一般口演 | セキュリティとプライバシー保護
一般口演4
セキュリティとプライバシー保護
2019年11月22日(金) 09:00 ～ 11:00 H会場 (国際会議場 3階中会議室304)

[2-H-1-04] 捕食出版社から医療機関に送信される迷惑メールのSMTPヘッダ情報を用いた送信戦略の予測と阻止方略の検証

○渡辺 淳[1]、仲野 俊成[1] （1. 関西医科大学 大学情報センター）

キーワード：Predatory Publisher , Unsolicited Commercial E-mail, SMTP Header, Association Analysis

近年、医療機関に向けて営利目的の捕食（ハゲタカ・ predatory)出版社からの迷惑メールが大量に送信され、その数は増加の一途をたどっている。本研究では、それらの検出・阻止を目的として、まず、2016-17年に医科大学のメール受信中継サーバに着信した捕食出版社からの迷惑メール約15万通の SMTPエンベロープヘッダ情報の特徴および時系列に沿った送信元ドメイン変化の傾向を調べた。アソシエーション分析によって、送信者アドレスのドメイン部、送信サーバの IPアドレス、送信サーバ FQDNのドメイン部、接続時に送信サーバが名乗る helo/ehloの4つの項目の間に関連性が観察された。大量送信をおこなう出版社の送信パターンは 1)送信サーバを変えずに送信者アドレスのドメイン部を次々と変化させる方式、2) 送信者アドレスのドメイン部をあまり変化させずに送信サーバを次々と変化させる方式、そして3) 送信者アドレスのドメイン部と送信サーバの組を刻々と変化させながら送信する方式に大別されることが判明した。これらのことから、メール送信に用いる送信業者および送信者アドレスのドメイン部等を変化・増加させることによって迷惑メールフィルターの回避を企図していることが推定された。また、上述の4項目に、さらに送信に用いられる通信業者等が用いている IPアドレス範囲の情報を加えてヘッダ情報の変化を予測することにより、捕食出版社からの迷惑メールを検出・阻止できる可能性が示唆された。そこで、2018年初頭から2019年上半期に捕食出版社から送信された迷惑メール（約46万通）について、上述の推定に基づいて策定した検出ルールを受信中継サーバの MTAにセットし、予測の妥当性を検出・阻止の精度を指標として検証した。その結果、捕食出版社によるヘッダ情報を刻々変化させながらの大量送信に対して、送信された迷惑メールの98%を阻止できた。

©一般社団法人 日本医療情報学会

捕食出版社から医療機関に送信される迷惑メールの SMTP ヘッダ情報を用いた送信戦略の予測と阻止方略の検証

渡辺 淳[*1]、仲野 俊成[*1]、
*1 関西医科大学 大学情報センター

Prediction of Delivery Strategy of Spam Messages from Predatory Publishers to a Medical Institution using SMTP Header Information, and Validation of Blocking Strategy based on the Prediction.

Jun Watanabe[*1] , Toshiaki Nakano[*1]
*1 University Information Center, Kansai Medical University

Recently, spam messages from predatory publishers becomes increase in fraudulent campaigns targeting doctors and researchers. To block them, we firstly examined the signatures of the SMTP envelope header information using 150,000 messages from the publishers in 2016-17. Relationships were found among the domain part of the sender address, IP address of the "sender server" (SMTP client), FQDN of the sender server, and helo/ehlo. The message delivery patterns of the publishers could be divided into 1. changing the sender address without changing the sender server, 2. changing the sender server without changing the sender address, and 3. changing both the sender address and the sender server frequently. The predatory publishers may plan to avoid spam filters by changing the sender address and the mail service providers. The information on IP address range of the mail service providers used by the publishers may thus be helpful to the blocking. We implemented filters based on these predictions in the MTA of the primary inbound gateway server and examined about 500,000 spam messages from the publishers between Jan 2018 to Jun 2019 for determining whether the suggested strategies helpful for the spam message prevention using the blocking rate as an indicator. About 98% of spam messages from the publishers were blocked with the filter even if the publishers made change the sender address and the mail service providers frequently. Abstract in English comes here.

Keywords: Predatory Publisher, Spam messages, SMTP Header, Association Analysis.

1. はじめに

近年、医療機関に向けて捕食出版社 (predatory publishers; ハゲタカ出版社)から送出される、おもに投稿料の奪取を主目的とした迷惑メール（宣伝メール）が増加しつつある。それらの捕食出版社からは偽学会(bogus/fake conference)への参加費奪取・詐取を企図した迷惑メール（CFP spam, call for paper spam）も送信されている。

過去に論文を出版したり大規模な国際学会で発表したことのある研究者の電子メールと姓名は PubMed 等の Web サイトで公開されている。一般に知名度の低い捕食出版社等では、電子メールが投稿勧誘や会議への参加要請を宣伝するための強力かつ現実的に唯一の手段となっていると考えられる。

捕食出版社や偽学会（以下、捕食出版社等と呼ぶ）については科学研究の質向上と維持を危うくすることが指摘されていること 1-5)に加え、捕食出版社等から大量に送信される迷惑メール（本稿では、以下、捕食メール-predatory messages-と称する）が医療機関の医師・研究者等の診療や研究等の業務の妨げとなっている。

