Vol.2014-IOT-26 No.4
2014/6/28

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

小刀稱 知哉[1]　中本 菜桜美[2,†1]　清水 光司[2]　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た「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を検知している．運用結果を分析したところ，同じクライアント・サーバ間の通信において，しきい値を超過する場合と超過しない場合の通信が繰り返し観測された．また，パケット送受信回数がしきい値をわずかに超える通信において，検知漏れが生じていた．上記の通信には，正規ユーザも含まれている．本論文では，検知漏れ改善のために，しきい値をわずかに超過した通信を分析した．分析結果をもとに，パケットの計数方法を見直した．さらに，従来のしきい値を変更し，新しい攻撃者検知基準の妥当性を調査した．新しい検知基準を用いてシステムを運用したところ，今まで検知漏れしていた通信を検知することができた．しかし，パケット送受信回数が，新しいしきい値を下回る正規ユーザを誤検知した．

Improvement of the SSH password cracking attacks detection system and its operational results

Tomoya Kotone[1]　Naomi Nakamoto[2,†1]　Kouji Shimizu[2]　Minoru Ikebe[2]　Kazuyuki Yoshida[3]

Abstract: There are many malicious attacks in the Internet. In patricular, we found many illegal access penetrates into SSH servers. Incidents of illegal access are increasing every year. We have been developing a SSH Password Cracking Attack Detection system called SCRAD. We were confirmed many password cracking attacks to the SSH servers by our system. But, we found some false negative. Because the packet count per connection was more than current threshold slightly. So, we investigated the packet data. And we improved new threshold and examined validity of new threshold. As a result, new threshold was able to detect attacker that was not able to detect in previous system. However, we found some false positive.

1. はじめに

インターネットの普及に伴い，ネットワークを通じて様々な情報がやり取りされている．Web ページの閲覧や電子メールなどのコミュニケーション手段に留まらず，インターネット上での行政手続やクレジットカード番号を利用した電子決済など公共性の高いサービスも提供されている．そのため現在では，ネットワークは社会的基盤の一つとして生活に不可欠な存在になっている．しかし，ネットワークを利用した不正通信も多く存在する．それは，プログラムの脆弱性を利用した攻撃や，ネットワークやホストの存在を探索 (スキャン) する攻撃など様々な脅威である．IBM が発表した 2013 年上半期 Tokyo SOC 情報分析レポート [1] によると，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 FTP サー

[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，株式会社スリーエイ・システム

ⓒ 2014 Information Processing Society of Japan

ビスのアカウントが不正使用された事例が確認されている．また，我々が開発した scan 攻撃や DoS 攻撃を検知する「不正通信検知システム [2]」における運用データから，22 番ポート (SSH) に対する scan 攻撃が多いことが判明している．大分大学では，22 番ポートは一部のサブネットをファイアウォールにより遮断，その他のセグメントに関してはユーザの利便性のために制限していない．そのため SSH に対する scan 攻撃やパスワードクラッキング攻撃が多く観測されており，SSH に対する攻撃の監視は重要である．

SSH の認証方式には主にパスワード認証方式と公開鍵認証方式の 2 種類が存在する．パスワード認証方式は，ログイン時に SSH サーバ側のユーザパスワードを入力する認証方式である．攻撃者がパスワードクラッキング攻撃によって，パスワードを入手すると，SSH サーバに不正侵入する．また，公開鍵認証方式は，ログイン時に SSH クライアントの秘密鍵と，SSH サーバにあるクライアントの公開鍵を用いて認証する認証方式である．秘密鍵が漏洩しない限り，公開鍵認証方式がパスワード認証方式より安全であるが，ユーザが意識していないところで SSH のサービスがデフォルトの設定 (パスワード認証) のまま動作している場合がある．よって，セキュリティレベルが低い SSH サーバも含め，すべての SSH サーバを保護することが重要となる．

