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提案と評価

小刀稱 知哉† 池部 実‡ 吉田 和幸§

インターネットの普及に伴い，各組織は何らかの攻撃検知システムを導入する必要に迫られている．我々は scan 攻撃や DoS 攻撃を検知する「不正通信検知システム」，SSH 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．現在 2 つの攻撃検知システムは，検知する攻撃の種類が異なるため独立して運用している．2 つの攻撃検知システムのログを分析すると，scan 攻撃後にパスワードクラッキング攻撃を仕掛ける攻撃者が観測された．本論文では，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ため，2 つの攻撃検知システムを連携した攻撃者検知手法を提案する．また，提案手法を実装し，従来の 2 つの攻撃検知システムを独立して運用していた際の検知結果と比較することで，提案手法の有用性を調査した．その結果，提案システムは，より早期に攻撃者を検知し，従来の SCRAD で検知していなかった攻撃者を検知できた．

Proposal for a detection method based on cooperation of multiple Intrusion Detection Systems and its evaluation

Tomoya KOTONE† Minoru IKEBE‡ Kazuyuki YOSHIDA§

The network management cost is increasing with the spread of the Internet. So, each organization have to operate an intrusion detection system. Therefore, we have been developing 2 intrusion detection systems. One of the systems is Anomaly Detection System which mainly detects “scan attack” and ”Denial of Services attack”. The other is SSH Password Cracking Attacks Detection system called SCRAD. We operate 2 IDSes individually. Because, the 2 IDSes differ in the detection targets. We analyzed the result of the 2 IDSes, then we found a behavior which some attackers performs the password cracking attack after the scan attack. In this paper, we propose a new detection method based on cooperation of the 2 IDSes. Our proposal method can detect attackers earlier than the previous method that the 2 IDSes operate individually. We implement the proposed method and operate it. Then, we compare the result of two methods. As a result, our proposal method can detect attackers earlier than the previous method. And, our proposal method is able to detect attackers which SCRAD failed to detected.

1 はじめに

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，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．

† 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
‡ 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
§ 大分大学学術情報拠点情報基盤センター
Center for Academic Information and Library Services, Oita University

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に迫られている．そこで我々は，scan 攻撃や DoS 攻撃を検知する「不正通信検知システム」[2] や SSH 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)」[3] を開発・運用してきた．また，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，遮断していない．よって，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ため，SSH サービスに対する攻撃の監視は重要である．

我々が開発した不正通信検知システムと SCRAD は，検知する攻撃の種類が異なるため，独立して運用している．2 つの攻撃検知システムのログを分析すると，ある攻撃者 IP アドレスにおいて scan 攻撃後にパスワードクラッキング攻撃を仕掛ける挙動が観測された．本論文では，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ため，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検知手法を提案する．また，提案手法を実装し，従来の 2 つの攻撃検知システムを独立して運用していた際の検知結果と比較することで，提案手法の有用性を調査する．

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，2 つの攻撃検知システムのログを分析し，得られた攻撃者の挙動と予備実験の結果について述べる．第 5 章は，提案手法の構成や検知の流れを述べる．第 6 章は，提案手法の実験結果について考察した結果を述べる．第 7 章にて，まとめと今後の課題について述べる．

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 [4] は，IDS のイベント出力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．イベントは”Attack Signature”, “Destination Port”, “Source IP”, “Desination IP” の 4 つのパラメータを用いている．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．情報エントロピー値は各イベント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，イベント頻度を用いて異常性を判定する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，一定期間データの蓄積が必要であり，リアムタイム検知は困難である．

また，Chi-Chun ら [5] は IDS が出力したアラートをその他の IDS へと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」[2] と「SSH パスワードクラッキング攻

撃検知システム (SCRAD)」[3] について述べる．

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．

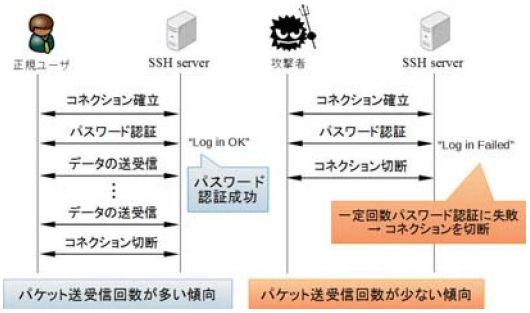

図 1　1 コネクションあたりのパケット送受信回数

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．よって，組織内外の攻撃者を検知することができる．SCRAD は，組織内外の攻撃者をリアルタイムに検知するため，トラフィックを解析する手法を用いた．また本システムは，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．

