks. In this paper, we describe the concept of a distributed cooperative monitoring architecture, which collects attacking packets and build the model of them efficiently with the cooperation of distributed small-range of monitoring networks. We also report the result of the preliminary analysis of the collected attack traffic.

1. はじめに

インターネットの急速な拡大に伴い，ネットワークに接続されている計算機の数も急速に増加し，それらの間で交換される電子化された情報量も飛躍的に増大した．そこでは，人間生活に関わる様々な情報が距離を意識することなく交換されるだけでなく，多様な商取引や新しいサービスが提供されるに至っており，インターネットは完全に社会基盤の一部として浸透している．その一方で，機密情報や個人情報など意図しない流出や，サービス提供サイトに対する DDoS 攻撃等によるサービスの停止など問題が生じているのも事実である．これらの情報漏洩の影響は蓄積される情報の種類や量が増えるにつれて大きくなり，また，人間生活のネットワークに対する依存度が増えれば増えるほどサービス不能攻撃等による影響は深刻になり，今後ますます大きな問題となってくるであろう．

このような問題に対処するためにインターネットの機構を根底から変えることは，これだけ広く浸透してしまったことを考えると不可能である．したがって，現在のインターネット環境上もしくは高い親和性を持った形で防御基盤を実現することが重要になってくる．そのためには，インターネット上に流れている攻撃性トラフィックを収集し，それらを解析・モデル化することで，実際に行われている様々な攻撃に対処することが重要である．これまでに幾つかのプロジェクトでインターネット上の定点観測による攻撃性トラフィックの収集が行われている．これらの観測では，「巨大な☆」観測専用のアドレス空間を用意し，そこに到着する攻撃性トラフィックを収集している．しかし，全ての組織が「巨大な」アドレス空間を用意して観測し，その情報を防御に使うことは不可能である．

そこで，各組織が割り当てられたネットワークのアドレス空間のうち一部を用いて攻撃の監視を行い，複数の組織が協調することで全体として広いアドレス空間の監視を実現することが必要になってくる．これにより，実際に利用しているネットワークのアドレス空間 (利用アドレス空間) の隙間に攻撃性トラフィックを監視するアドレス空間 (監視アドレス空間) が滲み

†1 豊橋技術科学大学
Toyohashi University of Technology
†2 国立情報学研究所
National Institute of Informatics
†3 大阪大学
Osaka University
†4 NTT 未来ねっと研究所
NTT Network Innovation Laboratories
†5 早稲田大学
Waseda University

☆ 大きいところでは /8 (16,777,216 アドレス) のところもある

込むように広がった環境を生み出すことができ，攻撃の特性をよく表した情報収集が可能になることが期待される．また，観測した攻撃情報を利用アドレス空間の制御や運用自体にフィードバックし，利用アドレス空間と監視アドレス空間を動的に変えて行くことにより，「監視と利用の連動した」ネットワーク防衛基盤を構築することができる．

本稿では，このような分散協調インターネット監視基盤の構築を目指して現在進めている攻撃性情報の収集やモデル化の方法の検討について述べ，実際の収集データの解析結果を示すことで，目標とする監視機構の効果を示す．

2. インターネット攻撃検知

インターネットにおける攻撃の検知手法は，アクティブ (能動的) なものとパッシブ (受動的) なものに大別される．アクティブな手法の代表例としては Honeypot や Honeynet[1] と呼ばれるシステムが挙げられる．これらのシステムでは，攻撃に対してその攻撃をうけたソフトウェアの挙動を模倣することで，攻撃の詳細な挙動の情報を収集したり攻撃者が送り込もうとした Virus や Worm そのものを捕獲したりすることを目的としている．これらは，攻撃の非常に詳細な情報を収集できるという利点はあるが，一方で攻撃に反応してしまうため backscatter のような攻撃の余波が外部に流れることや，処理の負荷のために多数のネットワークアドレスに対して適用することが難しいという問題がある．

