

# 類似メールを利用したばらまき型メールの検出

藤城 透<sup>†1</sup> 三浦 綾斗<sup>†1</sup> 原田 隆史<sup>†1</sup>

**概要:** 近年ばらまき型メールが流行し、マルウェア感染被害が報告されている。ばらまき型メールの多くは、スパムボットにより送信されている。このようなスパムボットには、メール文のテンプレート、送信先リスト、送信元リストなどを保持しているものが存在する。そして、メール文のテンプレートを使いまわし、送信先及び送信元を変えながらメールを送信する。このため、受信したユーザから見ると、同一または類似するメールが様々な送信元から受信される。本論文では、この特徴を利用して、送信元が異なり、本文や添付ファイルの類似するメールをばらまき型メールとして検出する方法を提案し、その有効性を検証する。

**キーワード:** 迷惑メール、ばらまき型メール、スパムメール、スパム検出

## A method to detect indiscriminate spam emails focusing on similarity of messages body and attachments

Toru Fujishiro<sup>†1</sup> Ryoto Miura<sup>†1</sup> Takafumi Harada<sup>†1</sup>

**Abstract:** In recent years, the number of spam emails has been increased and a lot of malware infection resulted from those emails have also been reported. Most of indiscriminate spam emails are sent by spambots. The spambots have message templates, list of sender and recipient addresses and other configurations. Some of them spread spam emails made with the same template changing the sender and recipient address. Therefore, recipients receive identical or similar emails from different senders. In this paper, we suggest a method to detect emails whose senders are different and message body and attachments are similar as spam, and validate its effectiveness.

**Keywords:** spam, malspam, spam detection

### 1. 研究背景

近年、ネットワークの発展により、電子メール（以下「メール」と称する）が広く利用されている。これに伴い、受信者が望まない広告や嫌がらせなどの迷惑メールも多く送信されている。国内のISPの取り扱うメールでは、全体のうち40%前後もの迷惑メールが存在している[1]。

このような迷惑メールの中には、不特定多数に大量に送信されるメールやマルウェアが添付されているメールなども存在する。これらは、受信者にとって迷惑になるだけでなく、フィッシングサイトへの誘導やマルウェア感染など、様々な被害を引き起こす。

迷惑メールの対策には、送信させない仕組みと受信しない仕組みの大きく分けて2つがある。迷惑メールを送信させない仕組みとしては、OP25B (Outbound Port 25 Blocking) などがある。受信しない仕組みには、ブラックリスト、フィルタリング、送信ドメイン認証などがある。

これらの対策により大部分の迷惑メールを防ぐことができているが、すり抜けて受信者に届く迷惑メールも依然として存在している。その中でも、マルウェア付きの迷惑メールは、ユーザが間違えて実行した場合、機器や情報資

産に対して与える影響は大きい。このようなマルウェア付きのメールは不特定多数に送信されることが多く、ばらまき型メールなどと呼ばれる。

ばらまき型メールは、基本的にスパムボットから送信される。このようなスパムボットは、「テンプレート（メールの本文や添付ファイル・URL）」、「送信先リスト」、「送信元に利用する情報のリスト（メールアドレスやパスワード、SMTPサーバ、ポート番号など）」などを保持していることがある。また、C&Cサーバからダウンロードし、定期的に更新される場合もある。

これにより送信されるメールは、テンプレートの大部分を使いまわし、送信先及び送信元を変えながらメールを送信することがある。このため、受信する側からみると、様々な送信元アドレスから、本文または添付ファイルが同一または類似性の高いメールを受信することになる。このようなメールをここでは類似メールと呼ぶ。

スパムボットからの迷惑メールに対して有効な対策には、前述のOP25Bや、Greylisting、分散協調フィルタなどの対策がある。

OP25Bは、25番ポートへのSMTP通信をブロックし、外部のメールサーバを直接利用できないようにしたもの

<sup>†1</sup> キヤノン IT ソリューションズ株式会社  
Canon IT Solutions Inc.