3.2.1　パスワードクラッキング攻撃検知条件

以下の 2 つの特徴から SSH パスワードクラッキング攻撃を仕掛けてきた攻撃者を検知する．

- 1 コネクションあたりのパケット送受信回数
  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 1 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．

- コネクション接続回数
  正規ユーザと攻撃者のコネクション接続回数の違いを説明する．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．そのため，短期間に大量のコネクションを繋ぐ傾向にある．一方，正規ユーザは SSH サーバと通信したい時にコネクションを接続するため，短期間に大量に接続することは少ない傾向にある．

我々は，先行研究 [3][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．しかし，攻撃者の中には，しきい値未満の通信が 10 回以下である挙動が観測されており，現状の SCRAD では検知漏れする問題点が存在する．

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 攻撃者の挙動の分析

2 つの攻撃検知システムは，検知する攻撃の種類が異なるため，独立して運用している．2 つの攻撃検知システムのログを分析したところ，以下の 2 つの挙動が観測された．本章ではこれらの挙動について述べる．

(A) scan 攻撃後のパスワードクラッキング攻撃

(B) 期間を空けたパスワードクラッキング攻撃

4.1 (A)scan 攻撃後のパスワードクラッキング攻撃

2 つの攻撃検知システムのログを調査すると，共通した攻撃者 IP アドレスを確認した．この攻撃者の挙動を調査すると，攻撃を仕掛ける最初の段階で学内ネットワークの 22 番ポートに対し，水平 scan 攻撃を仕掛けていた．その後，応答のあった SSH サーバにパスワードクラッキング攻撃を仕掛けていた．この攻撃者は scan 攻撃の段階で不正通信検知システムが検知し，SSH パスワードクラッキング攻撃を仕掛けた段階で SCRAD が検知していた．

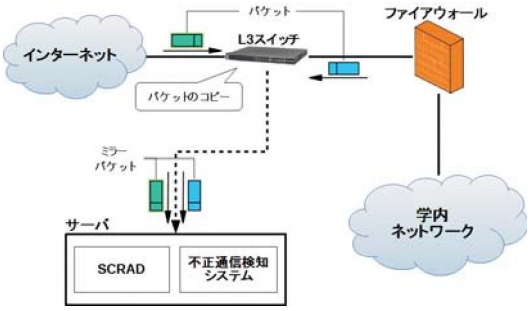

図 2　従来手法の構成図

表 1　検知結果 (不正通信検知システム)

攻撃タイプ	検知回数	IP アドレス数
type1	155,680	45,927
type2	386,514	24,482
type3	57,750	32,616
合計	599,944	99,862
22 番ポートに攻撃パケットを送信した攻撃者数	74,963	2,337

4.2　(B) 期間を空けたパスワードクラッキング攻撃

SCRAD の攻撃者ログを調査すると，同一の攻撃者 IP アドレスを異なる期間で複数回検知していた．この送信元の挙動を調査すると，一度パスワードクラッキング攻撃を仕掛け，SCRAD が検知した後，数時間から数日の期間を空けて，再びパスワードクラッキング攻撃を仕掛け，再度攻撃者として SCRAD が検知していた．

4.3　予備実験

4.1，4.2 節で述べた 2 つの挙動 (A)(B) に当てはまる攻撃者数を調査するため，(1) 不正通信検知システムと SCRAD が共に検知した攻撃者数と (2)SCRAD が検知した攻撃者 IP アドレス別検知回数を調査した．(1) には 4 節の (A) が，(2) には (B) が対応している．今回使用したデータセットは，2014 年 5 月 1 日から 5 月 31 日までに大分大学で収集した 22 番ポートに関するパケットである．これらは，図 2 の L3 スイッチからミラーしたパケットを tcpdump により収集した．

