

SYN flood 攻撃被害観測システムについて

1. 概要

SYN flood 攻撃は、DoS 攻撃の一種であり、攻撃目標とするインターネット上のサーバに攻撃用のパケットを撃ち込み続けることで、その機能を妨害するものである。その際、攻撃手法によっては、撃ち込まれた攻撃用のパケットが、ある決まった形で跳ね返り、インターネット上にばらまかれる現象が発生することが知られている。

その跳ね返ったパケットを、警察庁のインターネット定点観測網で待ち受け、拾い集めることによって、この攻撃方法がどの程度行われているか、また対象となっているサーバはどこであるか、という分析が可能である。(図1)



図1 SYN flood 攻撃の検知

本レポートは、これまでに当庁において観測された跳ね返りパケットの観測によって、一般的な SYN flood である、攻撃パケットの送信元 IP アドレスを無作為に詐称した DoS 攻撃がインターネット上でどのように行われているのかを推定したものである。

2. SYN flood 攻撃

(1) SYN flood 攻撃

SYN flood とは、TCP 接続の開始手順（スリーウェイ・ハンドシェイク（図 2））を悪用した攻撃である。攻撃者は、通信の開始要求（SYN パケット）を攻撃対象のサーバに送り、サーバから送り返される SYN/ACK パケットには応答しない。（図 3）これを大量に繰り返すことにより、サーバに ACK パケット待ちが発生して、新たな要求の受け付けが不可能となる。

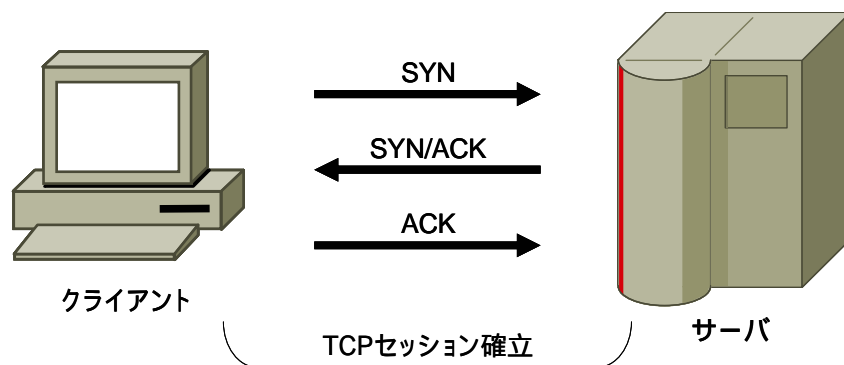


図 2 正常なスリーウェイ・ハンドシェイク

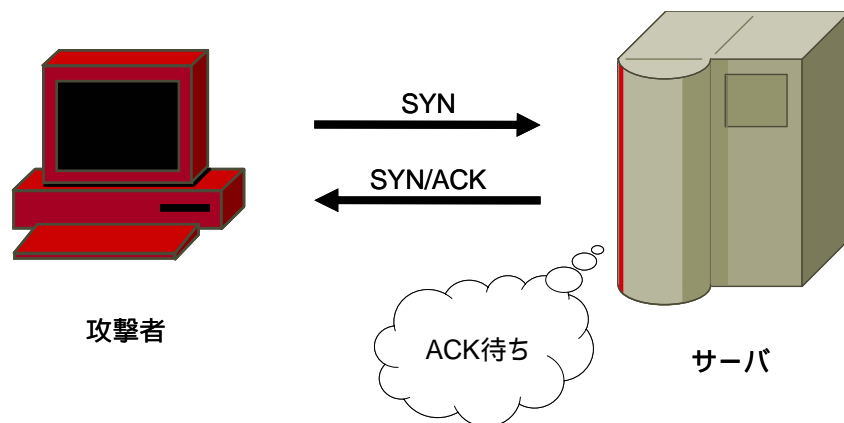


図 3 SYN/ACK に応答しない攻撃者

(2) SYN flood 攻撃の検知

SYN flood 攻撃において、攻撃者が送信する SYN パケットは、パケットの発信元の判別を困難にするために、発信元 IP アドレスを詐称することが行われることが多い。この場合、サーバは詐称された IP アドレスに対して SYN/ACK パケットを返信する。このため、この詐称された IP アドレスを持つホストには、接続要求を出していないサーバから、突然 SYN/ACK パケットが到達することになる。以下、このような SYN パケットに対する、詐称された IP アドレスへのこのような SYN/ACK パケットを、「跳ね返りパケット」と呼ぶ。(図 4)