である。しかし、OP25Bを導入していないISPからの送信や、正規の認証情報を利用している場合は防ぐことができない。

Greylistingは、新規の送信元に対して一時拒否を返信し、再配送されたメールのみを受信する方法である。通常のメールサーバであれば一定時間経過後、再配送を行うが、スパムボットは再配送を行わないことが多い。このため、スパムボットからのメールを遮断することが可能である。しかし、通常の新規メールも同様に扱うため配送遅延が生じる問題や対応していないメールサーバからのメールを受信できない問題がある。

分散協調フィルタは、同一の内容の迷惑メールが大量に送信されていることを利用したものである。ユーザからの報告によって、迷惑メールと判定したメールからシグネチャを作成する。このシグネチャを利用して迷惑メールを検出する。しかし、迷惑メールの判定にユーザの何かしらの報告が必要となり、実際にブロックされるまでに時間がかかるという問題がある。

本研究では、ばらまき型メールを自動で検出する手法を提案し、有効性を検証することを目的とする。

本論文は次のような構成である。2章では、関連研究や関連調査について説明し、3章で提案手法について説明する。その後、4章で提案手法を用いた実験及び結果・考察を示し、5章にてまとめと今後を述べる。

## 2. 関連研究

本章では、迷惑メールの特徴やスパムボットに関する関連研究や関連調査について述べる。

文献[2]では、迷惑メールの調査を行った結果、本文の再利用が行われるメール数が25%程度存在していること。また、受信者が初受信時に迷惑メールとして振り分けられ、あとは単純なパターンマッチングでフィルタリングが可能であると記載されている。

文献[3]では、スパムボットのサーバ上には、7億以上のメールアドレスのリストが存在し、また送信に使用するアカウントの認証情報は約8,000万件であると報告されている。

さらに、文献[4]によると、1台のスパムボットに対して、1か月で50種類以上のテンプレートが送られ、1つのテンプレートを送信する宛先リストは数千件単位であることが報告されている。

上記のことから、スパムボットはテンプレートを頻繁に更新し、膨大な送信先・送信元情報を用いてメールを送信することができると考えられる。このため、手動でフィルタリングすることは難しく、自動で検出することが望ましい。そこで、本研究ではテンプレートの数に対して、送信先や送信元情報の数の方が圧倒的に多いこと。また、同一のテンプレートを複数の送信先に送信していることを利

用し、テンプレートを用いるばらまき型メールを自動で検出する方法を提案する。

## 3. 提案手法

### 3.1 ばらまき型メールの特徴

本研究では、ばらまき型メールの特徴を利用して検出を行う。このため、まずは実際に届いたばらまき型メールを確認する。

図1は、ばらまき型メールのうちの1種類のテンプレートから送信されたと思われる類似メール一覧である。そして、図2は、この類似メールの内容である。これらを確認すると、ほぼ同一の内容のメールが、様々な送信元から受信していることが確認できる。

件名	差出人	送信日時	サイズ
Re: 2018.5月分請求データ送付の件	<ko3@ab[redacted].ne.jp>	2018/05/16 15:55:11	79,928
2018.5月分請求データ送付の件	<ko3@ab[redacted].ne.jp>	2018/05/16 15:58:23	79,958
Fwd: 2018.5月分請求データ送付の件	<hnr[redacted]@m[redacted].ne.jp>	2018/05/16 15:58:50	80,035
2018.5月分請求データ送付の件	<pl[redacted]@m[redacted].ne.jp>	2018/05/16 16:08:41	80,021
2018.5月分請求データ送付の件	<mc[redacted]@m[redacted].ne.jp>	2018/05/16 19:31:04	80,314
Fwd: 2018.5月分請求データ送付の件	<sk[redacted]@ar[redacted].ne.jp>	2018/05/16 19:32:52	79,951
Fwd: 2018.5月分請求データ送付の件	<roy[redacted]@l[redacted].ne.jp>	2018/05/16 19:33:02	80,477
Re: 2018.5月分請求データ送付の件	<mc[redacted]20.rkn@m[redacted].ne.jp>	2018/05/16 19:36:19	79,954

