Vol.2015-CSEC-69 No.16
Vol.2015-IOT-29 No.16
2015/5/21

ボットネットによるSSHパスワードクラッキング攻撃の検知のための予備調査

清水 光司[1,a)]　小刀稱 知哉[1,†1]　池部 実[2]　吉田 和幸[3]

概要：インターネットを利用した不正アクセスが多く存在する．その中でも，SSH サーバに対する不正アクセス行為の発生件数は依然として多い．そこで，我々は SSH へのパスワードクラッキング攻撃を検知することを目的として「SSH パスワードクラッキング攻撃検知システム（SCRAD）」を開発・運用してきた．本システムでは SSH サーバと送信元間の 1 コネクションあたりのパケット送受信回数からパスワードクラッキング攻撃の通信を判断している．SCRAD では，攻撃の通信を 10 回連続で観測した送信元を攻撃者として検知し，遮断する．しかし，運用結果を分析したところ，ボットネットからの攻撃を検知漏れしていた．ボットネットからの攻撃は，異なる IP アドレスから特定の SSH サーバに対して 1 回から 5 回程度仕掛けられるため，1 つの送信元 IP アドレスから連続 10 回攻撃を観測した送信元 IP アドレスを攻撃者として検知する SCRAD の検知基準では検知できなかった．そこで本論文では，ボットネットからの SSH パスワードクラッキング攻撃を分析し，その結果から攻撃を検知するための特徴を調査した．調査結果から，ボットネットからの攻撃には，短時間に異なる送信元 IP アドレスから，1 つの宛先 IP アドレスに対して 1 回から 5 回の攻撃する特徴が判明した．得られた特徴から，1 つの宛先 IP アドレスに対する送信元 IP アドレス数と，仕掛けた攻撃の回数により，ボットネットからの攻撃を検知する．

Preliminary investigation for detection of SSH password cracking attacks by botnet

Abstract: There are many malicious attacks in the Internet. In particular, there are many illegal accesses penetrates into SSH servers. So we have been developing a SSH Password Cracking Attack Detection system called SCRAD . Our system detects attacker's connection using the number of packets per connection between the SSH client and server. And,SCRAD denies the source IP address when repeating 10 times of the attacker's connection. However, we found some false negative in the SCRAD's log files. The cause of false negative is botnet. The harder attacks some SSH server from 1 to 5 times. Our system assumed to attack from one source. Therefore, SCRAD couldn't detect attacks from botnet. In this paper, we analyze the characteristics of SSH password cracking attacks from botnet. As a result, we found the three characteristics. The feature of attacks from botnet are to attack from 1 to 5 times to a destination IP address from several source IP address in short term. Therefore, we detect the attack from botnet using unique source IP addresses and attacker's connection to a destination IP address.

1. はじめに

インターネットの普及に伴い，我々はネットワークを通して様々な情報のやり取りをしている．そのため現在では，ネットワークは社会的基盤の 1 つとして生活に不可欠な存在である．しかし，ネットワークを利用した不正通信も数多く存在する．IBM が発表した 2014 年上半期 Tokyo SOC 情報分析レポート [1] では，Web サイト改ざんの原因の 1 つとして，Web サーバ管理のために利用する SSH や

[1] 大分大学大学院工学研究科知能情報システム工学専攻
Course of Computer Science and Intelligent Systems, Graduate School of Engineering, Oita University
[2] 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
[3] 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
[†1] 現在，三菱電機株式会社
[a)] v15e3014@oita-u.ac.jp

FTP サービスのアカウントを不正利用された事例が報告されている．また，我々の先行研究において開発した scan 攻撃や DoS 攻撃を検知する「不正通信検知システム」[2] の運用結果から，22 番ポート（SSH）に対する攻撃が多いことが判明している．大分大学では，インターネットから学内への 22 番ポートに対する通信は一部のサブネットをファイアウォールにより遮断，その他のサブネットに関してはユーザの利便性を優先して遮断していない．そのため SSH サーバに対するパスワードクラッキング攻撃を多く観測しており，SSH に対する攻撃の監視は重要である．

また，ボットに感染したホストが自組織内から組織外へパスワードクラッキング攻撃を仕掛ける場合も考えられる．よって，組織内・外に存在する攻撃者を検知することが必要となる．そこで我々は，SSH へのパスワードクラッキング攻撃を検知し，遮断することを目的とした「SSH パスワードクラッキング攻撃検知システム (SCRAD)」[3] を開発・運用してきた．SCRAD は送信元 IP アドレスと SSH サーバ間で送受信する 1 コネクションあたりのパケット数を用いて攻撃のコネクションを判断する．SCRAD では，攻撃の通信を 10 回連続で観測した送信元を攻撃者として検知し，遮断する．