一方，パッシブな手法ではファイアウォールのフィルタで遮断されたトラフックのログや，ホストの存在しないネットワークアドレスに対して到着するパケットを収集し，それらを解析することでインターネット中の攻撃情報の解析を行う．前者の例としては，JPCERT/CC によるインターネット定点観測システム (ISDAS)[2] や警察庁によるインターネット定点観測[3]，WCLSCAN[4] などが挙げられる．これらの手法では実際に運用している機器のフィルタログを用いるために，システム運用の負荷は比較的小さい．しかし，稼働しているサービスに対する DoS のような攻撃については，正常トラフィックであるか攻撃性トラフィックであるかの判別が困難である．一方，後者の例である Internet Motion Sensor[5] や Darknet[6][7] と呼ばれる手法では，インターネットに広報されているが使用されていないアドレス空間を利用し，そこに到達するパケットを全て収集する．その宛先アドレスは未使用である，つまりホストは存在しないので攻撃性のトラフィックのみを収集することが可能になる．Darknet による収集では，アドレスブロックが広ければ広いほど多数のデータを収集できるので良いとされており，実際にも/8 程度の大規模なネットワークで監視が行われている．しかし，そのような大きなアドレスブロックを用意することは一般的には困難である．

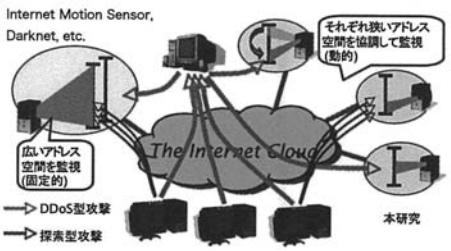


図 1　分散協調型監視アーキテクチャ

3. 分散協調監視アーキテクチャ

本研究では，二つの攻撃性情報収集手法のうち主としてパッシブな手法を用いる．特に，負荷の面でも収集される情報の質でも利点があると考えられる Darknet の手法を用いて，攻撃性トラフィックの監視基盤を構築する．しかし，現在行われている少数の大規模アドレスブロックによる Darknet では，それぞれの Darknet が収集した攻撃性トラフィックの発信元には相関が殆どないことが知られている．そのため，そこで得られた情報から新たな攻撃の種類程度は知ることができるが，攻撃の変動等の特徴から一般的な攻撃情報を抽出するのは容易ではない．つまり，ある大規模な Darknet の監視により得られた攻撃情報を，ネットワーク全域の防御に応用するのは困難であると考えられる．

一方で，管理者の経験的な知識からはネットワークに対する攻撃が万遍なく均一に行われることはなく，ある種の連続性や偏りがあることが予想される．したがって，機器を接続して利用しているネットワークアドレス空間の近くにある Darknet から得られる攻撃性トラフィックの情報は，比較的直接防御に応用できるのではないかという期待がある．

IP アドレスの枯渇が騒がれている昨今の事情を鑑みると，大規模なアドレス空間を用意しての観測は困難であり，各組織が独自に大規模な Darknet を運用して防御に生かすという形態は現実的ではない．そこで，各組織のネットワークで部分的に余っている未使用アドレスを使って小規模な Darknet を構成し，それらが連携して全体として大きなアドレス空間の監視を行う，分散協調型監視アーキテクチャを提案する (図 1)．通常，各組織には 2 の冪乗の個数の IP アドレスが割り当てられているので，それを完全に使い切っているということは稀であり，多くの組織である程度の未使用 IP アドレスが存在する．それらの断片として存在する未使用アドレス (断片アドレス) を利用する

ことで，大規模なアドレス空間を用意しなくても十分な攻撃監視を可能にすることを目指している．また，各組織が収集した攻撃性情報の情報を統計処理し，処理後の結果を相互に交換することにより，解析処理の分散化と交換情報 (データ) の削減が可能となるので，全体として効率良い攻撃解析が実現できる．さらに，このアーキテクチャでは利用アドレス空間の隙間に監視アドレス空間が滲み込むように広がることになり，防御したい利用ネットワーク空間の近傍を観測しつつ，広いアドレス空間に対して十分な広がりとばらつきを持った監視空間の設定が可能になる．