4.3.1　不正通信検知システムと SCRAD が共に検知した攻撃者数

不正通信検知システムの検知結果を表 1 に示す．表 1 の合計 IP アドレス数は，実験期間中に攻撃を仕掛けてきたユニークな IP アドレス数を示している．また，SCRAD のコネクション検知回数とクライアント検知回数を表 2 と表 3 にそれぞれ示す．調査期間中に不正通信検知システムが検知した攻撃者 IP アドレスのうち，22 番ポートに攻撃パケットを送信した攻撃者 IP アドレス数は 2,337 件であった．また，表 3 において，SCRAD が検知した攻撃者 IP アドレス数は 179 件であった．2 つの攻撃検知システムが共に検知した攻撃者 IP アドレス数を調査した結果，SCRAD で検知した攻撃者 IP アドレスのうち，142 件を不正通信検知システムでも検知していた．この調査結果から，不正通信検知システムの検知結果を SCRAD で利用することで，それぞれ独立してシステムを運用するより早期に攻撃者を検知できると考える．

表 2　SSH コネクション検知回数 (SCRAD)

しきい値未満の通信数	7,184
しきい値以上の通信数	872
合計	8,056

表 3　SSH クライアント検知回数 (SCRAD)

	検知回数	IP アドレス数
攻撃者	674	179
正規ユーザ	–	67
重複検知	–	3
合計	–	243

4.3.2　SCRAD が検知した攻撃者 IP アドレス別検知回数

SCRAD が実験期間中に検知した攻撃者 IP アドレス別検知回数を調査した．その結果，1 つの攻撃者 IP アドレスを最大で 203 回検知していた．また SCRAD において，179 件中 97 件の攻撃者 IP アドレスを複数回検知していた．従来手法は前回攻撃を仕掛けてきた攻撃者 IP アドレスを保持しておらず，同一 IP アドレスが期間を空けて複数回攻撃した場合，それぞれ別の攻撃として判定していた．しかし，この調査結果から，前回 SSH サーバに攻撃してきた攻撃者 IP アドレスの情報を保持し，参照することで，より早期に攻撃者を検知できると考える．

5　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

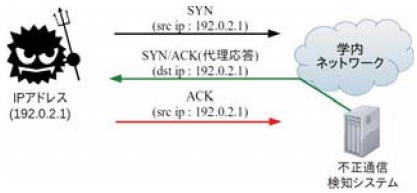

図 3　ルール 1 の挙動

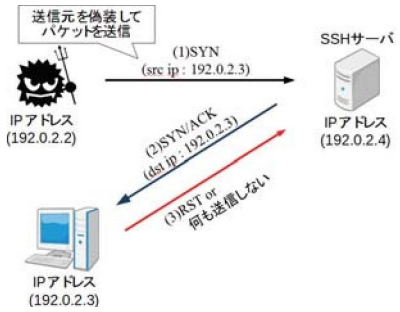

図 4　ルール 2 の挙動

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と，攻撃者がパスワードを試行する回数が減少する．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が低減する．よって，攻撃の早期発見は重要である．提案手法では，2 つの攻撃検知システムの検知結果を 1 つに集約し，参照する．また，参照した結果から SCRAD の検知条件を変更する．

5.1　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 回を 1 回に変更

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 回を連続 3 回に変更

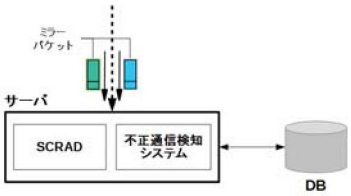

図 5　提案手法の構成図

2 つのルールを設定したのは，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)．よって，攻撃者 IP アドレスが送信元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 4)．攻撃者が送信元を偽装してパケットを送信する際にも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 4 の 192.0.2.3) は，実際は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．

5.2　提案手法の構成

図 5 に提案手法の構成図を示す．提案手法では，図 2 の L3 スイッチからミラーリングしたパケットを 2 つの攻撃検知システムの入力とした．不正通信検知システムと SCRAD は同一サーバ上で運用している．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サーバに存在する．

以下に，提案手法の流れを示す．

(1)　不正通信検知システムと SCRAD が検知した攻撃者情報を DB に保存

(2)　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

(3)　DB の検索結果により，SCRAD の攻撃者検知条件を変更

表 4　攻撃者テーブル

attacker-ip-address	attack-type	detection-time
4176167024	0	1380593699
2384234212	2	1380532323
・・・	・・・	・・・

