TCP SYN Flood 攻撃の可視化によるネットワーク管理者のネットワーク運用支援

佐々木玲生* 池部実* 吉田和幸**
(大分大学 *工学部知能情報システム工学科 **学術情報拠点情報基盤センター)

１ はじめに

悪意のあるユーザからの攻撃が増加しており，ネットワークセキュリティの重要性は高まっている．これまで，我々は大分大学宛トラフィックを可視化し，管理者のために運用を支援するトラフィック表示システムを開発してきた．先行研究においては水平 scan 攻撃を可視化した[1]．本研究では，DoS(Denial of Service)攻撃の発見を目的として，DoS 攻撃のひとつである TCP SYN Flood 攻撃の可視化に取り組む．大分大学宛のトラフィックに含まれる TCP パケット中の SYN の比率を可視化し，TCP SYN Flood 攻撃によるトラフィックの変化を観測する．本論文では，大分大学宛の通常のトラフィックと DoS 攻撃を発生させたトラフィックにおける TCP パケット中の SYN の比率を可視化する．

２ TCP SYN Flood 攻撃

TCP では，サーバは接続元からの TCP 通信の接続要求（SYN）に対して，確認応答の SYN/ACK を送信する．接続元は確認応答の ACK を返送し，スリーウェイハンドシェイクにより，通信を確立する(図 1 左)．TCP SYN Flood 攻撃においては，攻撃者から確認応答である ACK が返送されない(図 1 右)．TCP SYN Flood 攻撃を受けると，サーバは攻撃者からの ACK の応答待ちが大量に発生し，新たな要求を受け入れることができなくなる[2]．

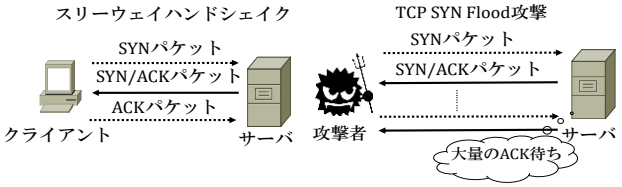

図 1. TCP SYN Flood 攻撃

３ 研究目的および実験

３．１ 研究目的

攻撃者は TCP SYN Flood 攻撃により，攻撃対象のサーバに SYN を送信し続けるため，TCP SYN Flood 攻撃が発生していない通常時よりも SYN パケットの割合が増加する．大分大学宛てのトラフィックのうち，SYN パケットの占める割合を可視化して，TCP SYN Flood 攻撃を検出する．

３．２ 実験内容

本論文では，大分大学宛ての通常トラフィックに，仮想環境内で発生させた TCP SYN Flood 攻撃を収集し，通常トラフィックと TCP SYN Flood 攻撃を混在させたトラフィックにおける SYN パケットの割合を可視化した．まず，5 分間，大分大学宛トラフィック(TCP)を収集した．実際の TCP SYN Flood 攻撃を収集するのは難しいため，仮想計算機環境上において，Web サーバを構築し，DoS 攻撃を発生させるツール synk4 を用いて Web サーバへの TCP SYN Flood 攻撃を再現し，5 分間のトラフィックデータを収集した．これらのデータにおける SYN パケットの割合を可視化した．

４ 実験結果

大分大学宛の通常トラフィックと，通常トラフィックに TCP SYN Flood 攻撃のトラフィックを混在させたトラフィックにおける SYN パケットの割合を可視化し，比較した．表 1 に 2 つのトラフィックのパケット数を示す．また，図 2 に収集した 300 秒のデータのうち，最初の 15 秒間の 1 秒毎の SYN の割合を可視化した結果を示す．synk4 では，流量調節ができないため，1 秒間に約 5600 パケットで 300 秒間 TCP SYN Flood 攻撃を実施した．通常のトラフィックに対して約 5%の SYN パケットの増加を確認した．

表 1. パケット数(5 分間)

	パケット数	平均PPS	SYN パケット (SYN 割合)	平均 PPS(SYN)
大分大学宛	9,615,424	32,051	335,607 (3.7%)	1,185
DoS	1,672,233	5,574	557,411 (33.3%)	1,858
マージ	11,287,657	37,625	913,018 (8.1%)	3,043

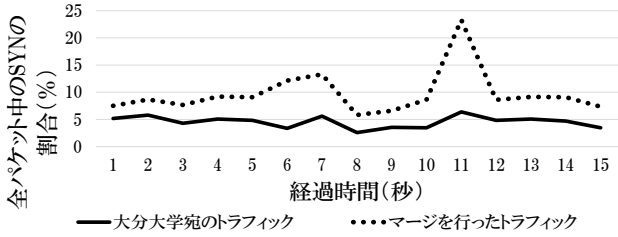

図 2. 2 つのトラフィックの SYN の比率の可視化結果

５ おわりに

通常時のトラフィックと通常時と DoS 攻撃を混在させたトラフィックにおける，TCP パケット中の SYN の比率を可視化した．TCP SYN Flood 攻撃が発生すると，SYN の割合が増加する．しかし，TCP SYN Flood 攻撃が行われていなかったとしても，通常ユーザの接続要求が増加することで SYN の割合が 5%，あるいは，それ以上増加する事が十分に考えられる．今後は SYN の割合を変化させながら可視化し，どの程度であれば TCP SYN Flood 攻撃を発見できるか調査する．さらに，トラフィック表示システムに SYN パケットの比率を表示する機能や， TCP SYN Flood 攻撃発生時，管理者が必要とする IP アドレスやポート番号などの情報を抽出し表示システム上で表示する機能を開発する．

参考文献

[1]田中瑤子, 小刀祢知哉, 松井一乃, 池部実, 吉田 和幸: “Web ブラウザにて閲覧可能なトラフィック表示システムを用いた水平 scan 攻撃の可視化”, 平成 26 年度電気・情報関係学会九州支部連合大会, pp.88-88, 2014 年 9 月
[2]警察庁, “SYN flood 攻撃被害観測システムについて”, https://www.npa.go.jp/cyberpolice/server/rd_env/pdf/synflood_detect.pdf, 2014 年, (参照 :2016 年 8 月 7 日)