SCRAD の運用結果を分析したところ，2014 年 7 月において複数の異なる送信元 IP アドレスから 1 つの宛先 IP アドレスに対して，1 回から 5 回の攻撃のコネクションを観測した．これは，正規ユーザにおいても生じる可能性のある挙動である．しかし，この挙動を 30 分間の短時間に計 22 個の宛先 IP アドレスにおいて観測した．このような挙動は正規ユーザの挙動とは考えにくく，攻撃と考えられる．SCRAD では，この攻撃を検知できておらず，攻撃の検知漏れが生じていた．このように複数の異なる送信元が 1 つの宛先 IP アドレスを攻撃する挙動は，ボットネットからの攻撃と推測できる．SCRAD の送信元 IP アドレスにもとづく検知手法では，ボットネットからの攻撃の場合は 1 つの送信元からの FAIL コネクション数が連続 10 回のしきい値に満たないため検知できないことがある．そこで本論文では，ボットネットからの攻撃を検知するための特徴を調査することを目的とする．

以下に本論文の構成を示す．2 章では，ボットネットからの攻撃の検知に関する研究について述べる．3 章では，SCRAD について述べる．4 章では，ボットネットからの攻撃を調査する．5 章では，まとめと今後の課題について述べる．

2. ボットネットからの攻撃検知の関連研究

ボットネットからの攻撃の検知に関する研究としては，Mobin らの手法 [4] が挙げられる．Mobin らの手法では，sshd の認証ログを入力として，複数の送信元から SSH サーバに対する攻撃を検知するシステムを提案している．本システムは，Aggregate Site Analyzer と Attack Participants Classifier の 2 つのコンポーネントから構成される．Aggregate Site Analyzer は，sshd の認証ログ全体からログイン試行の失敗回数により複数の送信元からの攻撃の可能性があるログと，単一の送信元からの攻撃ログに分類する．Attack Participants Classfier は，Aggregate Site Analyzer の出力結果と，過去に認証に成功した送信元 IP アドレスのログ，ブラックリストを入力として，送信元を正規ユーザと攻撃者に分類する．Attack Participants Classifier では，過去にログイン試行に成功した送信元を正規ユーザに分類する．ボットネットからの攻撃の場合には，ログイン試行するサーバやホストユーザ名やログイン試行回数の共通性を評価して，単一の送信元 IP アドレスによる攻撃と複数の送信元 IP アドレスによる攻撃を分類する．

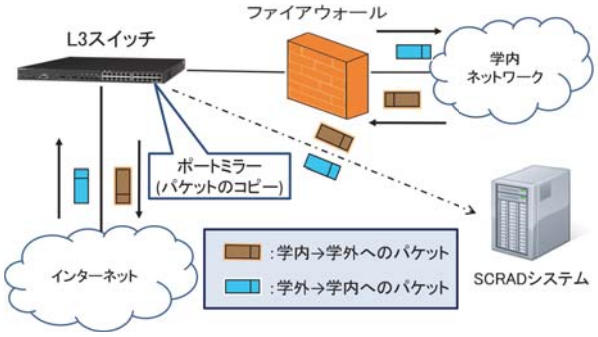


図 1: SCRAD システムの構成図

また，ボットネットからの攻撃の検知手法として，本多らの手法 [5] が挙げられる．本多らは，宛先 IP アドレスと検知時刻を軸にネットワーク監視ログを散布図を用いて可視化した．この散布図においては，送信元 IP アドレスを判別できるように，送信元 IP アドレスごとに色や形を変えてプロットしている．この可視化結果から，複数の異なる送信元からの攻撃を複数の宛先 IP アドレスにおいて発見した．さらに，複数の異なる送信元 IP アドレスによる攻撃を分析することで，ログイン試行回数が従来の攻撃よりも少ない特徴，攻撃者が IP アドレスを使い捨てる特徴を発見した．これらの特徴を用いて，宛先 IP アドレスごとの送信元 IP アドレス，検知時刻，ログイン試行回数から，相関の高い宛先がある場合，同じボットから攻撃を受けているものと判断し，被害を受けている宛先 IP アドレスを抽出する手法を提案している．

3. SCRAD システム

3.1 SCRAD の概要

SCRAD は，インターネットと学内ネットワークの双方向のパケットから 22 番ポートに関するパケットを tcpdump のフィルタ機能を用いて抽出する（図 1）．各コネクションの確立から終了までのパケット送受信回数を計数する．さらに送信元ごとにパケット送受信回数の少ないコネクショ

