Vol.2011-IOT-12 No.41
2011/3/1

Quagga を用いた scan 攻撃の遮断について

熊谷悠平[†]　有馬竜昭[†]
永山聖希[††]　藤原健志[††]　吉田和幸[†††]

scan 攻撃とは、ネットワークを介した攻撃において、攻撃者がネットワークに接続されたサーバや PC の IP アドレスや提供しているサービスの情報を収集する行為のことである。攻撃者は scan 攻撃実行後に DoS(Denial of Service)攻撃を始めとした破壊行為を行う。我々はこれ注目し、scan 攻撃を遮断することにより攻撃者の情報収集を妨害し、その後行われる攻撃を防ぐことができると考えた。本論文では、Quagga を用いた scan 攻撃遮断システムの概要について述べ、利点と欠点を示した後、実際の運用で得られたログの詳細について述べる。

Blocking scan attacks using Quagga

Yuhei Kumagai[†] Tatsuaki Arima[†]
Toshiki Nagayama[††] Takeshi Fujiwara[††] Kazuyuki Yoshida[†††]

The scan attack, in attacks over the network, is that the improper act of gathering information about connecting to a network server or PC's IP addresses or provided service in network attack. Attackers do DoS (Denial of Service) attacks and some sabotage after the scan attack. We would like to disturb information collecting action from attackers by blocking the scan attack, then subsequent attacks made by them can be prevented. In this paper, we described a summary of the Quagga system for scan attack interception, and showing the advantages and disadvantages of this method, lastly discuss and analyze the log information obtained in actual operation.

1. はじめに

ネットワークを介した攻撃の際、攻撃者はセキュリティホールが残っているホストや、サービスを調べるために scan 攻撃を行うことが多く、この攻撃が後を絶たない。大分大学においても、不正侵入検知装置に多くの警告が記録されている。scan 攻撃によりこれらの情報が攻撃者に伝わると、対象のホストが攻撃にさらされる危険がある。また、サーバを踏み台として利用され、他のホストへの攻撃の中継や spam メールの中継、フィッシング詐欺へ利用される危険などもある。このため、scan 攻撃を検知・遮断することがその後の攻撃を防ぐ上で重要である。本研究室では scan 攻撃を検知・遮断するシステムの開発し、大学内で運用を行っていた。このシステムでは、攻撃者の IP アドレスを LAN スイッチに登録し外部からのパケットを遮断することを計画していた。しかし、この方法の場合 1 つの LAN スイッチに負担が集中し、通信速度の低下が発生する可能性がある。また、使用する LAN スイッチにより IP アドレスの登録可能数や命令文の形式などに違いがあり、機種依存性が高くなると考えられる。

そこで、scan 攻撃者に情報を与えないことと機種依存性の解決を目的として Quagga[1]を用いた攻撃遮断システムを開発した。このシステムでは学内から攻撃者に送信されるパケットを遮断し、攻撃者にホストやサービスの情報を与えないことで scan 攻撃を妨害する。このシステムを実現するために Quagga のルーティング機能を利用している。

本論文では、Quagga を用いた検知・遮断システムの構成について説明し、本システムの利点と欠点、検知システムの運用結果について述べる。

2. 関連研究

scan 攻撃への対策ソフトには、IDS(Intrusion Detection System)である snort[2]や BroIDS[3]が挙げられる。

snort はプリプロセッサにより scan 攻撃の検知を行っている。ステルススキャンと呼ばれる TCP の 3-way ハンドシェイクを確立させないことで、攻撃対象にログを残さない方式の scan 攻撃も検知可能である。しかし、検知基準は「一定時間あたりのコネ

[†] 大分大学　工学部　知能情報システム工学科
Department of Computer Science and Intelligent Systems, Faculty of Engineering, Oita University
[††] 大分大学大学院　工学研究科　知能情報システム工学専攻
Computer Science and Intelligent Systems, Graduate School of Engineering, Oita University
[†††] 大分大学　学術情報拠点　情報基盤センター
Center for Academic Information and Library Services, Oita University

クション要求回数」のみであるため、送信間隔を長くすることで容易に回避される。また、web クローラやプロキシを使用した通信などはアクセス回数が多くなってしまい、閾値を超えることが多く、誤検知されることもある。

