2015年度 修士論文

スパムトラップによる
マルウェア付スパムメールの特徴分析

提出日：2016年2月1日

指導：後藤滋樹教授

早稲田大学 基幹理工学研究科 情報理工・情報通信専攻
学籍番号：5114F049-6

志村　正樹

目次

第 1 章　序論 **5**

1.1　研究の背景 5

1.2　研究の目的 5

1.3　本論文の構成 6

第 2 章　電子メールおよびスパムメールの概要 **7**

2.1　電子メールの概要 7

2.1.1　電子メール送信の原理 7

2.1.2　メール送信に使用されるデータ 8

2.2　スパムメールの概要 9

2.2.1　スパムメールとは 9

2.2.2　スパムメールの問題 9

2.2.3　スパムメールの目的 9

2.2.4　スパムメールによるマルウェア感染 10

2.3　スパムトラップ 10

第 3 章　提案手法 **11**

3.1　先行研究 11

3.2　提案手法の概要 11

3.3　抽出するファイル 12

第 4 章　データの概要 **14**

4.1　データ収集環境 14

4.2　メール数 14

第 5 章　分析結果 **16**

5.1　マルウェアスパムメールの分析 16

5.1.1 マルウェア種別ごとのメール数 16
5.1.2 拡張子ごとのマルウェアスパムメール数 17
5.2 スパムメールとの差異分析 21
5.2.1 送信先メールアドレスの分析 21
5.2.2 送信先メールアドレスのドメインの分析 21
5.2.3 メールの到着時間の分析 22

第 6 章 考察 **24**
6.1 マルウェアスパムメールの分析結果 24
6.2 スパムメールとマルウェアスパムメールの比較結果 24

第 7 章 結論 **26**
7.1 まとめ 26
7.2 今後の課題 26
7.2.1 分析内容の追加 26
7.2.2 Web 経由のマルウェア配布への対応 27

謝辞 **28**

参考文献 **29**

図一覧

2.1 電子メールの送信原理 7
2.2 電子メール本体の構成 8

3.1 提案手法の概要 12

4.1 観測期間のメール数の時系列変化 15

5.1 マルウェア数の時系列 17
5.2 .zip ファイル付メール数の時系列 19
5.3 .exe ファイル付メール数の時系列 19
5.4 .doc ファイル付メール数の時系列 20
5.5 .pdf ファイル付メール数の時系列 20
5.6 スパムメールの 1 時間ごとのメール送信数 23
5.7 マルウェア付スパムメールの 1 時間ごとのメール送信数 23

表一覧

4.1 スパムトラップに使用されるドメイン数 14
4.2 観測期間全体のメール数 15

5.1 マルウェア種別ごとのメール数 17
5.2 観測期間全体のメール数 18
5.3 ユニークな送信先アドレス数 21
5.4 送信先ドメインごとのメール数の割合 22
5.5 送信先ドメインの TLD ごとのメール数の割合 22

第 1 章

序論

1.1 研究の背景

スパムメールに添付されたマルウェアによる被害が拡大している．スパムメールは主に広告などを目的としたメールであるが，その中にはマルウェア感染を目的とし，マルウェアを添付して送信されるスパムメールが存在する．このようなマルウェアに感染すると，ボットネットとして攻撃に加担させられる，個人情報が流出する，他のマルウェアをダウンロードさせられるなどの被害が生じる．このようなマルウェアを添付するスパムメールは，広告などを目的としたものとは性質が異なり，通常のメールを装って送信される．そこで本研究では，スパムメールの中でもマルウェアを添付しているものに着目し，添付されたマルウェアを分類し，一般的なスパムメールとの比較を行い，特徴を分析する．

1.2 研究の目的

第 1.1 節で述べたように，スパムメールに添付されたマルウェアによる被害が拡大している．マルウェアが添付されたスパムメールは広告目的のものとは異なり，ユーザにファイルを実行させ，マルウェアに感染させることを目的としている．そのため，広告サイトへの誘導などが主な目的である一般的なスパムメールと比較して，その性質が異なると考えられる．そこで本論文では，マルウェアが添付されたスパムメールであるマルウェア付スパムメール (以下では単にマルウェアスパムメールと書く) の特徴を，マルウェアスパムメール自身の特徴と，一般的なスパムメールとの比較を通じて明らかにすることを目的とする．マルウェアスパムメールの特徴を分析することで，メールによるマルウェア感染活動の実態の調査や，マルウェアスパ

ムメールの防御手法などに活用することができる.