そこで、本研究では捕食メール（捕食出版社・偽学会からの迷惑メール）の検出・阻止を目的とし、まず、2016-17 年に調査対象の医科大学宛に送信された捕食メールの SMTP エンベロープヘッダ（以下 SMTP ヘッダと略称）に記載されている項目のそれぞれについて特徴を調べた。そして、それらを手がかりに検索し得る隠蔽された情報 6) をも加味して各項目間の関係を調べることで、捕食メール送信戦略の推定を試みた。次に、それまでに得た特徴と推定される送信戦略に基づいた阻止ルールを策定してメール受信中継サーバ 7)にセットし、2018 年初頭から 2019 年上半期にかけて、捕食メールの阻止率を指標として予測の妥当性を検証した。

2. 材料と方法

前段の解析プロセスには 2016 年 1 月から 2017 年 12 月の 2 年間に調査対象機関の主メール受信中継サーバ (primary incoming mail gateway server) に接続した電子メールの SMTP エンベロープヘッダ情報を用いた。解析対象とした SMTP エンベロープヘッダ項目は、送信者アドレス（アカウント部とドメイン部）、送信サーバ（SMTP セッションにおける SMTP クライアント）の FQDN（fully qualified domain name）と IP アドレス、送信サーバが接続の際に greeting message で名乗る helo/ehlo（自サーバ名：以下 helo と称する）である。また、これらの記載事項をもとに whois を検索して入手した送信者アドレスのドメイン部の登録情報（ドメイン登録日、登録組織の名称と住所、匿名化されている場合は匿名化組織・機関の名称）と送信サーバ FQND のドメイン部の登録情報、および BGP tool kit 8)を用いて調べた送信サーバの IP アドレスを管理・所有する組織の保持する IP アドレス範囲について、上述の SMTP エンベロープヘッダ項目と合わせて解析した。

後段の検証プロセスには、2018 年 1 月から 2019 年 6 月の間に主メール受信中継サーバに接続してきた電子メールを用いた。上述の SMTP エンベロープヘッダ情報等による特徴抽出・解析を実施するとともに、それらの情報から推定される捕食メールの送信戦略を想定した。次に想定に則した阻止フィルタを構成してメール受信中継サーバにセットし、捕食メールの検出率・阻止率を指標として予測の妥当性を検証した。

2.1 捕食出版社が送信したメールの同定

捕食メールの同定は 2016 年末まではおもに Beall’s List

9) を参照し、リスト収載の出版社・雑誌および web サイトの検索等によってそれらの出版社と関係が認められた出版社・雑誌が所有するドメインから送出されたメールを捕食メールと判定した。 Beall's List 9)の公開終了後については、送信者アドレスドメイン部が検出時点から遡って 2-3 年以内に取得・登録されている、登録場所が出版社の所在と異なる、出版社・雑誌の web site の内容、Web of Science 10)の Journal Citation Reports (JCR) journal impact factor ranking 11) または Clarivate Analytics の Master Journal List 12)への収載が無い（または JCR/Clarivate Analytics 以外の IF: impact factor を自社の web に掲載している）等に加え、研究者や出版関係者の web、blog 記事等を検索して得られた情報を統合して判定した。なお、2018 年後半からは Beall's List の後継リスト（Stop Predatory Journals 13）および Beall's list of predatory journals and publishers 14) を判定に用いた。

2.2 特徴抽出と送信戦略の推定

SMTP エンベロープヘッダの各項目および登録情報からの特徴抽出には用手・目視法とテキストマイニングを併用し、テキストマイニングによって、各項目から抽出した特徴相互の間の関連性の描出を試みた。テキストマイニングには、多言語版 KH coder 15) を用い、おもに中心性指標を用いたネットワーク分析を実施した。ネットワーク分析によって関連性（共起関係）が示された特徴（特徴の組）を、用手法を用いたアソシエーション分析に供した。アソシエーション分析にはアプリオリのアルゴリズムを用い、検証の対象となった特徴の有無（組み合わせを含む）を「前提部」、捕食出版社のメールであることを帰結部」として、特徴（特徴の組み合わせ）毎に信頼度と支持度を求めた 16)。また、抽出した特徴のそれぞれについて感度と特異度とを算出した。これらの結果にもとづいて、正規表現で記述した阻止フィルタ群を作成するとともに、マイニングの結果に基づき、用手法を用いて送信戦略を推定した。

2.3 阻止効果の検証

調査対象機関における電子メール受信中継サーバの MTA（Mail Transfer Agent: 実装は Postfix）に検証・阻止のためのフィルタを設定した 7)。最初はログに標識 (reject_warning) を付して受信者に配信し、次に再送要求 (応答コード 450 で拒否；soft fail) し、誤検出（偽陽性）が発生しなかったものを恒久拒否（応答コード 554）としてログに predatory タグを付加した。経過観察中に偽陽性が発生する可能性が判明した場合には送信者アドレスまたは送信サーバをホワイトリストに登録した。 なお、通常（8 週中 7 週）はセットしたフィルタ群の後段に、DNS-ブラックリスト (DNS-BL; zen.spamhaus.org 17) および BarracudaCentral 18)）を配し、8 週のうち1週は、DNS-BL をフィルタの前段に移設して DNS-BL での阻止率を調べた。