一方 BroIDS はコネクション状況を監視し、送信されたパケットに対する ACK パケットがないものやエラーが返ったものの数を計測する。送信元の ACK パケットなしの回数やエラー数の合計が閾値を超えた場合、その送信元を scan 攻撃の送信元と判断する。これにより、snort と比較してご検知が少ない。しかし、この方法も送信元 IP アドレスを偽装した攻撃に対しては送信元を誤検知する可能性がある。

3. 検知システムの概要

Scan 攻撃検知システム（以後、本システム）は Ruby で記述されている。本システムは本研究室でこれまで開発されていたシステム[4]（以後、旧システム）の検知アルゴリズムを踏襲して新規に作成した。scan 攻撃には TCP を用いた物、UDP を用いた物などがあり、TCP を用いたものには以下の物が挙げられる。

- TCP スキャン: 3-way ハンドシェイクを利用した探索。
- SYN スキャン: 送信先ホストからの SYN/ACK パケットによりホストを探索。
- FIN スキャン: FIN パケットを送り、ポートの使用状況を探索。
- NULL スキャン: TCP フラグを全て 0 に設定したパケットを送る探索手法。
- クリスマスツリースキャン: FIN/URG/PSH のフラグを 1 に設定したパケットを送信する。

本システムではこの中でも TCP スキャンと SYN スキャンを検知・遮断することを目的としている。それ以外の scan 攻撃は TCP フラグの状態が異常であることや、TCP コネクションが不成立であるにも関わらず FIN パケットが送信されるなどの特徴があるため、本学で使用しているファイアウォールにより遮断可能である。

加えて、旧システムからの変更点として、一定条件により送信元登録リストからの削除機能、遮断対象からの解除機能を追加した。

3-1. システム構成

本システムの構成を図 3.1 に示す。

本システムは、検知システムと Quagga デーモンの二つから構成される。攻撃者の検知は検知システムで行い、攻撃者へのパケットの遮断は Quagga で行う。これらを稼動させるサーバは学内ネットワーク内に設置され、検知システムはファイアウォールの外側に設置された外部 LAN スイッチから、通過するパケットの複製を受け取る。ファイアウォールの外側からパケットを取得しているので、ファイアウォールで遮断されているパケットも収集していることから、ファイアウォールで遮断されるポートへの攻撃も検知可能である。検知システムはここで収集されたパケットから攻撃者を検知し、攻撃者へのパケットを Quagga の Blackhole インタフェースにルーティングするように静的経路登録する。

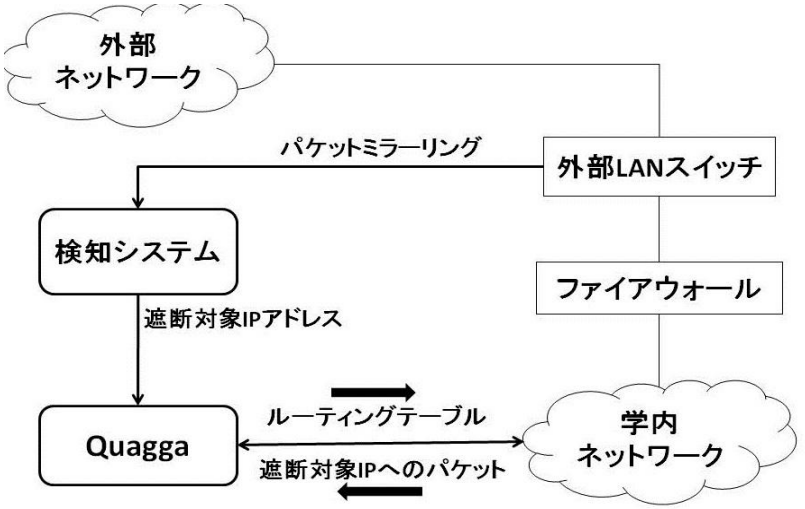

図 3.1 scan 攻撃検知システムネットワーク構成

Quagga では OSPF デーモンが稼動しており、学内の他のルータと経路情報を交換している。これに攻撃者の IP アドレスを Blackhole へ経路づけする情報を追加することで攻撃者へのパケットが外部へ送信されず、Quagga 稼働サーバへ送信されるようになる。このパケットを破棄することで、学内ネットワークから外部へでていくことがなくなりパケットを遮断できる。これについては 3-3 で詳しく述べる。