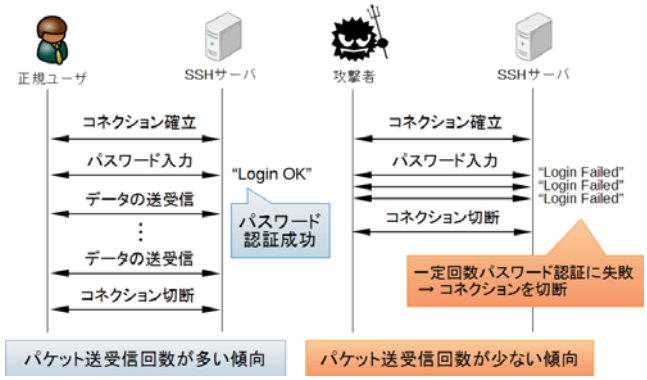


図 2: 攻撃者と正規ユーザにおける 1 コネクションあたりのパケット数の違い

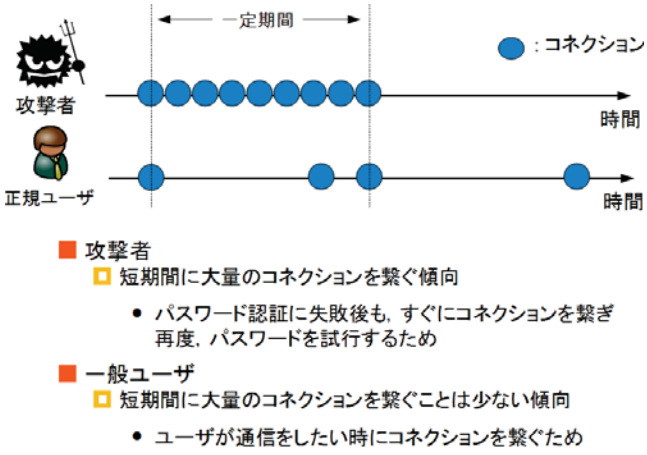


図 3: 攻撃者と正規ユーザにおけるコネクション接続回数の違い

ンを計数することで，パスワードクラッキング攻撃を検知する．SCRAD は，インターネットと学内ネットワークの間を流れる双方向のミラーパケットを入力とするため，送信元が学内外のどちらの場合でもリアルタイムにパスワードクラッキング攻撃を検知できる．

3.2 1 コネクションあたりのパケット数の違い

SCRAD は，攻撃者と正規ユーザにおける 2 つの挙動の違いに着目し，攻撃を検知する．この 2 つの挙動の違いについて説明する．

まず，SSH サーバと通信する 2 種類のユーザについて説明する．本論文では 1 ユーザは，SSH クライアントを意味する．正規ユーザは，SSH サーバにて正規の ID のパスワード認証されるユーザである．攻撃者は，不正侵入を試みるユーザである．

正規ユーザのコネクションと攻撃者のコネクションにおけるパケット数の違いを図 2 に示す．正規ユーザと SSH サーバの通信は，ユーザ認証プロセスによりユーザを認証した後にデータの送受信が発生する．よって，1 コネクションあたりのパケット送受信回数が多い傾向にある．

一方，攻撃者と SSH サーバの通信は，ブルートフォース攻撃や辞書攻撃によって何度もユーザ認証プロセスを繰り返す．一定回数（通常は 3 回）パスワード認証に失敗した場合，TCP コネクションは切断される．攻撃者の通信において，正規ユーザの通信にあるデータの送受信は生じないため，1 コネクションあたりのパケット送受信回数は少ない傾向にある．

正規ユーザと攻撃者におけるコネクション接続回数の違いを図 3 を示す．正規ユーザの場合，任意のタイミングでコネクションを接続し，データを送受信する．短期間に大量のコネクションを繋ぐことは少ない．一方，攻撃者は，一定回数パスワード認証に失敗し，コネクションが切断された後，即座にコネクションを接続し，再びパスワード認証を試行する．よって短期間に大量のコネクションを繋ぐ傾向にある．

SCRAD は，これらの正規ユーザと攻撃者の 1 コネクションあたりのパケット数の傾向の違いを攻撃者の検知の基準として用いる．

3.3 攻撃検知基準

我々の先行研究 [3] より，SSH パスワードクラッキング攻撃を検知するためのしきい値は 1 コネクションあたりのパケット送受信回数において 50 パケット未満と定義した．SCRAD システムにおいて，1 コネクションあたりのパケット送受信回数とは，送信元の SYN パケットを観測後，送信元と SSH サーバ間で最初の FIN パケットまたは RST パケットを観測するまでのパケット数である．先行研究 [3][6] により，パケット数の計数からデータサイズ 0 の TCP パケットと再送パケットを除外している．パケット送受信回数がしきい値（50 パケット）未満のコネクションを FAIL コネクション，しきい値以上のコネクションを SUCCESS コネクションと定義する．誤検知を考慮して，10 回連続で FAIL コネクションを観測した送信元を攻撃者として検知する．