1.3　本論文の構成

本論文は以下の章により構成される.

第 1 章 序論

本論文の概要について述べる.

第 2 章 電子メールおよびスパムメールの概要

スパムメールやマルウェアスパムメールの概要を紹介する.

第 3 章 提案手法

本研究の提案手法を説明する.

第 4 章 データの概要

本研究で用いたデータの概要について説明する.

第 5 章 分析結果

提案手法に基づいた分析結果を述べる,

第 6 章 考察

分析結果に基づいた考察を述べる.

第 7 章 結論

本研究の結論と今後の課題を述べる.

第 2 章

電子メールおよびスパムメールの概要

2.1　電子メールの概要

2.1.1　電子メール送信の原理

電子メールとはインターネット初期から存在する通信手段であり，SMTP というプロトコルを用いてメールが送信される．メール送信の概要図を図 2.1 に示す．電子メールの送信は，メールを送信するサーバである MTA と，メールを送受信するクライアントである MUA からなる．電子メールは送信側の MUA から送信側の MTA に SMTP を用いて配送される．その後，送信側 MTA はメール受信側の MTA に SMTP を用いてメールを送信する．その後，受信側の MUA は，POP や IMAP のようなプロトコルを用いてメールを受信する．

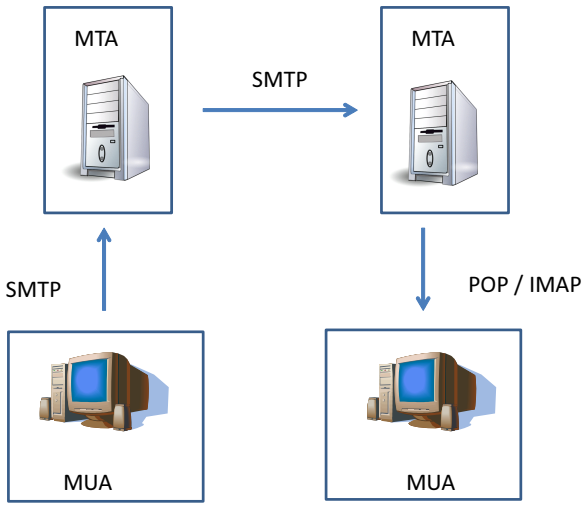


図 2.1: 電子メールの送信原理

2.1.2　メール送信に使用されるデータ

メール送信に使用されるデータは，メール本体とエンベロープと呼ばれる送信制御に使われる情報から成り立っている．

電子メールのエンベロープは，メール送信に使われる SMTP 通信の際に使用される情報である．エンベロープの情報には，メール送信元のアドレスと，メールの送信先のアドレスが含まれており，エンベロープで指定された送信先アドレスにメール本体が送信される．そのためエンベロープに含まれるアドレスを調べることで，メールが実際に送信されているメールアドレスを調べることができる．

メール本体の構成図を図 2.2 に示す．メール本体は，メールヘッダおよびメールボディによって構成される．メールヘッダには，宛先メールアドレスを示す To ヘッダなどが含まれている．しかし To ヘッダに含まれるメールアドレスは送信者側が自由に設定することができ，To ヘッダのメールアドレスがエンベロープアドレスと一致するとは限らない．メールボディにはメールの本文や添付ファイルのような，送信者が実際に送信したい内容が記述されている．



図 2.2: 電子メール本体の構成

2.2　スパムメールの概要

2.2.1　スパムメールとは

スパムメールとは迷惑メールとも呼ばれ,「大量送信される、匿名の迷惑なメール」[1] や「不特定多数の相手に送られる，内容として広告・宣伝・誘導・詐欺等の性質が強いメール」とされている．ただしスパムメールの明確な定義は定められておらず，スパムメールの定義に関しては幅広い見解がある．

スパムメールは，2015 年 6 月時点で世界のメールトラフィックの 49.7%を占めており [2]，依然として大きな問題となっている．

2.2.2　スパムメールの問題

スパムメールによって引き起こされる問題としては，以下の様なことがあげられる．

- メール整理に伴う時間の浪費
- 重要なメールの見落とし
- ネットワークトラフィックの圧迫
- メール保存容量などのサーバ資源の圧迫
- マルウェアの感染やフィッシング詐欺などの被害