検知システムは『取得部』『分別部』『送信元登録部』『遮断対象登録部』『検知・削除部』『解除部』の 6 つのサブシステムから成り立っている。その内部を図示したものが図 3.2 である。

以下では、それぞれの構成部分の解説を行う。

- **取得部**

取得部では外部 LAN スイッチのポートミラーリングを用いて通過パケットのミラーリングを行っている。パケットの取得には Ruby/Pcap[5]を用いて行っており、取得するパケットは外部からの SYN パケットと学内からの SYN/ACK パケットに限定している。また、それぞれのパケットの内８０番や４４３番といった、誤検知の可能性が高いポートへのパケットに関しては取得対象から除外している。

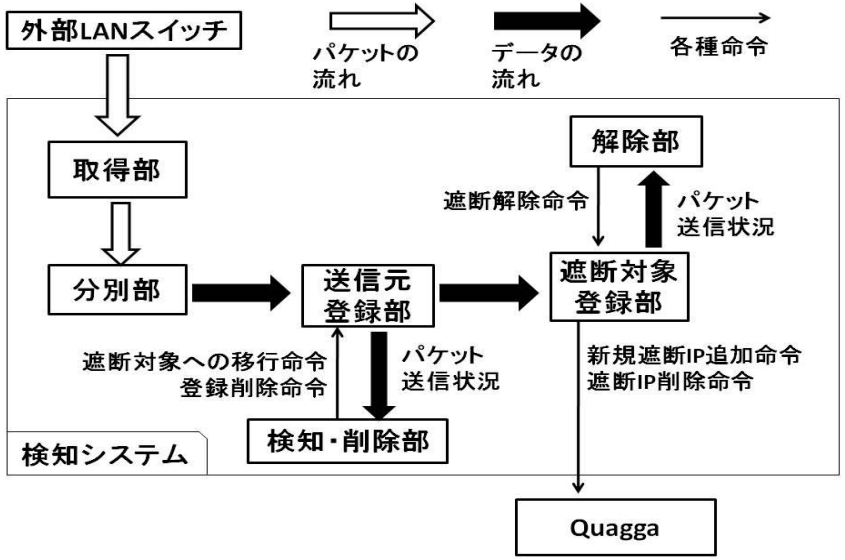

図 3.2　検知システム内部構成

- **分別部**

分別部では取得部から受け取ったパケットから必要となる以下のデータを抽出し、構造体に格納する。

- ソース IP アドレス
- ソースポート番号
- ディスティネーション IP アドレス
- ディスティネーションポート番号
- TCP フラグビット

この構造体のうち、外部からのものは送信元登録部へ送られ、送信元登録用のハッシュに登録される。学内からのものは送信元登録ハッシュの該当する宛先 IP アドレスの構造体に応答があったとして記録する。

- **送信元登録部**

送信元登録部では分別部から受け取った外部送信元の構造体を送信元リストに保存する。また、検知・削除部から遮断対象へ移行する命令があった場合は遮断対象登録部へ該当 IP アドレスの構造体を送信し、登録削除命令があった場合は該当する構造体を削除する。

- **遮断対象登録部**

遮断対象登録部では送信元登録部より送信された構造体を遮断対象リストに保存する。登録された構造体の送信元 IP を遮断対象 IP として Quagga に通知、登録する。また、解除部から遮断解除命令があった場合は、該当 IP アドレスの構造体をハッシュから削除し、Quagga のルーティングテーブルからも削除する。

- **検知・削除部**

検知・削除部は一定間隔で動作し、起動すると送信元リストのデータを取得する。リストに登録された送信元の中で、表 3.1 で述べる検知基準に該当するものを攻撃者として遮断するよう送信元登録部へ命令を出す。また、１時間以上新規の送信がないものはリストから削除させる。

- **解除部**

解除部は一定間隔で動作し、起動すると遮断対象リストのデータを取得する。リストに登録された遮断対象の中で、１時間以上新規の送信がないものは遮断を解除するよう遮断対象登録部へ命令する。

表 3.1　攻撃者の検知基準と詳細

・検知基準	・基準の詳細
コネクション確立の監視	５回以上 SYN パケットに対する SYN/ACK パケットが返されなかった通信を行った送信元 IP アドレスを遮断対象とする。
一定時間当たりの SYN パケット数	１秒間あたりの SYN パケット送信数が、１０を超える送信元 IP アドレスを遮断対象とする。