なお、ログから predatory タグが付与されたものを毎日1回抽出し、誤検出の有無を確認した、同時に、論文投稿や学会出席の勧誘に関するメールの送信者アドレスに頻用される単語の一部（例えば publish, journal, jrnl, editor, confere, congres 等）を指標として抽出した SMTP ヘッダについて、偽陰性によるすり抜けの有無を調べるとともに、正規出版社・学会からのメールが偽陽性に誤検出されずにユーザに配信されているかどうかを調べた。

なお、囮アカウントで捕捉したメールについて、MUA (Mail User Agent: 実装は Thunderbird）での迷惑メール判定との比較を試みた。

3. 結果と考察

3.1 受信メール数の推移

2016 年 1 月から 2017 年 12 月の 2 年間に主メール受信中継サーバとの間で SMTP セッションが成立した電子メールの総数は 9, 478,333 通（SMTP セッション開始直後に接続断となったメール約 90 万通を除く）で、そのうち迷惑メールと判定できたものは 2,024,763 通あった（オプトインバルクメールは迷惑メールに含んでいない）。捕食メールは調査開始から徐々に増加の傾向を示（図 1A) し、2年間の総数は 163,735 通に達した。これらのうち、抹消アカウント宛のもの (8,320 通) および他種の迷惑メールと誤判定したもの（2,916 通）を除く、152,499 通の捕食メールのヘッダを解析対象とした。捕食メールは 2016 年には全迷惑メールの数%を占める程度で数もあまり変化しなかったが、2017 年後半から増加傾向を示し、2017 年末には週によっては全迷惑メールの 10-15%を占めた。

2018 年 1 月から 2019 年 6 月までの 1.5 年間では、電子メール総数 9,145,244 通(セッション開始直後に接続断となった約 120 万通を除く）のうち、迷惑メールと判定されたのは 2,834,742 通であり、捕食メールは 509,978 通（後日、捕食メールと判定されたものも含む）に達した。この期間の捕食メールの増加は顕著で、週によっては全迷惑メールの 30%以上を占めた（図 1B)。

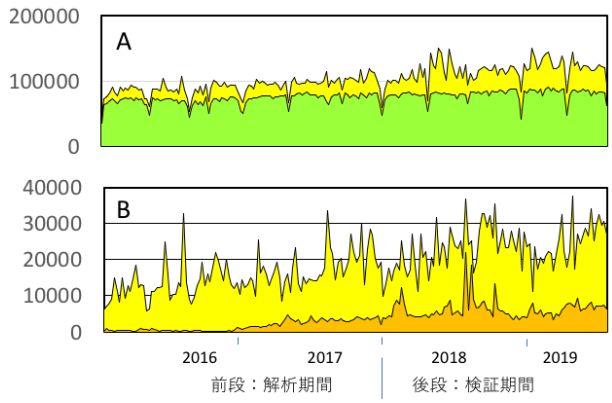

図 1 着信メール数の推移
2016 年 1 月～2019 年 6 月における正規メール（緑）と迷惑メール（黄）数の推移（図 1A)、および捕食出版社からの迷惑メール（橙）と、それ以外の迷惑メール（黄）数の推移(図 1B)。軸の値は週あたりのメッセージ数。

3.2 特徴抽出

SMTP エンベロープヘッダに記載されている項目について、捕食メールの特徴を抽出し、各項目間および各項目の記載事項を手がかりとして検索し得る情報（隠蔽情報を加味したデータ間の関係についてマイニング技法を用いて描出した。

3.2.1 SMTP ヘッダ各項の特徴

捕食メールの送信者アドレスのタイプは多様であったが、多くは 1, アカウント部に雑誌略称名、ドメイン部に出版社名を用いるもの、および 2, アカウント部に editor, cfp 等を語幹とする単語または単語の組み合わせを配し、ドメイン部に雑誌名（多様なドメインを使用する点は 1,と同様）を配するものが多い傾向があった。同一の捕食出版社であっても、 1 と 2 の型を併用する傾向があった。また、送信者アドレスドメイン部のトップレベルドメイン(TLD)には、com, net, org, info, us, co 等の他、ml, tk, xyz, online 等の新 gTLD を含めた多様な TLD

が使用され、TLD のみを次々と変化させて送信する傾向も観察された。2016 年 1 月から 2017 年 12 月(2 年間:前段解析期間)に着信した捕食メールにおいて、捕食出版社等から送信されたことが確定し、解析の対象となった 152,499 通における送信者アドレスのドメイン部の総数は 1,352 であった。送信者アドレスドメイン部は、多くのケースで送信サーバの FQDN のドメイン部と整合しなかった。

//送信サーバの FQDN のドメイン部には出版社名、雑誌名、あるいは特徴的な名称が用いられているケースが多かった。一部は大手メールサービスの送信網を併用しており、その場合の FQDN は当該メールサビス業者のドメインが用いられている場合と、捕食出版社が自社で登録した独自ドメイン名が用いられている場合があった。また、DNS にドメインを正しく登録しておらず、受信サーバで DNS を引けないためにログに unknown＋IP アドレスと記載されるケースも多かった。

Helo については送信サーバの FQDN と同じもの (正しい helo)は少数に留まり、多くはサーバ FQDN に雑誌名のドメインのひとつ、helo に出版社のドメインのひとつ(またはその逆)が用いられるなど、サーバ FQDN のドメイン部と異なった helo を名乗るものが過半を占めた。残り(約 1/3)は偽装されたもの、またはサーバ設定の不備に起因すると推定される不正な helo を名乗った。

