大規模分散ネットワーク防衛基盤

廣津登志夫 (第４工学系, 情報環境コア)

1　はじめに

現在のインターネット環境は，一般的な生活インフラストラクチャの一つとなっている。しかし、このインターネット基盤上では機密情報の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．このようなインターネットにおける攻撃に対処するためには，攻撃情報を観測・収集して，それらを解析・モデル化・類型化することで，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．しかし、これらの攻撃性情報は増大する一方であり、またネットワーク環境も広がる一方であり、それを十分に守りうるスケーラブルな監視・運用環境が非常に重要になる．現在、国内の複数の拠点で連携して攻撃性トラフィックの収集・解析と分散防衛基盤の研究を進めている。

2　分散協調型監視アーキテクチャ

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 [1, 2, 3, 4]．これらの観測では,「巨大な[1]」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が，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分散協調アーキテクチャの構築を目指している (図 1)。これは単に空間を広げることを目指しているだけでなく，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) が滲み込むように広がった環境を生み出すことで，攻撃の特性をよく表した情報収集が可能になることを狙っている。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の構築を目指している。このアプローチの特徴をまとめると、以下のとおりである。

- 未使用の断片アドレスを活用し、攻撃性トラフィック監視アドレス空間を確保する

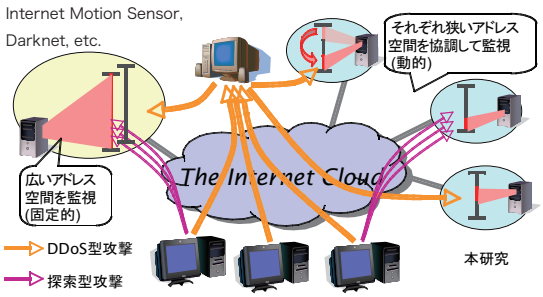

Fig. 1　**分散協調型監視アーキテクチャ**

- 監視アドレス空間の分布が広がりをもつことにより，より一般的な攻撃特性の検出を可能とする
- 利用アドレス空間と監視アドレス空間を動的に割り当てることで，攻撃状況に適した情報収集とサービスの保護を提供する

3　攻撃性トラフィックの収集と解析

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．図 2 と図 3 は到着した攻撃パケット (TCP SYN のみ) について、宛先アドレスを縦軸に時刻を横軸に 24 時間分をプロットしたものである。これを見ると特定のアドレスへの連続的な攻撃 (図で横線に見える) とアドレス空間にわたる探索的な動きが見て取れる。さらにこの宛先アドレスの第 4 オクテットに着目して (256 毎にアドレス空間を折り返して)1 週間分のパケット数を集計したものを図 4 と図 5 に示す。これを見ると、特定のアドレスに対して攻撃が集中している上に、さらにそれが異なる地点でも類似した傾向を示している。これによりアドレス断片の配置により狭い空間でも効率的な収集が可能であろうということが予想される。

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

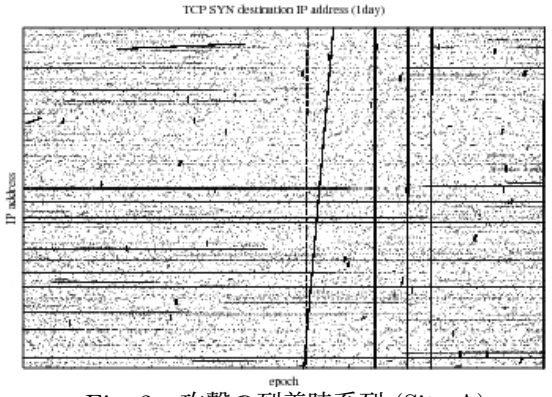

Fig. 2　攻撃の到着時系列 (Site A)