2.2.3　スパムメールの目的

スパムメールの目的は多岐にわたり，広告を目的としたもの，フィッシング詐欺などの情報の詐取を目的としたもの，マルウェア感染を目的としたものなどがあげられる．広告目的のスパムメールでは，メール受信者が興味を抱くようなキーワードを本文に使い，URL などへ誘導する傾向がある．それに対しマルウェア感染を目的としたスパムメールでは，受信者をマルウェアをダウンロードさせる URL への誘導や，マルウェアを添付ファイルとして送信するなどの方法でマルウェアに感染させる．

2.2.4　スパムメールによるマルウェア感染

マルウェア感染を目的としたスパムメールによる被害が拡大している．マルウェア感染を目的としたスパムメールは，マルウェアを添付ファイルとして送信する，マルウェアをダウンロードさせる URL をメールに記載して誘導するなどの方法でマルウェアを送信，感染させる．このうち，URL 経由で感染させるメールは，添付ファイルで感染させるメールの 3%ほど [2] であり，多くのスパムはマルウェアを添付することによってマルウェア感染を行う．2015 年の 5 月には，全体のメールトラフィックの 315 通に 1 通にマルウェアが添付されており [2]，メールがマルウェア感染の主要な経路になっていることが分かる．マルウェアが添付されたスパムメールでは，受信者に正規のファイルであるかのように錯覚させ，ファイルを実行させることによって感染する．マルウェア感染の手法には以下の様なものがある

- 拡張子を偽装し，実行ファイル (.exe など) をその他のファイルに偽装する
- PDF などの脆弱性を悪用する
- Microsoft Word など，ファイルのマクロ機能を使用してマルウェアをダウンロード，実行させる

2.3　スパムトラップ

スパムメールを分析するする手法として，スパムトラップがある．スパムトラップはハニーポットの一種で，スパムメールを収集することを目的としたメールサーバである．スパムトラップで使用されているドメインは，かつて使用されていたものの，現在は使用されていないドメインである．スパムトラップのドメインは現在使用されていないドメインであるため，スパムトラップに使用される前に使われていたメールアドレスに届くメールを除けば，正規なメールではないスパムメールである．そのためスパムトラップのメールを分析することによって，送信されているスパムメールの分析を行うことができる．

第 3 章

提案手法

3.1 先行研究

筆者らは先行研究 [3] において，スパムメールによって配布されるマルウェアに着目し，マルウェアスパムメールの分析を行った．具体的にはスパムメールの添付ファイルを Zip ファイル，実行ファイル，文書ファイルに分類し，マルウェアメールの特徴を添付ファイルごとの種別ごとに分析した．

3.2 提案手法の概要

本研究では，スパムメールのうちマルウェア感染を目的としたものに着目し，その特徴の分析を行った．スパムトラップを用いてスパムメールを収集し，スパムメールの中から特定の拡張子を持つ添付ファイルを持つメールを抽出した．その後，抽出されたメールに添付されたファイルがマルウェアであるか否かの判定を行った．そしてマルウェアと判定されたファイルが添付されたメールをマルウェアスパムメール，それ以外のメールをスパムメールとして分類を行った．そしてマルウェアスパムメールの分析，およびマルウェアスパムメールとスパムメールの送信活動の比較を行い，マルウェアスパムメールの送信活動の特徴を分析した．

本提案手法では，先行研究の内容に加え，マルウェアスパムメールとスパムメールの送信活動の比較を行った．スパムメールとの送信活動の比較を行うことで，マルウェアスパムメールにのみ見られる特徴を発見し，マルウェアスパムメールの研究や対策に活用することができる．本提案手法の概要を図 3.1 に示す．