図1 不審メール一覧

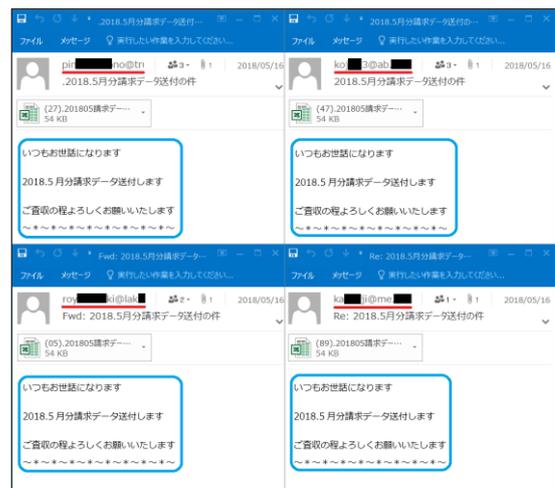


図2 不審メール内容一覧

このように受信した複数種類のばらまき型メールを観察することで、以下の特徴を持つことが多いことを確認した。

- A) 類似メールが複数の送信元から送信される
- B) 初めて受信する送信元（メールアドレスなど）
- C) 1種類の類似メールが届く期間が短い
- D) テンプレートが頻繁に更新される
- E) 添付ファイルまたはURLが付与されている

その他にも、本文が比較的短いこと、件名や添付ファイル名は異なっていることが多いなどの特徴もあった。

次に、本研究の検出対象を明らかにするために、類似メールの本文に使用される文章を以下のように分類した。



## 4. 実験

本章では、最初に実験データについて述べる。次に実験 1 では、ばらまき型メールの特徴 A)「類似メールが複数の送信元から送信される」状況を調査し、有効性を考察する。実験 2 では、設定を追加し、正規メールの検出率 (False Positive) を抑制する。実験 3 では、事前にメール文のランダム要素を除去するデータ加工を行うことで検出精度の向上を図る。実験 4 では、メールアドレス全体のみでなく、ドメインも考慮することで、False Positive をさらに抑制する。そして、実験 5 では、受信した順に検知処理を行うのではなく、受信済みメールに対して検出・分類を行う。

### 4.1 実験データ

実験には、2017 年 7 月～2018 年 6 月の間に弊社のラボ宛に送られた 57,588 件のメールを利用する。このメールを目視でチェックし、「正規メール」52,717 件、「迷惑メール」4,693 件、「マルウェア感染を狙ったと思われるメール (以降、マルウェア感染メール)」178 件に分類した。

分類を行うにあたり、先に正規メールと迷惑メールの 2 通りで分類し、その後、迷惑メールからマルウェア感染を狙ったと思われるメールを抽出した。迷惑メールは、マルウェア感染メールを除く迷惑メールである。

マルウェア感染メールは、添付ファイルがマルウェアと思われるメールおよび、マルウェアのダウンロードページに誘導することが知られているメールとした。基本的にばらまき型メールの多くはここに分類される。しかし、迷惑メールの中にも、ばらまき型メールが含まれている可能性がある。例えば、URL 付きのメールでは、事前にマルウェアをダウンロードすることが知られているメールのみしか分類していない。このため、実際に URL にアクセスした場合、マルウェアのダウンロードページに誘導されるばらまき型メールの可能性もある。

今回は、目視においても完全には、ばらまき型メールかどうかの判断が困難であったため、目安として「正規メール」、「迷惑メール (マルウェア感染メールを除く)」、「マルウェア感染メール」の 3 つに分類したデータを用いる。実験では、「正規メール」及び、ばらまき型メールが多い「マルウェア感染メール」の検出率を中心に評価を行う。

### 4.2 実験 1

最初に、ばらまき型メールの特徴 A)の類似メールが複数の送信元から送信される状況を調査した。検出対象とするしきい値 (類似メールの件数) は 2 件以上として実験を行った。また、送信元に関する情報は、ヘッダ From アドレス全体のハッシュ値のみで実験を行った。

### 4.2.1 実験結果

実験結果を下記に示す。検出された「正規メール」、「迷惑メール」、「マルウェア感染メール」のそれぞれについて、種類数 (異なるハッシュ値の数)、合計 (検出したメールの合計)、検出率を記載する。また、分割したパートのどのパートで検出したかわかるように、検出したパートごとの件数を表 1 に示す。

