SMTP AUTHに対するパスワードクラッキング攻撃におけるデータサイズを用いた検知システムPASSPIEの提案と評価

清水 光司[1,a)]　池部 実[2]　吉田 和幸[3]

概要：SMTP AUTH はメール送信時に送信者がユーザ本人であることを確認するための SMTP 拡張機能である．大分大学のメールサーバにおいて，SMTP AUTH に対するパスワードクラッキング攻撃を観測している．SMTP AUTH パスワードクラッキング攻撃が成功した場合，メールサーバは spam 送信の踏み台にされる危険性がある．そこで，本論文では SMTP AUTH に対する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，送信元と SMTP サーバ間のコネクションにおいて送受信するデータサイズに着目した SMTP AUTH に対するパスワードクラッキング攻撃検知システム PASSPIE を提案する．予備調査として，攻撃の通信とメール送信成功時の通信のそれぞれの 1 コネクションあたりの送受信するデータサイズをメールサーバのログから調査した．調査結果から，攻撃の検知のしきい値として，1 コネクションあたりのデータサイズを 1,000Byte 未満とした．PASSIPIE システムでは，誤検知防止のためにデータサイズが 1,000Byte 未満のコネクションを連続 10 回観測した送信元 IP アドレスを攻撃者として検知する．提案手法の有用性を，大分大学の SMTP サーバ宛のパケットデータを用いて評価した．実験結果より，検知結果の適合率は 0.51，再現率は 0.86，および F 値は 0.64 となった．誤検知した送信元について調査したところ，メールサーバにより SMTP コネクションが拒否されていた．メールサーバにより拒否された送信元を除けば，PASSPIE システムは SMTP AUTH に対するパスワードクラッキング攻撃を十分に検知できることが判明した．

キーワード：SMTP，メール，SMTP AUTH，不正通信検知，パスワードクラッキング攻撃

PASSPIE : Proposal and Evaluation for detection system using data size of SMTP AUTH password cracking attacks

KOUJI SHIMIZU[1,a)]　MINORU IKEBE[2]　KAZUYUKI YOSHIDA[3]

Abstract: SMTP AUTH is an extension of SMTP in order to confirm the validity of an email sender. We have observed SMTP AUTH password cracking attacks to mail servers in Oita University. If the attacker's SMTP password cracking attack is successful, there has a risk that mail server becomes to send spam. In this paper, we propose a detection system for SMTP AUTH password cracking attacks (PASSIPIE). PASSIPIE system detect SMTP AUTH password cracking attacks using data size of connection between SMTP client and server. Firstly, we investigated data size per connection the following cases, (1) Maximum data size of connection in SMTP AUTH password cracking attacks (2) Minimum data size of connection in successful of mail sending. As an investigation result, we decided to detection threshold values of less than 1000 bytes per connection for SMTP AUTH password cracking attacks. Our system detects SMTP client that connect less than 1000 bytes per connection to SMTP server 10 times continuously to avoid false positives. We evaluated the usefulness of PASSPIE using captured SMTP packet data to SMTP server. We calculated Precision, Recall and F-measure: Precision is 0.51, Recall is 0.86, and F-measure is 0.64. As a result, the detection results of PASSPIE system included some false positives. We investigated false positives. Our SMTP server rejected the SMTP clients. Therefore, the data size of false positives is less than benign connections. We confirmed to detect SMTP AUTH password cracking attacks by our PASSIPIE system except for rejected client by mail server.

Keywords: SMTP, Mail, SMTP Authentication, Anomaly Detection, Password Cracking Attacks

1. はじめに

インターネットの普及と発展に伴い，我々の生活に電子メールをはじめとしたネットワークを介したコミュニケーションは不可欠になっている．しかし，インターネットを利用した不正通信も数多く存在し，サービス妨害や攻撃の踏み台を得るために，多くの攻撃が行われている．

SMTP Authentication（以下，SMTP AUTH）[1] は SMTP クライアントがメール送信時に，送信者が正規のユーザであることを確認するユーザ認証プロトコルである．メールアカウントの悪用により spam 送信を目的とした SMTP AUTH に対するパスワードクラッキング攻撃が問題になっている [2]．大分大学の STMP サーバに対する SMTP AUTH を破ることを目的としたパスワードクラッキング攻撃を観測している．パスワードクラッキング攻撃により SMTP AUTH を破られた場合，spam 送信の踏み台にされる危険性がある．そのため，SMTP AUTH に対するパスワードクラッキング攻撃を検知し，対処する必要がある．

我々は，これまで 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）[3] を開発・運用してきた．SCRAD はインターネットと学内ネットワークの境界のパケットを収集し，送信元とサーバの間で送受信する 1 コネクションあたりのデータサイズからパスワードクラッキング攻撃を検知する．本論文では，SCRAD システムを応用し，収集したパケットから送信元と SMTP サーバ間の TCP コネクションを管理し，1 コネクションあたりのデータサイズをもとに SMTP パスワードクラッキング攻撃を検知する手法を提案する．