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 サーバへのパスワードクラッキング攻撃の検知し，SSH サーバとの通信を遮断すること目的として「SSH パスワードクラッキング検知システム (SCRAD)[3][4]」を開発・運用している．本システムは，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を計数し，その値が 45 パケット以下の場合をパスワードクラッキングとして検知している．本システムを学内で運用し，その結果を分析したところ，同じクライアント・サーバ間の通信において，しきい値を超過する場合と超過しない場合の通信が存在した．さらに，1 コネクションあたりのパケット送受信回数が 45 パケットをわずかに超過し，短時間にコネクションの接続を繰り返す送信元が存在した．しかし，しきい値をわずかに超過した通信には正規ユーザも含まれている．そこで本論文では，検知漏れ改善のために，しきい値をわずかに超過したすべての通信を分析し，検知基準を改善することを目的とする．

第 2 章では，SSH パスワードクラッキング攻撃の検知に関する関連研究について述べる．第 3 章では，SCRAD システムの構成，攻撃者検知アルゴリズム，及び検知基準を述べる．第 4 章では，しきい値をわずかに超過した通信について調査し，新しい検知基準を検討する．第 5 章では，新しい検知基準を用いてシステムを運用することで，その妥当性について述べる．第 6 章では，まとめと今後の課題について述べる．

2. 関連研究

トラフィックを解析し, SSH サーバへのパスワードクラッキング攻撃を検知する手法には Laurens[5] らや satoh[6] らが提案した手法が挙げられる．Laurens[5] らは，scan 攻撃の場合，1 コネクションあたりのパケット数が少ないが，単位時間あたりのコネクション数は多くなり，一方，パスワードクラッキングの場合は 1 コネクションあたりのパケット数が，scan 攻撃時に比べ多くなるが，単位時間あたりのコネクション数は少なくなるという特徴から，SSH サーバと送信元との間の 1 コネクションあたりのパケット数や単位時間あたりのコネクション数を監視することで，scan 攻撃やパスワードクラッキング攻撃をリアルタイムに検知する．また，satoh[6] らは SSH のユーザ認証方式により，送受信されるパケットの特徴が異なることに着目し，パケットを送受信する際の挙動を調査し，機械学習を用いて各認証方式を自動的に識別する手法を提案した．これにより，SSH の自動処理と SSH パスワードクラッキングを区別することが可能となり，検知の精度を向上させた．

3. SCRAD システム

3.1 システム構成

我々が開発している「SSH パスワードクラッキング攻撃検知システム (SCRAD)[3][4]」は，インターネットから学内ネットワークへ送信されるパケット，または学内ネットワークからインターネットへ送信されるパケットから，22 番ポート (SSH) に関するパケットを tcpdump[7] のフィルタ機能を用いて抽出する (図 1)．そして，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．その後，送信元ごとに 1 コネクションあたりのパケット送受信回数が 45 パケット以下の通信の数を計数することでリアルタイムに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いる．また，インターネットと学内ネットワークの間に存在するファイアウォールの外側に位置する L3 スイッチからポートミラーしたパケットを収集するため，送信元が学内外のどちらの場合においてもパスワードクラッキング攻撃も検知できる．

3.2 従来の検知基準

本システムは，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とコネクション接続回数をもとに攻撃者を判定する．また，本システムにおいて，1 コネクションあたりのパケット送受信回数とは，送信元が SYN パケットを送信後，送信元と SSH サーバとの間で最初の FIN パケットまたは，RST パケットが観測されるま