表 1 実験結果 1

正規メール								
	計	本文 0	本文 1	本文 2	添付 0	添付 1	添付 2	添付 3
種類数	441	4	9	2	417	8	1	0
合計	661	26	40	5	577	12	1	0
検出率(%)	1.3	0	0.1	0	1.1	0	0	0
迷惑メール								
	計	本文 0	本文 1	本文 2	添付 0	添付 1	添付 2	添付 3
種類数	26	23	0	1	1	0	0	1
合計	674	660	0	2	9	0	0	3
検出率(%)	14.4	14.1	0	0	0.2	0	0	0.1
マルウェア感染メール								
	計	本文 0	本文 1	本文 2	添付 0	添付 1	添付 2	添付 3
種類数	40	16	0	1	22	0	1	0
合計	107	24	0	12	70	0	1	0
検出率(%)	60.1	13.5	0	6.7	39.3	0	0.6	0

正規メールを 1.3% (52,717 件中 661 件)、迷惑メール 14.4% (4,693 件中 674 件)、マルウェア感染メール 60.1% (178 件中 107 件) を検出した。以下に、検出したそれぞれのメールを確認した結果を示す。

検出した正規メールには下記のようなメールが存在した。

- 空メール
- 改行のみのメール
- 短文のメール
- 自動生成文章のみのメール
- 配送不能メール (postmaster や MAILER-DAMON)
- 定期的なレポート (定型文) メール
- @example.com などのテストメール
- 転送メール、返信メール
- 同一ドメインの異なるアドレスからの同一のファイルやロゴなどの画像ファイルが添付されたメール

次に、検出した迷惑メールは下記のようなメールが存在した。

- 架空請求・情報商材メール
- 広告・宣伝、営業メール
- URL 付きで Web ページへ誘導する迷惑メール
- 返信用メールアドレス付きの迷惑メール

そして最後に、“未検出の”マルウェア感染メールには、下記のようなメールが存在した。

- 類似メールの 1 件目 (しきい値に達する前のメール)
- 元々類似メールがない (同様のメールが 1 件のみ)
- マルウェアをダウンロードする URL 付きのなりすましメール

- 同一のアドレスからのマルウェア付きメール

#### 4.2.2 考察

検出率をみると正規メールに比べ、迷惑メール、マルウェア感染メールの検出率が高いことがわかる。これより、正規メールでは、ばらまき型メールの特徴 A) が発生する状況が少ないことが確認できた。また、マルウェア感染メールでは 60.1% のメールを検出することができ、有効性を示すことができた。

次に、パートごとの検出を確認すると、正規メールでは添付 0 が多く、迷惑メールでは本文 0、マルウェア感染メールでは本文 0 と添付 0 の検出率が高いことがわかる。正規メールの添付 0 では、社内の転送メールや返信メールで添付ファイルを利用しているようなメールが多く検出されていた。ドメインは同一であるが、ローカルパートのみが異なっていた。迷惑メールの本文 0 では、空メールや改行のみのメールが多く検出された。

また、検出された迷惑メールには、ヘッダ From アドレスは異なるが、MTA の IP アドレスは同じまたは近い値であるものが存在した。このことから、ばらまき型メールのように様々なところから送信されているのではなく、同じところからヘッダ情報を変更して送信されていることがわかる。

実験 1 では、送信元に関する情報に、単純にヘッダ From アドレスのみを利用した。このため、ドメインが同一でローカルパートのみが異なるものや、MTA の IP アドレスが同一、または近いアドレスになっているメールも異なる送信元として扱われている。本手法では、送信元に関する情報の関連性が低いものをカウント対象とするため、ドメインや MTA の IP アドレスを考慮することでより False Positive を抑制できると考えられる。

False Positive を抑制する方法として、他にも検出対象とする各パートの最小サイズを制限することや、ホワイトリストを活用する方法などがある。これにより空メール、改行のみ、短文や自動生成文章のみのメールを除外することができる。

正規メールの転送メール・返信メールは、大半が社内メールであり外部から来たメールではない。このため、社内メールを除外することで不要な検出を抑制できる。また、配送不能は、元のメールを添付しているため検出対象となっていた。配送不能メールに関しても対象から外す必要がある。

実験 1 では、5.1 ばらまき型メールの特徴 A) のみを利用したが、B) ~ E) の特徴を含めることでよりばらまき型メールのみを検出する精度が向上すると考えられる。例えば、初めて受信する送信元のみを検出対象にすることなどが挙げられる。

