複数の攻撃検知システムの連携による攻撃者検知手法の運用結果

小刀稱 知哉[1]　清水 光司[2]　池部 実[2]　吉田 和幸[3]

概要：インターネットの普及に伴い，ネットワークを通して様々な情報がやり取りされている．そのため現在では，インターネット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，インターネットを利用した不正通信も多く存在する．このような現状から，各組織は何らかの攻撃検知システムを導入する必要がある．我々はこれまでに scan 攻撃や DoS 攻撃を検知する「不正通信検知システム」と SSH サーバへのパスワードクラッキング攻撃を検知する「SSH パスワードクラッキング攻撃検知システム」を連携させるシステムを提案し，開発してきた．本論文では，大分大学内で実際に提案手法を運用した結果を報告する．

Operational results for a proposal detection method based on cooperated between multiple intrusion detection systems

Tomoya Kotone[1]　Kouji Shimizu[2]　Minoru Ikebe[2]　Kazuyuki Yoshida[3]

Abstract: There are many information and services offered via the Internet by the spread of it. So, network is very important thing as one of the infrastructures for our life. However, there are many malicious attacks in the Internet. So, each organization have to operate an intrusion detection system. Therefore, we have been developed 2 intrusion detection systems. One is the Anomaly detection system which detect scan attacks and DoS attacks. The other is the SSH password cracking detection system called SCRAD. SCRAD detects SSH password cracking attacks. And we have proposed new detection method based on cooperation between Anomaly detection system and SCRAD. In this paper, we will report operational results of proposed method in Oita University.

1. はじめに

インターネットの普及に伴い，ネットワークを通し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，インターネット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，インターネットを利用した不正通信も多く存在する．それは，システムの脆弱性を突くものや，ネットワークやホストの存在を探索 (スキャン）するものなど様々な脅威が存在する．警察庁が発表した「平成 25 年中の不正アクセス行為の発生状況等の公表について」[1] によると，平成 25 年度における不正アクセス行為の認知件数は 2,951 件 (前年比+1,700 件)，検挙件数は 980 件 (前年比+437 件) と増加傾向にある．さらに，警察庁のデータによると「連続自動入力プログラムによる不正ログイン攻撃」による不正アクセス行為が約 80 万件観測されており，インターネットに接続することで，ユーザは脅威にさらされていることになる．このような現状から，各組織は何らかの攻撃検知シス

[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

テムを導入する必要がある．

これまでに我々は，大分大学宛の scan 攻撃や DoS 攻撃を検知する「不正通信検知システム」を開発・運用してきた．不正通信検知システムの運用結果から，大分大学への TCP/3389 番ポート (RDP:Remote Desktop Protocol)，TCP/1433 番ポート (SQL over TCP)，TCP/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，3389 番，1433 番ポートはインターネットと学内ネットワーク間のファイアウォールにより，インターネットからのアクセスはすべて遮断している．一方，22 番ポートは一部のセグメントをファイアウォールにより遮断しているが，その他のセグメントはユーザの利便性を考慮し，SSH の通信を許可している．そのため，学内の SSH サーバへの 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いる．以上の理由から，学内の SSH サービスに対する攻撃の監視は重要である．さらに我々は，SSH サーバへのパスワードクラッキング攻撃を検知する「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．また，我々は不正通信検知システムと SCRAD を連携させ，パスワードクラッキング攻撃をより早期に検知する手法を提案した．本論文では，提案手法を実際のネットワーク環境でシステムを運用した結果を報告する．

本論文の構成は以下の通りである．第 2 章は，複数の攻撃検知システムを組み合わせて運用する手法について，関連研究を述べる．第 3 章は，我々が開発・運用している「不正通信検知システム」と「SSH パスワードクラッキング攻撃検知システム (SCRAD)」について述べる．第 4 章は，提案手法の構成や検知の流れを述べる．第 5 章では提案手法を実際のネットワーク環境で運用した結果を報告する．第 6 章でまとめと今後の課題を述べる．