本論文の構成を以下に示す．2 章では，ネットワークトラフィックの解析による不正通信の検知に関する研究について述べる．3 章では，大分大学のメールシステムについて述べる．4 章では，SMTP AUTH に対するパスワードクラッキング攻撃検知システムの構成について述べる．5 章では，データサイズによる SMTP AUTH に対するパスワードクラッキング攻撃の検知手法について述べる．6 章では，SMTP AUTH に対するパスワードクラッキング攻撃検知システム PASSPIE の評価結果について述べる．7 章では，本論文のまとめと今後の課題について述べる．

[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, Oita 870-1192, Japan
[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, Oita 870-1192, Japan
[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, Oita 870-1192, Japan
[a)] v15e3014@oita-u.ac.jp

2. 不正通信の検知に関する研究

本章では，ネットワークトラフィックの解析によるトラフィックの異常やパスワードクラッキング攻撃の検知に関連する研究について述べる．

トラフィックを解析し異常検知する手法として Matthew らの手法 [4] が挙げられる．Matthew らは，トラフィックから異常検知に利用しないパケットをフィルタリングにより除外したうえで，パケットのヘッダ情報から SYN パケットや ACK パケット，21 番ポートや 23 番ポートに向けたパケットなど 9 つのモデルに分類する．さらに各パケットが該当するモデルの数だけ異常値を計算し，攻撃を検知する．パケットが複数のモデルに当てはまる場合は，それぞれのモデルで異常値を計算し，その合計を異常値として割り当てる．この手法では SMTP に限らず，広い範囲の異常を検知できるが，The 1999 DARPA off-line intrusion detection evaluation [5] を用いた評価実験では，scan 攻撃の検知率が優れていたものの，パスワードクラッキング攻撃の検知率が低い．

トラフィックの解析から 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として Vykopal らの手法 [6] が挙げられる．Vykopal らは，SSH へのパスワードクラッキング攻撃を分析し，パスワードクラッキング攻撃によるトラフィックのパターンを一般的な SSH トラフィックと比較することでリアルタイムに SSH に対するパスワードクラッキング攻撃を検知するとともに攻撃成功の判別を可能にした．SSH パスワードクラッキング攻撃の検知および SSH パスワードクラッキング攻撃の成功の判別には，決定木手法を用いている．この決定木にはトラフィックにおけるパケットの送信間隔や送信回数，データサイズの情報が含まれている．この手法を SMTP に応用することで SMTP パスワードクラッキング攻撃を検知できる可能性はあるが，SMTP へのパスワードクラッキング攻撃については着目されていなかった．

ネットワークトラフィックを解析し，パスワードクラッキング攻撃を検知する研究は存在するが，現在のところ，SMTP AUTH に対する攻撃を対象とした研究を確認できていない．

一方，SMTP AUTH パスワードクラッキング攻撃やフィッシングにより，ユーザ名とパスワードが漏れた際の対策としては SMTP サーバのメール送信ログをもとにパスワードの不正利用による spam 送信を抑制する対策手法としてメール送信元 IP アドレスの地理情報に着目した山井らの手法 [7] が挙げられる．本手法はメール送信時のログを監視する．ログ中の送信元 IP アドレスを抽出し，GeoIP[8] により地理情報を取得する．さらに取得した地理情報から送信元の国を割り出し，24 時間以内に 4 ケ国以上

からの接続を検出基準としてパスワードを不正取得した送信元によるメール送信をアカウント停止後に Postfix を再起動することで抑制する．この手法ではメールアカウントの不正利用による spam 送信を抑制することを目的としており，SMTP AUTH に対するパスワードクラッキング攻撃そのものを検出することはできない．

3. 大分大学のメールシステム

本章では，大分大学のメールシステムについて述べる．大分大学には，2 つの SMTP サーバが存在する．ひとつは MX レコードに記載のある SMTP サーバ (1)，もうひとつは，大分大学のユーザがメールを送信する際に利用する SMTP サーバ (2) である．本論文では，インターネットからの SMTP AUTH パスワードクラッキング攻撃を多く観測している MX レコードに記載のある SMTP サーバ (1)(以降，メールサーバと呼ぶ) を観測対象とする．

メールサーバでは，TCP/25，TCP/587，TCP/465 でサービスを提供しており，3 つのどのポートにおいても SMTP AUTH を提供している．特に，TCP/25 宛の SMTP AUTH 試行を多く観測している．3 つのポートにおいて観測した SMTP AUTH 試行の中には正規ユーザによる試行の他に攻撃者による SMTP AUTH 失敗も存在している．メールサーバでは，SMTP AUTH の要求を受信すると，メールサーバのプロセスは，SASL(Simple Authentication and Security Layer) デーモンである saslauthd へ，アカウント情報を渡す．saslauthd では，LDAP によりアカウント情報を確認する．LDAP にアカウントが存在しない，パスワードが一致しない場合には，saslauthd が，/var/log/messages（以下，messages）に認証失敗と記録する．saslauthd により認証失敗したとの結果が，メールサーバのプロセスへ返る．そうすると，メールサーバは，“did not issue MAIL/EXPN/VRFY/ETRN during connection to (宛先)” と/var/log/maillog（以下，maillog）に出力して，送信元からの SMTP コネクションを終了する．