#### 4.3 実験 2

実験 2 では、いくつかの設定を追加し、正規メールの検出率 (False Positive) を抑制する。実験 1 の設定に加え、「イントラネットのメール及び配送不能メールの除外」と「各パートの最小サイズ制限」の設定を追加した。

「イントラネットのメール及び配送不能メールの除外」は、図 3 の 1. メール受信の時点で除外を行い、除外されたメールは 2. 以降の処理は行わない。

「各パートの最小サイズ制限」は、2. 情報抽出の時点で実施する。各パートに分割し、サイズ制限以上になったパートのみ情報の抽出を行う。

##### 4.3.1 実験結果

実験結果を下記に示す。イントラネットのメール及び配送不能メールを除外した結果、対象のメール数が表 2 のようになった。

表 2 除外前後のメール数の比較

	正規メール	迷惑メール	マルウェア感染メール
除外前	52,717	4,693	178
除外後	17,435	4,693	178

除外されたイントラネットのメール及び配送不能メールは全て正規メールとして、本研究のばらまき型メール判定を行わずに転送または受信を行う。

次に、検出された正規メール、迷惑メール、マルウェア感染メールのそれぞれについて、種類数、合計、検出率を表 3 に示す。ここで、検出率は除外後の総数から算出した。

表 3 実験結果 2

正規メール								
	計	本文 0	本文 1	本文 2	添付 0	添付 1	添付 2	添付 3
種類数	5	1	0	0	3	1	0	0
合計	19	15	0	0	3	1	0	0
検出率(%)	0.1	0.1	0	0	0	0	0	0
迷惑メール								
	計	本文 0	本文 1	本文 2	添付 0	添付 1	添付 2	添付 3
種類数	22	20	0	0	1	0	0	1
合計	59	47	0	0	9	0	0	3
検出率(%)	1.3	1.0	0	0	0.2	0	0	0.1
マルウェア感染メール								
	計	本文 0	本文 1	本文 2	添付 0	添付 1	添付 2	添付 3
種類数	46	13	1	0	23	5	4	0
合計	89	18	1	0	55	8	7	0
検出率(%)	50.0	10.1	0.6	0	30.9	4.5	3.9	0

正規メールを 0.1% (17,435 件中 19 件)、迷惑メール 1.3% (4,693 件中 59 件)、マルウェア感染メール 50.0% (178 件中 89 件) を検出した。

##### 4.3.2 考察

「イントラネットのメール及び配送不能メールの除外」と「各パートの最小サイズ制限」を設定したことで、正規メールの検出を 5 種類まで削減できた。また、検出率も実

験1よりも1.2%減少し、0.1%まで抑制できた。

検出した正規メールは、5種類全て単一のドメインからのメールであり、ローカルパートのみが異なっていた。このため、今回の実験データに関しては、ドメインを考慮することで、正規メールのFalse Positiveを0件にすることが可能である。

迷惑メール、マルウェア感染メールに関しては、除外による影響はなかった。しかし、サイズ制限を設けることで、迷惑メール、マルウェア感染メールともに検出率が減少した。これは、空メールにマルウェアのみを添付しているメールやHTMLメールが多かったためである。

本文0のパートが空または改行のみのtext/plainであり、本文1がtext/htmlになっているメールが数多く存在した。特に迷惑メールでは、609件存在したため合計が大幅に減少している。

スパム対策では、False Positiveの方がFalse Negativeよりも業務等に影響があり問題になる。このため、本研究ではFalse Positiveを減少させることを優先している。

#### 4.4 実験3

実験3では、パートごとに分割したデータの加工を行う。具体的には、図3の2. 情報抽出において、パートごとに分割後、ハッシュ値を算出する前にデータの加工を行う。データの加工は、「改行のみの行の削除」および「URL・メールアドレスの削除」を行った。これにより、メール文のランダム要素をある程度除去することができ、検出精度が向上すると考えられる。その他の設定は、実験2と同様である。