2. 関連研究

複数の攻撃検知システム (IDS) を組み合わせて運用する手法を竹森らや Chi-Chun らが提案している．

竹森ら [2] は，IDS が出力したアラートに関する情報理論的な曖昧度を情報エントロピーにより算出し，長期間の統計分布の平均と標準偏差を用いて，短期間の異常性を評価する手法を提案した．竹森らの手法は”Attack Signature”, “Destination Port”, “Source IP”, “Desination IP” の 4 つのパラメータを用いて攻撃を検知する．4 つのパラメータに関して，時間軸上と空間軸上でのイベント頻度の分布を算出し，通常時との乖離値を評価する．竹森らのシステムが検知する攻撃のモデルは，scan 攻撃・DDoS 攻撃などである．例えば scan 攻撃の場合，単位時間あたりの Source IP の種類は全体の割合に対し少なく，Destination IP 数は多くなる．情報エントロピー値は各パラメータの占める割合に注目するため，曜日や時間の影響を受けにくい安定した傾向を持ち，局所的攻撃によるイベントの偏りを検知できる．しかし，提案手法には検知漏れが存在する．そこで，従来研究のシステムと並行して使用した結果，データセットの攻撃を全て検出した．しかし竹森らのシステムは，エントロピーを用いて攻撃を検知するため，データを一定量蓄積する必要があり，リアムタイム検知は困難である．

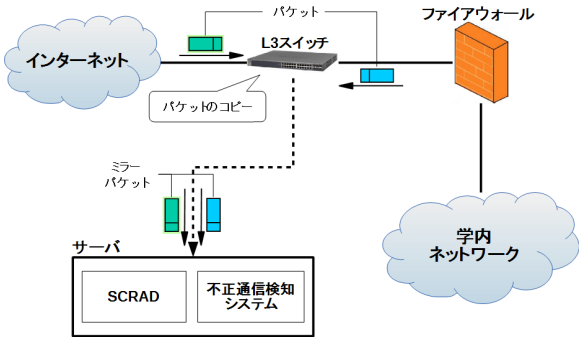

図 1 従来手法の構成図

また，Chi-Chun ら [3] は IDS が出力したアラートをその他の IDS へ通知するシステムを提案した．Chi-Chun らは IDS として，Snort を使用した．1 つの IDS が攻撃者を検知すると，その他の IDS へアラートを通知する．半数以上の IDS から同じ攻撃者のアラートを検知すると，その攻撃者のアラートレベルを上げる．アラートレベルが最大になると，攻撃者からのパケットが観測された段階で，Snort のシグネチャと比較することなく破棄する．よって，通常の Snort より早期に攻撃を検知できる．また，観測された攻撃がある程度通常の分布から乖離した場合のみアラートを通知するため，誤検知によるアラートの誤通知も防いでいる．さらに，他の IDS からアラートの通知を受けるため，実際に攻撃を観測していない IDS も未然に攻撃を防ぐことが可能である．しかし上記のシステムは，全て同じ種類の IDS を用いるため，検知漏れは考慮していない．

3. 攻撃検知システム

本章では，我々が開発・運用している「不正通信検知システム」[4] と「SSH パスワードクラッキング攻撃検知システム (SCRAD)」[5] について述べる．2 つの攻撃検知システムは同一のサーバ上で運用している (図 1)．また，図 1 の L3 スイッチからミラーリングしたパケットを 2 つのシステムの入力としている．

3.1 不正通信検知システム

不正通信検知システムは，TCP のスリーウェイハンドシェイクの状態に着目し，不正通信を検知する．本システムは，scan 攻撃や DoS 攻撃が主な検知対象である．scan 攻撃とは，攻撃者が攻撃対象ネットワーク内の情報 (存在するホストやサービスなど) を収集する行為である．攻撃者は scan 攻撃により得た情報から具体的な攻撃 (パスワー

ドクラッキング攻撃や DoS 攻撃など) を実行する可能性がある．よって，scan 攻撃は事前攻撃と捉えることができる [6].

3.1.1 不正通信検知条件

以下の 3 つの検知条件のうち，いずれかの検知条件を満たすと，その送信元を攻撃者として検知する．

- 代理応答への応答回数 (type1)
  scan 攻撃には，攻撃対象ネットワークに存在するホストやサービスを探索するため，無作為に SYN パケットを送信する手法がある．本システムは，外部ホストから大分大学のライブネット内の未使用 IP アドレスに，SYN パケットが送信されると，本システムが送信元 IP アドレスを偽装し，外部ホストへ SYN/ACK パケットを代理で返信する．その後，代理応答パケットに対し，外部ホストから ACK パケットが返信された場合，外部ホストが送信元を偽装せず，実際に攻撃パケットを送信していることが確認できる．代理応答への応答回数が 3 回を超えると，送信元を type1 の攻撃者として検知する．
- TCP コネクションの未解決状態数 (type2)
  スリーウェイハンドシェイクの手順を無視してパケットを送信することを TCP コネクションの未解決状態と呼ぶ．例えば，スリーウェイハンドシェイクにおいて，学内ホストや不正通信検知システムが，送信した SYN/ACK パケットに対し，ACK パケットが返信されない場合や，学内ホストや不正通信検知システムが送信した SYN/ACK パケットに対し，外部ホストから RST パケットが返信された場合などがある．TCP コネクションの未解決状態数が 5 回を超えると，送信元を type2 の攻撃者として検知する．
- 1 秒間のコネクション要求送信回数 (type3)
  scan 攻撃や DoS 攻撃の場合，1 つの外部ホストが短期間に大量のコネクション要求 (SYN) パケットを学内ネットワークへ送信する．1 つの外部ホストから 1 秒間に SYN パケットを 10 個以上観測すると，送信元を type3 の攻撃者として検知する．