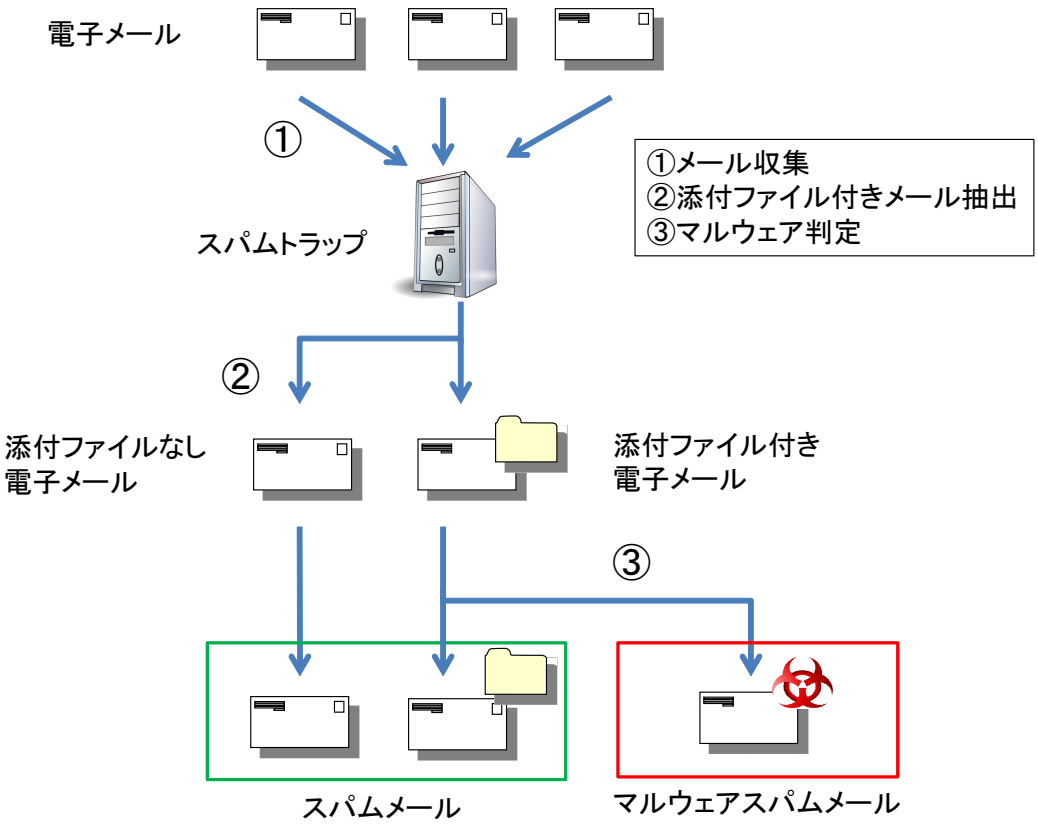


図 3.1: 提案手法の概要

3.3　抽出するファイル

本研究ではマルウェアに使用されることが多い Zip 圧縮ファイル，実行ファイル，Microsoft Office ファイル，PDF ファイルを抽出して分析対象とした．分析対象とした添付ファイルの拡張子を以下に示す．

- Zip 圧縮ファイル
  - .zip：Zip 圧縮ファイルの拡張子
- 実行ファイル
  - .exe：プログラムファイルの拡張子
  - .com：MS-DOS プログラムの拡張子
  - .bat：バッチファイルの拡張子

  - .scr：スクリーンセーバーファイルの拡張子
  - .pif：MS-DOS プログラムへのショートカットの拡張子

- Microsoft Office ファイル
  - .doc, .docx：MS Word 用拡張子
  - .xls, .xlsx：MS Excel 用拡張子

- PDF ファイル
  - .pdf：PDF ファイルの拡張子

第 4 章

データの概要

4.1 データ収集環境

本節では，本実験で使用したデータの概要について述べる．

本研究では，スパムトラップを設置・運用して電子メールの定点観測を行った．本研究で使用したスパムトラップは，かつてメールサービスが使用されていたドメインで，現在は使用されていないドメイン宛に送信されるメールを収集している．

本実験に用いたスパムトラップでは，合計で 65 のドメインを利用してスパムメールの収集を行った．表 4.1 に本実験で用いたドメイン数をトップレベルドメインごとに示す．

表 4.1: スパムトラップに使用されるドメイン数

TLD	com	net	jp	org
ドメイン数	46	13	5	1

4.2 メール数

本実験では，スパムトラップを用いて 2013 年 10 月から 2015 年 7 月に送信されたスパムメールを収集し分析対象とした．収集されたスパムメールの中から，分析対象となる Zip 圧縮ファイル・実行ファイル・Microsoft Office ファイル・PDF ファイルを添付ファイルとして持つメールを抽出した．この添付ファイルを，オンラインのファイルスキャンサービスである VirusTotal [4] を用いてスキャンし，5 種類以上のアンチウイルスソフトでマルウェアと判定された場合，マルウェアであるとの判定を行った．