3. 2. 2 各項間の関係と送信傾向の解析

送信者アドレスのドメイン部と送信サーバ FQDN のドメイン部は上述のように必ずしも一致するとは限らなかったが、一致しない場合においても、送信者アドレスのドメイン部と送信サーバの FQDN との間には、多くの場合、共起関係が観察された。また、送信者アドレスのドメイン部と送信サーバの FQDN に含まれるドメイン部との間には多対1または多対多の関係が観られる傾向があった。

送信サーバの FQDN と IP アドレスの間には、DNS に登録された FQDN と IP アドレスの関係が反映されるため、大半のケースで密な関係が観察された。IP アドレスと送信業者の保有している IP アドレス範囲の間には、当然、密接な関係が認められることから、送信サーバの FQDN と IP アドレス範囲との間にも関係が描出された。送信者アドレスのドメイン部は日々数個から 80 個程度増加し、送信サーバの FQDN の数ヶ月の間隔で変化するケースがしばしば見られ、送信サーバの FQDN の変化と同時に送信業者が変更されて IP アドレスも変化する事象が観察された。

捕食メールの 80%以上は南アジアおよび欧米の特定のホスティング業者から送信され、大量送信を企図している場合には、送信の過程で送信業者を変更または増やして送信する傾向が観察された。DNS へのドメイン(特に送信者アドレスのドメイン部に用いられるドメイン)の登録には多くの捕食出版社が特定の通信業者を多用する傾向がみられた。

共起ネットワーク分析を用いた捕食メールの送信者アドレス、送信サーバ、IP アドレス相互間の関係解析の1例を示す(図2)。

上述のように、捕食メールでは多様な送信者アドレス(アカウント部、ドメイン部とも)に加えて、多様なサーバを用いる傾向が観察された。さらに、1, 新しいドメインを次々に取得して送信者アドレスのドメイン部(場合によっては送信サーバ FQDN のドメイン部も)を次々と変化させる、2, 送信者アドレスドメイン部と送信サーバのドメイン部との組み合わせを変更する、3, 送信業者を変更・追加する、などの挙動が観察された。これらは、この期間に大量送信を行なっていた Omics group 、 Gabin Publishers 、 Insight Medical Publishing (iMedPub)等から送信されたメールで顕著であった。他方、それら以外の捕食出版社の多くは送信サーバ FQDN のドメイン部の変更は比較的まれであった。これらのことから、捕食出版社が迷惑メールフィルタの回避を企図して送信者アドレスのドメイン部、や送信サーバ FQNN のドメイン部を変更していること、および送信サーバのある通信業者・メールサービス業者(すなわち送信サーバの IP アドレス範囲)については変更・増設してゆく出版社等と、あまり変化・増加させない出版社等があった。

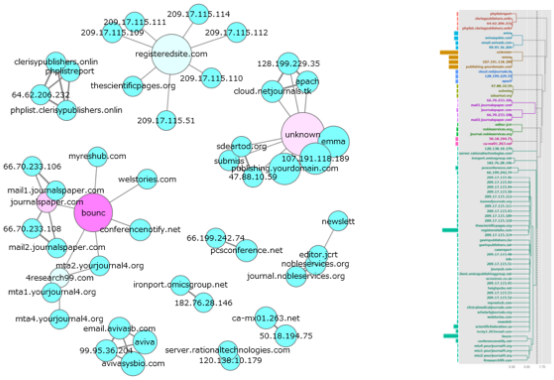

図2 データマイニングの例
共起ネットワーク分析 (左:中心性指標)と階層クラスタ分析を用いた捕食メールの送信者アドレス、送信サーバ、IP アドレス相互間の関係解析。

3. 2. 3 阻止の試行と問題点の洗い出し

前段の解析期間中に明らかとなってゆく特徴をもとに、検出・阻止フィルタを構成して逐次改良しつつ、検出率・阻止率を指標としてそれぞれの特徴 (signature) が検出・阻止にどれだけ寄与するかを調べた。

検出・阻止率は 2016 年前半=72%、2016 年後半=81%、2017 前半=86%と段階的に向上してゆき、2017 年後半では、1 段目に送信者アドレスのドメイン部のリスト(2032 ドメイン収載:感度 92%、特異度 100%)、2段目に送信サーバ FQDN のリスト(感度 68%、特異度:ホワイトリスト併用で 100%)、3段目に送信サーバ群の IP アドレスリスト(感度 78%、特異度:ホワイトリスト併用で 100%)を配置した捕食メール捕捉フィルタ群、によって、捕食メールの 95%を阻止可能となった。同時期、捕食メールに対する2種の DNS-BL のみによる阻止率は 10%未満と算出された。

前段の解析期間では、日々増加する送信者アドレスドメイン部に関してフィルタへの登録漏れが生じた場合でも、2,3 段目のフィルタで漏れの大半をカバーできた。しかしながら、フィルタのメンテナンスを中断すると、1~2 週間以内には送信サーバの FQDN または IP アドレス領域が変化したり、新たな送信サーバが別のアドレス領域に出現することなどによって、新規ドメインから最初に送信された数十通がフィルタをすり抜けてしまう事象が発生した。そのため、上述の3種のフィルタを常に最新状態にしておかないと阻止率が低下することが判明した。さらに、2017 年後半から送信数が増加傾向を示したこともあって、フィルタの改善・整備による対応は「いたちごっこ」の様相を呈し初めてきた。