3.2 SSH パスワードクラッキング攻撃検知システム

パスワードクラッキング攻撃検知には，アクセスログの監視やトラフィックを解析する手法がある．アクセスログを監視する手法はログイン情報を用いるため，検知精度は高い．しかし，事前に全 SSH サーバを把握する必要がある．また，自組織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攻撃者を検知できない．一方トラフィックを解析する手法は，検知精度が比較的低いが，組織内のネットワークにおける全 SSH 通信をリアルタイムに監視できるため，組織内外の攻撃者を検知することが可能である．SCRAD は，組織内外の攻撃者をリアルタイムに検知することを目的とし，トラフィックを解析する手法を用いた．

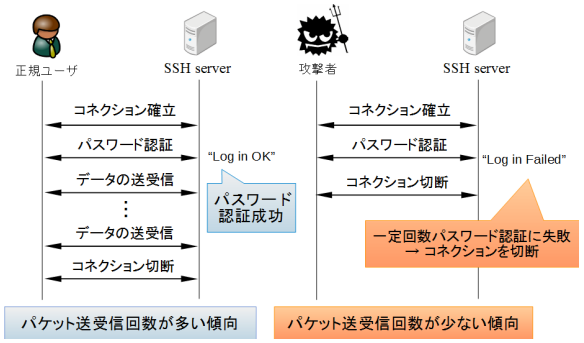

図 2 1 コネクションあたりのパケット送受信回数の違い

3.2.1 パスワードクラッキング攻撃検知条件

SCRAD 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により攻撃者を判定する．SCRAD 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．

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，データの送受信を開始する．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り，何度もユーザ認証プロセスを繰り返す．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，コネクションは切断される．このため，正規ユーザとの通信にある，データの送受信は発生しない．よって，正規ユーザに比べ 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．

我々は，先行研究 [5][7] により，攻撃者の 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 50 パケット未満とした．また，パケットを計数する際は，データサイズが 0 の TCP パケットや再送パケットを除去している．さらに，誤検知防止のため，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 (50 パケット) 未満のコネクションを 10 回連続して観測した時点で，その送信元を攻撃者として検知する．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，50 パケット未満のコネクションを連続 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．

3.2.2 ログ出力部

攻撃者として検知した送信元に関する情報を「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以上のコネクション情報を格納する「正規通信ログ」，しきい値未満のコネクション情報を格納する「非正規通信ログ」をそれぞれ出力する．非正規通信ログは，攻撃者がパスワードクラッキング攻撃を仕掛けた通信と，正規ユーザがパスワードを入力ミスした通信が含まれる．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通信は SUCCESS，しきい値未満の通信は FAIL と記録する．

3.2.3 通信の遮断

SCRAD は攻撃者を検知すると，攻撃者と SSH サーバ間の通信を遮断する．スイッチのアクセス・コントロール・リスト，経路制御による遮断手法 [8] や OpenFlow を用いた遮断手法 [9] がある．また，攻撃者遮断時間は，攻撃者を遮断し，攻撃者からの最後のパケットを観測してから 180 秒経過するまでである．本来，攻撃者からの攻撃は長期間遮断することが望ましいが，正規ユーザを誤検知した際，通常の通信が長期間利用できなくなることを考慮し，遮断時間を設定している．

4. 2 つの攻撃検知システムを連携させた検知手法

提案手法は，検知する攻撃の種類が異なる 2 つの攻撃検知システムを組み合わせることで，より早期に SSH サーバ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いる．攻撃を早期に発見し，攻撃者と SSH サーバとの通信を遮断することにより，攻撃者によるパスワード試行回数は減少する．したがって，攻撃された SSH サーバの管理者に，対策を施す猶予を与えることができる．これにより，SSH サーバへの侵入リスクを低減させることができると考えられる．攻撃を早期発見するために，提案手法では，2 つの攻撃検知システムの検知結果を 1 つに集約する．また，攻撃検知システムの検知結果を参照し，SCRAD の検知条件を変更する．

4.1 攻撃者検知条件の変更

現在の SCRAD は，しきい値 (50 パケット) 未満のコネクションを連続 10 回観測すると，その送信元を攻撃者として検知する．提案手法は集約した情報により，SCRAD の攻撃者検知条件のひとつである” 連続 10 回” を変更する．攻撃者検知条件を変更するためのルールは以下の通りである．