上記の表は旧システム[5]の基準に準拠している。

3-3.　Quagga を用いた応答パケットの遮断

本システムにおける遮断は、ルータのルーティング機能を利用して行う。LAN 内部に Quagga を用意し、他のルータとダイナミックルーティングを行えるようにして、Quagga に Blackhole インタフェースへのスタティックルーティングに攻撃者の IP アドレスを設定し、この経路を公開することで Quagga の稼働サーバへ攻撃者への応答パケットがルーティングされる。このパケットを破棄させることで、外部ネットワークへ応答パケットが出て行くことがなくなり、攻撃者は応答パケットを取得することが不可能となる。

4.　Quagga を用いる利点と欠点

4-1.　利点

遮断機能の中心である Quagga はルータとして機能するので、ネットワークのどこに設置してもよいからネットワーク構成の変更が不要である。

前述の理由により、ネットワーク構成の重要箇所にサーバを設置する必要がないの

で、システムトラブルの際に強制停止させてもネットワークへ影響を与えない。
Quagga が動作する環境があれば良いのでハードウェアのコストが低い。
機種依存性が低い。

4-2. 欠点

常に Quagga のルーティングテーブルを更新し、OSPF で学内のルータとテーブルを更新する必要が有るため、他のルータや L3 スイッチへの負担が増加する可能性がある。
攻撃者への応答パケットの遮断を目的としているので、DoS 攻撃やウィルスの送信など応答を必要としない攻撃には対応できない。

5. 検知システムの運用結果

これまでに述べたシステムの、遮断を含まない検知システムの運用結果を以下で述べる。運用期間は２０１０年１２月１６日～２０１０年１月１日までの１７日間である。この中で、１２月１８日～１２月２４日までの１週間と１２月２５日～１２月３１日の一週間のログを比較対象として使用する。