3.4 検知手法の問題点

1 章で述べたように，SCRAD は 2014 年 7 月において，攻撃を検知漏れしていた．SCRAD が正規ユーザと判断した送信元 IP アドレスの中から，検知漏れした送信元 IP アドレスを抽出して調査するため，SCRAD の検知基準とは異なる基準で，すべての送信元 IP アドレスを分類した．2014 年 7 月 1 日から 2014 年 7 月 31 日の期間に図 1 の L3 スイッチから収集したパケットデータを用いて，正規ユーザ・攻撃者・不明なユーザの 3 つに分類した．分類した送信元をそれぞれの送信元における真の値と定義する．送信元の分類方法を以下に示す．

- 正規ユーザ
  パケット送受信回数が 100 パケット以上のコネクショ

表 1: 2014 年 7 月における真の値

(a) SSH クライアント

クライアントの種類	真の値	全体に対する割合
正規ユーザ	63 件	16.3%
攻撃者	172 件	44.6%
不明なユーザ	150 件	38.9%
合計	385 件	100%

(b) SSH コネクション

通信の種類	真の値	全体に対する割合
正規ユーザによるコネクション	803 件	13.8%
攻撃者によるコネクション	4,821 件	83.0%
不明なユーザによるコネクション	180 件	0.3%
合計	5,804 件	100%

```
20 72.9.86.203 -> 133.37.A.B 2014 07/06 4:41:55
20 70.176.48.241 -> 133.37.A.B 2014 07/06 4:41:59
21 178.140.67.11 -> 133.37.A.B 2014 07/06 4:42:07
20 122.166.145.12 -> 133.37.A.B 2014 07/06 4:42:18
20 212.164.161.121 -> 133.37.A.B 2014 07/06 4:42:23
21 212.164.88.140 -> 133.37.C.D 2014 07/06 5:06:40
20 93.95.103.177 -> 133.37.C.D 2014 07/06 5:06:43
21 178.140.83.62 -> 133.37.C.D 2014 07/06 5:06:48
19 217.20.17.253 -> 133.37.C.D 2014 07/06 5:06:54
20 69.71.163.58 -> 133.37.C.D 2014 07/06 5:06:58
```

図 4: 不明なユーザによる FAIL コネクションの SCRAD システムにおける FAIL ログ

ンを 1 回以上観測した送信元

- 不明なユーザ
  パケット送受信回数が 100 パケット以上のコネクションを 1 回も観測しなかった送信元であり，かつ検知したコネクション数が 3 回以下である送信元
- 攻撃者
  正規ユーザ，不明なユーザ以外の送信元

正規ユーザは，1 コネクションあたりのパケット数が 100 パケット以上のコネクションを 1 回以上観測した送信元である．これまでの SCRAD の運用結果により，100 パケット以上のコネクションの場合は，パスワードクラッキング攻撃の通信ではないことが判明している．よって上記の挙動を示す送信元は正規ユーザと定義した．不明なユーザとは，パケット送受信回数 100 パケット以上のコネクションを 1 回も観測せず，かつ観測したコネクション数が 3 回以下の送信元である．このような送信元は，攻撃者の挙動がなく，かつ正規ユーザと断定できない送信元である．不明なユーザには，何らかの理由でパスワードの紛失でログイン認証に失敗し，そのままその送信元 IP アドレスからのログインを諦めた正規ユーザと，SCRAD システムにおける送信元にもとづく検知手法では判断できない攻撃者の 2 種類のユーザの存在が考えられる．よって上記の送信元を不明なユーザと定義した．攻撃者は，パケット送受信回数 100 パケット以上のコネクションを 1 回も観測せず，かつ観測したコネクション数が 4 回以上の送信元である．

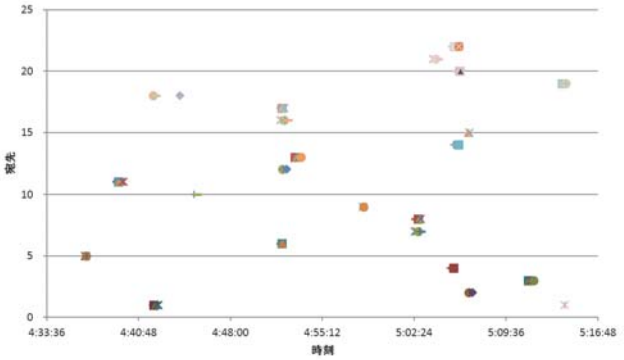


図 5: 2014 年 7 月におけるボットネットからの攻撃のコネクション

2014 年 7 月における真の値の調査結果を表 1 に示す．これまでの月ごとにおける真の値ではクライアント数全体に対して不明なユーザを 15〜20%観測してきた．しかし，表 1(a) より，2014 年 7 月の真の値においては，全体の 37%の不明なユーザに分類された．そこで，2014 年 7 月に観測した 180 件の不明なユーザによるコネクションについて分析した．