観測期間における全受信メール数，添付ファイル付きメール数，マルウェアスパムメール数，スパムメール数を表 4.2 に示す．ここでスパムメールは全受信メールのうち，マルウェアスパムメールではないと判定されたメールである．この表から，ファイルが添付されたメールの内，約 86%がマルウェアスパムメールと判定されたことが分かる．ここから，スパムトラップに送信されたメールに添付されるファイルの多くはマルウェアであることがわかる．

表 4.2: 観測期間全体のメール数

	メール数
全受信メール	30,193,779
添付ファイル付きメール	422,594
マルウェアスパムメール	363,042
スパムメール	29,830,737

観測されたメール数の時系列の変化を図 4.1 に示す．2014 年 9 月にはメールの収集が出来なかったためにデータが欠損している．図より，スパムメールの送信量の時系列には大きな変化があることがわかる．

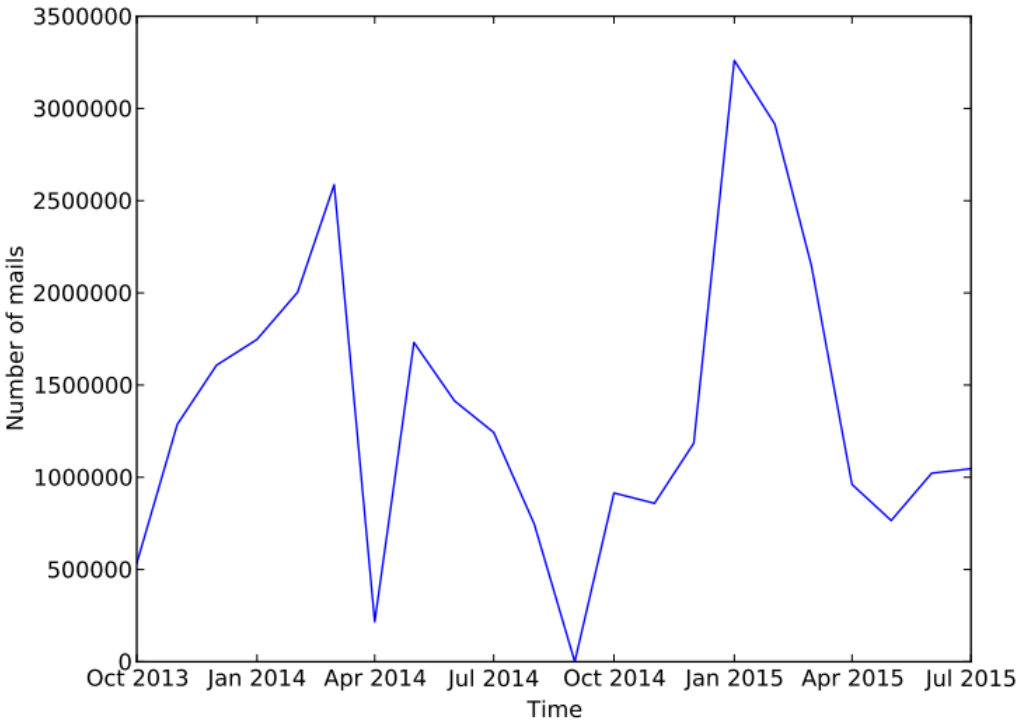


図 4.1: 観測期間のメール数の時系列変化

第 5 章

分析結果

5.1 マルウェアスパムメールの分析

本節では，マルウェアスパムメールの特徴を分析する．

5.1.1 マルウェア種別ごとのメール数

メールに添付されたマルウェアの種類を分析する．VirusTotal を用いて分類した，観測期間全体のマルウェアの種別ごとのメール数を表 5.1 に，月ごとのマルウェア種別ごとのメール数を図 5.1 に示す．本実験では，マルウェアを Mydoom，Upatre，Zbot，Trojan，other の 5 種類に分類した．Mydoom [5] はスパムメール送信機能を持つワーム型のマルウェアであり，感染した端末から自身のコピーを送信することで感染を拡大する．Upatre [6] はトロイの木馬型のマルウェアであり，感染すると内部で複製され，さらなる不正ファイルのダウンロードと実行を行う．Zbot [7] は銀行取引などの個人情報を盗み出すことを目的としたトロイの木馬である．Trojan はその他のトロイの木馬型のマルウェア，other は Mydoom，Upatre，Zbot，Trojan のいずれとも判定されなかったマルウェアである．Mydoom などのワーム型のマルウェアよりも，さらなるマルウェア感染や情報収集に繋げるためのトロイの木馬型のマルウェアが主流となっていることがわかる．また送信されるマルウェアの量も，時系列による変化が大きいことがわかる．