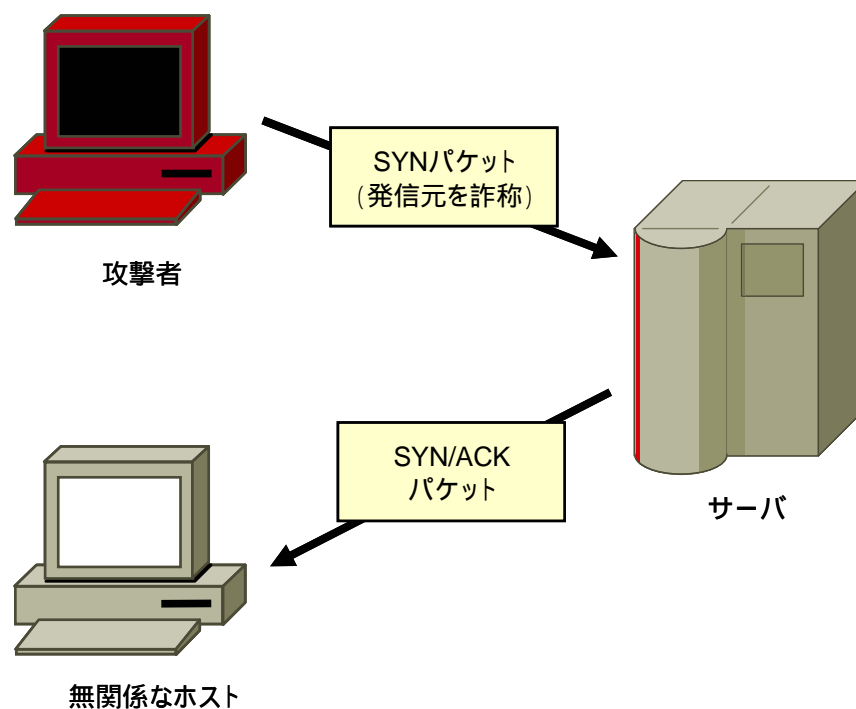


図 4 SYN/ACK の跳ね返り

攻撃者が発信元 IP アドレスをランダムに詐称した場合、跳ね返る SYN/ACK パケットの到達先もランダムである。このため、SYN flood 攻撃が行われた際に、第三者が跳ね返りパケットを監視することで、SYN flood 攻撃を検知できる可能性がある。(図 5)

なお、跳ね返りパケットから得られる情報は、SYN flood 攻撃を受けている被害サーバの IP アドレスであり、攻撃者の IP アドレスについての情報は、得ることができない。

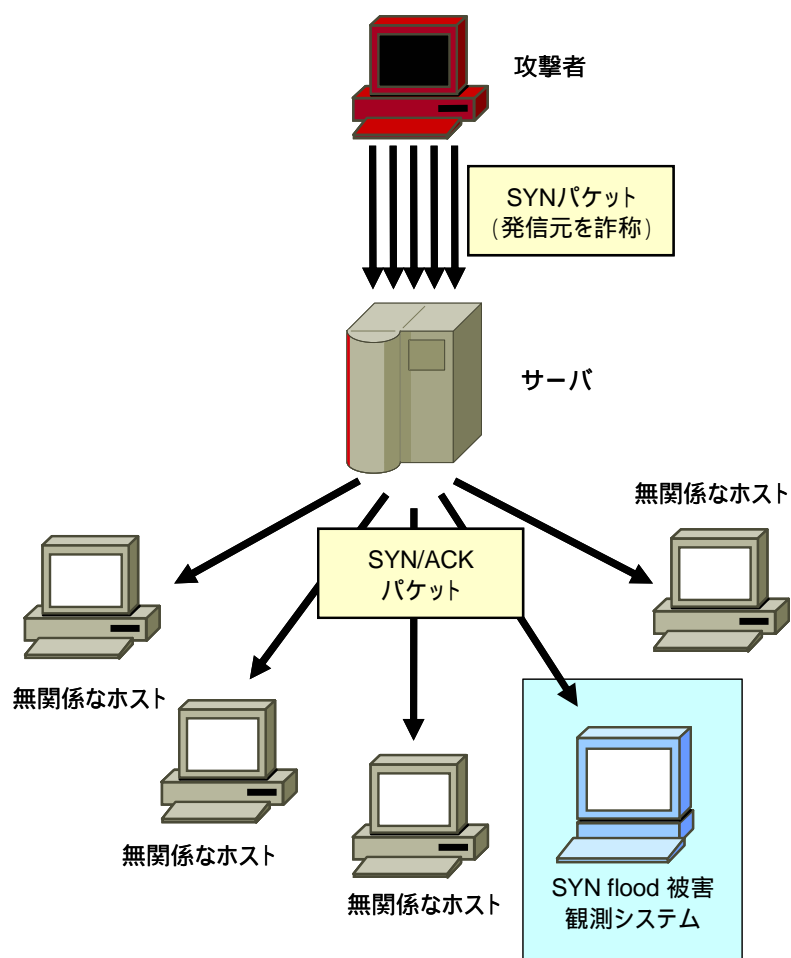


図 5 SYN flood 攻撃検知の原理

3. SYN flood 被害観測システム

(1) SYN flood 被害観測システム

警察庁では、全国の警察組織に設置したファイアウォールを利用してインターネットの定点観測を行っており、今回これを利用して跳ね返りパケットの観測を開始した。跳ね返りパケットを監視することで SYN flood 攻撃を検知することを目指し、以下では本観測システムを「SYN flood 被害観測システム」と呼ぶ。

(2) SYN flood 被害観測システムの検知能力

IP アドレスは、原理的には約 43 億 (2 の 32 乗) 個が存在する。攻撃者が発信元 IP アドレスを詐称する際に、この約 43 億個をランダムに利用した場合、一つの跳ね返りパケットが、ある IP アドレスを持つホストに向けて送信される確率は $1/2^{32}$ 、IP アドレス数が n 個であるとする $n/2^{32}$ となる。 n か所の SYN flood 被害観測システムで監視した場合、 N 個の跳ね返りパケット中、 m 個のパケットを検知する確率は二項分布 $B_N(m, n/2^{32})$ に従う。