ⓒ 2014 Information Processing Society of Japan

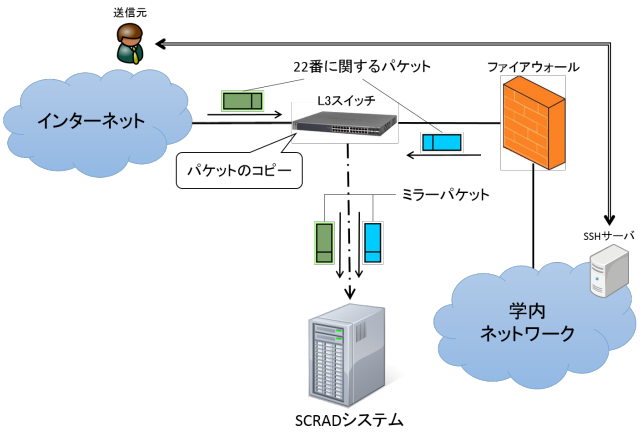

図 1 システム概要

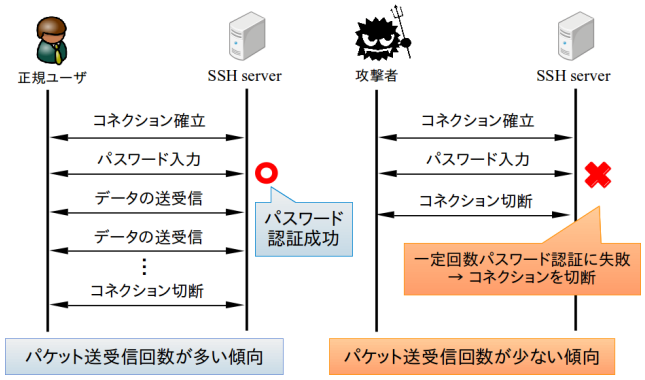

図 2 1 コネクションあたりのパケット送受信回数の違い

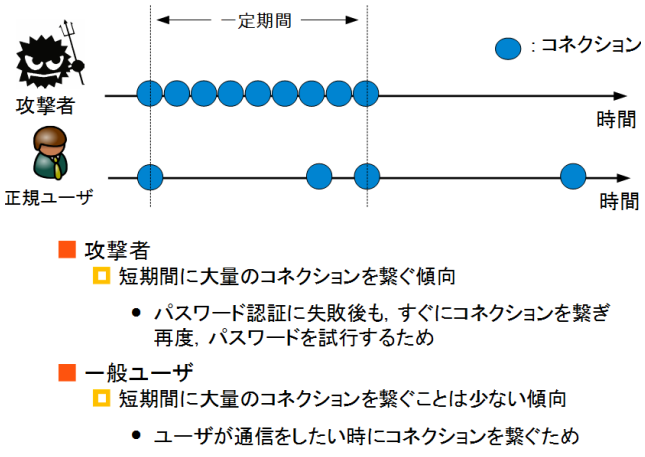

図 3 コネクション接続回数の違い

でのパケット数である．

はじめに，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送受信回数の違いについて説明する (図 2)．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の認証をした後データを送受信する．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くなりやすい傾向にある．一方，攻撃者と SSH サーバの通信において，ユーザ認証プロトコルの際に，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を繰り返す．しかし，一定回数以上 (通常は 3 回程度) 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．このため，正規ユーザの場合にあるようなデータの送受信が行われないため，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．

次に，正規ユーザと攻撃者のコネクション接続回数の違いについて説明する (図 3)．正規ユーザの場合，自分が SSH サーバと通信をしたい時にコネクションを接続し，データを送受信する．よって，短期間に大量のコネクションを繋ぐことは少ない傾向にある，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．

我々は先行研究 [8] により，SSH サーバと送信元との通信を調査し，1 コネクションあたりのパケット送受信回数を集計した．集計結果より，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を，1 コネクションあたりのパケット送受信回数が 45 パケット以下とした．しかし，1 回のコネクションのパケット送受信回数で攻撃者を判定すると，パスワードを入力ミスした場合に正規ユーザを誤検知する可能性がある．よって本システムでは，1 コネクションあたりのパケット送受信回数が 45 パケット以下であるコネクションを 10 回連続して観測した時点で，送信元を攻撃者として検知する検知基準を設定した．1 コネクションあたりのパスワード試行回数は通常 3 回程度であるため，45 パケット以下のコネクションを連続で 10 回観測した場合，パスワードを連続で 30 回失敗したことになる．このような挙動は，正規ユーザでは考えにくい．そのため，本システムは誤検知を最小限に抑えるため，連続 10 回という値を設定した．

3.3 ログ出力部

ログ出力部では，本システムが攻撃者として検知したホストに関する情報を「攻撃者ログ」として出力する．その他にも，1 コネクションあたりのパケット送受信回数がしきい値を超過した場合のコネクション情報を格納する「正規通信ログ」，しきい値以下の場合のコネクション情報を格納する「非正規通信ログ」をそれぞれ保持している．非正規通信ログには，攻撃者がパスワードクラッキング攻撃を仕掛けた場合と正規ユーザがパスワード入力ミスをした場合の 2 種類が含まれる．また，1 コネクションのパケット送受信回数がしきい値以上の場合は SUCCESS，しきい値未満の場合は FAIL と記録する．