ルール 1

SCRAD，または不正通信検知システムの type1 で以前検知されていた場合は連続 10 回観測から 1 回観測に変更

ルール 2

不正通信検知システムの type2，または type3 で以前検知されていた場合は連続 10 回観測を連続 3 回観測に変更

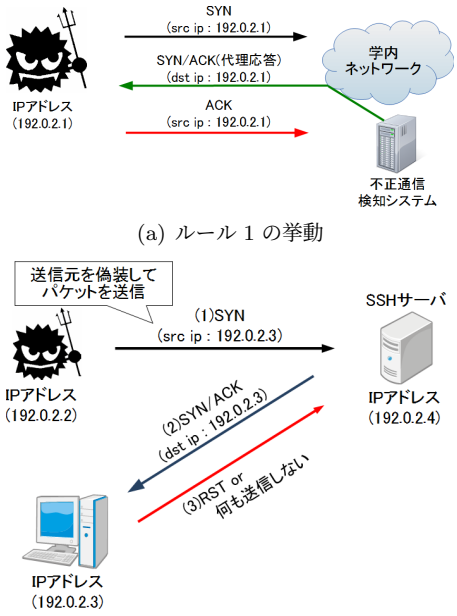

図 3 攻撃者検知条件を変更するためのルール

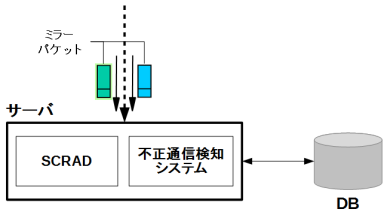

図 4 提案手法の構成図

に変更

2 つのルールを設定した理由は，攻撃者の IP アドレスの偽装を考慮したためである．ルール 1 に含まれる送信元は，スリーウェイハンドシェイクにおいて，SSH サーバや不正通信検知システムが送信した SYN/ACK パケット対し，ACK パケットを返信している (図 3(a))．よって，攻撃者が送信元 IP アドレスを偽装していない可能性が高いため，しきい値未満のコネクションを 1 回検知した時点で早期に攻撃者として検知する．一方，ルール 2 に含まれる攻撃者は，SSH サーバからの SYN/ACK パケットに対し，RST パケットを返信する [10]．あるいはパケットを返信しない (図 3(b))．攻撃者が送信元 IP アドレスを偽装してパケットを送信した場合にこのような挙動が観測される．そのため，ルール 2 で検知された IP アドレス (図 3(b) の 192.0.2.3) は，実際は攻撃者ではなく，攻撃者とは関係のない正規ユーザの可能性がある．正規ユーザの誤検知を抑えるため，ルール 1 に比べ検知条件を緩和した．

4.2 提案手法の構成

図 4 に提案手法の構成を示す．2 つの攻撃検知システムの検知結果を 1 つのデータベース (以下，DB) に保存する．DB は 2 つの攻撃検知システムが存在するサーバとは別の

表 1 攻撃者テーブル (tbl_attackers)

attacker-ip-address	attack-type	detection-time
4176167024 (112.64.235.248)	0	1380593699 (2013/09/30 18:12:03)
2384234212 (228.134.28.142)	2	1380532323 (2013/10/01 11:14:59)
・・・	・・・	・・・

表 2 attack-type の一覧

attack-type	説明
0	SCRAD にて検知
1	不正通信検知システムの type1 にて検知
2	不正通信検知システムの type2 にて検知
3	不正通信検知システムの type3 にて検知

表 3 正規ユーザテーブル (tbl_successes)

normal-ip-address	packet-count	detection-time
23434934223 (207.183.212.116)	2000	1380593891 (2013/09/30 12:15:47)
12394834395 (219.41.202.226)	19843	1380510947 (2013/10/01 11:18:11)
・・・	・・・	・・・

サーバに存在する．

以下に，提案手法による検知の流れを示す．

- 不正通信検知システムと SCRAD が攻撃者を検知すると，攻撃者情報を DB に保存
- SCRAD が新しい送信元からの接続を確認すると，その IP アドレスを DB から探索
- DB の検索結果により，SCRAD の攻撃者検知条件を変更

4.3 検知結果を蓄積するする DB

検知結果を保存する DB には，Elasticsearch[11] を用いた．Elasticsearch は，Elasticsearch 社が開発したオープンソースの検索エンジンであり，JSON 形式でデータを保持する．我々の先行研究 [12] において，様々な種類のログデータを JSON 形式で統一的に管理するシステムを提案している．よって本提案手法においても，JSON 形式でログデータを扱うことで，統一的に管理できるようにしている．