大分大学のメールサーバでは，SMTP AUTH の認証成否に関するログを saslauthd が messages に出力する．また，メールに関するログは maillog にメールサーバのプロセスが出力する．

2016 年 7 月 4 日から 7 月 10 日までの 1 週間のメールサーバにおける SMTP AUTH 失敗数を messages より調査したところ，49,827 件存在した．SMTP AUTH 攻撃を検知し，攻撃を防ぐためには送信元 IP アドレスを用いて，インターネットと学内ネットワークの境界やメールサーバにおいて，ファイアウォールにより遮断することが有効である．しかし，messages には，SMTP AUTH の認証が失敗した場合，“saslauthd: do_auth: auth failure: [user=libserv] [service=smtp] [realm=oita-u.ac.jp] [mech=ldap] [reason=Unknown]” のように出力される．このように saslauthd の出力ログには，送信元 IP アドレスが含まれない．一方，maillog には，SMTP AUTH 失敗に起因するログとして，“did not issue MAIL/EXPN/VRFY/ETRN during connection to (宛先)” と出力されるが，SMTP AUTH 以外のエラーの場合にも同様のログが出力される．そのため，メールサーバのログを常時監視するだけでは，SMTP AUTH に対するパスワードクラッキング攻撃を検出することはできない．

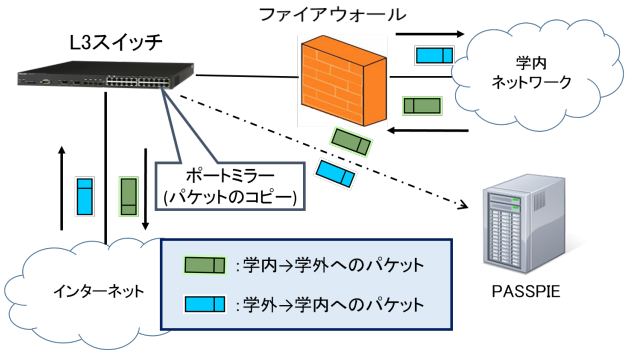

図 1: PASSPIE システムの構成図

4. SMTP AUTH に対するパスワードクラッキング攻撃検知システム PASSPIE の提案

3 章で述べたように，大分大学のメールサーバではログの監視により SMTP AUTH へのパスワードクラッキング攻撃を検出することが難しい．そこで，我々がこれまでに提案した SSH パスワードクラッキング攻撃検知システム SCRAD のネットワークトラフィックを解析し，攻撃者を検知する手法を SMTP AUTH に対するパスワードクラッキング攻撃に応用し，攻撃の検知に対する有用性を評価する．

4.1 PASSPIE の概要

SMTP パスワードクラッキング攻撃を検知するために，本論文では PASSPIE（Prevention for password cracking Attack of Smtp authentication by Smtp Packet InspEction）システムを提案する．PASSPIE システムは，インターネットと学内ネットワークの境界を通過するパケットを LAN スイッチのポートミラー機能で複製し，tcpdump を用いてパケットをリアルタイムにキャプチャする（オンラインモード）．PASSIPIE システムでは，tcpdump のフィルタ機能を用いて TCP/25，465，587 番ポートに関するパケットのみを抽出する（図 1）．

また，送信元 IP アドレスをキーとして，各コネクションにおける SYN パケットのシーケンス番号と FIN パケットのシーケンス番号からデータサイズを算出する．PASSIPIE システムでは，算出したデータサイズを用いて攻撃を判定する．PASSIPIE システムにおけるパスワードクラッキン