5.1 ２４時間の運用状況の詳細

以下では１日のログの詳細について述べる。
１８日土曜日のログは以下のようになっている。

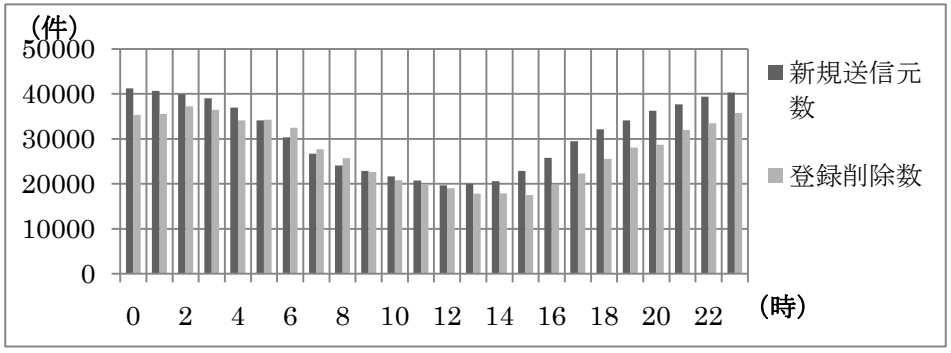

図 5.1 １８日の新規送信元登録数と登録削除数の状況

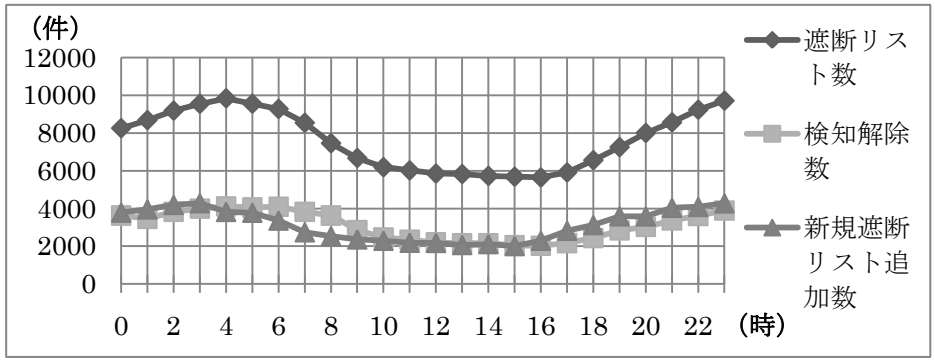

図 5.2 １８日の各時間の検知状況

まず､図 5.1 では１８日の各時間に送信元登録リストに追加された IP アドレス数と、同じリストから削除された IP アドレス数の量を示している。これによると、０時をピークとし新規送信元の追加量は減少を始め、１２時に最小を記録している。そこから増加へ転じ、２３時には０時とほぼ同じ量まで戻っている。また、登録削除数は各時間の新規送信元数の約８割以上に当たる量が削除されていると記録されている。登録削除の機能は､対象となる送信元からの SYN パケットが１時間以上送信されないことが条件であるので、実際に削除されている送信元はその１時間以上前に新規登録されたものである。１時間前の送新規送信元数と削除数を比較しても８割以上が削除されている事がわかる。０時から１２時の間では同一の時間において、新規登録数を削除数が上回っている。
次に図 5.2 では、各時間の始めに遮断リストに登録されている数と、各時間ごとの検知解除数、新規に遮断リストに追加された数を示している。遮断リスト数は０時から増加を始め、４時でピークに達した後減少に移り、１６時から再び増加している。検知解除数とリスト追加数もほぼそれと同じ形をしている。解除数がリスト追加数に遅れて減少しているのは、検知解除まで１時間以上の送信が無いことが必要だからである。図 5.1 と比較すると､増加と減少が新規送信元数に比例していることがわかる。

１８日以外の３１日までの全ての日において、上記のグラフの形状は同じであったため、件数の差はあっても曜日ごとに違いは無いと考えられる。
０時周辺で攻撃が増加する理由は、攻撃元が海外の PC からの攻撃が多いからではないかと考える。scan 攻撃の多くは、攻撃者本人が行うものではなく、BOT に感染した PC が自動的に行っているものが多い。この BOT に感染した PC をユーザが起動することで scan 攻撃が開始され、シャットダウンすることで停止する。また、PC の総

数は日本や中国、韓国などの極東地域よりも、アメリカやヨーロッパのほうが格段に多い。加えて、ニューヨークとの時差は－１４時間、ロンドンでは－９時間、これらより東にあるモスクワで－６時間である。新規送信元と遮断リスト追加数の増加が始まる時間が約１４時であるのでモスクワが８時の時であり、ピークとなる０時（２４時）ではアメリカで１０時である。以上より、PC の台数が多いヨーロッパやアメリカが朝を迎えていくのに合わせて新規送信元と攻撃者数が増えていることが明らかである。