4. しきい値をわずかに超過した通信の調査

4.1 従来のしきい値の問題点

従来のしきい値では，1 コネクションあたりのパケット送受信回数が 45 パケット以下の通信をパスワードクラッ

キング攻撃として検知している．攻撃者通信ログを調査したところ，同じクライアント・サーバ間の通信において，しきい値を超過する場合と超過しない場合の通信が存在した．さらに，正規通信ログを調査したところ，1 コネクションあたりのパケット送受信回数が 45 パケットをわずかに超過し，短時間にコネクションの接続を繰り返す送信元が存在した．短期間にコネクションの接続を繰り返す挙動は，攻撃者の挙動と類似している．調査したところ，従来のしきい値で検知漏れしている攻撃者の通信であった．しかし，しきい値をわずかに超過する通信には正規ユーザの通信も存在する．よって本章では，しきい値をわずかに超過したすべての通信について調査した結果を述べる．また，調査結果から検知漏れを是正する新しい検知基準を設定する．

4.2 同じクライアント・サーバ間の通信によるパケット数の差異

同じクライアント・サーバ間の通信において，しきい値を超過する場合と超過しない場合の通信について調査した．その結果，1 コネクションあたりのパケット送受信回数に 1 から 3 パケット程度の差異が生じていた．これらの通信のパケットデータについて調査すると，データサイズが 0 の TCP パケットが多く送信されていることが判明した．よって以降では，データサイズが 0 の TCP パケットがしきい値の設定に影響することを防ぐため，1 コネクションあたりのパケット送受信回数を計数する際，データサイズが 0 の TCP パケットを取り除いた．

4.3 しきい値を超過していた通信の調査

正規通信ログを調査したところ，1 コネクションあたりのパケット送受信回数が 45 パケットをわずかに超過し，短時間にコネクションの接続を繰り返す送信元が存在した．これらの通信の攻撃対象となっていた SSH サーバと送信元間の認証回数を調査すると，3 回，6 回または 7 回であった．現在の検知基準は，認証回数がデフォルトの 3 回を想定して設定している．認証回数が 3 回より多い場合，その分パケット送受信回数も多くなり，現在の検知基準を超過すると考えられる．

そこで，1 コネクションあたりのパケット送受信回数が 45 パケットをわずかに超過していた通信の SSH サーバを抽出し，認証回数やパケット送受信回数を調査した．調査する際には，クライアント OS を Windows と Linux の 2 種類を用意し，クライアントから上記の SSH サーバにアクセスした．そして，クライアント OS ごとに 1 コネクションあたりのパケット送受信回数と，パケットの状態を分析した．パケットの状態とは，各パケットの通信方向，TCP フラグ，パケットのデータ長である．

調査方法は以下の 2 通りである．

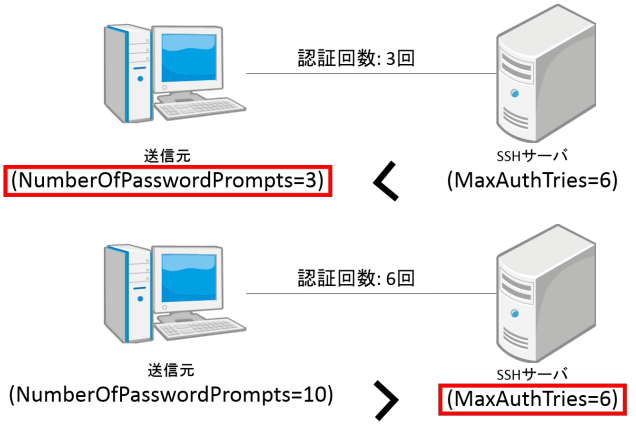

図 4 クライアントと SSH サーバの認証回数の関係

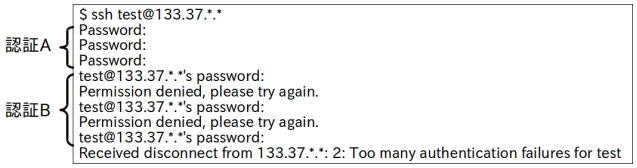

図 5 NAS の認証回数

(1) TeraTerm で接続した際のパケットを，送信元で Wireshark[9] を用いて収集 (WindowsOS).