4.3.1 DB に格納する情報

DB は不正通信検知システムと SCRAD の攻撃者情報を格納する「攻撃者テーブル (tbl_attackers)」と，SCRAD の正規ユーザ情報を格納する「正規ユーザテーブル (tbl_successes)」の 2 つのテーブルを有する．SCRAD が攻撃者を検知すると，攻撃者情報を攻撃者テーブルへと格納する．また，SCRAD がしきい値以上の通信 (SUCCESS コネクション) を検知すると，送信元の情報を正規ユーザテーブルへと格納する．

攻撃者テーブル (tbl_attackers) のフィールド名を表 1 に示す．攻撃者テーブルは 3 つのフィールドを持つ．1 つ目のフィールドは検知された攻撃者 IP アドレス (attacker-ip-address) を整数値として格納する．2 つ目のフィールドは攻撃タイプ (attack-type) を格納する．攻撃タイプの一覧を表 2 に示す．表 1 の 3 つ目のフィールドは攻撃者検知時刻 (detection-time) を UNIX 時間として格納する．

また，正規ユーザテーブル (tbl_successes) のフィールド名を表 3 に示す．正規ユーザテーブルは 3 つのフィールドを持つ．1 つ目のフィールドは正規ユーザ IP アドレス (normal-ip-address) を整数値として格納する．2 つ目のフィールドは 1 コネクションのパケット送受信回数 (packet-count) を格納する．3 つ目のフィールドはコネクション検知時刻 (detection-time) を UNIX 時間として格納する．

正規ユーザテーブルを作成した理由は，正規ユーザの誤検知に対処するためである．これまでの SCRAD の運用結果から，scp や rsync などを用いて，少量のデータを送受信すると，正規ユーザを誤検知する問題が確認されている．[5]．また，提案手法は一度正規ユーザを誤検知すると，以降その正規ユーザを何度も攻撃者として誤検知する可能性があるため，通常の通信が困難となる．この問題点への対策として正規ユーザテーブルを作成した．具体的には，攻撃者テーブルに送信元 IP アドレスが格納されていても，正規ユーザテーブルに情報が格納されている場合，検知基準を連続 10 回から変更しない．

4.3.2 攻撃者の検索方法

攻撃者テーブルに対する検索クエリの例を図 5 に示す．攻撃者テーブルを検索する際は送信元 IP アドレスをキーとする．検索クエリに対応するレコードが存在する場合は，過去に対象の送信元 IP アドレスが攻撃者として検知されていることを意味する．一方，レコードが存在しない場合は，現在まで対象の送信元 IP アドレスが検知されていないことを意味している．また，検索されたレコードが複数存在する場合には，attack-type 値が最小のレコードを 1 つ抽出する．検索するレコードは検索した時刻から 30 日 (2,592,000 秒) 以内の情報を利用する．30 日以内は暫定的な値である．検索結果として，表 1 の攻撃者 IP アドレス，攻撃タイプ，検知時刻の 3 つの情報を JSON 形式で得る．

```
'{
 "from":0,"size":1,
 "query":{"term":{"attacker-ip-address":4176167024} },
 "filter":{
  "range":{
  "detection-time":{"from":138001799,"to":1380593799}
  }
 },
 "sort":[{"attack-type":{"order":"asc"}}]
}'
```

図 5 検索クエリの例 (攻撃者テーブル)

表 4　実験結果 (SCRAD)
(a) コネクション検知回数

	5 月	7 月	12 月
FAIL コネクション数	1,597	1,804	3,915
SUCCESS コネクション数	872	594	782
合計	2,469	2,398	4,697

(b) クライアント検知回数

	検知回数			ユニーク IP アドレス数		
	5 月	7 月	12 月	5 月	7 月	12 月
攻撃者	788	652	1,170	195	166	563
正規ユーザ	–	–	–	67	67	70
重複検知	–	–	–	(3)	(3)	(1)
合計 *	–	–	–	259	230	632