5.2 １週間ごとの詳細

続いて１週間ごとの遮断対象リスト追加数と遮断リスト削除数、新規送信元登録数と登録削除数の推移について述べる。

まず、１２月１８日～１２月２４日までのログは以下のとおりである。

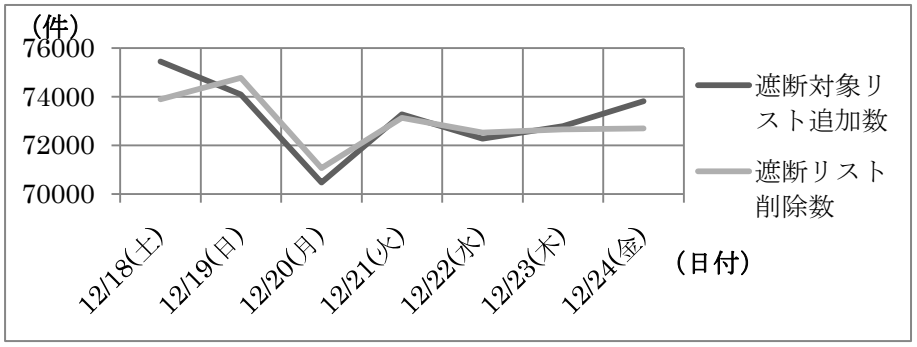

図 5.3 １８日～２４日の検知リストへの追数と削除件数

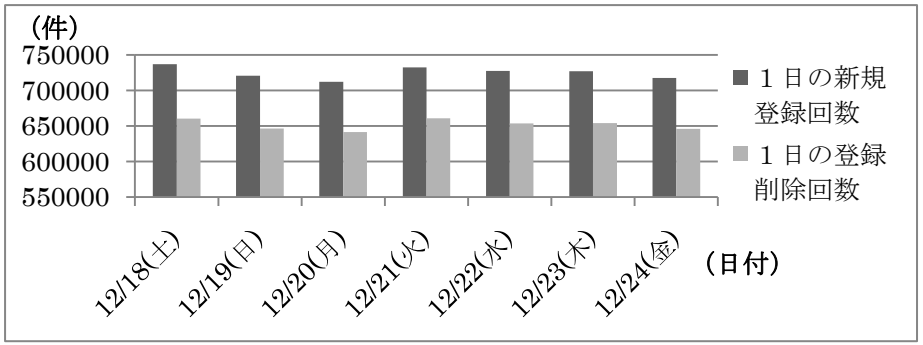

図 5.4 １８日～２４日の送信元リストへの登録と削除件数

図 5.3 では１日に行われた遮断対象リストへの追加回数とリストからの削除回数の合計の推移を示している。この中には同一の IP アドレスが１日の中で何度も追加と削除を繰り返したものも含まれている。図 5.4 では送信元登録リストの追加と削除の件数を示している。これも同様に、同一の送信元が何度も追加と削除を繰り返したものも含まれている。

次に、２５日～３１日のログを示す。図 5.5 と図 5.6 を比較して分かることは、各日の差が少ないながらも１日の新規登録回数が多くなると検知数も増加し、登録回数が減ると検知数も減少しているということである。また、各日の遮断リストからの削除数は登録数とほぼ一致している。これは 5.1 で述べたように、深夜から早朝に行われる scan 攻撃が収束し削除されることと、午後から夜にかけて scan 攻撃が増加し追加される IP アドレスが増えることが理由であると考えられる。この相関は１８日～２５日のログにも言える。また、ここにはグラフを示すことができなかったが、学外から送信される SYN パケット数とも検知数は関係しており、１２月２０日には他の日に比べ SYN パケットの送信数が減少しており、１２月３０日には増加している。図 5.3 と図 5.4 を見るとわかるように２０日は検知数、削除数とも減少しており、３０日には増加している。図 5.3 と図 5.5 を比較すると、その推移には共通性が見られず、また図 5.4 と図 5.6 の間でも目立った共通性は見られない。週ごとに攻撃数の推移には違いがあると考えられる。これに関しては検証のためのデータが不足しているため、今後テストを繰り返し、データを蓄積していく必要がある。