前段の解析期間の終盤に至って、これまで大量の迷惑メールを送信していた OMICS と iMedPub からの送信数は減少

した (ただし、OMICS が主催する偽学会からの送信数はほとんど減少しなかった)。それらに代わって Medtext Publications、Remedy Publications、Austin Publishing Group からの送信数が増加しはじめた。これらの捕食出版社は、利用する送信業者を増やしたり、同一の送信業者を使っていても送信に用いる IP アドレス範囲を次々と増加・変化させたりすることに加えて、一定範囲の IP アドレス療育に並べられたサーバから送信時の IP アドレスを次々と変化させて送信を繰り返す「Snowshoe（かんじき）」型攻撃 19)を採用しはじめたことがログに残された SMTP ヘッダの送信サーバ FQDN および IP アドレス特徴から推定された。また、これらの送信業者が出版社名・雑誌名・学会名を類推できない、例えば ip234.ip-145-239-163.eu のような送信サーバ FQDN を用いはじめていることもわかってきた。

これらのことから、上述のフィルタ群のうち、特に送信サーバ FQDN フィルタが無力となる可能性、および IP アドレスフィルタのセーフティネットとしての機能低下が推測され、このまま対応を続けた場合には対策が破綻し、阻止が困難となることが懸念された。

3.4 送信戦略の推定

上述の解析結果から、捕食出版社等は他種の迷惑メール送信者と同様、標的への到達率を向上・維持させるために迷惑メールフィルタの回避を企図して送信していることが示唆された。また、迷惑メールフィルタ回避の方策として、送信者アドレスおよび送信サーバ (FQDN と IP アドレス)を逐次変化（または増加・多様化）させて、既知の情報に基づいて構成されたフィルタの効果を低減させる手法を用いていることが予測された。

送信者アドレスのドメイン部については、安価に大量のドメインを入手可能な状態となっていることから、これまでと同様、捕食出版社は新規のドメインを次々と入手して使用できる。送信者アドレスのドメイン部のフィルタは、誤検出の発生が少なく比較的容易に用いることができるため、送信者が新たに用いるアドレスを受信側で的確に予測することは容易でない。また、送信に用いられるサーバの FQDN は、上述のように、今後、有効性が低下することが予測された。

送信サーバの IP アドレスについては、IPv4 アドレスが枯渇して大量入手が困難となっているものの、一部の送信業者が急速に規模を拡大し続けており、それらの中には安価でアドレスブロックまたは比較的良質な VPS サーバ群を提供している。加えて他種の迷惑メールの送信状況等から、それらの中に契約者の大量送信に関する規制が甘いと推測される大手通信業者が存在することが明らかとなってきた。さらに、2017 年末からの捕食出版社等からの送信数の増加傾向を考慮すると、規制の甘い大手通信業者の保有する IP アドレス領域から、snowshoe 攻撃の手法を用いた大量送信が行われ、捕食メールのアウトブレーク発生の可能性が強く示唆された。Snowshoe 攻撃によるアウトブレークでは、短時間に大量の迷惑メールが着信するため、着信したメールの SMTP ヘッダ情報からフィルタを構成していたのでは間に合わない（大量のすり抜けが発生する）ことが推測された。

3.5 阻止戦略の策定

上述の推定に沿って、規制の甘い大手通信業者の保有する IP アドレス領域から snowshoe 攻撃が実施されるとの作業仮説の下、該当すると思われる通信業者（DigitalOcean, UnifiedLayer, OVH 他 2 社）が保有する IP アドレス範囲を BGP tool kit 8)を用いて特定した。続いて、Talos 20)を用いてそれらの範囲から未使用の IP アドレス領域を抽出し、それらの IP アドレス領域をカバーするフィルタを構成した。また、これまでの送信動態から、送信数が増加の一途を見せている Medtext Publications 、 Remedy Publications 、 Austin Publishing Group について snowshoe 型送信を行う可能性が高い捕食出版社と想定した。

3.6 阻止率を指標とした推定（仮説）検証

捕食メールのアウトブレークに対応するため、1 段目に捕食出版社が送信に用いるサーバが名乗る helo に対するフィルタ、2 段目に送信者アドレスのドメイン部フィルタ、3 段目に送信サーバ FQDN フィルタ、4 段目に送信サーバ群の IP アドレス領域フィルタを配したフィルタセットを用いた。