表 5.1: マルウェア種別ごとのメール数

	メール数
Trojan	184,011
Upatre	103,669
Zbot	72,848
Mydoom	2,355
other	122

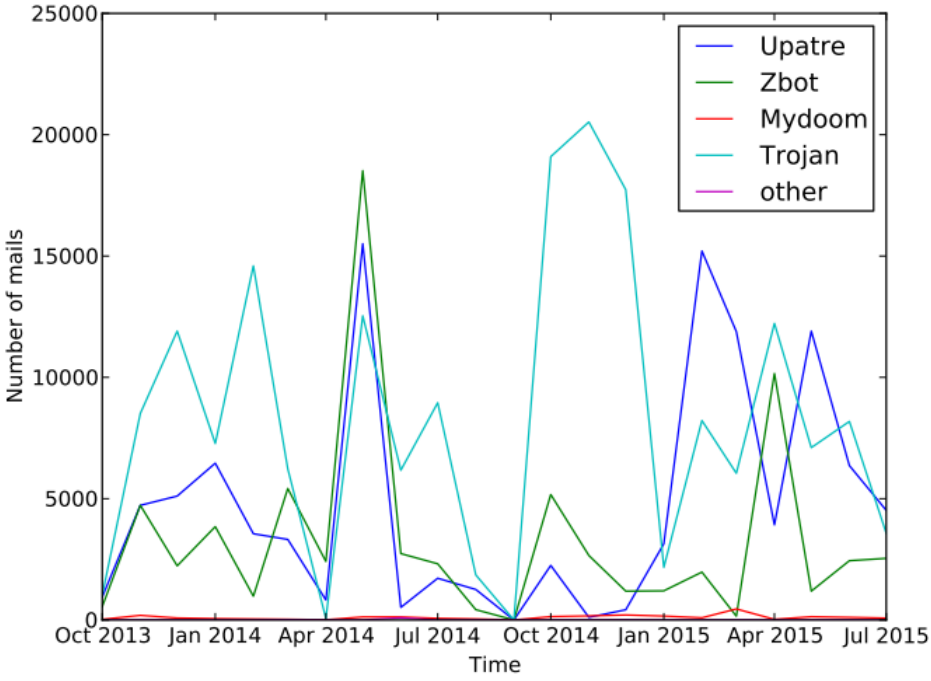


図 5.1: マルウェア数の時系列

5.1.2　拡張子ごとのマルウェアスパムメール数

添付ファイルの拡張子ごとの，添付ファイル付電子メール数およびマルウェアスパムメール数を表 5.2 に示す．表より，.exe，.bat などの実行形式のファイルや，.zip といった Zip 圧縮ファイルは殆どのファイルがマルウェアと判定されたことが分かる．また Microsoft Office ファイルや PDF ファイルなどは，マルウェアである割合が低くなっている．これは Microsoft Office や PDF などの文書作成に使用されるファイルは，詐欺などのマルウェア以外の悪性活動に使

用される場合があるためと考えられる．

表 5.2: 観測期間全体のメール数

ファイル種別	拡張子	添付ファイル付メール数	マルウェアスパムメール数
圧縮ファイル	.zip	353,552	347,656
実行ファイル	.exe	1,722	1,583
	.scr	344	337
	pif	100	96
	.com	65	63
	.bat	46	43
Microsoft Office ファイル	.xls	32,202	480
	doc	19,836	11,175
	.docx	3,689	25
	.xlsx	4,262	19
PDF ファイル	.pdf	8,017	1,440

また，マルウェアメールの総量が 1000 通以上である.zip，.exe，.doc，.pdf ファイルについて，添付ファイル付メール数およびマルウェアスパムメール数の時系列をそれぞれ図 5.2，図 5.3，図 5.4，図 5.5 に示す．