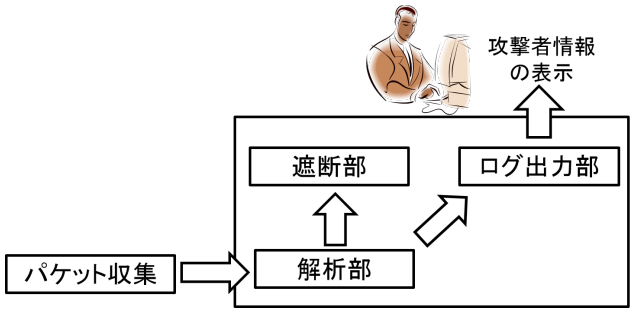

図 2: PASSPIE システムの内部構成

グ攻撃検知手法については，5 章で詳述する．

PASSIPIE システムでは，IPv4 アドレスからの攻撃を対象としている．送信元 IP アドレスごとの情報を，送信者ツリーと攻撃者ツリーの 2 つのパトリシアツリーを用いて管理する．送信者 IP アドレス，攻撃者 IP アドレスをパトリシアツリーにて管理する理由としては，IPv4 アドレスにおける共通のプレフィックスをまとめて管理するため，木の深さが最大 32 となり，検索時間が安定するためである．オンラインモードでは，ミラーリングパケットをキャプチャし，取得したパケットデータから送信元 IP アドレスごとのデータサイズの小さいコネクション数を計数することにより，リアルタイムでパスワードクラッキング攻撃を検知する．さらに，検知した送信元 IP アドレスは送信者ツリーから攻撃者ツリーへ挿入する．攻撃者ツリーに挿入した IP アドレスは経路制御にて SMTP サーバからの戻りのパケットを破棄することにより攻撃を防ぐことができる．しかし，複数の送信元 IP アドレスを用いることで 1 つの送信元 IP アドレスあたりの攻撃数が少ないボットネットによる攻撃や，既にフィッシングの被害により SMTP AUTH のユーザ名とパスワードの組み合わせが漏れている場合は対処できない．提案システムは，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パスワードクラッキング攻撃を検知できる．また，検知のために個人的な情報が含まれる可能性のあるペイロード部分に着目する必要がない．この 2 点は，ネットワークトラフィックの解析による手法の利点である．

PASSPIE システムはミラーリングしたパケットを直接収集するオンラインモードの他に，pcap ファイルを入力データとするオフラインモードがある．オフラインモードでは，あらかじめ収集した pcap ファイルを入力することで，リアルタイムでなくとも攻撃判定が可能である．

4.2 PASSPIE の構成

PASSPIE システムは「解析部」「遮断部」「ログ出力部」の 3 つのコンポーネントから構成されている (図 2)．遮断部については未実装のため，遮断部以外のそれぞれのコンポーネントについて述べる．

4.2.1 解析部

解析部では収集したパケットの IP ヘッダ，TCP ヘッダから送信元 IP アドレス，宛先 IP アドレス，送信元ポート番号，宛先ポート番号，TCP フラグ，シーケンス番号の 6 つのデータを抽出し，パスワードクラッキング攻撃かどうかを判定する．本システムでは，SMTP クライアントから SMTP サーバに対して，SYN パケットのみが送信された場合，SMTP サーバに対する探索行為である scan 攻撃として認識し，該当する SMTP クライアントのコネクション情報を破棄する．

4.2.2 ログ出力部

ログ出力部では，解析部によりパスワードクラッキング攻撃と判定した送信元に関する情報を「攻撃者ログ」として出力し，管理者に提示する．その他にも，1 コネクションあたりのデータサイズが 1,000Byte 以上の場合のコネクション情報を記録する「正規通信ログ」，1,000Byte 未満の場合のコネクション情報を記録する「非正規通信ログ」がある．すべてのログには 1 コネクションあたりのデータサイズ，パケット送受信回数，送信元 IP アドレス，送信元ポート番号，宛先 IP アドレス，宛先ポート番号，パケット最終検知時刻を記載している．

また，PASSPIE システムは処理中のパケットの送信元 IP アドレスが攻撃者ツリーに存在する場合，コネクション管理をせずに，そのパケットの送信元 IP アドレス，送信元ポート番号，宛先 IP アドレス，TCP フラグ，パケット取得時刻を「再検知ログ」に出力している．

5. データサイズによる SMTP AUTH に対するパスワードクラッキング攻撃の検知手法

SMTP パスワードクラッキング攻撃検知システム PASSPIE では，TCP ヘッダのシーケンス番号からデータサイズを求め，そのデータサイズをしきい値として攻撃を判定する．本章では，PASSPIE システムにおけるデータサイズを用いた SMTP AUTH に対するパスワードクラッキング攻撃の検知手法を述べる．提案システムの手法では，SMTP AUTH に成功し，メールを送信したコネクションと，SMTP AUTH の突破を試みて認証に失敗したコネクションを区別することを目的としている．まず，予備調査として正規ユーザによるメール送信成功時と攻撃の通信におけるデータサイズの差異を確認するため，メール送信成功時のコネクションと攻撃者のコネクションにおいて送受信されるパケットのデータサイズを調査した．なお，データサイズの算出には，クライアントとサーバの双方向におけるコネクションの SYN パケットと FIN または RST パケットのシーケンス番号の差を用いている．また，調査には，クライアントとサーバの双方向におけるデータサイズを合計したデータサイズを用いる．