##### 4.4.1 実験結果

検出された正規メール、迷惑メール、マルウェア感染メールのそれぞれについて、種類数、合計、検出率を表4に示す。実験2と実験3の比較結果を表5に示す。

表4 実験結果3

正規メール								
	計	本文0	本文1	本文2	添付0	添付1	添付2	添付3
種類数	5	1	0	0	3	1	0	0
合計	19	15	0	0	3	1	0	0
検出率(%)	0.1	0.1	0	0	0	0	0	0
迷惑メール								
	計	本文0	本文1	本文2	添付0	添付1	添付2	添付3
種類数	185	114	69	0	1	0	0	1
合計	475	343	120	0	9	0	0	3
検出率(%)	10.1	7.3	2.6	0	0.2	0	0	0.1
マルウェア感染メール								
	計	本文0	本文1	本文2	添付0	添付1	添付2	添付3
種類数	43	13	1	0	20	5	4	0
合計	89	22	1	0	51	8	7	0
検出率(%)	50.0	12.4	0.6	0	28.7	4.5	3.9	0

表5 実験2と実験3の比較

加工なし			
	正規メール	迷惑メール	マルウェア感染メール
種類数	5	22	46
合計	19	59	89
検出率	0.1%	1.3%	50.0%
改行のみの行・URL・メールアドレスの削除			
	正規メール	迷惑メール	マルウェア感染メール
種類数	5	185	43
合計	19	475	89
検出率	0.1%	10.1%	50.0%

正規メールを0.1%、迷惑メール10.1%、マルウェア感染メール50.0%を検出した。

##### 4.4.2 考察

各パートに分割後、「改行のみの行の削除」および「URL・メールアドレスの削除」を行った。これにより、マルウェア感染メールでは、全体の検出率は変化しなかったが、本文0での検出率が増加し、添付ファイルでの検出率が減少した。マルウェア感染メールを確認すると、本文に改行の有無による違いや、ランダムな文字列等がある場合でも、添付ファイルが同一であることが多かった。

迷惑メールでは、約8.8%検出率が向上した。新たに検出したメールからは、メール本文内に送信元のアドレスや誘導先のURL、返信用のメールアドレスなどが記載されているメールが複数確認できた。

検出した迷惑メールの中でも「URL付きでWebページへ誘導するメール」、「返信用メールアドレス付きのメール」は、ばらまき型メールと同様の特徴が見られた。この特徴をもつ迷惑メールは、ばらまき型メールと同様または類似した攻撃インフラを使用している可能性が考えられる。

#### 4.5 実験4

実験4では、ドメイン情報を利用し、送信元情報の関連性が低いメールのみをカウントすることで、より正確な有効性の検証を行う。

実験2では、正規メールにおいて、メールアドレスのローカルパート部分は異なるが、単一ドメインであるメールが検出された。実験1~3では、簡単のためヘッダFromアドレスのみで実験を行っていたが、本手法では、送信元情報の関連性が低いメールの件数をカウントする必要がある。実験4では、より正確な有効性を確認するためドメイン情報も考慮した実験を行った。

ドメイン情報を考慮するにあたり、図3の2. 情報抽出で、メールアドレスのハッシュ値だけでなく、ドメインのハッシュ値も取得する。その後、4. 類似メール判定処理で分割したパートごとに、同一のハッシュ値かつ異なる送信元であるメール数（類似メールの数）がしきい値以上であること、さらに、異なるドメインの数がしきい値以上なら

ば、検出対象とするように変更した。

実験は、実験3と同様の設定で、異なるドメインのしきい値を2とした。2つ以上のドメインを持つときに検出する。

#### 4.5.1 実験結果

検出された正規メール、迷惑メール、マルウェア感染メールのそれぞれについて、種類数、合計、検出率を表6に示す。

表6 実験結果4

正規メール								
	計	本文0	本文1	本文2	添付0	添付1	添付2	添付3
種類数	0	0	0	0	0	0	0	0
合計	0	0	0	0	0	0	0	0
検出率(%)	0.0	0	0	0	0	0	0	0
迷惑メール								
	計	本文0	本文1	本文2	添付0	添付1	添付2	添付3
種類数	155	84	69	0	1	0	0	1
合計	395	263	120	0	9	0	0	3
検出率(%)	8.4	5.6	2.6	0	0.2	0	0	0.1
マルウェア感染メール								
	計	本文0	本文1	本文2	添付0	添付1	添付2	添付3
種類数	42	12	1	0	20	5	4	0
合計	87	20	1	0	51	8	7	0
検出率(%)	48.9	11.2	0.6	0	28.7	4.5	3.9	0