SCRAD のログから，2014 年 7 月 6 日のある 30 分間の不明なユーザによるコネクションの一部を図 4 に示す．ログの数値は左から，パケット送受信回数，送信元 IP アドレス，宛先 IP アドレス，パケット最終受信時刻を表している．図 4 より，短時間に異なる送信元から，1 つの宛先に対し 1 回から 5 回のコネクションを観測した．さらに，この挙動を 22 個の学内の SSH サーバにおいて観測した．これは正規ユーザによる挙動とは考えにくく，攻撃と考えられる．よって，SCRAD は攻撃を検知漏れしていたことになる．この攻撃は，同期間に異なる送信元 IP アドレスが攻撃していることから，ボットネットからの攻撃と考えられる．

4. ボットネットからの攻撃の調査

本章では，ボットネットからの攻撃を検知するための特徴を発見するため，ボットネットからの攻撃について分析する．また，2 章で述べた本多らの報告における特徴について着目し，調査する．

4.1 ボットネットからの攻撃の特徴の調査

2014 年 7 月 6 日に観測したボットネットと思われる SSH クライアントからの攻撃の各コネクションについて，縦軸を宛先 IP アドレス，横軸を検知時刻とした散布図を図 5

表 2: 宛先 IP アドレスごとの送信元 IP アドレス数

宛先 IP アドレス	FAIL コネクション数	送信元 IP アドレス数
宛先 1	5	5
宛先 2	5	5
宛先 3	5	5
宛先 4	5	5
宛先 5	5	5
宛先 6	5	5
宛先 7	5	5
宛先 8	5	5
宛先 9	2	2
宛先 10	3	3
宛先 11	5	5
宛先 12	5	5
宛先 13	5	5
宛先 14	5	5
宛先 15	2	2
宛先 16	5	5
宛先 17	5	4
宛先 18	5	5
宛先 19	5	5
宛先 20	5	5
宛先 21	5	5
宛先 22	5	5

に示す．この図に示したコネクションでは，各 SSH サーバに対して平均 26 秒，最長 35 秒の間隔で 2 回から 5 回の FAIL（ユーザ認証に失敗したと思われる）コネクションを観測した．また，図 5 に示された攻撃を 22 個の宛先 IP アドレスに分類した．宛先 IP アドレスごとの FAIL コネクション数，送信元 IP アドレス数を表 2 に示す．本多らの報告によると，ボットネットからの攻撃では，送信元 IP アドレスを使い捨てる傾向がある．表 2 より，2014 年 7 月に観測した攻撃において，22 個中 21 個の宛先で，送信元 IP アドレス数と FAIL コネクション数が等しいことから，それぞれの FAIL コネクションにおける送信元 IP アドレスはすべて異なる．また，表 2 におけるすべての 98 個の送信元 IP アドレスのうち，3 つの送信元 IP アドレスだけが重複していた．このことから，本多らの報告のように，IP アドレスを使い捨てて攻撃を仕掛けたと考えられる．よって，今回観測したボットネットからの攻撃の特徴としては，以下の 3 点が挙げられる．

(1) 短時間にコネクションを接続
(2) 1 つの送信元 IP アドレスからの FAIL コネクション数が SCRAD の想定する攻撃回数（連続 10 回）よりも少ない
(3) 1 つの宛先 IP アドレスに対して送信元が IP アドレスを使い捨ててコネクションを接続

SCRAD では，送信元 IP アドレスにもとづき攻撃者を検知し，遮断している．しかし，今回の調査結果から，ボットネットからの攻撃は IP アドレスを使い捨てて攻撃を仕掛けており，送信元にもとづく従来の検知では同一送信元からの FAIL コネクションがしきい値に到達せずボットネットからの攻撃を検知することが難しい．そこで，異なる送信元 IP アドレスから 1 つの宛先 IP アドレスに対してコネクションを接続する特徴に着目して，宛先 IP アドレスにもとづく検知が有効であるか検証する．