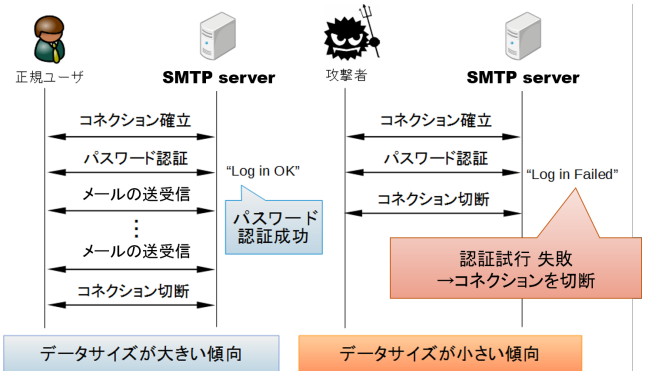

図 3: 1 コネクションにおけるデータサイズの違い

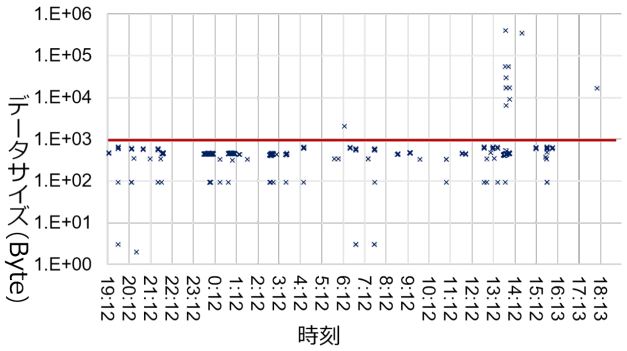

図 4: SMTP AUTH に失敗したコネクションにおけるデータサイズ

5.1 SMTP コネクションにおいて送受信するデータサイズの傾向

正規ユーザによる SMTP コネクションと攻撃者による SMTP コネクションのデータサイズの傾向の違いを図 3 に示す．外に移動した正規ユーザが SMTP サーバにメールを中継させる際の通信は，認証メカニズムを交換したあと，ユーザが要求した認証メカニズムによりユーザを認証する．その後にメールを送受信する．よって，正規ユーザが 1 コネクションあたりに送受信するデータサイズは大きくなる傾向にある．一方，攻撃者と SMTP サーバの通信は，パスワードクラッキング攻撃によって何度もユーザ認証を繰り返す．ユーザ認証に失敗すると，TCP コネクションは切断される．そのため，正規ユーザの通信にあるメールの送受信は生じない．よって，攻撃者による 1 コネクションあたりのデータサイズは小さくなる傾向にある．

5.2 SMTP コネクションにおけるデータサイズの予備調査

5.1 節で述べたように，正規ユーザと攻撃者の SMTP コネクションのデータサイズには，傾向の違いがある．本節では SMTP AUTH パスワードクラッキング攻撃を検知するためのデータサイズのしきい値を決定するため，攻撃者の SMTP コネクションで送受信するパケットのデータサイズ，正規ユーザの SMTP コネクションで送受信するパケットのデータサイズを調査した．本調査における攻撃者と正規ユーザの分類は，メールログにおいて，メール送信に失敗したコネクションを攻撃者のコネクション，メール送信に成功したコネクションを正規ユーザのコネクションとした．調査方法については，以下の項で詳しく述べる．

5.2.1 攻撃者のコネクションにおけるデータサイズの調査

攻撃者のコネクションで送受信するデータサイズの最大値を調査した．2016 年 5 月 26 日 19 時 14 分から 2016 年 5 月 27 日 18 時 03 分の約 1 日分の期間に図 1 の L3 スイッチから tcpdump により収集したパケットデータを用いて，1 コネクションあたりの送信元と SMTP サーバの間で送受信されるデータサイズを調査した．

本調査のために，まず，SMTP AUTH に失敗した送信元 IP アドレスを抽出する必要がある．大分大学のメールサーバでは，認証失敗ログ (messages) とメールログ (maillog) を別のプロセスにより出力するため，SMTP AUTH に失敗した送信元 IP アドレスを直接調査することはできない．そこで，messages と maillog，さらに tcpdump により収集したパケットデータを PASSPIE システムにより分析し，得られたコネクションごとの情報の 3 つを照合することにより調査した．本調査で用いた PASSPIE システムでは攻撃判定のためのしきい値は設定していないため，約 1 日分の収集したパケットデータに含まれるすべてのコネクションについて，4.2.2 項で述べたログ情報が得られる．

messages における SMTP AUTH 失敗ログの出力時刻と，maillog のメッセージを比較したところ，SMTP AUTH に失敗した時刻とほぼ同時刻に maillog では”did not issue MAIL/EXPN/VRFY/ETRN during connection to (宛先)“メッセージが出力されている．そこで，maillog における SMTP AUTH に失敗したと考えられるメッセージから抽出した送信元 IP アドレスと時刻を PASSPIE システムの出力ログを照合し，SMTP AUTH に失敗したと考えられるコネクションのデータサイズを調査した．なお，ログ中の”did not issue MAIL/EXPN/VRFY/ETRN during connection to (宛先)“メッセージは，SMTP コネクションを接続した状態で，有効なコマンドの発行がないままタイムアウト切断したときに出力されるため，必ずしも SMTP AUTH の失敗が原因とは限らない．しかし，SMTP AUTH に失敗した場合は，このメッセージとなる．

maillog を照合した結果，調査対象となるコネクションは 1,130 件存在した．調査結果について，縦軸をデータサイズ，横軸を時刻としたグラフを図 4 に示す．1,130 件のうち，98%が含まれる 1,000Byte をしきい値として，分類し分析した．図 4 のグラフ中の赤線は，データサイズ 1,000Byte を示している．1,130 件のコネクションのうち，14 件のコネクションがデータサイズ 1,000Byte を超えて