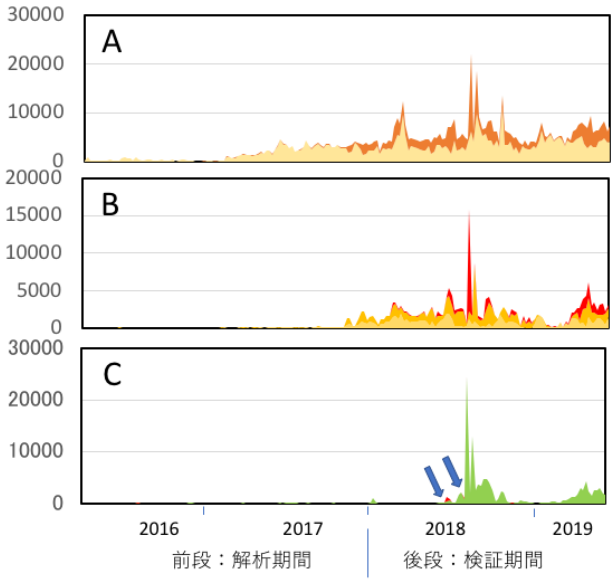

図 3 2016 年 1 月から 2019 年 6 月までに捕食出版社・偽学会から送信された電子メールの推移
上（A) Austin, Remedy, Medtext からの送信数（橙)とそれら以外の捕食出版社等からの送信数（薄橙)。中（B) Austin（薄橙)、Remedy（橙)、Medtext （赤）からの送信数。 下（C) OVH の″ip[0-9].*¥.ip-[0-9].*-[0-9].*-[0-9].*¥.eu″にマッチする FQDN を持つサーバ群から送信された捕食メール。薄緑：フィルタで阻止、赤（矢印部分）フィルタすり抜け（偽陰性）。

2016 年末から迷惑メールは増加の傾向を示し、増加の大半は捕食メールの増加によるものであった（図1B)。捕食メールは 2016 年末から増加の一途を辿り（図1B、図 3A)、受信数は 2018 年春に1回目のピークを迎えた。この時点における捕食メール SMTP ヘッダの特徴は、helo、送信者アドレスドメイン部、送信サーバ FQDN ドメイン部、送信領域（IP アドレス）のいずれも、前段の調査期間に判明した特徴からあまり変化しなかった。大規模な snowshoe 攻撃を予測して準備した「急成長中で規制の甘い通信業者の保有する IP アドレス範囲」に対するフィルタ（4 段目）で捕捉される捕食メールは少数で、調査期間と同様、大部分は前3段のフィルタで捕捉された。なお、2017 年後半には、OMICS および iMedPub 等、それまで大量送信を行なっていた捕食出版社からの送信数が減少に転じ、代わりに Austin Publishing Group 、Remedy Publications、Medtext Publications 等から送信される捕食メー

ルが出現・増加した（図 3 A,B）。しかしながら、2018 年春 に出現した捕食メール送信数の1回目のピークは、それまで送信を続けていた捕食出版社から従来の手法を中心として送信されたものが大半を占め（図 3B）、予測していた Austin、Remedy、Medtext,からの大規模 snowshoe 攻撃によるアウトブレークはこの時点では発生しなかった。ただし、この期間において、Austin の FQDN を冠したサーバから Remedy や MedText の送信者アドレスドメイン部を持つ捕食メールが頻繁に観察されたり、MedText の FQDN を冠したサーバから Austin や Remedy の送信者アドレスドメイン部を持つ捕食メールが観察され、加えて、それらが送信に用いている送信業者が共通することなどから、これら3社間の関連性が強く示唆された。

2018 年夏から秋にかけて、第2のピークが到来した（図 3 A,B）。このピークは3峰性で、最初の波は1回目のピークと良く似た傾向を示したが、増加の主体はおもに Austin と Remedy であった。送信数は一端減少したが、まもなく2番目の波が到来した。この第2波は Austin、Remedy、Medtext を主体とした Snowshoe 攻撃によるアウトブレークであり、おもに通信業者の OVH が保有する IP アドレス領域から実施された (図 3C)。 Snowshoe 攻撃による送信数は週あたり最大で 1 万 5 千通に達した。

なお、第2波の到来直前に、Austin・Remedy によって、通信業者に OVH 用いた小規模の snowshoe 攻撃が発生した。この時点では、フィルタは用意されていたものの、発生を推定してから半年以上を経過していたため、送信 IP アドレス領域をカバーするフィルタの一部が阻止（恒久拒否・再送要求）でなく検出するためのフィルタ（reject_warning の標識を付けて配信）となっていたこと、および、一部が OVH への割り振り情報が未反映の領域から送信されたことで、アウトブレークの直前に、約 1,200 通の「すり抜け（偽陰性）」が発生した（図 3C）。

第2波に引き続き、第2波のような先鋭なピークは示さないものの、約2ヶ月間にわたるブロードな峰（第3波）が観察された。第２波の後半から第３波にかけて、OVH からは Austin、Remedy、Medtext 以外にも Fortune Journal 等の捕食出版社からの送信が観察された。

捕食メールの送信に用いられた OVH の IP アドレス領域はおもに欧州および北米（カナダ）のデータセンターであったため、捕食メールの大量送信が行われる場所が、それまでの南アジア・米国中心から拡大されることとなった。なお、Remedy、Austin、Medtext は、従前通り南アジアを中心とした送信も継続して行なわれていた。

この時期に Remedy、Austin、Medtext 等から OVH を介して送信されたメールの大半では送信に用いられたサーバ群は ip234.ip-145-239-163.eu[145.239.163.234]のような命名規約に即していたため、正規表現を用いてこの規則に則した FQDN を検出するフィルタを構成することができた。送信 IP アドレス領域はおもに/28 から/27 の IP アドレスブロックを単位として行われていた。また、同時に離散した数単位から送信され、1週間ごとに送信に用いるアドレスブロックを変化させながら送信されていることが判明した。これらの特徴を踏まえて、捕食出版社からの送信が予測される（他者が未使用の）IP アドレスブロックを再送要求で拒否しておき、そこに上述の特徴を持つ FQDN を付されたサーバの存在を検出した時点で恒久拒否に移行する方法を採用した。