.zip ファイルや.exe ファイルは，添付ファイル付メール数とマルウェアスパムメール数のグラフがほぼ重なっていおり，ほとんどの添付ファイル付メールがマルウェアスパムメールと判定されたことがわかる．また.exe ファイルは 2015 年 1 月および 4 月のメール数が多くなっており，時系列の変化が大きくなっている．

doc ファイルは，2014 年 11 月から. マルウェアスパムメール数の割合が急増していることが分かる．これはマクロ機能を利用したマルウェアの増加によるものと考えられる [8]．

.pdf ファイルは，観測期間のうち 2014 年 5 月のみマルウェアスパムメール数が急増しており，その他の期間ではマルウェアと判定されていない．

このように，マルウェアスパムメールに使用される添付ファイルの種別には流行が存在し，時系列変化が大きくなっていることがわかる．

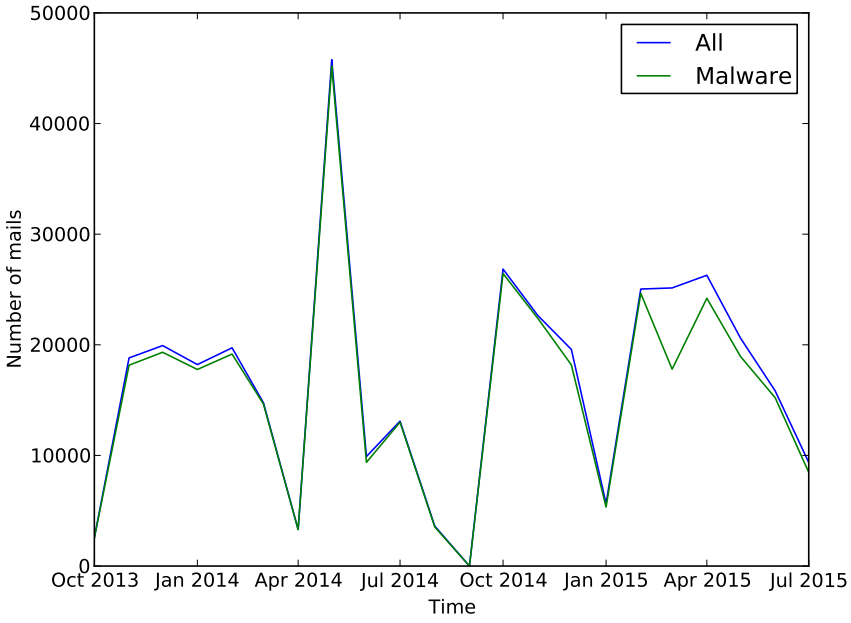


図 5.2: .zip ファイル付メール数の時系列

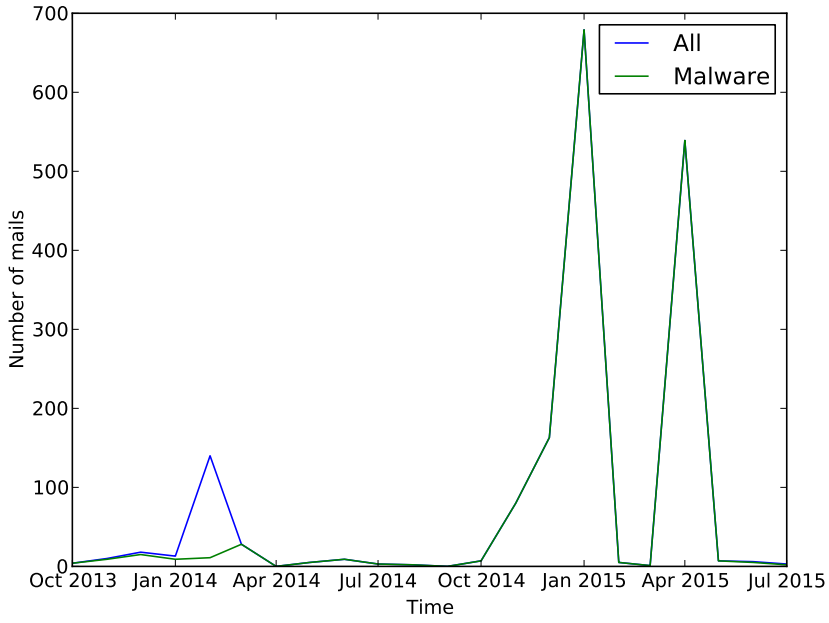