これから計算した、今回観測を開始した被害観測システムによる SYN flood 攻撃の検知確率の理論値を図 6 に示す。なお、横軸は対数軸であり、図中のトラフィックは、攻撃が 3 時間にわたっていた場合のおよその値である。

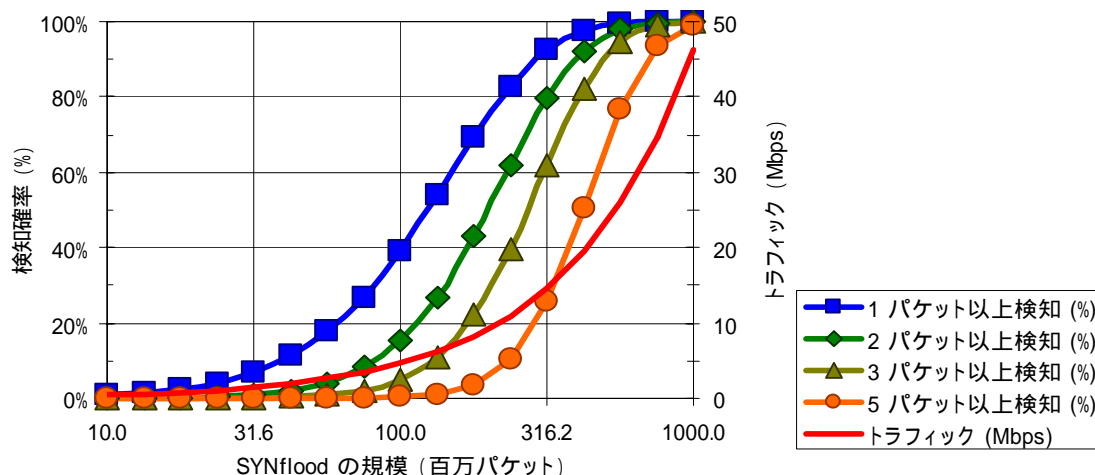


図 6 SYN flood 被害観測システムの検知確率

図から 1 億パケット規模の SYN flood 攻撃であれば、本被害観測システムで検知できる可能性があることが分かる。

4. SYN flood 被害観測システムの検知状況

平成 16 年 7 月～9 月の、SYN flood 被害観測システムでの検知状況は以下の通り。

(1) 各ポートの状況

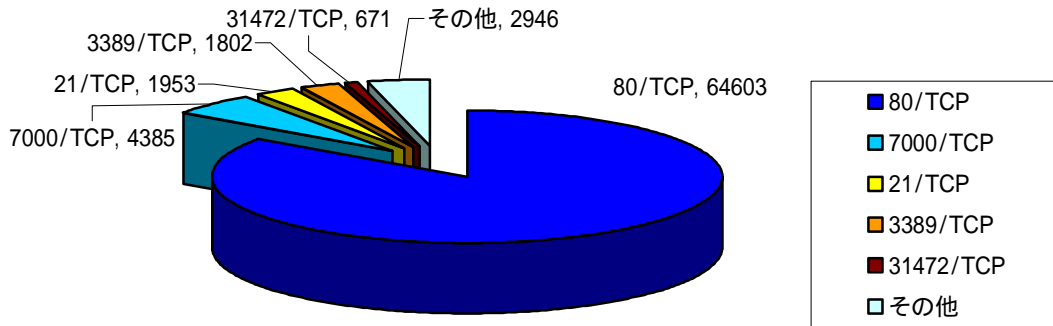


図 7 ポート毎の検知件数

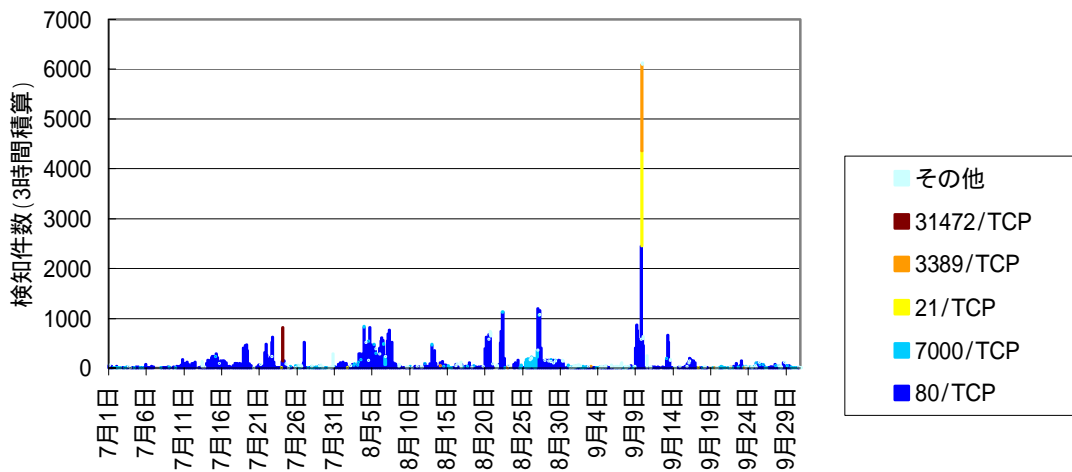


図 8 3 時間毎の検知件数（ポート別、積み上げ）

ウェブの閲覧に利用される 80/TCP の跳ね返りパケットが大半となっており、SYN flood 攻撃がウェブサーバに対して行われることが多いという現状が推測できる。