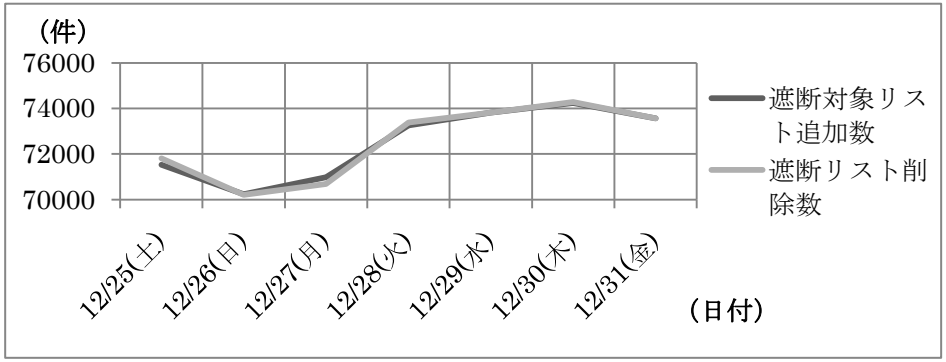

図 5.5 ２５日～３１日の検知リストへの追数と削除件数

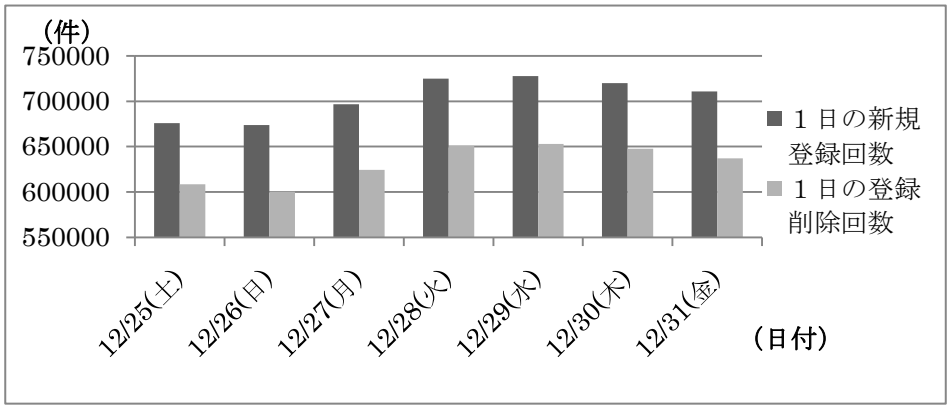

図 5.6　２５日～３１日の送信元リストへの登録と削除件数

5.3　攻撃対象の IP アドレス

攻撃対象となった IP アドレスには偏りが見られ、一部のアドレスに集中して scan 攻撃が行われていた。

１８日の被攻撃アドレスと攻撃回数のグラフと、攻撃数が上位のアドレスをそれぞれ図 5.7 と表 5.1 に示す。

6.　結論

本論文では Quagga を用いた scan 攻撃の遮断方法とそのシステムに使用する検知システムの運用結果について述べた。本研究の目的として、Quagga を用いることで LAN スイッチへの負荷を減らし、遮断解除を行うことでシステム自体の負担を軽減することができるのではないかと考え、実証用のシステムの開発を行っていた。検知システムを運用した結果、海外からと思われる scan 攻撃が大半であったこと、それにより scan 攻撃の多くは夜間に集中していることがわかった。一方、本論文で用いた２週間のログを比較しても１週間の攻撃やアクセス数の推移には規則性が見られなかった。しかし、これに関してはデータが不足しているためさらなる検証が必要である。加えて、scan 攻撃の対象となった IP アドレスは特定のアドレスが多く、局所化していることがわかった。

現段階においては Quagga を用いた遮断機能は完成していないため、その有効性の検証が行えていないが、図 5.2 に示した運用結果より最大で一万件の IP アドレスのルーティングが必要となることから、他のルータへ負担をかける可能性が高いため、現在のシステムには何らかの対策が必要である。現在はファイアウォールの外側の LAN スイッチを通過するパケットにより検知を行っている。これをファイアウォールの内側の LAN スイッチを通過するパケットで検知するように変更することで負荷の軽減が図れると考えられる。

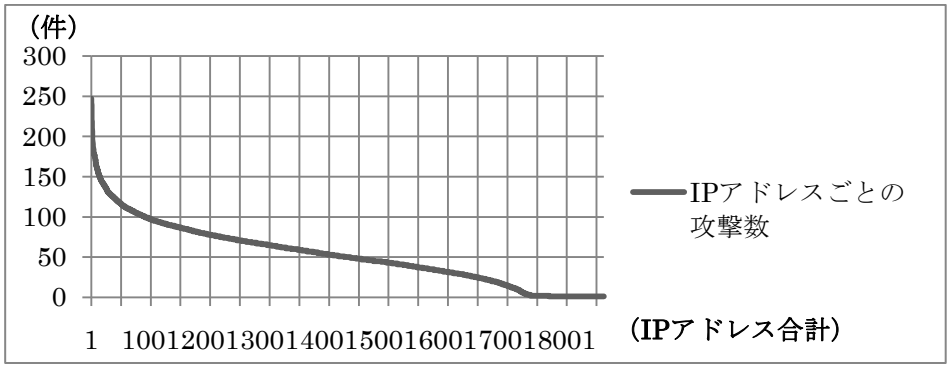

図 5.7　被攻撃アドレスと攻撃回数

表 5.1　攻撃数が上位の IP アドレス

順位	IP アドレス	順位	IP アドレス
1	133.37.a.1	6	133.37.e.6
2	133.37.b.19	7	133.37.f.109
3	133.37.c.117	8	133.37.g.29
4	133.37.d.33	9	133.37.h.24
5	133.37.e.40	10	133.37.g.96

参考文献

[1] Quagga Routing Suite : http://www.quagga.net/
[2] Snort : http://www.snort.org/
[3]BroIDS : http://www.bro-ids.org/
[4] 大塚贊治, 藤原健志, 吉田和幸 : “TCP コネクション確立の偽装とその計数による scan 攻撃検知システムとその運用について”, マルチメディア, 分散, 協調 とモバイル（DICOMO2009）シンポジウム pp.1285-1290, 2009.7
[5]Ruby/Pcap リファレンス: http://www.goto.info.waseda.ac.jp/~fukusima/ruby/pcap-j.html