FQDN フィルタと IP アドレス範囲をカバーするフィルタの併用は強力で、複数の広大な IP アドレス領域において上述の捕食出版社が送信に用いる領域を増加させたり変化させたりしても、これらのフィルタを組み合わせることで、ほぼ全数の検出・阻止が可能となった。

2018 年夏の第2のピークの後、OVH を介する snowshoe 攻撃は一旦休止した。この時期、それまで阻止対象となっていた Bentham Science Publishers が出版する数百タイトルの雑誌のうち、数十タイトルが JCR に収載されて IF が付与されたことが判明したことから阻止対象から除外したが、捕食メールの総数は減少せず、高値を示した。

2019 年春、Austin、Remedy、Medtext からの snowshoe 攻撃を主体とする第3のピークが出現した。この時期、FQDN に OVH の送信サーバと同様の特徴を持つサーバ群からの snowshoe 攻撃が、OVH 以外に予測していた通信業者のうちのひとつ（SendGrid）からも出現した。検証期間終了時の6月末日まで、snowshoe 攻撃を用いて送信された捕食メールについて、ほぼすべてを阻止することができた。また、検証期間中もフィルタ群を随時改良していたことから、snowshoe 攻撃以外で送信される捕食メールの阻止率も 98%前後を維持できた。これらによって、検証期間後半は捕食メールの検出・阻止率は 99%前後に達し、検証期間前半と合わせても検証期間中（2018 年から 2019 年 6 月の 18 ヶ月間）に着信した捕食メール約 51 万通のうち 50 万通強を阻止できた。

FQDN フィルタと IP アドレス領域フィルタは、それらがカバーする特徴・場所からのメールをすべて捕捉する。そこで、これらの中に正規メールや他種の迷惑メールが混在していた場合には誤検出（偽陽性）が発生する。事前にそれらの通信業者からの大量送信を予測していたことから、当該送信業者の保持する IP アドレス領域から過去に送信された全メールの SMTP ヘッダ情報に基づいて予めホワイトリストの準備や他種の迷惑メールに対するフィルタを準備できた。また、捕食出版社の用いるサーバ・IP アドレス領域に関しては、少なくとも現時点までは、ホワイトリストに登録すべきホストはごく少数しかなく、さらに捕食メール以外のメールの大半は他種の迷惑メールであった。他種の迷惑メールに捕食メールのタグを付して拒否したケースはわずかにあったものの、捕食メールフィルタ群での正規メールの誤検出（偽陽性）は生じなかった。送信者アドレスのドメイン部も日々増加したが、それらについてはたとえ登録漏れが生じた場合でも、他のフィルタで漏れの大半をカバーできた。なお、捕食メールに対する DNS-BL（2種）のみによる阻止率は 40%に増加した。これは、snowshoe 型送信が急増したことで、DNS-BL がそれらの送信元サーバの大半からの送信をブロックするようになったことによると推測された。

本研究の検証期間終了時における捕食メールフィルタ群の阻止効率は、1 段目の送信サーバが名乗る helo に対するフィルタ単体では感度 32%、特異度 100%、2 段目の送信者アドレスのドメイン部フィルタ単体では感度 89%、特異度 100%、3 段目の送信サーバ FQDN フィルタ単体では感度 83% 、特異度 99.9%（ホワイトリスト併用で 100%）、4 段目の送信サーバ群 IP アドレス領域フィルタ単体では感度 81%、特異度 99.7%（ホワイトリストと他種の迷惑メール分離用リストの併用で 100%）であった。

3.7 問題点・今後の課題

捕食出版社の中には、今後、良質の出版社に変わってゆく可能性があるものが存在すると推定される。そこで、各出版社および刊行されている Open Access 雑誌の評価について継続してフォローアップする体制を構築しておく必要があることが明らかとなった。

検証期間終了時点において、送信元から直接送信された捕食メールについては 99%以上が阻止可能となった。しかしながら、他機関で中継されて転送されてきた捕食メールが阻止率を低下させた。転送メールでは送信サーバの IP アドレスに関する情報が中継によって書き換わる。のため、転送メールに含まれる捕食メールの多くについてすり抜け（偽陰性）が発生し、検証期間の1年6ヶ月間だけで 3,000 通強がユーザに配信された（上述の「すり抜け」数に含まれている）。

さらに、捕食出版社が送信に用いているサーバの多くが適切に構成されていたのに対し、正規の学会・研究会等がクラウドに設置したサーバの中には設定不良のものが少なくなく、DNS-BL に登録されるものもあった。その結果、捕食メールを含む迷惑メールを高い精度で阻止するためには阻止フィルタ群に加えてホワイトリストの整備が必要となり、相当程度の工数・時間を要することとなった。そこで、作業の効率化を企図し、阻止フィルタの代わりにコンテンツフィルタ（実装は SpamAssasin）を用いた阻止について検討した。特にコンテンツ本文に記載された URL を指標とした検出の有用性を期待したが、捕食メールのコンテンツでは URL リダイレクトの利用や正規インデックスサイト等の URL の記載による欺瞞措置に加えて、出版社名を画像化するなど、コンテンツフィルタ回避策が講じられているケースが観察された。また、投稿勧誘や学会参加要請メールについては正規出版社のものと捕食出版社で文面の特徴が似ていることから他種の迷惑メールと較べてスコアに差が生じにくい傾向があり、正規出版社のメールの誤判定が生じやすくなることが判明した。加えて、近年、一部の雑誌に正規の IF が付与されて正規出版社と（同等に）なった元捕食出版社のひとつは、以前と同様の投稿勧誘メールを大量送信し続けている。こうして送信されているメールと捕食出版社の稿勧誘メールについてコンテンツを主対象として区別するのは容易でなく、SpamAssasin を用いた判定でも送信者アドレス、サーバ FQDN、送信 IP アドレス領域等の SMTP セッション情報およびそれらを元に得た付帯情報が重要とならざるを得なかった。