(2) ssh コマンドを用いて接続した際のパケットを，送信元で tcpdump を用いて収集 (LinuxOS).

また，試行回数はそれぞれ 5 回である．

4.3.1 WindowsOS での実験結果

WindowsOS から上記の SSH サーバに対し，SSH でアクセスした場合，認証回数は 6 回または 7 回であった．認証回数が 7 回の SSH サーバについては NAS(Network Attached Storage) との通信であった．NAS との通信の詳細については，4.3.2 節で述べる．その際の 1 コネクションあたりのパケット送受信回数の最大値は 50 パケットであった．また，データサイズが 0 の TCP パケットを除いて計数した場合は 33 パケットであった．

4.3.2 LinuxOS での実験結果

LinuxOS から上記の SSH サーバに対し，SSH でアクセスした場合，認証回数は 3 回であった．一般的に，LinuxOS のクライアントと SSH サーバ間の認証回数は，SSH クライアント側に存在する ssh_config 内の NumberOfPasswordPrompts の値 (デフォルトは 3) と SSH サーバ側に存在する sshd_config 内の MaxAuthTries の値 (デフォルトは 6) のうち，少ないほうが選択される (図 4)．NumberOfPasswordPompts とはクライアント側が SSH サーバに対し，パスワードを試行する回数であり，MaxAuthTries とは SSH サーバ側がクライアントからのパスワード試行を許容する回数である．今回の実験では，クライアント側の NumberOfPasswordPrompts の値はデフォルト値である 3 を設定していたため，認証を 3 回繰り返していた．そこで，

ⓒ 2014 Information Processing Society of Japan

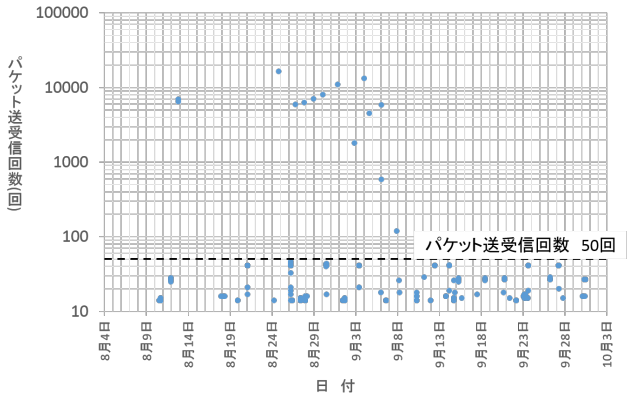

図 6 しきい値を超過していた通信の SSH サーバに対する 1 コネクションあたりのパケット送受信回数

SSH クライアント側を NumberOfPasswordPromts=10 と設定し，上記の SSH サーバに対しアクセスした．この場合，認証回数はが 6 回であった．その際の 1 コネクションあたりのパケット送受信回数の最大値は 49 パケットであった．また，データサイズが 0 の TCP パケットを除いて計数した場合は 28 パケットであった．

また，NumberOfPasswordPrompts=3 と設定した場合でも，認証が 6 回繰り返された通信が存在した．この通信の SSH サーバを調査したところ，NAS であった．NAS との通信の場合，NumberOfPasswordPrompts=3 と設定すると，最初の認証 (以降，認証 A と呼ぶ) を 3 回繰り返した後，指定したユーザでの認証 (以降，認証 B と呼ぶ) を 3 回繰り返していた (図 5)．また，SSH クライアント側の NumberOfPasswordPromts=10 と設定し，NAS に対し SSH でアクセスした．この場合，認証 A が 7 回繰り返された．その際の 1 コネクションあたりのパケット送受信回数の最大値は 67 パケットであった．また，データサイズが 0 の TCP パケットを除いて計数した場合は 46 パケットであった．