Darknet として使用するアドレス空間を別途割り当てないということは，利用アドレス空間と監視アドレス空間を自動的に管理する仕組みがないと実際の運用は困難になることが予想される．そこで提案する分散協調監視アーキテクチャには，この自動管理をさらに推し進めたアドレス空間動的入れ替えの機能を持たせる．これにより，ネットワークに対する攻撃の偏りの傾向に応じて，監視アドレス空間と利用アドレス空間の割り当てを動的に変更することで，攻撃頻度の高い部分の集中的な監視と攻撃頻度の低い部分でのサービス提供の双方の機能を提供できるようになる．

本提案アーキテクチャで期待される効果をまとめると以下のとおりである．

- 未使用の断片アドレスの活用による攻撃性トラフィック監視アドレス空間の確保
- 監視アドレス空間の分布の広がりによる，より一般的な攻撃特性の検出
- 利用アドレス空間と監視アドレス空間の動的割り当てによる，攻撃状況に適した情報収集とサービスの保護

4. 攻撃性トラフィックの解析

分散協調型の監視基盤の有効性を見積もるために，まず，ある程度規模の大きな Darknet を設定し，そこで収集されたデータについて初期的な解析を行った．ここで解析に用いたデータは，二つのサイトの darknet で収集したもので，一つ目のサイトである Site A では/18 のアドレスブロックを 1 本，二つ目のサイトである Site B では/22 のアドレスブロックを 10 本分観測している．以下のグラフにおいて，Site B の IP アドレスが軸方向に取られる場合には，各/22 のアドレスブロック同士の間に隙間をいれて表示してある．

4.1 攻撃先アドレス・ポートの偏り

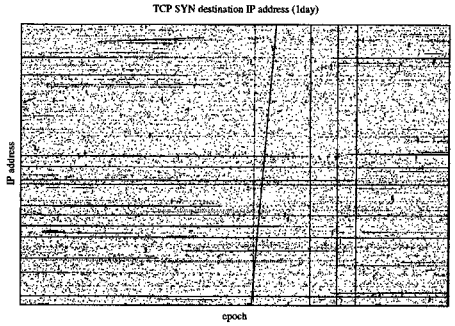
まず最初に，各々の darknet で収集された攻撃トラフィックの攻撃先がどのような分布になっており，時系列的にどう変化するかをみるために，時刻を横軸にとり縦軸に IP アドレスまたはポート番号をとって，分布の時系列的推移を表示した．図 2〜図 4 にその結果を示す．ここで，グラフの横幅は 24 時間分であり，全てのグラフは同一の日時のものである．それぞれのグラフは，TCP の SYN フラグのみが付いたパケット，TCP の SYN フラグと ACK フラグが付いたもの，UDP に分けて表示した．TCP SYN はサーバの探査や DoS 攻撃，設定ミスによる誤ったアドレス向けの接続要求等が含まれると考えられる．一方 TCP SYN+ACK は通常は SYN の戻りパケットなので，観測アドレスを詐称して行われた DoS 攻撃の backscatter の可能性が考えられる．

TCP SYN に関しては，どちらの Site のグラフにも縦縞と横縞がみられる．縦方向に走る筋はネットワーク全域に対する走査的なパケットである考えられる．一方，横向きに走る筋は，特定サーバアドレスを狙った DoS 攻撃や設定ミスによる大量転送であると考えられる．ここで，注目すべきは，IP アドレス空間には走査が起こるのに対して，ポート番号の空間では走査が同時には起こっていないことである．つまり，所謂ポートスキャンのような全サービスに対する探索的攻撃はあまり行われておらず，特定のサービスを狙った攻撃が主体になっていることがわかる．