囮アカウントを用いた MUA（実装は Thunderbird）での迷惑メール振り分け機能による捕食メールの検出においても同様の傾向が観察され、一定数の捕食メールを処理させた後に正規出版社からのメールを誤判定するケースが多発した。

配信された捕食メールの URL リンクを押した場合のブラウザ（Edge, FireFox, Chrome, Safari）および proxy server (実装は IWSS)の組み合わせでは、Phishing サイトへのアクセスの過半を阻止したものの、捕食出版社の web サイトへのアクセスは、少数が詐欺サイトとして阻止されたものの、ほとんど阻止できなかった。

AI 利用による効率化については、Scikit-learn の Phython ライブラリを用いた「教師あり学習」（機械学習）において、阻止率 80%程度を期待できる結果が得られつつある。しかしながら、機械学習に際しても、送信 IP アドレス領域を保有する送信業者やメール送信者が捕食出版社であるかどうかなど、SMTP セッション情報で明示されない付帯的な暗黙知に属する情報が必須であり、それらの調査に必要な whois 検索等に際して機械的なブラウザクローリングが困難なため、現時点では、工数削減の効果は顕著でない。深層学習については、現時点では、有用性を示す証左を得るに至っていない。

4. 結語

医療機関を標的とする捕食出版社・偽装学会からの迷惑メール送信の実態の一端を解明し、SMTP エンベロープヘッダの特徴解析と送信動態に基づいて想定した送信戦略に対応した迷惑メーッルフィルタを構築することで、捕食出版・偽装学会社から送出された迷惑メールの 98%以上を阻止した。

5. 謝辞

本研究の一部は JSPS 科研費 23590626, 26330337 の補助を受けて実施された。すり抜けメールを転送していただいた関西医科大学ネットワークユーザ有志各位に深く感謝申し上げる。

参考文献

1) Beall J. Predatory publishers are corrupting open access. Nature 2012; 489: 179.
2) Butler D. Investigating journals: The dark side of publishing. Nature 495, 2013; 433-35.
3) Kaye DH Flasky Academic Journals, http://flakyj.blogspot.com/ (cited 2019-Aug-29)].
4) 栗山 正光 ハゲタカオープンアクセス出版社への警戒. 情報管理 2015: 58:92-99.
5) Towers S, Predatory Journals and Conferences, Polymatheia, Dec. 19, 2018 (how to spot predatory journals, conferences, and misleading advertising) [http://sherrytowers.com/2018/12/19/predatory-journals-and-conferences/ (cited 2019-Aug-29)]]
6) 渡辺 淳，仲野 俊成，松本 掲典，新貝 欣久，高木 真平. SMTP ヘッダにおける限定された情報を用いた詐欺メール送信者の意思決定の道筋解析と展開予測に及ぼす暗黙知の影響. 医療情報学 2012: 32S, 642-45.
7) 渡辺淳，仲野俊成，松本掲典，新貝欣久. 医療機関における SMTP セッション情報を用いた迷惑メール対策. 医療情報学 2007: 27s, 1114-17.
8) Hurricane Electric Internet Services. BGP Toolkit. https://bgp.he.net/ (cited 2018-Feb-01)
9) Beall J. Beall's List: Potential, possible, or probable predatory scholarly open-access. [https://scholarlyoa.com/publishers/ (cited 2017-Jan-10) [公開終了]
10) Claryvate Analytics. Web of Science https://apps.webofknowledge.com (cited 2019-Aug-29)
11) Claryvate Analytics. Journal Citation Reports https://jcr.clarivate.com/ (cited 2019-Aug-29)
12) Claryvate Analytics. Master Journal List http://mjl.clarivate.com/ (cited 2019-Aug-29)
13) Stop Predatory Journals. https://predatoryjournals.com (cited 2019-Aug-29)
14) Beall's list of predatory journals and publishers https://beallslist.weebly.com/ (cited 2019-Aug-29)]
15) 樋口耕一. テキスト型データの計量的分析 -2 つのアプローチの峻別と統合-. 理論と方法 2004: 19, 101-15.
16) 渡辺淳，仲野俊成，松本掲典，新貝欣久，高木真平，西野典宏. 某大手フリーメール業者から送信される詐欺メールにおける流出ログイン情報の利用. 医療情報学 2013: 33S, 1006-09.
17) Spamhaus https://www.spamhaus.org/ (cited 2019-Aug-29)
18) BarracudaCentral: http://www.barracudacentral.org/ (cited 2019-Aug-29)
19) 渡辺淳，新貝欣久，松本掲典，仲野俊成，畑森浩孝. APML を用いた隠蔽・暗黙関係の描出と展開予測-SMTP snow-shoe 攻撃組織の関係解析を用いた検証-医療情報学 2009: 29S :859-64
20) Cisco Systems. Talos https://talosintelligence.com/ (cited 2019-Aug-29)]