(2) 80/TCP

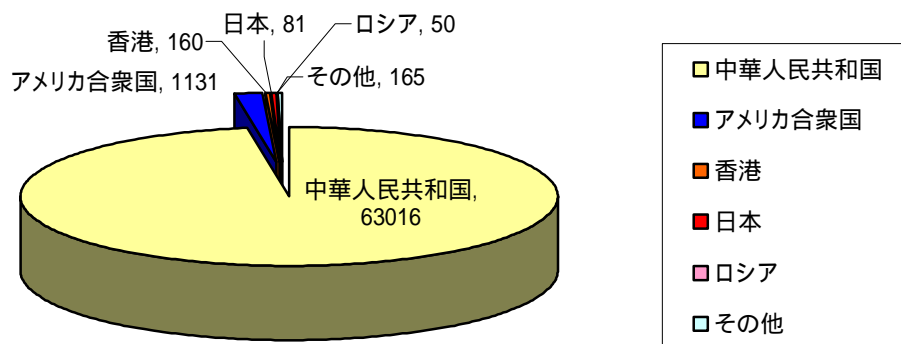


図 9 80/TCP の検知件数

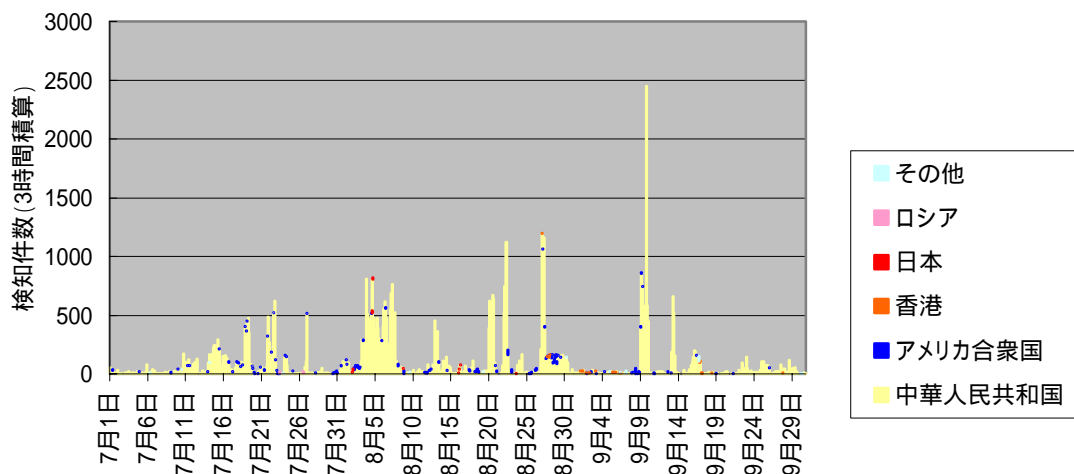


図 10 80/TCP の 3 時間毎の検知件数 (積み上げ)

80/TCP はウェブの閲覧に使用されるポートである。

検知したパケットの大半は発信元が中華人民共和国であるが、発信元が中華人民共和国となっているものについては、ウェブページが設置されていないなどホストの使用目的がはっきりしないものが多く、検知したパケットの中にはサーバに対する攻撃でないものが含まれている可能性がある。