表 5　正規ユーザテーブル

normal-ip-address	packet-count	detection-time
23434934223	2000	1380593891
12394834395	19843	1380510947
・・・	・・・	・・・

表 6　攻撃タイプの一覧

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

5.3　検知結果を保存する 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．よって本研究においても，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た．

5.3.1　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」と，SCRAD の正規ユーザ情報を格納する「正規ユーザテーブル」の 2 つのテーブルを有する．各テーブルのフィールド名を表 4 と表 5 に示す．攻撃者テーブル (表 4) 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 6 に示す．表 4 の 3 つ目のフィールドは攻撃者検知時刻 (detection-time) を UNIX 時間の形式で格納する．また，正規ユーザテーブル (表 5) 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 時間の形式で格納する．

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

図 6　検索クエリの例 (攻撃者テーブル)

また，正規ユーザテーブルを作成した理由として，SSH の自動ログイン機能を用いてデータを送受信するコマンドにより，少量のデータを送受信すると，正規ユーザを誤検知する [3] 問題点が挙げられる．提案手法は，一度正規ユーザを誤検知すると，次回以降何度も攻撃者として誤検知するため，通常の通信が困難となる可能性がある．この問題点への対策として，正規ユーザテーブルを用意した．提案手法は攻撃者テーブルに情報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．

5.3.2　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 6 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．検索された複数のレコードの中から attack-type 値が最小のものを 1 つ抽出する．また，検索するレコードは検索した時点から 30 日 (2,592,000 秒) 以内の情報を利用する．30 日以内というのは暫定的な値である．検索結果として，表 4 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．

6　提案手法の実験結果

本実験では，4.3 節と同様のデータセットを用いて SCRAD の検知結果を，独立して運用した場合 (従来手法) と提案手法の場合で比較した．

6.1　実験結果

6.1.1　レコード数と DB へのアクセス頻度

不正通信検知システムの検知結果は 4.3.1 節の表 1 と同様である．検知した攻撃検知回数は 599,944 件であった．よって攻撃者テーブルには，不正通信検知システムから 599,944 件のレコードが挿入される．

SCRAD の検知結果のうち，コネクション検知回数とクライアント検知回数を比較した結果を表 7，表 8 に示す．提案手法において，検知した攻撃者 IP ア

表 7　SSH コネクション検知回数の比較 (SCRAD)

	従来手法	提案手法
しきい値未満の通信	7,184	1,597
しきい値以上の通信	872	872
合計	8,056	2,469

表 8　SSH クライアント検知回数の比較 (SCRAD)

	従来手法		提案手法	
	検知回数	IP アドレス数	検知回数	IP アドレス数
攻撃者	674	179	788	195
正規ユーザ	–	67	–	67
重複検知	–	3	–	3
合計	–	243	–	259

ドレス数は 195 件であった．よって SCRAD から攻撃者テーブルに 195 件のレコードが挿入される．さらに，しきい値以上の通信が 872 件観測されたため，SCRAD から正規ユーザテーブルに 872 件のレコードが挿入される．

また，提案手法が DB へアクセスするタイミングとして，以下の 4 つがある．

1. 不正通信検知システムが攻撃者を検知すると，攻撃者テーブルへ攻撃者情報を挿入
2. SCRAD が攻撃者を検知すると，攻撃者テーブルへ攻撃者情報を挿入
3. SCRAD がしきい値以上の通信を検知すると，正規ユーザテーブルへ正規ユーザ情報を挿入
4. SCRAD が保持していない送信元から接続を確認すると，攻撃者テーブルと正規ユーザテーブルから送信元の情報を参照

実験期間中における 1 から 4 の DB へのアクセス時刻を調査し，1 秒あたりの DB へのアクセス件数を計測した．また，図 5 において，2 つの攻撃検知システムが動作するサーバと DB サーバ間の RTT(Round Trip Time) を計測したところ，約 0.32 ミリ秒であった．