4.4 新しい検知基準の設定

新しい検知基準を設定するために，しきい値をわずかに超過していた通信の SSH サーバに対する 1 コネクションあたりのパケット送受信回数を調査した．調査期間は，2013 年 8 月 10 日から 2013 年 9 月 30 日までである．調査結果を図 6 に示す．図 6 の縦軸は 1 コネクションあたりのパケット送受信回数を対数で示している．また，横軸はコネクションを検知した日付をそれぞれ示している．

4.3 節で調査した結果，1 コネクションあたりのパケット送受信回数は 50 パケットを超過することはなかった．図 6 にも，50 パケット以下のコネクションが多く観測されていた．これらの通信は短期間に多くのコネクションを確立しており，攻撃者の挙動と推測される．よって，我々はデータサイズが 0 の TCP パケットを除去して 1 コネクションあたりのパケット送受信回数を計数する．そしてパスワードクラッキング攻撃と判断するためのしきい値を，従来の 45 パケット以下の通信から 50 パケット以下の通信と変更する．また，50 パケット以下の通信を連続で 10 回観測した場合，その送信元を攻撃者と判定するように新しい検知基準を設定した．

表 1 SSH コネクション検知数

通信の種類	コネクション数
攻撃の通信	18,630 件
正規の通信	4,998 件
合計	23,628 件

表 2 SSH クライアント検知数

クライアントの種類	検知数
攻撃者	364 件
正規ユーザ	366 件
重複検知	8 件
合計	730 件

4.5 正規ユーザの 1 コネクションあたりのパケット送受信回数

パケット送受信回数が，新しいしきい値である 50 パケットを下回った正規ユーザ数は 70 件であった．この送信元を調査したところ，新しいしきい値以下の通信を連続で複数回 (最大で 6 回) 観測した後，しきい値を大きく上回る通信が観測された．よって，これは正規ユーザのパスワード入力ミスであると考える．新しい検知基準でも従来の検知基準と同様にしきい値以下のコネクションを連続で 10 回観測すると攻撃者と検知するため，パスワードを入力ミスした送信元は，誤検知にはならないと考えられる．

5. 新しい検知基準での運用結果

5.1 運用環境

新しい検知基準を用いて，SCRAD システムを運用した．運用期間は，2013 年 10 月 1 日から 2013 年 12 月 31 日までの 3 ヶ月間である．また，攻撃者の挙動確認のため，tcpdump により同期間のパケットデータを収集した．

5.2 運用結果

運用期間中に本システムが検知した SSH コネクション検知数を表 1 に，SSH クライアント検知数を表 2 にそれぞれ示す．表 2 の重複検知とは，運用期間中に攻撃者と正規ユーザの両方に判定された IP アドレスを意味する．重複検知された送信元は，新しい検知基準で検知漏れしている送信元，または誤検知している送信元を含んでいる．

5.3 考察

運用期間中に検知した 18,630 件の攻撃の通信について，1 コネクションあたりのパケット送受信回数をコネクションごとに集計したグラフを図 7 に示す．グラフは縦軸に 1 コネクションあたりのパケット送受信回数，横軸にコネクションを示している．図中の青線は従来のしきい値 (45 パケット)，赤線は現在のしきい値 (50 パケット) をそれぞれ示している．以下では，検知基準変更前後の攻撃者検知数の比較や誤検知，検知漏れの観点から考察する．