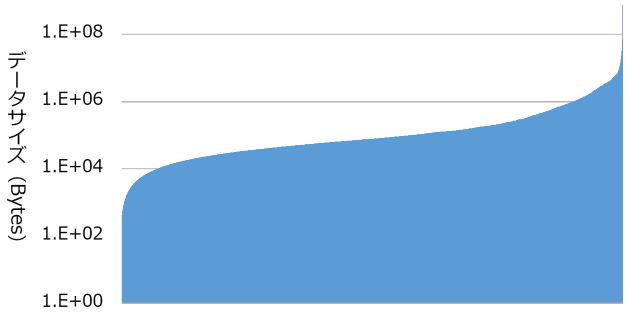

図 6: メール送信成功時におけるデータサイズ（昇順）

表 1: メール送信成功時におけるデータサイズの詳細

項目	データサイズ (Byte)
最小値	271
最大値	751,696,733

いた．14 件のコネクションと対応する maillog を詳細に調査したところ，SSL 証明書のやり取りについての設定の食い違いが原因で接続がタイムアウトしたため，”did not issue MAIL/EXPN/VRFY/ETRN during connection to ***(宛先)”が出力されたと判断した．

また，本調査におけるデータサイズ 1,000Byte 未満での最大値は 982Byte であった．そのため，本論文における調査では，データサイズ 1,000Byte 未満のコネクションを SMTP に対するパスワードクラッキング攻撃として検知できると考えられる．

5.2.2 正規ユーザのコネクションにおけるデータサイズの調査

正規ユーザによるメール送信成功時のデータサイズの最小値を調査するために，maillog をもとにメールの送信に成功したコネクションで送受信するデータサイズを調査した．調査は 2016 年 5 月 1 日 0 時 0 分 0 秒から 5 月 16 日 1 時 4 分 4 秒までに観測した 1,000,000 行のメール送信に成功したログを対象として，対象のログにおけるデータサイズを抽出した．メール送信成功の判断には，図 5 に示すメールログ中のメッセージ ID が含まれるかどうかを基準とした．また，データサイズは size の項目より抽出した．抽出した結果を縦軸をデータサイズとして昇順にソートしてプロットした結果を図 6，正規ユーザのコネクションにおけるデータサイズの最小値・最大値を表 1 に示す．図 6 と表 1 からメール送信に成功した際のデータサイズは大半が 1,000Byte を超過していた．最小値が 271Byte となっており，1,000,000 件中 664 件においてデータサイズが攻撃者の最大値である 1,000Byte を下回っていた．664 件は，わずか 0.07%であるが誤検知であることから，この 664 件のコネクションについて詳細に調査したところ，送信元メールアドレスの大半が携帯電話会社のキャリアメールであった．よって，携帯キャリアによるメール送信においては，データサイズが 1,000Byte を下回る可能性がある．さらに，メール送信成功時にデータサイズが 1,000Byte を下回ったコネクションを観測したその他のメールアドレスについては，通信間隔が不定期であり，おそらくメール受信確認として本文のないメールを送信したためにデータサイズが小さくなったと考えられ，攻撃の可能性は低いと判断した．

表 2: PASSPIE による検知結果

検知結果	検知コネクション数
SUCCESS コネクション	139,645
FAIL コネクション	65,563

表 3: 期間内における攻撃に関する集計

集計項目	集計数
検知した攻撃者による FAIL コネクション (A)	33,649
攻撃者ツリー挿入期間内の攻撃コネクション (B)	44,564
SMTP AUTH 失敗数 (C)	46,909
検知した攻撃における正解数 (D)	40,228

5.3 データサイズによる検知手法の提案

5.2 節の予備調査より，提案システムの詳細な検知手法を決定した．

- 1 コネクションで送受信するデータサイズが 1,000 バイト未満のコネクションを攻撃のコネクション（FAIL コネクション）とする
- 誤検知防止のため，FAIL コネクションを 10 回連続で観測した送信元を攻撃者として検知する
- 誤検知防止のため，提案システムでは携帯キャリアメールによる通信を送信元 IP アドレスにより排除

6. PASSPIE システムの評価

提案システムの有用性について検証するために，2016 年 8 月 23 日 12 時 02 分から 8 月 30 日 12 時 03 分までの 1 週間に収集したパケットデータを用いて評価実験をした．実験内容は，パケットデータに含まれる SMTP コネクションを PASSPIE システムが攻撃のコネクションとメール送信に成功したコネクションに分類し，分類の精度を評価した．