実験で用いたパケットデータにおける DB へのアクセス件数は，1 秒間あたり最大で 38 件であった．また，1 件のレコードを挿入する時間は約 1.71 ミリ秒であり，送信元を DB から検索する際の時間は約 1.74 ミリ秒であった．よって，38 件のアクセスは，66.12 ミリ秒で完了する．以上から，1 秒以内にすべての DB に関する処理が完了するため，提案手法の運用に問題はないと考える．

6.1.2　重複検知

表 3 の重複検知とは，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．これらの送信元は，SCRAD が検知漏れ，または誤検知したことを意味する．重複検知された送信元は，攻撃者テーブルと正規ユーザテーブルの両方のテーブルに情報が格納されている．重複検知した 3 件の送信元を調査すると，従来手法と提案手法で同一の IP アドレスであった．このうち，2 件は大分大学が保有している IP アドレスと他の大学が保有している IP アドレスであった．2 件の送信元の挙動を調査すると，攻撃者として検知された期間以外に，パケット送受信回数がしきい値を大きく超過した通信を複数回観測していた．またコネクションの接続間隔も不均一であった．この送信元 IP アドレスの利用者に確認すると，先行研究 [3] と同様に，SSH の自動ログイン機能を用いてデータを送受信するコマンドにより，少量のデータを送受信していた．よってこれらの送信元は誤検知と判断した．

また，誤検知と判断した 2 件の送信元を除く，1 件の送信元の挙動を調査した．その結果，この送信元は短期間に大量の接続を繰り返していた．これは攻撃者の挙動と類似している．その後ある 1 つの SSH サーバに，パケット送受信回数がしきい値を大きく超過する通信が観測された．

6.2　提案手法の考察

本節では，SCRAD の検知結果を，独立して運用した場合 (従来手法) と提案手法の場合で比較し，考察する．

6.2.1　しきい値以上の通信の比較

表 7，表 8 より，従来手法と提案手法を比較すると，しきい値以上の通信数や正規ユーザ数に差はなかった．また，6.1.2 節で示した重複検知された送信元のうち，2 件の誤検知した正規ユーザは，しきい値未満の通信を全部で 134 件観測した．仮に正規ユーザテーブルがなく，攻撃者テーブルだけで提案手法を運用すると，一度正規ユーザを誤検知した場合，その後何度も攻撃者として検知され，SSH サーバとの通信を遮断される．よって，正規ユーザの通信が正常にできない可能性がある．しかし，正規ユーザテーブルを用いると，一度正規ユーザと判断された場合，攻撃者検知条件が変更されないため，正規ユーザの通信を保証できる．

表 9　前回検知された攻撃の種類

ルール	attack-type	検知回数
ルール 1	0(password crack)	595
	1(type1)	84
ルール 2	2(type2)	50
	3(type3)	25
該当なし		34
合計		788

6.2.2　しきい値未満の通信の比較

従来手法において，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未満である通信数は 7,184 件であった．一方，提案手法は，1,597 件観測された．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ため，その後のコネクションは観測されない．また，提案システムでは，従来システムで検知した攻撃者 IP アドレスを全て検知できていた．表 9 に SCRAD で検知した攻撃者において，前回検知された攻撃の種類を示す．また，595 件の攻撃者 IP アドレスが前回 SCRAD により検知されていた．これは攻撃者テーブルへの検索方法において，1 つの送信元が複数の攻撃タイプで検知されている場合，最小の attack-type 値が選択されるため，このような結果となったと考えられる．さらに 159 件の攻撃者 IP アドレスが，前回不正通信検知システムにより検知されていた．提案手法は，前回検知された攻撃の種類から SCRAD の検知基準を変更するため，パスワードクラッキング攻撃の通信を連続 10 回観測する前に検知できる．以上のことから，提案手法は従来システムと比較すると，より早期に攻撃者を検知できた．

また，34 件の攻撃者 IP アドレスが，DB に情報が格納されていない段階でパスワードクラッキング攻撃を仕掛けていた．これらの送信元の中には，1 つの攻撃者が複数の送信元を用いて攻撃を仕掛ける場合が考えられる．攻撃の流れとして，初めに，ある送信元を用いて scan 攻撃を仕掛け，応答のあった SSH サーバのリストを作成する．その後，リストをもとに scan 攻撃を仕掛けた IP アドレスとは別の IP アドレスを用いてパスワードクラッキング攻撃を仕掛ける場合である．