ⓒ 2014 Information Processing Society of Japan

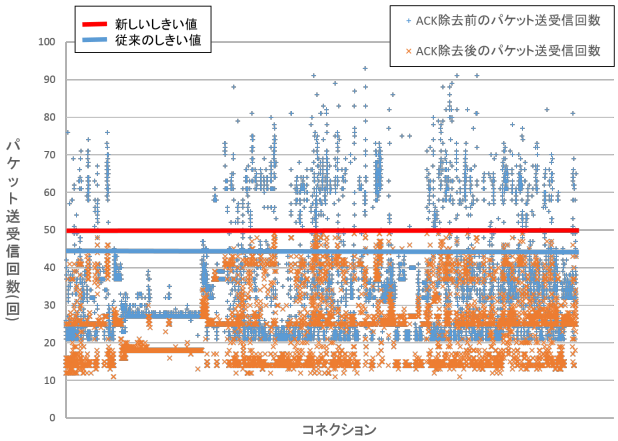

図 7 攻撃者の 1 コネクションあたりのパケット送受信回数

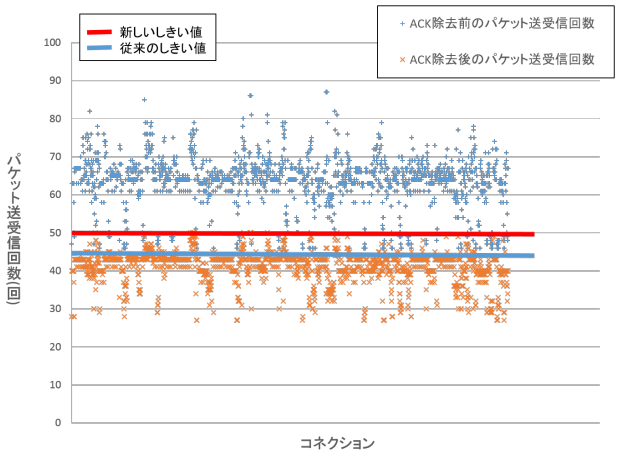

図 8 従来のしきい値では検知漏れしていたコネクションの 1 コネクションあたりのパケット送受信回数

```
65 36 133.37.*.* -> *.*.11.81 FAIL 2013 10/31 19:38:37
70 42 133.37.*.* -> *.*.11.81 FAIL 2013 10/31 19:39:18
57 32 133.37.*.* -> *.*.11.81 FAIL 2013 11/01 11:10:03
66 36 133.37.*.* -> *.*.11.81 FAIL 2013 11/01 11:10:06
63 42 133.37.*.* -> *.*.11.81 FAIL 2013 11/01 13:26:48
49 32 133.37.*.* -> *.*.11.81 FAIL 2013 11/01 20:16:16
44 29 133.37.*.* -> *.*.11.81 FAIL 2013 11/01 20:16:39
44 29 133.37.*.* -> *.*.11.81 FAIL 2013 11/01 20:29:59
61 41 133.37.*.* -> *.*.11.81 FAIL 2013 11/01 20:30:03
48 32 133.37.*.* -> *.*.11.81 FAIL 2013 11/01 20:30:06
```

図 9 誤検知した正規ユーザの通信

5.3.1 攻撃者検知数の比較

図 7 の通信の中で攻撃者として検知した送信元のうち，従来のしきい値では検知漏れしていたコネクションを抜粋したものを図 8 に示す．従来の検知基準と比較すると，コネクションは 2,895 件，攻撃者 IP アドレスは 109 件多く観測することができた．