6.1 実験結果

実験結果を表 2 に示す．評価基準としては適合率，再現率，および F 値を用いた．適合率は PASSPIE の検知結果にどの程度実際の攻撃のコネクションが含まれるかを示す．再現率は実際の攻撃のコネクションを PASSPIE がどの程度検知できたかを示す．一般に適合率が高い場合，再現率が低くなり，再現率が高い場合，適合率が低くなるトレードオフの関係にあるため，適合率と再現率の調和平均をとった F 値により，PASSPIE の検知精度を評価した．適合率

May 27 19:57:04 : u4RAv4vw015199: from=<example@example.com>, size=10577,
class=0, nrcpts=2, msgid=<05ed01d1b80684706cd08d514670@example.com>, proto=ESMTP,
daemon=MTATO, relay=smtp.example.com [SrcIPaddr]

図 5: メール送信成功時の maillog

と再現率の算出のために，実験データの収集期間内におけるメールサーバの maillog，messages，および PASSPIE のログについて調査した（表 3）．4.2.2 項で述べたように，PASSPIE システムはオフラインモードでの実験の際にも，攻撃者ツリーに存在する送信元 IP アドレスのパケットをコネクション管理せずに再検知ログに出力する．本章の実験において比較対象となる messages や maillog では調査期間内のすべての通信ログが含まれるため，再検知ログのパケットについてもコネクション単位で計数し，検知した攻撃コネクションの計数に含める必要がある．表 3 中の攻撃者ツリー挿入期間内の攻撃コネクションは，再検知ログの送信元 IP アドレスと送信元ポート番号をもとに攻撃者として検知している期間中の攻撃の通信を計数した値である．また，SMTP AUTH 失敗数は実験データの収集期間と同様の期間におけるメールサーバの messages に含まれる”do_auth:　auth failure:”の行を集計した．検知した攻撃における正解数は，maillog における SMTP AUTH 失敗時のログを送信元 IP アドレスごとに集計し，PASSPIE が検知した送信元 IP アドレスごとの FAIL コネクション数，および redetect 数と比較し，攻撃の通信を正確に検知した値を算出した．実験結果より調査した表 3 の値を用いて適合率，再現率，および F 値を算出した結果を以下に示す．

適合率

$$Precision = \frac{D}{A+B} = \frac{40228}{78213} = 0.51433$$

再現率

$$Recall = \frac{D}{C} = \frac{40228}{46909} = 0.85757$$

F 値

$$F - measure = \frac{2 \times Precision \times Recall}{Precision + Recall} = 0.64029$$

適合率が 0.51，再現率が 0.86 となり，この 2 値の調和平均である F 値が 0.64 となった．適合率が 0.51 となった原因として，SMTP AUTH 失敗のコネクションではないにもかかわらず，データサイズ 1,000Byte を下回るコネクションを多く誤検知した．誤検知については次節で詳細な調査結果を示す．再現率が 0.86 となり，パスワードクラッキング攻撃の検知の観点においては十分に検知可能な値と判断した．しかし，適合率が低いため，F 値による総合的な評価では 0.64 となったため，今後は誤検知を減らすための改善が必要となる．

表 4: エラーコード別のメール送信拒否数

エラーコード	原因	観測数
418	FROM のドメイン部が DNS に未登録	4,287
451	greylist により再送要求	23,692
452	FROM のドメイン部が oita-u.ac.jp	50
453	FROM のドメイン部が local で終わる	96
455	不正中継メール	27
472	FROM のドメイン部が悪性ドメイン	1,644
475	MTA が Black List に登録されている	13
516	FROM のドメイン部が MX レコードが DNS に未登録	7
551	MTA が Black List に登録されている	1,816
573	TO のドメイン部の打ち間違い	10
User unknown	FROM のローカルパート部が LDAP に存在しない	4,287

6.2 誤検知の考察

実験において PASSPIE システムの誤検知数は表 3 より，(A+B)-D=37,985 件存在している．PASSPIE が検知した送信元 IP アドレスのうち，maillog からは SMTP AUTH への攻撃が確認できなかった送信元 IP アドレスの maillog を図 7 に示す．maillog の記述によると，この送信元 IP アドレスのメール中継をメールサーバが拒否しているため，実際にはメールが送信されていない．そのため，1 コネクションあたりのデータサイズが 1,000Byte を下回ったと考えられる．よって，誤検知した原因は，メールサーバのポリシーによってメールの送信が拒否されたことで，図 3 に示す SMTP AUTH 失敗時と同じような通信の挙動になったためと考えられる．図 7 における reject=452 のメッセージは，大分大学のドメインでないメールアドレスによってインターネットから学内へメール送信する際に，SMTP AUTH による認証が行われない場合，送信元 IP アドレスの偽装とみなしてメール送信を拒否する独自のポリシーが適用されたことを示す．メールサーバのポリシーによってメール送信が拒否されたことが原因となった誤検知を，エラーコード別に表 4 に集計した．表 4 における観測数は，実験期間中に観測した数を示す．このようなメールサーバのポリシーによるメール送信拒否を表 4 の観測数の合計よ

```
Aug 25 08:44:27 u7ONiK3B010049: from=<foo@oita-u.ac.jp>, size=3980 ,..., relay=mail.example.co.jp [srcIP:A]
Aug 25 08:44:27 u7ONiK3B010049: ruleset=check_mail, arg1=<foo@oita-u.ac.jp>, relay=mail.example.co.jp [srcIP:A], reject=452
4.5.2 src address forged
```