(3) 7000/TCP

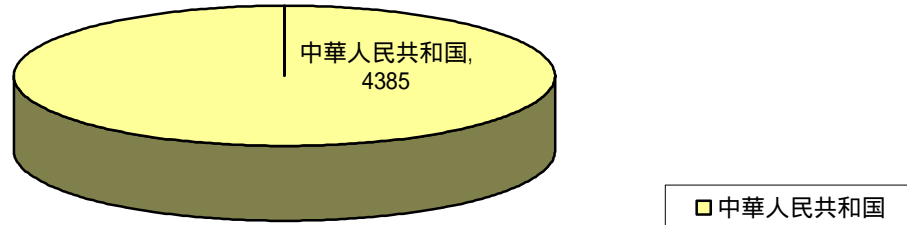


図 11 7000/TCP の検知件数

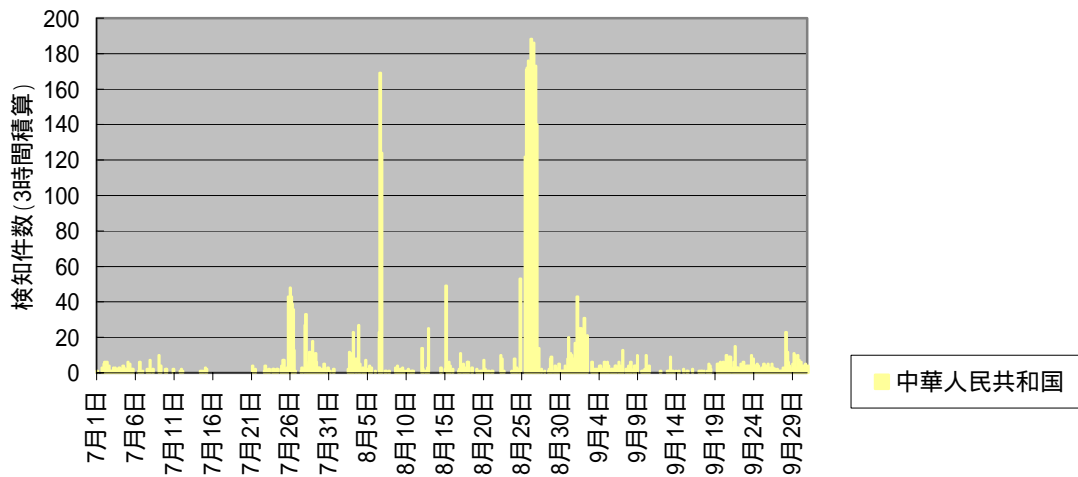


図 12 7000/TCP の 3 時間毎の検知件数

7000/TCP は、各種のアプリケーションで利用されるポートである。

今回検知したパケットはすべて中華人民共和国から送信されたものであった。このポートの具体的な用途は不明であるが、SYN flood 攻撃が複数回行われたものと考えられる。

(4) 各国・地域の状況

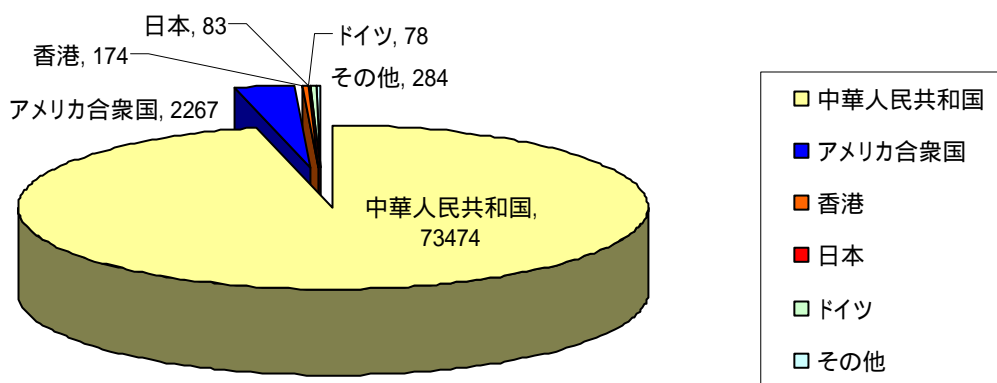


図 13 国・地域ごとの検知件数

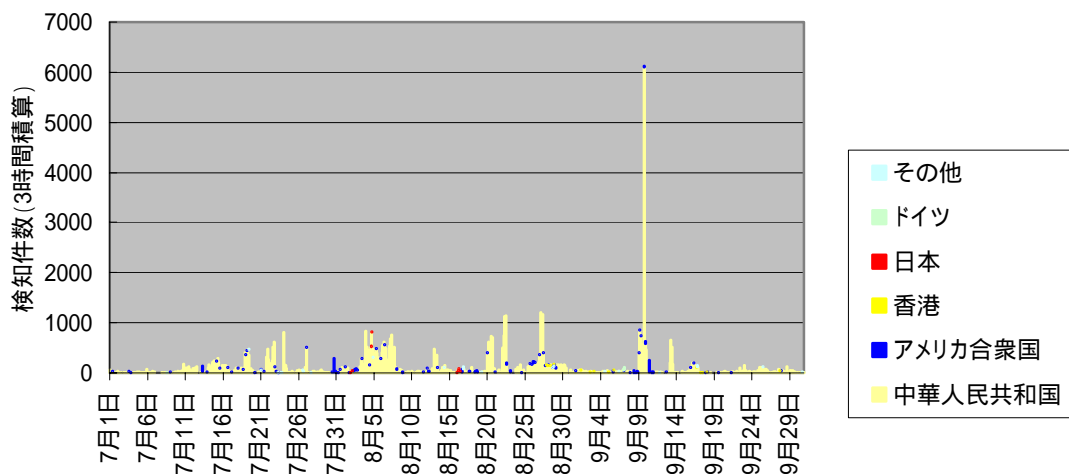


図 14 3 時間毎の検知件数 (国・地域別、積み上げ)

中華人民共和国を発信元 IP アドレスとするパケットが大半であり、アメリカ合衆国がこれに続く。この二国からのパケットは定常的に検知しており、両国に対する SYN flood 攻撃が常態化していると考えられる。