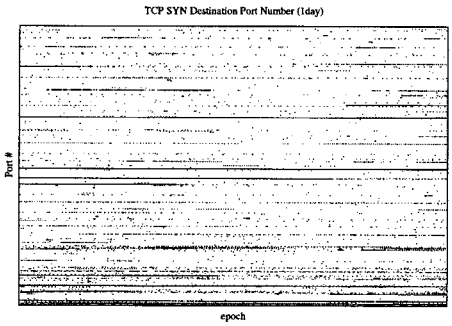
TCP SYN+ACK になると TCP SYN のような特定アドレス・ポートへの集中は少なく，比較的全アドレス空間に広がったパケット到達となっている．UDP は IP アドレス空間は全面的に埋まっているが，ポートアドレス空間はごく特定の一部が狙われているのが見て取れる．ここで，SYN+ACK の IP アドレスに関するグラフ (図 3(a), 図 3(c)) をよく見ると IP アドレス毎に濃淡の縞が比較的強く出ている．この縞は周期性を持っているようにもみえるので，特定アドレス空間を対象とした周期的な分布になっていることが予想される．そこで，観測している個々のアドレスに単位時間当たりにくるパケット数を計測して，それをプロットしてみた．結果を図 5〜図 6 に示す (縦方向は対数軸である)．ここで，横軸は IP アドレス，縦軸は 10 分間の各アドレス向けのパケット数である．

観測結果としては，ある程度の数 (10 パケット/10 分) までは均一に流れているが，極端に多くのパケットが送り込まれるアドレスは少数であることがわかる．そこで，この多数のパケットを受けるノードの存在アドレスの規則性を見るために，横軸を第 4 オクテットだけすなわち幅 256 で折り返して重ねた形の表示にした．結果を図 7 図 8 に示す．これを見ると，TCP SYN に関しては/24 のサブネット中でも，集中的に狙われているアドレス存在することが見て取れる．また，TCP SYN+ACK については 256 個中の上半分と下半分で全く傾向が異なるという，非常に興味深い結果となった．

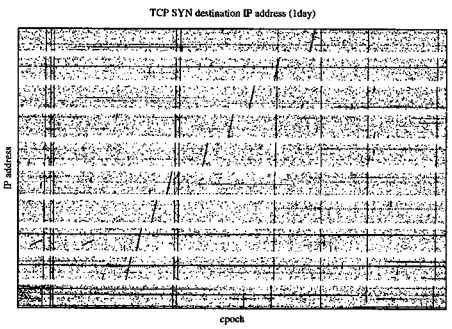
以上の解析結果から，実際の攻撃性トラフィックには予想していたような偏りが実際に存在し，また，攻撃性のトラフィックはある程度の期間は継続することがわかった．



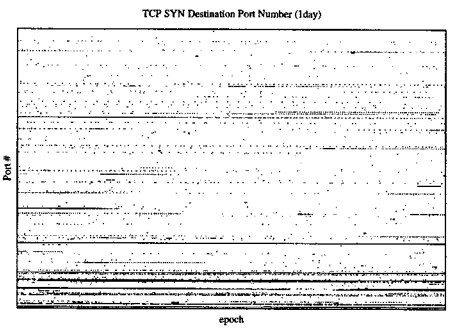
(a) IP アドレス (Site A)



(b) Port 番号 (Site A)

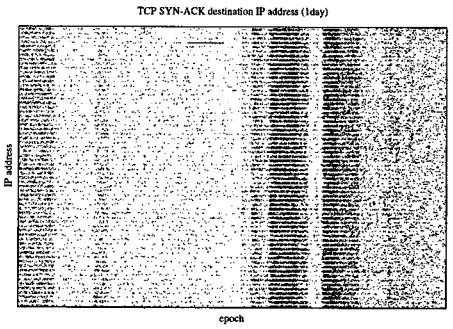


(c) IP アドレス (Site B)

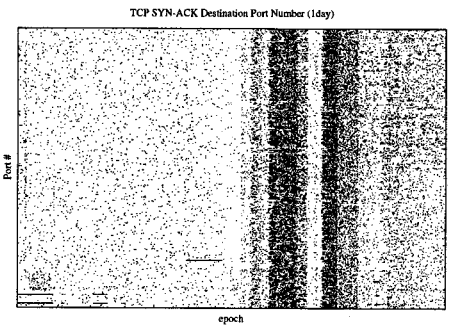


(d) Port 番号 (Site B)