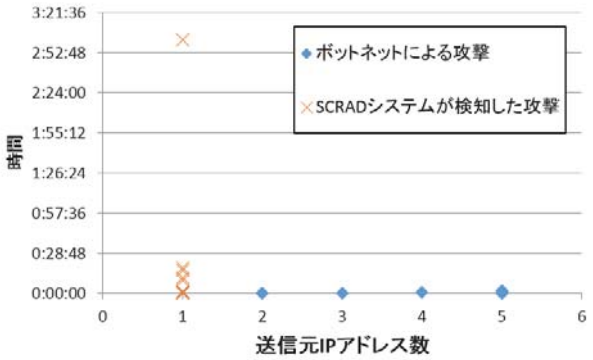
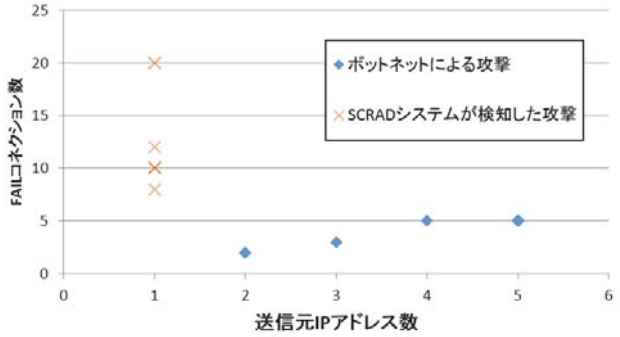


図 6: ボットネットの攻撃における時間と送信元 IP アドレス数の関係

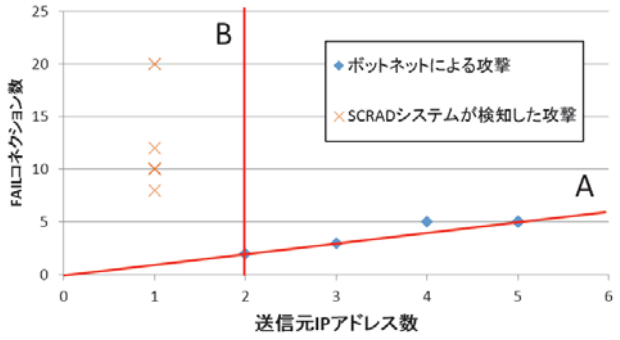
4.2 ボットネットからの攻撃の FAIL コネクション数と送信元 IP アドレス数の調査

4.1 節の調査で判明したボットネットからの攻撃の特徴を踏まえ，宛先 IP アドレスにもとづく検知のために必要な特徴量を調査する．まずは，SCRAD が検知した攻撃者による攻撃を受けた宛先 IP アドレスと，2014 年 7 月 6 日のある 30 分間にボットネットからの攻撃を受けた宛先 IP アドレスについて，縦軸を時間，横軸を送信元 IP アドレス数として図 6 に示す．縦軸に示す時間は，送信元 IP アドレスに関わらず，1 つの宛先 IP アドレスに対して最初に観測した FAIL コネクションの検知時刻と最後に観測した FAIL コネクションの検知時刻の差である．図 6 より，時間にもとづいてボットネットからの攻撃と，単一の送信元による攻撃を区別して検知することが可能である．しかし，攻撃の開始時刻と終了時刻を検知基準として用いる場合，リアルタイム検知において，どのコネクションを攻撃の開始，終了と判定するかが困難である．

次に，SCRAD システムが検知した攻撃者による攻撃を受けた宛先 IP アドレスと，2014 年 7 月 6 日のある 30 分間にボットネットから攻撃を受けた宛先 IP アドレスについて，縦軸を FAIL コネクション数，横軸を送信元 IP アドレス数として表した結果を図 7 に示す．図 7(a) より，ボットネットからの攻撃における送信元 IP アドレス数の最小値が 2 となっている（図 7(b)）．図 7(b) における 2 本の直線 A の上側，直線 B の右側にボットネットからの攻撃がすべて分布している．図 7(b) における 2 本の直線 A，B についてそれぞれ説明する．まず，直線 A について説明する．図 7(b) のグラフは，縦軸を FAIL コネクション数，横軸を送



(a) ボットネットからの攻撃における FAIL コネクション数と送信元 IP アドレス数の関係



(b) ボットネットからの攻撃における FAIL コネクション数と送信元 IP アドレス数の最小値

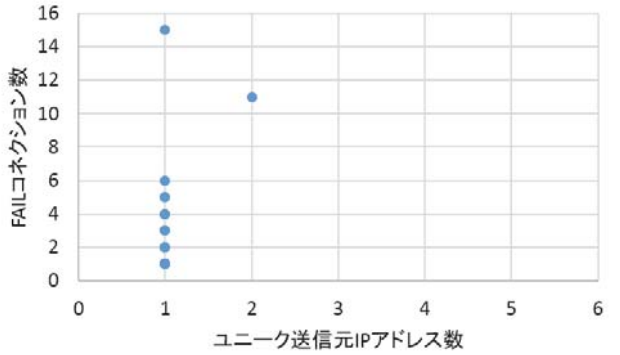
図 7: ボットネットの攻撃における FAIL コネクション数と送信元 IP アドレス数の関係