検知件数が 3 位以下の香港、日本、ドイツは、一時的に検知されることがあるのみで、検知件数が 0 となる日が大勢を占め、月によって順位は変動した。

(5) 中華人民共和国

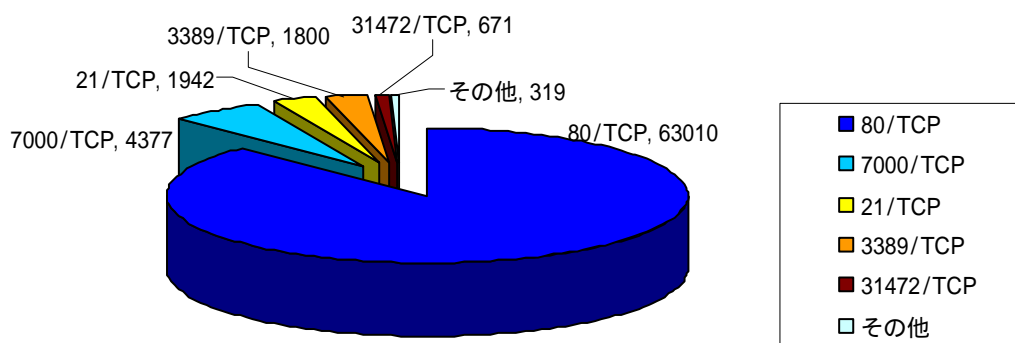


図 15 発信元 IP アドレスが中華人民共和国である検知件数

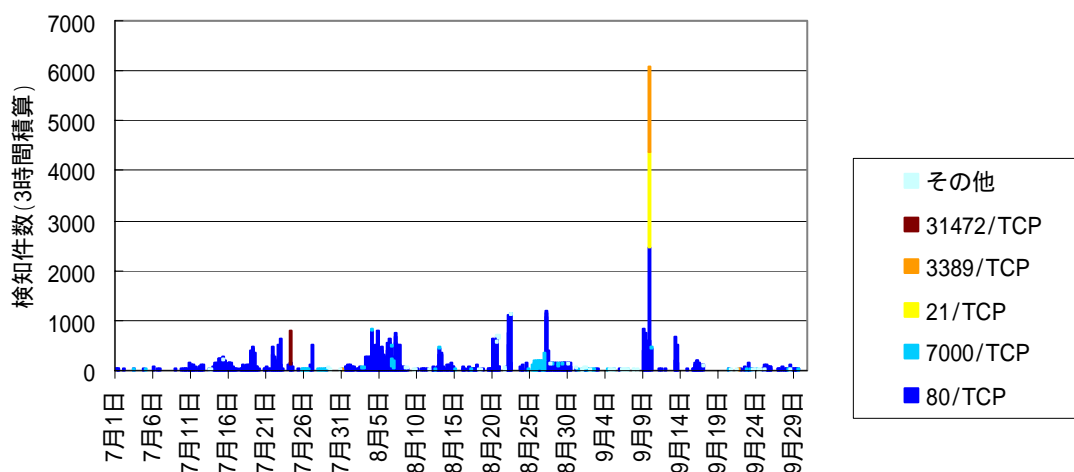


図 16 発信元 IP アドレスが中華人民共和国の3時間毎の検知件数（積み上げ）

他国と比較して、中華人民共和国を発信元 IP アドレスとする検知数はきわめて多いが、実際にサーバとして運用されているかどうかを確認できないホストも多い。

9月9日に、中華人民共和国の特定の IP アドレスを発信元とし、21/TCP、80/TCP、3389/TCP を発信元ポートとするトラフィックを検知している。3389/TCP は、Microsoft 社の Windows の RDP（リモートデスクトッププロトコル）で使用されるポートであり、Windows で運営されているサーバに対して、脆弱性を狙うなどの何らかの攻撃が行われた可能性が考えられる。なお、特定の範囲の IP アドレスを持つセンサーのみがこのトラフィックを検知しているため、攻撃者が発信元 IP アドレスを詐称する際に使用した IP アドレスは、完全にランダムなものではなかったと考えられる。このため、実際に行われた攻撃の規模から期待される検知件数に比較して、今回の検知件数は大きなものである可能性が高い。