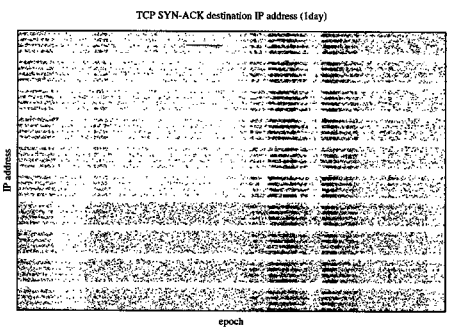
図 2　TCP SYN の到着傾向



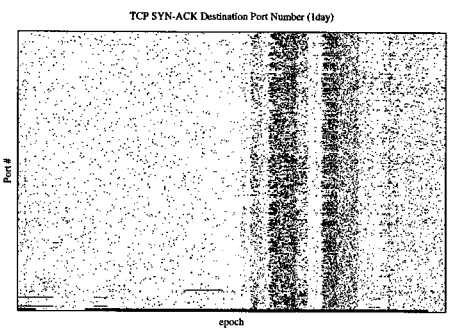
(a) IP アドレス (Site A)



(b) Port 番号 (Site A)

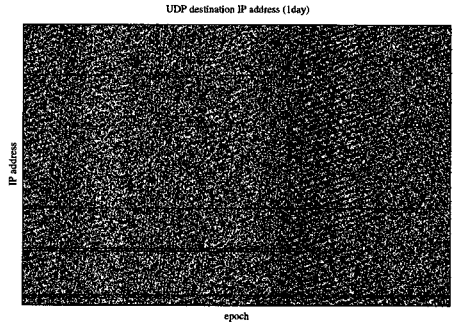


(c) IP アドレス (Site B)

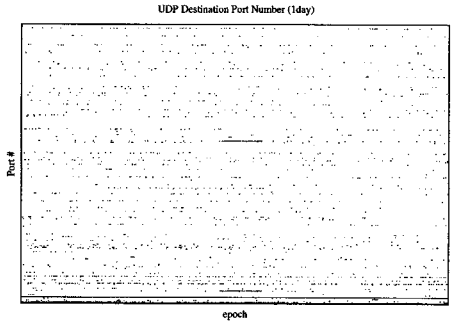


(d) Port 番号 (Site B)

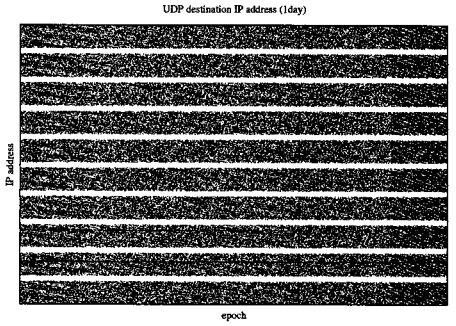
図 3　TCP SYN+ACK の到着傾向



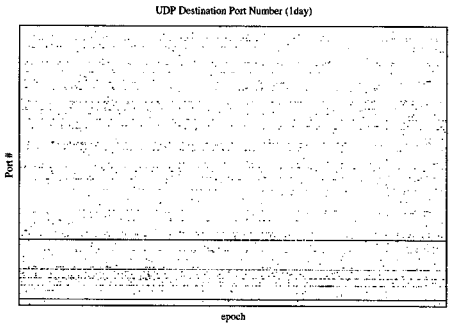
(a) IP アドレス (Site A)



(b) Port 番号 (Site A)

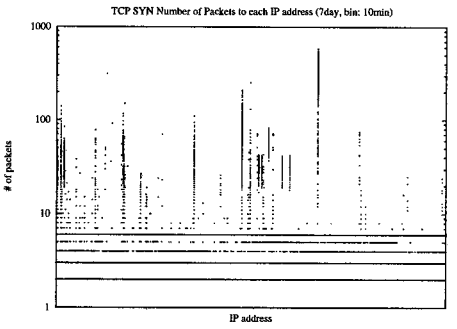


(c) IP アドレス (Site B)