正規メールは検出率0.0%(0件)で検出しなかった。迷惑メールは8.4%、マルウェア感染メールは48.9%を検出した。

#### 4.5.2 考察

メールアドレスのドメイン情報を利用して、より正確に送信元情報の関連性を考慮することで、通常メールのFalse Positiveを0件にすることができた。ただし、今回の実験データにおいてFalse Positiveが0件であるだけで、全ての環境に適用できるわけではない。しかし、有効な環境が存在することが確認できた。

迷惑メールについても検出率が減少した。実験3までの結果では、迷惑メールは、ドメインが同一でローカルパート部分が複数あるものや、ランダムなものがいくつか検出されていた。実験4でも検出していない迷惑メールの中には、メールアドレスのドメインがランダムなものも存在している。このような迷惑メールを確認すると、MTAのIPアドレスが近い値であることが多い。このため、MTAのIPアドレスを考慮することで、ばらまき型メールのみを効率的に検出できると考えられる。

マルウェア感染メールに関しては、検出数が2件減っただけであり、ドメインを考慮しても影響少ないことがわかる。マルウェア感染メールには、ばらまき型メールが多く、送信元が異なる場所から送られてくるため影響が少なかったと考えられる。MTAのIPアドレスを確認しても、大きく異なるIPアドレスであった。

以上より、送信元に関する情報の関連性が低く、本文・

添付ファイル等の類似度が高いという特徴を利用することで、ばらまき型メールが検出できることを確認できた。

#### 4.6 実験5

最後に、実験4で行った設定で受信済みメールの分類を行う。実験1～実験4では、実際の運用を想定して、時系列に受信した順番に処理を行っていた。このため、類似メールのしきい値に達する前のメールは、検出されずそのまま転送・受信していた。

実験5では、しきい値に達する前のメールも含めて検出を行う。これにより、未検出のマルウェア感染メールがどのようなメールであるかを明らかにする。

#### 4.6.1 実験結果

検出された正規メール、迷惑メール、マルウェア感染メールのそれぞれについて、種類数、合計、検出率を表7に示す。

表7 実験結果5

正規メール								
	計	本文0	本文1	本文2	添付0	添付1	添付2	添付3
種類数	0	0	0	0	0	0	0	0
合計	0	0	0	0	0	0	0	0
検出率(%)	0.0	0	0	0	0	0	0	0
迷惑メール								
	計	本文0	本文1	本文2	添付0	添付1	添付2	添付3
種類数	155	84	69	0	1	0	0	1
合計	631	404	213	0	10	0	0	4
検出率(%)	13.4	8.6	4.5	0	0.2	0	0	0.1
マルウェア感染メール								
	計	本文0	本文1	本文2	添付0	添付1	添付2	添付3
種類数	41	12	1	0	20	5	3	0
合計	121	32	2	0	70	13	4	0
検出率(%)	68.0	18.0	1.1	0	39.3	7.3	2.2	0

迷惑メール13.4%、マルウェア感染メール68.0%を検出した。未検出のマルウェア感染メールは57件あり、表8のようなメールがあった。

表8 未検出マルウェア感染メールの本文の内訳

マルウェア感染メールの種類	件数
添付ファイルが無いURL付きなりすましメール	20
送信先と同じドメインに偽造したメール	12
同一のアドレスからのメール	8
類似メールが1件目のみ(類似メールがない)	8
ランダムな文字列を含むメール	3
パートの違い	3
送信側のエンコードミス	3

#### 4.6.2 考察

しきい値に達する前のメールも含めると68%のマルウェア感染メールを検出することができた。ばらまき型メー

ルは、短期間で大量に送信されるため、サーバで 10 分前後の遅延時間を設けることで、しきい値に達する前のメールも検出できる可能性があると考えられる。

表 8 の添付ファイルが無い URL 付きのなりすましメールは、本文に記載の URL がマルウェアのダウンロードページになっている。このなりすましメールは、ヘッダ From アドレスが同一であること、複数の候補の中から選択された文が本文の一部に使用されていることから、検出できていない。しかし、MTA の IP アドレスは大きく異なっていた。このため、本文の URL からダウンロードするマルウェアのハッシュ値等が同一であれば、検出させる方法はあると考えられる。

送信先と同じドメインに偽造したメールは、今回の実験ではドメインを 2 つ以上としたため検出できなくなった。しかし、これも MTA の IP アドレスを利用することで検出することが可能であると考えられる。