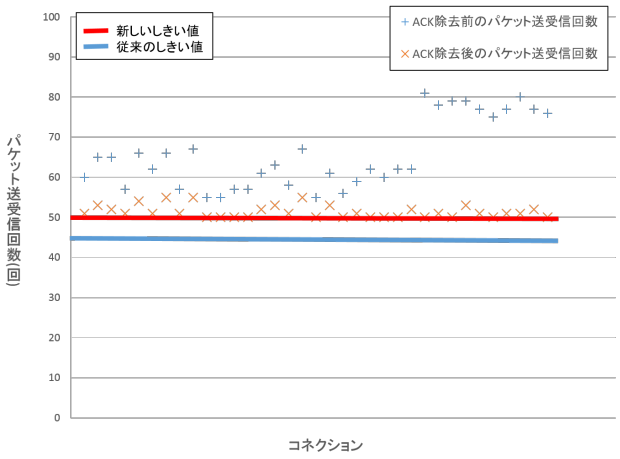

図 10 しきい値の変更後も検知漏れしている通信の 1 コネクションあたりのパケット送受信回数

5.3.2 誤検知

重複検知した 8 件の送信元を調査したところ，5 件は大分大学が保有している IP アドレスであり，1 件は他の大学が保有している IP アドレスであった．これら送信元の挙動を調査したところ，攻撃者として検知された期間以外の通信は，パケット送受信回数がしきい値を大きく超過していた．誤検知した送信元の攻撃者ログを図 9 に示す．一番左の列がデータサイズが 0 の TCP パケットを除去する前，左から 2 列目がデータサイズが 0 の TCP パケットを除去して計数した 1 コネクションあたりのパケット送受信回数を示している．この送信元は従来の検知基準であれば，しきい値を超過するために誤検知することはない．しかし，新しい検知基準ではしきい値を下回る通信を 10 回連続で観測したため誤検知した．送信元の挙動を調査したところ，SSH 接続による分散バージョン管理ツールを用いて，外部サーバのリポジトリにデータを送信していた．また，この送信元は公開鍵暗号方式を用いていた．よって，これらの送信元は誤検知と判断した．新しい検知基準では，SCP コマンド等で自動ログインを用いて少量のデータを送受信する際に誤検知する可能性がある．

5.3.3 検知漏れ

重複検知された 8 件の送信元のうち，誤検知と判断した 6 件を除く，2 件の送信元について調査した．2 件の送信元は，1 コネクションあたりのパケット送受信回数が新しいしきい値をわずかに超過し，短時間に大量のコネクション接続を繰り返していた．これは攻撃者の挙動を類似している．よって，これらの送信元は検知漏れと判断した．検知漏れした通信の 1 コネクションあたりのパケット送受信回数を集計した結果を図 10 に示す．tcpdump で図 10 のパケットデータを調査したところ，データサイズ，シーケンス番号やタイムスタンプの情報が同一のパケットを多数送信していた．よって，これらは再送パケットであると判断した．再送パケットが原因で攻撃者を検知漏れしていたた

ⓒ 2014 Information Processing Society of Japan

め，今後は再送パケットを計数しないようにする．

6. おわりに

6.1 まとめ

本論文では，SCRAD システムにおいて，従来のしきい値をわずかに超過する通信を調査した．そこで我々は，検知漏れ改善のために従来の検知基準を変更し，システムを運用することでその妥当性について調査した．

調査結果から，パケットの計数方法を見直し，従来のしきい値を変更した．また新しい検知基準を用いてシステムを運用した．その結果，従来の検知基準では検知できなかった通信を検知することができた．しかし，再送パケットが原因で，未だに検知基準を超過する通信が存在していたため，今後は再送パケットを計数しないようにする．また，SSH の自動ログインを用いて少量のデータを送受信する際に誤検知する可能性がある．

6.2 今後の課題

再送パケットを計数から除外した効果の検証は，今後の課題である．

参考文献

[1] IBM: 2013 年上半期 Tokyo SOC 情報分析レポート. https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/tokyo_soc_report2013_h1?lang=ja
[2] 小刀稱 知哉, 天本 大地, 小埜 勇貴, 有馬 竜昭, 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論文集，pp. 278–278 (2012 年 9 月)
[3] 小刀稱 知哉, 天本 大地, 池部 実, 吉田和幸：SSH パスワードクラッキング検知システムとその遮断の効果について，マルチメディア，分散，協調とモバイル (DICOMO2013) シンポジウム論文集，pp. 742–748 (2013 年 7 月)
[4] 中本 菜桜美, 小刀稱 知哉, 池部 実, 吉田和幸：SSH パスワードクラッキング攻撃の検知基準の改善，第 66 回電気関係学会九州支部連合大会論文集，pp. 441–441 (2013 年 9 月)
[5] Hellemons, L., Hendriks, L., Hofstede, R., Sperotto, A., Sadre, R. and Pras, A.: SSHCure: A Flow-Based SSH Intrusion Detection Sytem, *International Conference on Autonomous Infrastructure, Management, and Security, AIMS 2012*, pp. 86–97 (2012)
[6] Satoh, A., Nakamura, Y. and Ikenaga, T.: SSH Dictionary Attack Detection based on Flow Analysis, pp. 51–59 (2012)
[7] tcpdump: http://www.tcpdump.org/
[8] 天本 大地, 小刀稱 知哉, 池部 実, 吉田和幸：scan 攻撃検知システムを用いた SSH に対する攻撃についての調査，第 65 回電気関係学会九州支部連合大会論文集，pp. 279–279 (2012 年 9 月)
[9] wireshark: http://www.wireshark.org/

ⓒ 2014 Information Processing Society of Japan