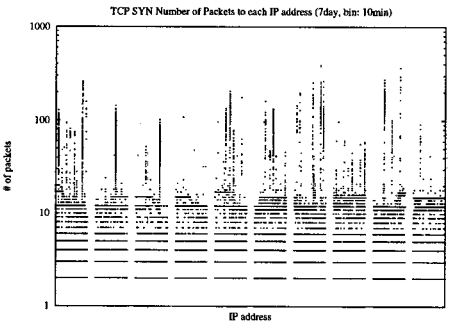


(d) Port 番号 (Site B)

図 4 UDP の到着傾向



(a) Site A



(b) Site B

図 5 単位時間当たりパケット到着数の分布 (TCP SYN)

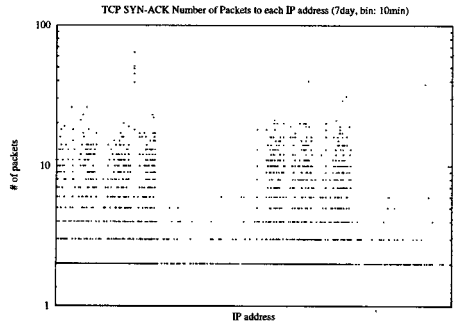
4.2 発信元アドレスの分布特性

次に，どの程度離れたアドレスブロックまでなら攻撃性トラフィックに類似性があるかについての解析を行った．ここでは，Site A の darknet に到着したトラフィックについて，darknet の観測空間を/24 ずつに分割した各々の部分ネットワーク間でどの程度の相関があるかを調べた．図 9 に，個々の/24 アドレスブロックにに到着したパケット数の時系列 (1 分単位，24h 分) の，/24 アドレスブロック単位での空間相互相関を示す．

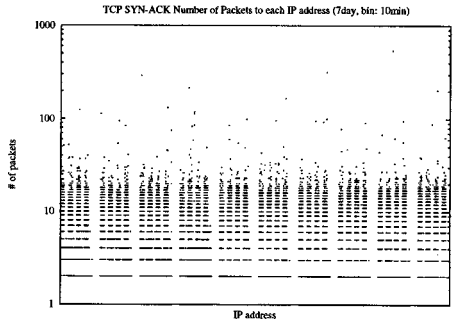
この相互相関からは，アドレスブロックが近いところでは相互に強い相関が得られるという，想定通りの結果が得られている．また，この結果からは/24 アドレスブロックにして 15 個程度，つまり/20 程度の範囲ではある程度の相関が得られており，その幅に一ヶ所程度トラフィック観測空間が存在するのが良いと考えられる．

5. おわりに

本稿では，ネットワーク中に存在する断片アドレス空間を有効に活用し，実際に使われているネットワークアドレス空間の隙間に観測空間が入り込む，分散協

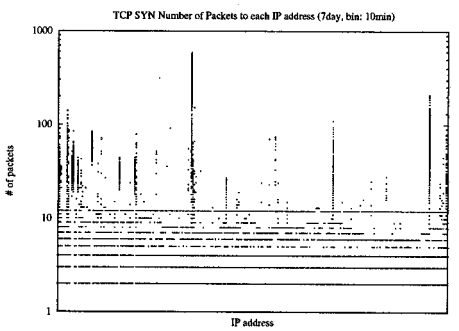


(a) Site A

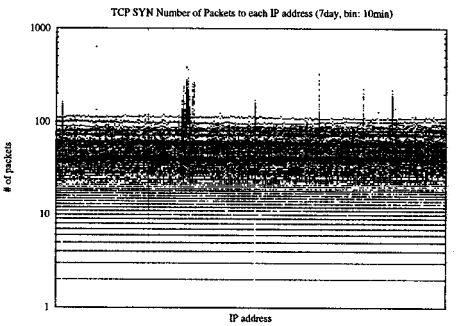


(b) Site B

図 6 単位時間当たりパケット到着数の分布 (**TCP SYN+ACK**)



(a) Site A



(b) Site B

図 7 単位時間当たりパケット到着数の分布 (**TCP SYN**, 横軸 **4octet** 目)