* 合計 = 攻撃者数 + 正規ユーザ数 - 重複検知数

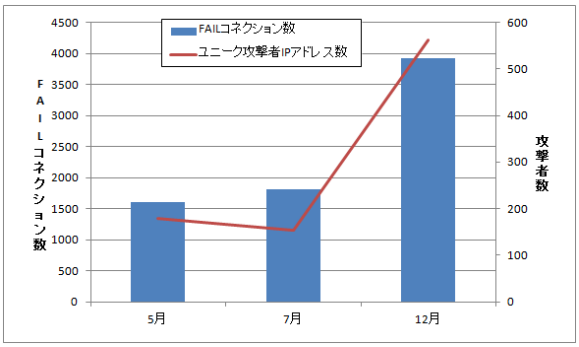

図 6　FAIL コネクション数，攻撃者数の比較

5. 提案手法の運用結果

2014 年 12 月 3 日から 2015 年 1 月 2 日までの 1 ヶ月間，図 1 の L3 スイッチからミラーポートしたパケットを tcpdump により取得し，リアルタイムに攻撃者を検知した．本実験では，データセット (5 月，7 月) と 12 月の運用結果を比較した．比較対象は FAIL コネクション数と攻撃者数である．また，攻撃空白期間を調査した．

5.1 データセット

今回使用したデータセットは 2014 年 5 月 1 日から 5 月 31 日，7 月 1 日から 7 月 31 日までに大分大学とインターネットの境界で収集したパケットである．これらは，図 1 の L3 スイッチからポートミラーしたパケットを攻撃検知システムが存在するサーバ上で，tcpdump により収集したパケットデータである．また，データセットを収集する際，SCRAD が動作していたため，攻撃者の FAIL コネクションを 10 回連続で観測すると，攻撃者と SSH サーバとの通信を遮断している．

5.2 データセットとの比較

SCRAD の運用結果を表 4 に示す．

表 4 より，5 月，7 月と 12 月の FAIL コネクション数，攻撃者数を比較した．提案手法により，より早期に攻撃者を

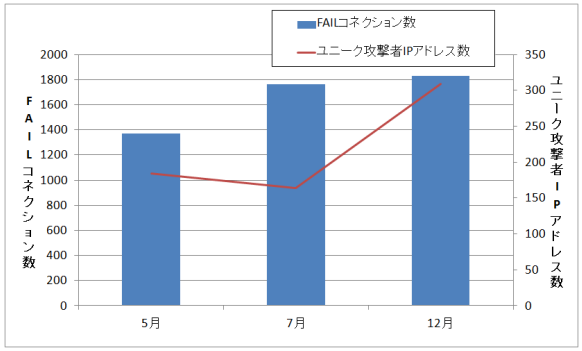

図 7　FAIL コネクション数，攻撃者の比較 (133.37.A と 133.37.B は除いて計数)

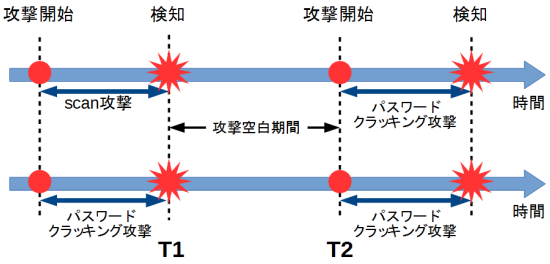

図 8　攻撃空白期間

検知し，攻撃者と SSH サーバとの通信を遮断すると，攻撃者が攻撃を早期に断念するのではないかと考えた．よって，5 月，7 月のデータセットに提案手法を用いた際の FAIL コネクション数よりも，12 月の FAIL コネクション数が減少すると予想した．FAIL コネクション数との比較結果を図 6 に示す．調査した結果，12 月の攻撃者が他の月と比較し，増加していた．そこで，12 月分の宛先 SSH サーバごとの FAIL コネクション数を調査した．その結果，複数の送信元から学内の 2 件の SSH サーバへ全体の 54%の FAIL コネクションが観測された．これらの攻撃の詳細については，5.4 節で述べる．5 月，7 月には上記のような攻撃は観測されなかった．よって，5 月，7 月，12 月で観測された FAIL コネクションの中から，宛先の IP アドレスが 133.37.A と 133.37.B であったコネクションを除いて計数した結果を図 7 に示す．その結果，FAIL コネクション数は他の月と比較し，大きな差異は確認できなかった．これは，攻撃者が遮断の時期に関係なく，攻撃を常時仕掛けていると推測する．

5.3 攻撃空白期間の調査

提案手法は，攻撃者テーブルや正規ユーザテーブルからレコード検索する際，検索時刻から 30 日以内の情報を利用する．現時点では暫定値として，30 日以内に設定している．よって，レコードを検索する際，対象となる送信元 IP アドレスにおける，現在時刻と 1 つ前のレコード挿入時刻との差 (攻撃空白期間) を調査した (図 8)．これは，前の攻撃 (scan 攻撃またはパスワードクラッキング攻撃) の検知