信元 IP アドレス数としている．この 2 つの数値において，

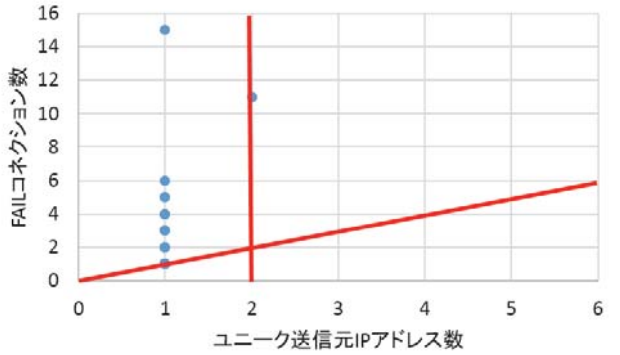
送信元 IP アドレス数 ≤ FAIL コネクション数

の関係が常に成り立つ．たとえば，2 つの異なる送信元 IP アドレスが攻撃した場合，最低でも 2 つの FAIL コネクションが存在する．よって，直線 A は FAIL コネクション数と送信元 IP アドレス数の関係から，自明で成り立つ直線となる．直線 A 上とその上側にボットネットからの攻撃が存在することになる．次に直線 B について説明する．送信元 IP アドレス数が 1 つの攻撃は，従来の SCRAD システムで検知可能である．よってボットネットからの攻撃として検知が必要な攻撃は，送信元 IP アドレス数が 2 以上となる直線 B 上とその右側の領域に存在している．

真の正規ユーザは，パケット送受信回数が 100 パケット以上のコネクションを 1 回以上観測した送信元である．このような真の正規ユーザのコネクションにおいても，パスワード入力ミスによる FAIL コネクションが存在する．そこで，正規ユーザの誤検知について調べるため，真の正規ユーザによる FAIL コネクションについても調査した．2014 年 7 月の 1 か月間に観測した真の正規ユーザ 63 件による FAIL コネクションについて，各宛先 IP アドレスにおける一日ごとの FAIL コネクション数と送信元 IP アドレス数の関係を図 8 に示す．図 8(a) に対して直線 A，B を引いた図を示す（図 8(b)）．図 8(b) より，正規ユーザによる FAIL コネクションにおいても，直線 A の上側，かつ直線 B の右側に存在することが判明した．この FAIL コネクションにおける送信元 IP アドレスは学内 IP アドレスである．よって，今回調査したボットネットからの攻撃の検知のための特徴量は，学外から学内へのボットネットからの攻撃を検知することは問題ない．学内から学外へのコネクションにおいては，学内の複数の送信元 IP アドレスが，同一の宛先 IP アドレスへコネクションを接続する場合がある．その場合，学内の複数の送信元 IP アドレスがパスワード入力ミスによるログイン認証失敗することで，今回調査したボットネットからの攻撃と類似した挙動となる．よって，学内から学外へのコネクションにおいて，正規ユーザによるコネクションを誤検知する可能性がある．この誤検知については，今後対応していく必要がある．