6.2.3　攻撃者検知回数の比較

従来手法で検知した攻撃者 IP アドレス数は 179 件であり，提案手法は 195 件であった．そこで提案手法だけ検知した 16 件の送信元 IP アドレスについて調査した．その結果，全ての送信元を不正通信検知システムが検知していた．16 件の送信元 IP アドレスは，しきい値以上の通信を 1 回も観測しなかったため，全て攻撃者だと推測される．また，パケットデータを調査すると，学内ネットワークの利用していない IP アドレスに SYN パケットを送信していた．よって，これらの送信元は scan 攻撃を仕掛けた後，パスワードクラッキング攻撃を仕掛けてきた攻撃者と考えられる．

```
16 A -> 133.37.B FAIL 2014 05/15 02:05:30
16 A -> 133.37.C FAIL 2014 05/15 02:05:48
16 A -> 133.37.C FAIL 2014 05/15 02:05:54
18 A -> 133.37.D FAIL 2014 05/15 02:22:33
```

図 7　非正規通信ログ (従来手法)

```
## 2014 05/15 02:05:30 A type1
16 A -> 133.37.B FAIL 2014 05/15 02:05:30
```

図 8　攻撃者ログ (提案手法)

16 件の攻撃者 IP アドレスのうち，ある 1 つの IP アドレス (A) を抽出し，その非正規通信ログ (従来手法) と攻撃者ログ (提案手法) を図 7 と図 8 にそれぞれ示す．図 7 は，左から，パケット数，攻撃者 IP アドレス，SSH サーバの IP アドレス，コネクションの判定，コネクションの検知時刻を表している．また，図 8 において，1 行目は左から，攻撃者検知時刻，攻撃者 IP アドレス，前回検知された攻撃の種類を表している．2 行目は図 7 と同様である．挙動を調査した結果，1 コネクションあたりのパケット送受信回数がしきい値未満である通信を 4 回連続で観測していた．その他の送信元 IP アドレスも，全ての通信がしきい値未満であり，しきい値未満の通信数が 10 回未満であった．従来手法は，しきい値未満の通信を連続 10 回観測した場合に，その送信元を攻撃者として検知する．しかし，今回観測した送信元のように，パスワードクラッキング攻撃を仕掛ける通信数が 10 回未満であった場合，その送信元を検知漏れする問題点があった．一方，提案手法において，この攻撃者 IP アドレスは不正通信検知システムの type1 で前回検知されているため，検知基準が連続 10 回から 1 回に減少する．よって，しきい値未満の通信数が 4 回でも検知できた．以上のことから，提案手法は従

来の SCRAD で検知していなかった攻撃者を検知できた.

7 おわりに

7.1 まとめ

本論文では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を連携させることで，より早期に攻撃者を検知するシステムを提案した．その結果，従来手法と比較すると，提案手法は，従来の 5 分の 1 の通信数で攻撃者を検知できた．また，攻撃者検知回数は増加していた．よって，提案手法は従来システムと比較すると，より早期に攻撃者を検知できた．さらに，従来の SCRAD で検知していなかった攻撃者を検知できた.

7.2 今後の課題

本実験は不正通信検知システムと SCRAD の情報を共有させた．不正通信検知システムが検知する攻撃は，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) の事前攻撃と捉えることができる．提案手法は，事前攻撃を仕掛けた後に具体的な攻撃が仕掛けられる挙動が観測される場合，有効であると考える．今後は，SSH サービスだけでなく，他のサービスへの攻撃を検知するシステムと不正通信検知システムを共有させていく．また，DB が許容できる最大レコード数の調査や，レコードの挿入・削除の負荷を調査することも今後の課題である．さらに，2 つの攻撃検知システムのしきい値の妥当性を検証していく必要がある.

謝辞

本研究の一部は JSPS 科研費 25870558 の助成を受けたものである.

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.

[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, 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.

[4] 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-025, pp. 31–36, 2004 年 5 月.

[5] L. Chi-Chun, H. Chun-Chieh, K. Joy. A cooperative intrusion detection system framework for cloud computing networks. In *2010 39th International Conference on Parallel Processing Workshops*, pp. 280–284, Sep. 2010.

[6] ポートスキャン. 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. 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 (Proposed Standard), February 2012.

[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.