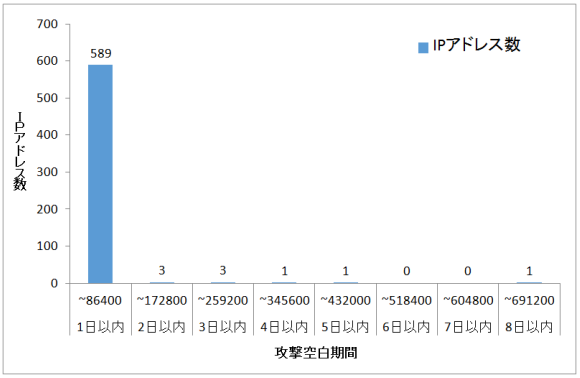

図 9 1 つ前の攻撃との差異 (日ごと)

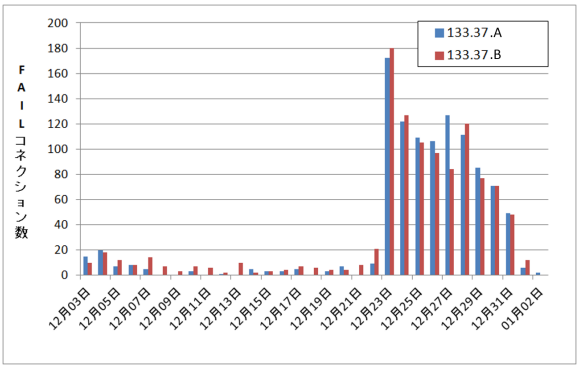

図 10 2 つの SSH サーバに仕掛けられた 1 日ごとの FAIL コネクション数

時刻と現在の攻撃 (パスワードクラッキング攻撃) 開始時刻との差異と等価である (図 8 の T2-T1)．調査結果を図 9 に示す．調査したところ，攻撃の空白期間としてもっとも多く攻撃者を検知したのは，1 日以内であった．また，最大の空白期間は 7 日以上 8 日以内であった．よって，DB にレコードを保持する期間は，最低でも 8 日必要である．現在のデータベースの検索する期間は，攻撃検知時刻から 30 日以内であるため，攻撃者が仕掛けた 1 つ前の攻撃を，DB から検索可能である．

5.4 ボットからの攻撃

今回のシステム運用期間において，学内の 2 つの SSH サーバ (133.37.A，133.37.B) に対して，複数の送信元からパスワードクラッキング攻撃を観測した．2 つの SSH サーバに対する 1 日ごとの FAIL コネクション数を図 10 に示す．調査すると，2 つの SSH サーバに対する FAIL コネクション数が共に 12 月 23 日から増加していた．また，133.37.A に攻撃を仕掛けた攻撃者 IP アドレス数は 245 件，133.37.B に攻撃を仕掛けた攻撃者 IP アドレス数は 259 件であった．このうち，212 件の攻撃者 IP アドレス数が 2 つの SSH サーバに攻撃を仕掛けていた．以上から，これらの攻撃者 IP アドレスは，ボットネットからの攻撃だと推測した．

上記の 2 つの SSH サーバに対する攻撃者 IP アドレス

```
13 C.137.117 → 133.37.A FAIL_CLOSE 2014 12/22 20:17:22
13 D.148.210 → 133.37.A FAIL_CLOSE 2014 12/22 20:17:28
13 E.25.92 → 133.37.A FAIL_CLOSE 2014 12/22 20:17:31
13 F.180.159 → 133.37.A FAIL_CLOSE 2014 12/22 20:17:36
13 G.139.198 → 133.37.A FAIL_CLOSE 2014 12/22 20:19:17
13 H.191.4 → 133.37.A FAIL_CLOSE 2014 12/22 20:19:22
13 I.161.43 → 133.37.A FAIL_CLOSE 2014 12/22 20:19:37
13 J.207.60 → 133.37.A FAIL_CLOSE 2014 12/22 20:19:42
13 K.208.212 → 133.37.A FAIL_CLOSE 2014 12/22 20:19:44
13 L.20.26 → 133.37.A FAIL_CLOSE 2014 12/22 20:21:13
13 M.161.10 → 133.37.A FAIL_CLOSE 2014 12/22 20:21:16
13 N.110.137 → 133.37.A FAIL_CLOSE 2014 12/22 20:21:19
13 O.33.57 → 133.37.A FAIL_CLOSE 2014 12/22 20:21:23
13 P.22.71 → 133.37.A FAIL_CLOSE 2014 12/22 20:23:21
13 Q.40.42 → 133.37.A FAIL_CLOSE 2014 12/22 20:23:26
13 R.93.52.86 → 133.37.A FAIL_CLOSE 2014 12/22 20:23:32
13 S.84.122 → 133.37.A FAIL_CLOSE 2014 12/22 20:23:37
13 T.6.245 → 133.37.A FAIL_CLOSE 2014 12/22 20:23:40
```