(6) アメリカ合衆国

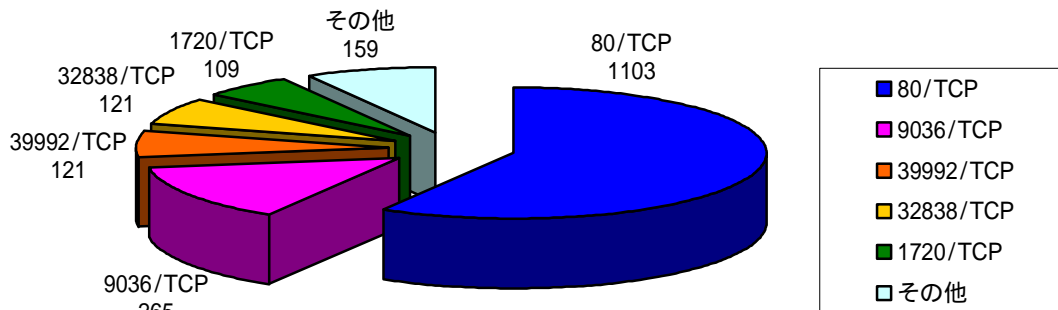


図 17 発信元 IP アドレスがアメリカ合衆国である検知件数

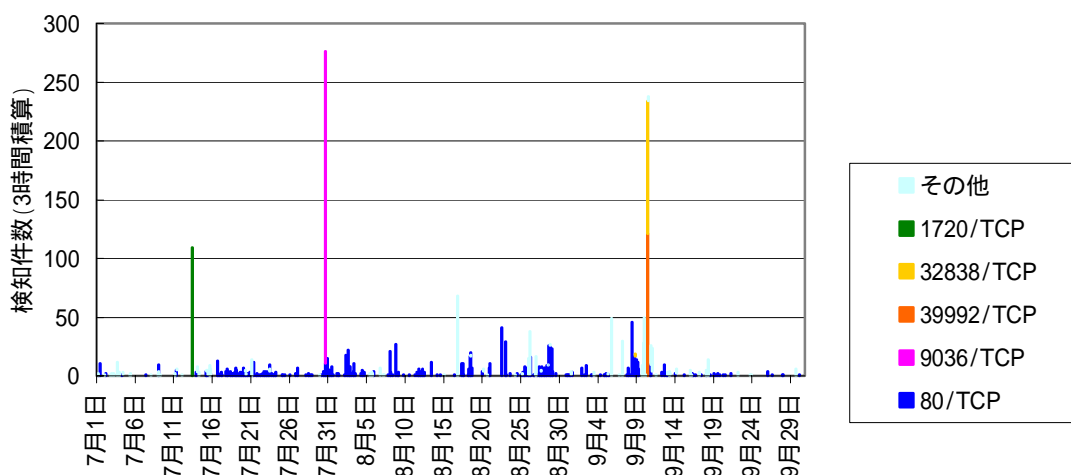


図 18 発信元 IP アドレスがアメリカ合衆国の 3 時間毎の検知件数（積み上げ）

中華人民共和国ほどではないが、アメリカ合衆国を発信元 IP アドレスとするパケットも多数検知しており、インターネット上での攻撃が日常化していると考えられる。ポートの傾向としては、ウェブの閲覧に使用される 80/TCP が多いが、他のポートに対する跳ね返りもかなりの数が存在し、特定のサーバの特定のサービスに対する攻撃が行われていると考えられる。

また、オンライン賭博サイトのウェブサーバからの跳ね返りパケットを検知しており、企業恐喝に SYN flood 攻撃が用いられている可能性が高い。¹

その他、7月13日、7月30日、9月10日にそれぞれ特定のサイトからの多数の跳ね返りパケットを検知しており、SYN flood 攻撃が行われたと推測される。

¹ @police 世界のセキュリティ事情「『あなたの会社を狙い始めた』企業恐喝」

http://www.cyberpolice.go.jp/international/north_america/20040423_000954.html

(7) 日本

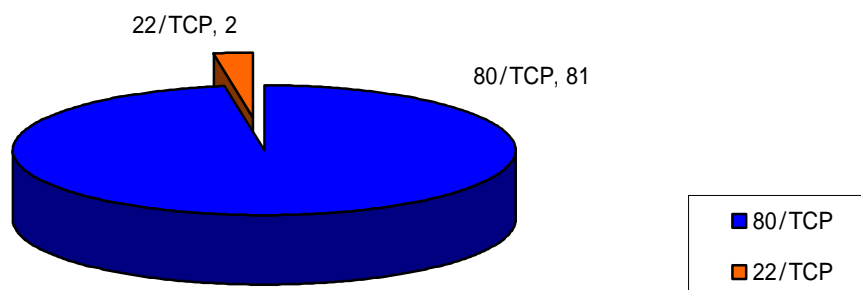


図 19 発信元 IP アドレスが日本である検知件数

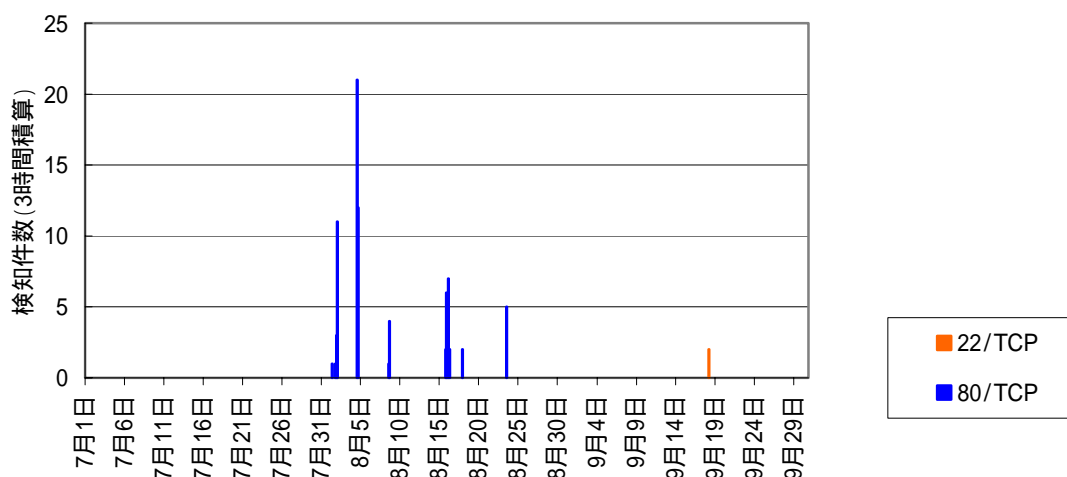


図 20 発信元 IP アドレスが日本の 3 時間毎の検知件数 (積み上げ)

22/TCP の跳ね返りパケットとして、9月18日にある企業のウェブサーバからのトラフィックを検知している。サーバの管理用のサービスに対する攻撃の可能性が考えられるが、定かではない。

80/TCP の跳ね返りパケットとしては、8月上旬に日本の各省庁のウェブサイトから、8月上旬以降に特定の団体及び特定の政治的主張を行っているウェブサイトからのトラフィックを検知している。該当する時期に、各ウェブサイトが閲覧不能になる状況が発生しており(図 21) これらのウェブサイトに対する攻撃に SYN flood が利用されたことが分かる。