図 7: 誤検知したと考えられるコネクションの maillog

り 35,987 件観測している．表 4 に示す挙動を PASSPIE システムが攻撃として誤検知しても，通常のメール送信の妨げになることはない．しかし，PASSPIE システムの目的として SMPT AUTH に対するパスワードクラッキング攻撃を検知することであったため，本論文では誤検知とした．誤検知を回避するために，今後はメールサーバのポリシーを考慮した検知手法を検討する必要がある．

7. おわりに

7.1 まとめ

大分大学のメールサーバにおいて，SMTP AUTH に対するパスワードクラッキング攻撃を観測した．SMTP パスワードクラッキング攻撃により，spam 送信の踏み台となる危険性がある．

そこで本論文では，SMTP AUTH に対するパスワードクラッキング攻撃を検知し，遮断するために，1 コネクションあたりのデータサイズに着目した PASSPIE システムを提案した．予備調査としてメール送信成功時におけるデータサイズと，SMTP AUTH 失敗時におけるデータサイズをそれぞれ調査した．それぞれの調査結果から，1 コネクションあたりのデータサイズが 1,000Byte を下回るコネクションを攻撃のコネクションとして検知できると考えた．しかし，メール送信成功時にも，データサイズが 1,000Byte を下回るメールログを観測したため，提案手法では，データサイズが 1,000Byte を下回るコネクションを連続で 10 回観測した送信元 IP アドレスを攻撃者として検知する．

収集したパケットデータを用いて提案手法の有用性を検証したところ，適合率が 0.51，再現率が 0.86，この 2 値の調和平均である F 値が 0.64 となった．適合率が 0.51 となった原因として，SMTP AUTH 失敗のコネクションではないにもかかわらず，データサイズ 1,000Byte を下回るコネクションを多く誤検知した．誤検知した送信元について調査したところ，メールサーバにより SMTP コネクションが拒否されていた．誤検知が多い要因として，メールサーバのポリシーによってメール送信が拒否されたログを多く観測した．メールサーバのポリシーによって一時的にメール送信を拒否された送信元を除けば，PASSPIE システムは SMTP AUTH に対するパスワードクラッキング攻撃を十分に検知できることが判明した．

7.2 今後の課題

誤検知について分析したところ，メールサーバのポリシーによりメール送信を拒否したコネクションがデータサイズ 1,000Byte を下回り，誤検知したことが判明した．そのため，今後はメールサーバのポリシーを考慮した検知手法を検討する必要がある．これまで我々が開発・運用してきた SSH パスワードクラッキング攻撃検知システム SCRAD では検知した攻撃者の送信元 IP アドレスを NULL ホストへの静的経路を設定し，攻撃者への戻りのパケット遮断してきたが，PASSPIE システムでは，検知した攻撃者 IP アドレスを Dynamic DNS を用いてグレーリストを作成し，一定時間経過後に再送を要求する処理を検討している．

参考文献

[1] R. Siemborski and A. Melnikov. Smtp service extension for authentication, July 2007. RFC4954.
[2] 渡辺 崇文. 迷惑メール送信を目的とした不正 smtp 認証の増加. Internet Infrastructure Review(online), インターネットイニシアティブ, Vol.20,pp.28-31(2013), 2013.
[3] 清水光司, 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におけるデータサイズを用いる検知手法の提案. マルチメディア，分散，協調とモバイル (DICOMO2015) シンポジウム, 2015 年 7 月.
[4] Matthew V. Mahoney. Network Traffic Anomaly Detection Based on Packet Bytes. In *Proceedings of the 2003 ACM Symposium on Applied Computing*, SAC '03, pp. 346–350, New York, NY, USA, 2003. ACM.
[5] Richard Lippmann, Joshua W Haines, David J Fried, Jonathan Korba, and Kumar Das. The 1999 {DARPA} off-line intrusion detection evaluation. *Computer Networks*, Vol. 34, No. 4, pp. 579 – 595, 2000. Recent Advances in Intrusion Detection Systems.
[6] J. Vykopal, T. Plesnik, and P. Minarik. Network-Based Dictionary Attack Detection 2009 International conference Future Networks. pp. 23–27, Mar 2009.
[7] 山井成良, 藤原崇起, 河野圭太, 大隅淑弘, 岡山聖彦. パスワード不正取得による迷惑メール発信に対する対策. 研究報告インターネットと運用技術（IOT）, Vol. 2014, No. 9, pp. 1–6, feb 2014.
[8] GeoIP. http://dev.maxmind.com/geoip/.
[9] 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, pp. 742–748, 2013 年 7 月.