(a) 真の正規ユーザにおける FAIL コネクション数と送信元 IP アドレス数の関係



(b) 真の正規ユーザにおける FAIL コネクション数と送信元 IP アドレス数の最小値

図 8: 真の正規ユーザにおける FAIL コネクション数と送信元 IP アドレス数の関係

以上から，直線 A，B をしきい値とした場合，ボットネットから攻撃を受けている宛先 IP アドレスを検知できる．

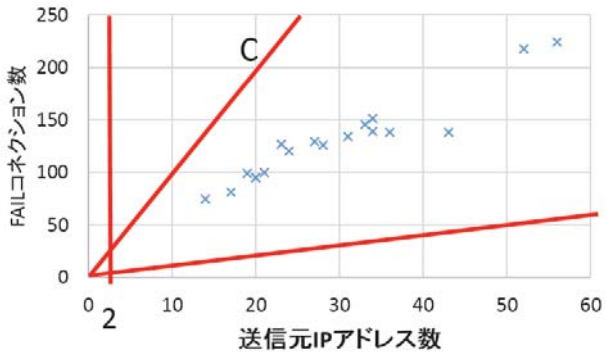


図 9: 2014 年 12 月のボットネットからの攻撃における送信元 IP アドレス数と FAIL コネクション数の関係

4.3 調査結果の検証

2014 年 7 月と同様に調査したところ，ボットネットからの攻撃を 2014 年 12 月にもボットネットの挙動と考えられる通信を観測した．12 月に観測した攻撃では，2 つの宛先 IP アドレスへの攻撃を 23 日から 31 日の 9 日間観測した．この攻撃は，2 つの宛先 IP アドレスにおける 9 日間の合計で，216 個の送信元 IP アドレスから，910 回の FAIL コネクションを観測した．216 個の送信元 IP アドレスのうち，10 個の送信元 IP アドレスを SCRAD で検知した．12 月 23 日から 31 日の期間に観測したボットネットからの攻撃を受けた 2 つの宛先 IP アドレスについて，縦軸を FAIL コネクション数，横軸を送信元 IP アドレス数とした散布図を図 9 に示す．ここでは，1 つの宛先 IP アドレスについて一日ごとに区切った FAIL コネクション数と送信元 IP アドレス数の関係について示す．一日ごとに区切るのは，SCRAD システムが送信元 IP アドレスを保持する期間が一日となっているためである．図 9 では，新たに 1 つの送信元 IP アドレスからの FAIL コネクション数が平均 10 回となる直線 C を引いている．この直線 C より上にある場合は，SCRAD によって検知される可能性が高い．一方，直線 C より下にある場合は，SCRAD で検知できない可能性が高い．しかし，図 9 では，すべての FAIL コネクションが直線 C より下に位置している．よって，残りの 206 個の送信元 IP アドレスについては，攻撃を検知漏れした．そこで，調査結果から得られた特徴量における 12 月に観測したボットネットからの攻撃における有用性を検証する．一日ごとに区切るのは，SCRAD システムが送信元 IP アドレスを保持する期間が一日となっているためである．図 9 より，12 月に観測したボットネットからの攻撃についても，4.2 節の調査結果どおり，直線 A の上側，直線 B の右側に観測した．よって，12 月に観測したボットネットからの攻撃においても，調査結果から得られた特徴量の範囲内に存在した．

5. おわりに

5.1 まとめ

本論文では，SCRAD において検知漏れしたボットネットからの攻撃を検知することを目的として，観測したボットネットからの攻撃を調査した．観測したボットネットからの FAIL コネクションについて，縦軸を宛先 IP アドレス，横軸を検知時刻としたグラフから，ボットネットからの攻撃の特徴を調査したところ，短時間に複数の異なる送信元 IP アドレスから 1 つの IP アドレスへ 1 回から 5 回の FAIL コネクションを接続する特徴を観測した．これらの特徴からボットネットからの攻撃を検知するために，特徴量を調査した．調査結果から，2 本のしきい値を設けたが，正規ユーザによる FAIL コネクションについて調査したところ，学内の正規ユーザによるログイン認証失敗を誤検知することが判明した．2014 年 12 月に観測したボットネットからの攻撃から，しきい値の有用性について調査した．調査結果から，12 月のボットネットからの攻撃においても，直線 A の上側，直線 B を右側に観測しており，しきい値の有用性が検証された．

5.2 今後の課題

調査結果から得られたしきい値では，学内から学外への通信において正規ユーザのログイン認証失敗についても誤検知する可能性がある．今後は，正規ユーザによる FAIL コネクションについても調査し，しきい値を再検討する必要がある．

参考文献

[1] IBM2014 年上半期 Tokyo SOC 情報分析レポート．https://www-304.ibm.com/connections/blogs/tokyo-soc/resource/PDF/tokyo_soc_report2014_h1.pdf.
[2] 小刀祢知哉, 天本大地, 池部実, 吉田和幸. scan 攻撃検知システムを用いた被検知ホストの挙動についての調査. 第 65 回電気関係学会九州支部連合大会, pp. 278–278, 2012 年 9 月.
[3] 小刀稱知哉, 中本菜桜美, 清水光司, 池部実, 吉田和幸. SSH パスワードクラッキング攻撃検知システムの改善とその運用結果. 情報処理学会研究報告 (インターネットと運用技術), Vol.2014-IOT-26, No.4, pp. 1–7, 2014 年 6 月.
[4] Mobin Javed and Vern Paxson. Detecting stealthy, distributed ssh brute-forcing. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer Communications Security*, CCS '13, pp. 85–96, November 2013.
[5] 本多聡美, 海野由紀, 丸橋弘治, 正彦武仲, 鳥居悟. 使い捨て IP による新型ブルートフォース攻撃の検出. コンピュータセキュリティシンポジウム (CSS)2013 論文集, 情報処理学会, No. 4, pp. 302–309, 2013 年 10 月.
[6] 清水光司, 小刀稱知哉, 池部実, 吉田和幸. 再送パケット除去による SSH パスワードクラッキング攻撃検知システムの検知方法の改善. 第 67 回電気・情報関係学会九州支部連合大会, pp. 87–87, 2014 年 9 月.