図 11 複数の送信元から 1 つの SSH サーバへのパスワードクラッキング攻撃

のうち，SCRAD は，約 250 件の攻撃者 IP アドレスを検知していた．しかし，攻撃者として検知されていない送信元も存在した．SCRAD に検知されなかった送信元のうち，133.37.A に関する非正規通信ログの一部を図 11 に示す．図 11 より，1 つの送信元から 1 つの FAIL コネクションを観測した．また，最右行に着目すると，これらの送信元はほぼ同時刻に単一の SSH サーバへ攻撃を仕掛けていた．さらに，最左行のパケット送受信回数に着目すると，1 コネクションあたりのパケット送受信回数は同一であった．よって，これらの送信元はボットに感染しており，攻撃者から命令を受け，攻撃を仕掛けてきたと推測される．また，不正通信検知システムではこれらの送信元は検知されていなかった．さらに，送信元のトップレベルドメイン (ccTLD) を調査した．ccTLD を調査すると，対象の IP アドレスが存在する国を特定できる．調査したところ，10 件の ccTLD を観測した．

SCRAD では，送信元 IP アドレスごとの FAIL コネクション数に着目し，攻撃者を検知している．また，これらの送信元は不正通信検知システムでは検知されていないため，1 つの送信元から 10 回の FAIL コネクション数を検知しないと，攻撃者として検知することはできない．以上から，提案手法において，ボットネットからの攻撃の検知は困難である．

6. おわりに

6.1 まとめ

大分大学内で提案手法を運用した．その結果，攻撃者は遮断の時期に関係なく攻撃を常時仕掛けていた．また，運用期間中に，提案手法においても検知しにくいボットネットからの攻撃を新たに観測した．

6.2 今後の課題

(1) 誤検知への対応
SCRAD は，ssh-agent 機能を用いた scp コマンドや rsync コマンドなどで公開鍵認証方式により，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ため，このような誤検知へ対策する必要がある．

(2) 攻撃検知システムの拡張
提案手法は，DB を用いて，不正通信検知システムと SCRAD を連携させた検知手法である．今後は，DB に様々なログ (例: tcpdump のログデータ，ハニーポットのアクセスログなど) を利用し，利用することで，より精度の高い攻撃検知システムを開発する必要がある．

(3) ボットからの攻撃を検知
現在の SCRAD では，5.4 節で述べた攻撃者は検知できない．今後は，ボットネットから仕掛けられた攻撃も検知していく必要がある．例として，現在は送信元 IP アドレスごとの FAIL コネクション数に着目しているが，宛先 SSH サーバごとの FAIL コネクション数に着目すると，検知できるのではないかと考える．

参考文献

[1] 警察庁.
平成 25 年中の不正アクセス行為の発生状況等の公表について. http://www.npa.go.jp/cyber/statics/h25/pdf040.pdf, 2014 年.
[2] 竹森敬祐, 三宅優, 田中俊昭, 笹瀬巌.
IDS ログから算出される情報エントロピー値の変動に注目した異常検出.
情報処理学会研究報告 (コンピュータセキュリティ), Vol. 2004-CSEC-25(54), pp. 31–36, 2004 年 5 月.
[3] L. Chi-Chun, H. Chun-Chieh and K. Joy. A cooperative intrusion detection system framework for cloud computing networks. *2010 39th International Conference on Parallel Processing Workshops*, pp. 280–284, Sep. 2010.
[4] 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.
[5] 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(4), pp. 1–7, 2014 年 6 月.
[6] portscan.
https://www.ipa.go.jp/security/fy14/contents/soho/html/chap1/scan.html.
[7] 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論文集, pp. 87–87, 2014 年 9 月.
[8] 小刀祢 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. 情報処理学会マルチメディア，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.
[9] 下川 大貴, 小刀称 知哉, 池部 実, 吉田 和幸. OpenFlow を用いた攻撃者遮断システムの提案と評価. 情報処理学会マルチメディア，分散，協調とモバイル (DICOMO2014) シンポジウム論文集, pp. 197–204, 2014 年 7 月.
[10] F. Gont and S. Bellovin. Defending against Sequence Number Attacks. RFC 6528, Feb. 2012. http://www.ietf.org/rfc/rfc6528.txt.
[11] Elasticsearch. http://www.elasticsearch.org/.
[12] 池部 実, 吉田 和幸.
MAC アドレスによる利用者認証における認証ログの統合・分析システムの提案と実装. 情報処理学会マルチメディア，分散，協調とモバイル (DICOMO2014) シンポジウム論文集, pp. 190–196, 2014 年 7 月.