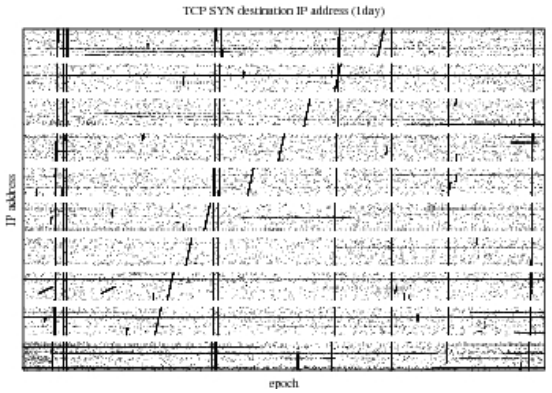

Fig. 3　攻撃の到着時系列 (Site B)

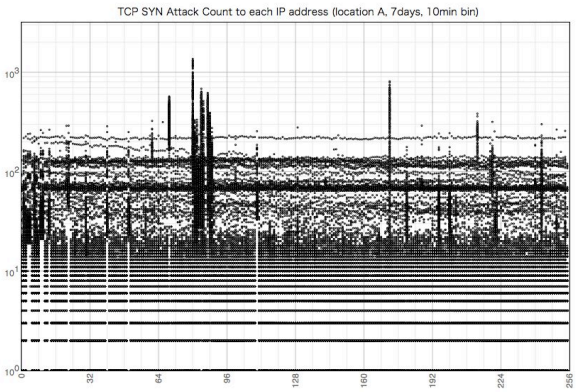

Fig. 4　アドレス毎の集中度 (Site A)

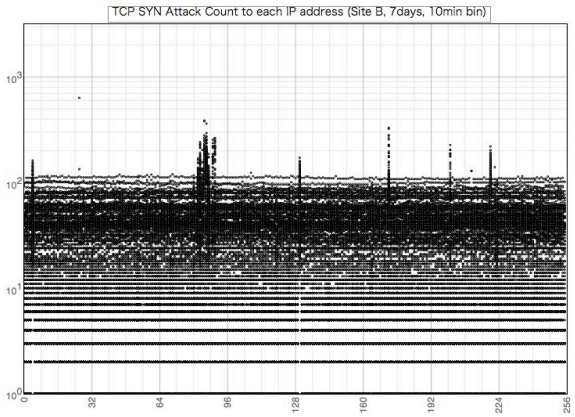

Fig. 5　アドレス毎の集中度 (Site B)

4　まとめ

現在、国内数拠点で連携して進めているインターネット攻撃データの収集とその初期的な解析について紹介した。現在、これまでのデータ解析の知見をもとに、分散協調型の収集・防衛基盤の構築を進めている。

発表論文

[1] M. Bailey, E. Cooke, F. Jahanian, J. Nazario, and D. Watson. The internet motion sensor: A distributed blackhole monitoring system. In *Network and Distributed System Security Symposium (NDSS'05)*, 2005.

[2] E. Cooke, M. Bailey, F. Jahanian, and R. Mortier. The dark oracle: Perspective-aware unused and unreachable address discovery. In *3rd Symposium on Networked Systems Design & Implementation (NSDI' 06)*, pp. 101–114, 2006.

[3] R. Pang, V. Yegneswaran, P. Barford, V. Paxson, and L. Peterson. Characteristics of internet background radiation. In *SIGCOMM Conference on Internet Measurement*, pp. 27–40, 2004.

[4] The Honeynet Project & Research Alliance. Know your enemy: Honeynets. Nov. 2003. http://www.honeynet.org/papers/honeynet/.

発表論文

[1] 福田, 廣津, 明石, 栗原, 菅原. 異常パケットトレースのアドレス局所性に関する解析. 情報処理学会 第 70 回全国大会 論文集, pp. 4K–5, Mar. 2008.

[2] 今間, 福田, 廣津, 菅原. 断片ダークネット・アドレス宛パケット収集ブリッジの開発と評価. 情報処理学会 第 70 回全国大会 論文集, pp. 3ZL–6, Mar. 2008.

[3] 廣津, 福田, 栗原, 明石, 菅原. 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. 情報処理学会研究報告 - システムソフトウェアとオペレーティング・システム (OS), p. 39.

[4] 廣津, 塩野, 福田, 菅原. 多地点断片ダークネットのための統合データ解析ツールの開発. 情報処理学会 第 70 回全国大会 論文集, pp. 5K–6, Mar. 2008.