調型の観測・防御アーキテクチャを提案した．このアーキテクチャで目指しているのは，単なる観測空間の拡大だけではなく，利用ネットワークアドレス空間と観測ネットワークアドレス空間の動的な入れ替えまでを含めて，実際の攻撃状況に適応的に対応し運用と観測に適切なアドレスを割り当てるネットワーク監視・防御基盤の構築である．この点については，本稿で示した darknet のトラフィック解析結果からは，

- 攻撃性トラフィックの到達空間には偏りがあり
- 攻撃的なトラフック集中は半日から一日以上の期間にわたる

ことは明らかになった．これらの事実を考慮すると，ここで目指している動的なアドレス空間の割り当ては，十分に効果を発揮することが期待できる．今後は，攻撃性トラフィックの空間的・時間的特性をさらに詳しく調べるとともに，システムソフトウェアとしての基盤の実現を進めていく予定である．

参 考 文 献

1) The Honeynet Project & Research Alliance: Know your Enemy: Honeynets. (2003). http://www.honeynet.org/papers/honeynet/.

2) JPCERT/CC: インターネット定点観測システム (ISDAS: Internet Scan Data Acquisition System). http://www.jpcert.or.jp/isdas/.

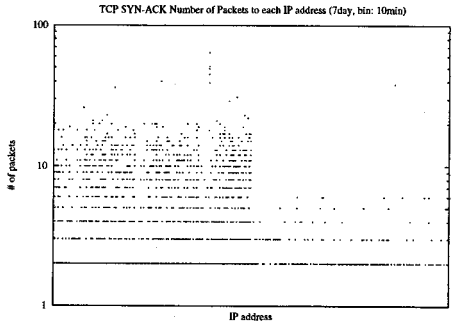
3) 警察庁:インターネット定点観測. http://www.cyberpolice.go.jp/detect/observation.html.

4) Ishiguro, M., Suzuki, H., Murase, I. and Ohno, H.: Internet Threat Detection System Using Bayesian Estimation, *The 16 the FIRST Annual Conference on Information Security Incident 2004* (2004).

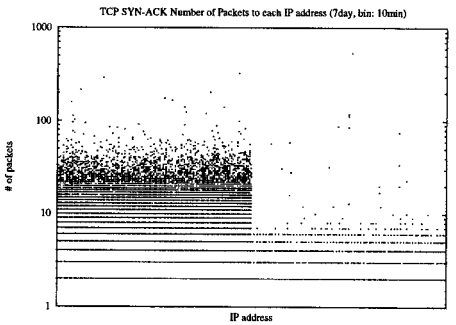
5) Bailey, M., Cooke, E., Jahanian, F., Nazario, J. and Watson, D.: The Internet Motion Sensor: A distributed blackhole monitoring system., Network and Distributed System Security Symposium (NDSS '05) (2005).

6) Cooke, E., Bailey, M., Jahanian, F. and Mortier, R.: The Dark Oracle: Perspective-Aware Unused and Unreachable Address Discovery, *3rd Symposium on Networked Systems Design & Implementation (NSDI' 06)*, pp.101–114 (2006).

7) Pang, R., Yegneswaran, V., Barford, P., Paxson, V. and Peterson, L.: Characteristics of In-



(a) Site A



(b) Site B

図 8 単位時間当たりパケット到着数の分布 (TCP SYN+ACK, 横軸 4octet 目)

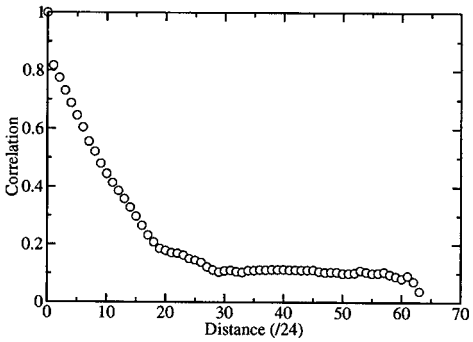


図 9 監視ブロック間の空間相互相関

ternet background radiation, *4th ACM SIGCOMM conference on Internet measurement*, pp.27–40 (2004).