今回は、パートごとに分割して、同一のパート間で類似判定を行った。このため、パートがずれている場合等では検出することができない。よって、パートを問わずに類似判定するなどにより、検出率が向上する可能性もある。

最後に、類似メールが 1 件しかなく、しきい値に達しなかったメールについて、本手法では、各パートのハッシュ値と送信元アドレスのハッシュ値の一部があれば検出に利用できる。例えば、メールアドレスのハッシュ値の先頭 5 文字程度があれば、件数をカウントするには十分である。このため、レインボーテーブルを用いても元のメールアドレスを求められず、開発元や他組織等と共有しやすくなると考えられる。サンプル数が増えれば検出精度が向上することが期待できる。

## 5. まとめと今後

本研究では、送信元に関する情報の関連性が低く、本文や添付ファイルなどの類似度が高いメールをばらまき型メールとして検出する手法を提案し、その有効性を確認した。送信元に関する情報としては、送信元アドレスのハッシュ値、ドメインのハッシュ値を利用した。本文や添付ファイルの情報としては、パートごとのハッシュ値を利用した。また必要に応じて、事前にデータを加工し、加工後のハッシュ値を用いて実験を行った。

実験の結果、事前に検出状況を調査し、社内メールや配達不能メールを検出対象外とし、パートごとのサイズ制限等を設定することで False Positive を発生させずに、ばらまき型メールを検出することができた。

ただし、本手法は全ての環境に適用できるとは限らず、

導入前に調査・調整する必要がある。特に添付ファイルは、通常の運用でも様々な送信元から同一のファイルが送られてくる可能性があることに留意する必要がある。

本手法はスパムフィルタの一つとして、既存のスパム対策・セキュリティソフト等と組合せ、見逃したものに適用することで、メールを受信するユーザの脅威の低減が期待できる。また、事後処理を警告文の追加や添付ファイルの分離などと工夫することにより、False Positive が発生した場合でも業務への影響を最小限に抑えられると考えられる。

その他にも、研究等で受信したメールから自動でマルウェア解析を行う場合の前処理や、情報システム部などが社内にも注意喚起する場合の不審メールの早期発見などの利用法が考えられる。

今後について、今回の実験では、送信元に関する情報として、ヘッダ From アドレスおよびドメインを利用したが、MTA の IP アドレス等を利用し、異なる送信元の判定精度を向上させる必要がある。

また、通常のハッシュ関数では、ランダムな文字列や複数の文から選択する文章や、少し変更を加えたマルウェアなどは検出できない。このため、ファジーハッシュを類似判定に利用するなど更なる改良の余地がある。

さらに、同一のテンプレートが利用される期間が短いため、ログの保存期間を短縮しても検出率が維持できるか検証する必要がある。

False Positive を抑制する方法としては、ばらまき型メールの特徴である初めて受信する送信元から送られてくることを利用する方法が挙げられる。このため、送受信履歴を用いて検出対象外の送信元を制御する方法の有効性を検証する。

**謝辞** 本研究を行うにあたり、他業務の調整や研究全般の協力いただいたラボのメンバー及び上司の皆様には感謝の意を表す。

## 参考文献

- [1] “迷惑メール対策ハンドブック 2017”.  
[https://www.dekyo.or.jp/soudan/data/anti\\_spam/h2017/HB17\\_0\\_all.pdf](https://www.dekyo.or.jp/soudan/data/anti_spam/h2017/HB17_0_all.pdf), (参照 2018-07-18).
- [2] 神谷造, 柴田賢介, 佐野和利, 荒金陽介, 塩野入理, 金井淳史. 迷惑メールの外見的特長についての一考察. 電子情報通信学会技術研究報告. ISEC, 情報セキュリティ 107(141), 123-127, 2007-07-13
- [3] “Troy Hunt: Inside the Massive 711 Million Record Onliner Spambot Dump”. <https://www.troyhunt.com/inside-the-massive-711-million-record-onliner-spambot-dump/>, (参照 2018-07-18).
- [4] “国内ネットバンキングを狙うマルウェアスパムボットネットに「潜入調査」 | トレンドマイクロ セキュリティブログ”. <https://blog.trendmicro.co.jp/archives/14538>, (参照 2018-07-18).