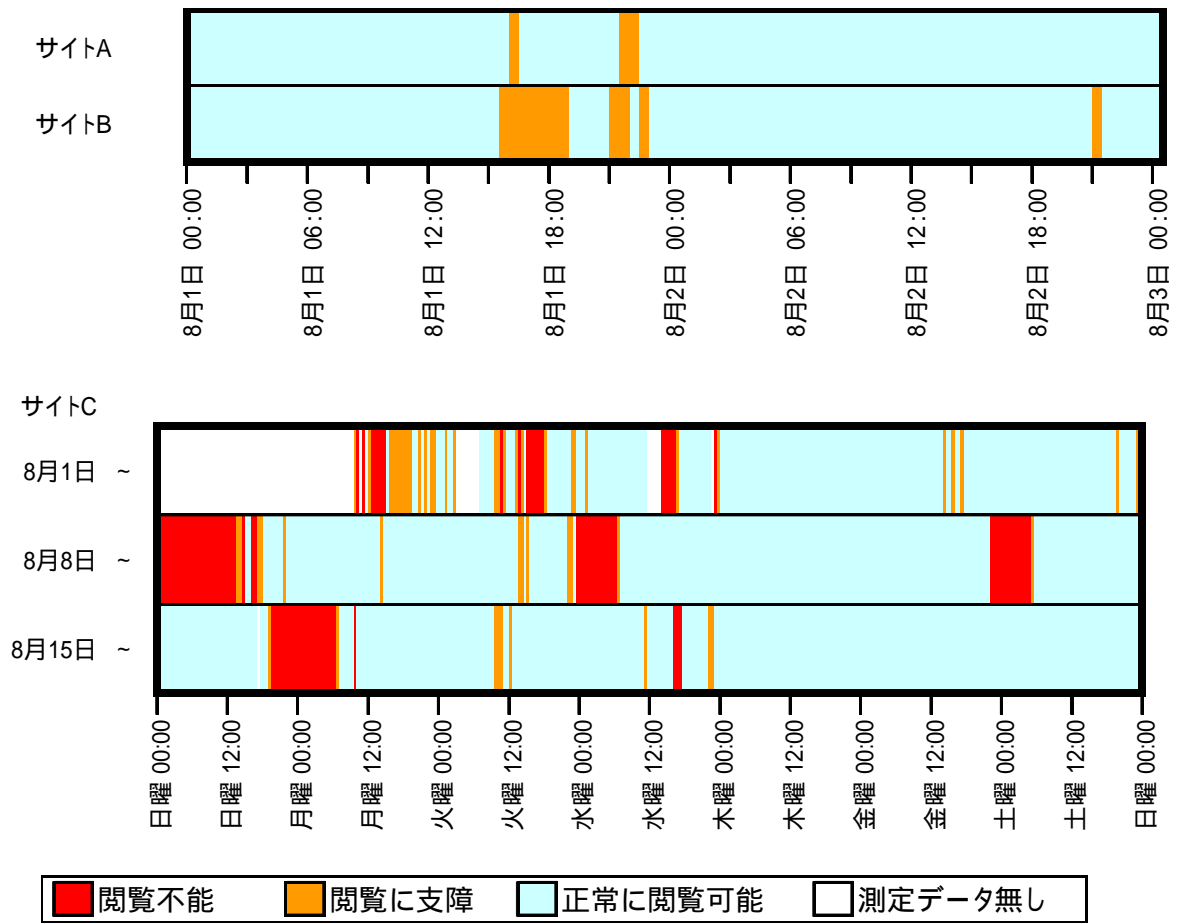


図 21 跳ね返りパケットを検知し、
同時期に閲覧状況が悪化していたウェブサイトの動作状況^{2,3,4}

² 閲覧不能・閲覧に支障となる原因は、SYN flood 攻撃によるものとは限らない。

³ 15 秒以内に関覧できなかった場合を閲覧失敗とし、複数回の閲覧試行の内、閲覧失敗の割合が 1 割以上で「閲覧に支障」、1/3 以上で「閲覧不能」と分類した。

⁴ 図中の全ての期間で監視を行っていたわけではないため、測定データの無い期間が存在する。

5. おわりに

警察庁では、インターネット定点観測で収集している情報を利用し、SYN flood 攻撃の第三者による検知を目指して、2004年7月から試験観測を開始した。8月に発生した日本の各省庁のウェブサイトに対する攻撃も検知しており、10月25日以降、正式に「SYN flood 被害観測システム」として利用することとしている。

中華人民共和国及びアメリカ合衆国に関しては、数多くのパケットを検知しているが、関係各国のインターネット治安情勢について、更なる分析を行うとともに、法執行機関等への情報提供についても推進していく予定である。

また、本レポートで述べた SYN flood 攻撃の他、UDP flood 攻撃等にも対応するよう本被害観測システムを拡張中であり、これについても新たな情報が判明次第、レポートを予定している。

参考

- ・ @police 「DoS/DDoS 対策について」
http://www.cyberpolice.go.jp/server/rd_env/pdf/DDoS_Inspection.pdf
- ・ @police 「DoS/DDoS 対策について (検証)」
http://www.cyberpolice.go.jp/server/rd_env/pdf/DDoS_Inspection_2.pdf

本レポートには、エイチツーソフト (Tel:0422-28-5212 Fax:0422-28-5211) 製、「マスタークリップ」のクリップアートを使用しています。