図 5.3: .exe ファイル付メール数の時系列

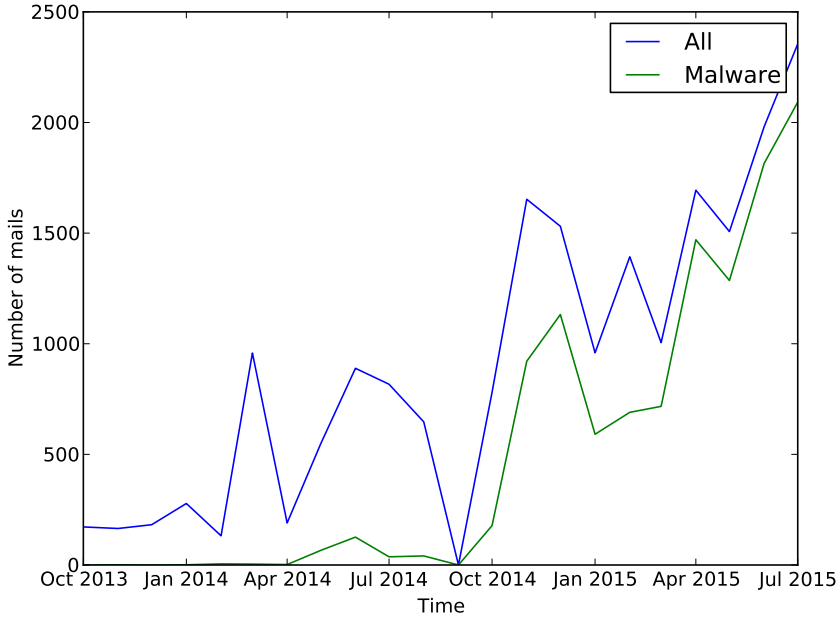


図 5.4: .doc ファイル付メール数の時系列

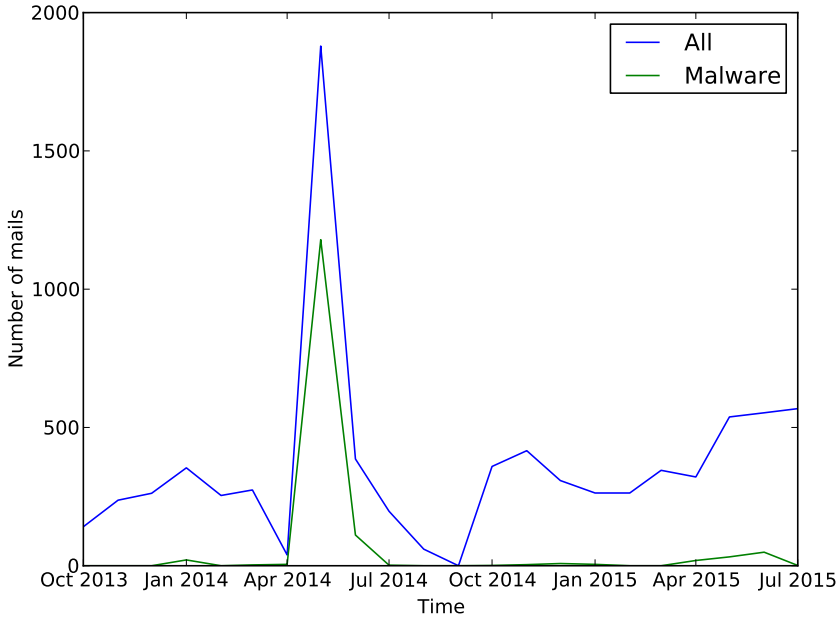


図 5.5: .pdf ファイル付メール数の時系列

5.2　スパムメールとの差異分析

5.2.1　送信先メールアドレスの分析

メールの送信先アドレスに着目した比較を行う．なお，本実験ではエンベロープで指定されたアドレスを送信先アドレスとする．表 5.3 に，観測されたユニークなアドレス数，および 1 アドレスあたりの平均のメール数を示す．マルウェアスパムメールの 1 アドレスあたりの平均数は，スパムメールと比較して多くなっている．ここから，マルウェアスパムメールはスパムメールと比較して特定のアドレス宛に集中して送信される傾向があることがわかる．

表 5.3: ユニークな送信先アドレス数

	ユニークアドレス数	1 アドレスあたりの平均メール数
マルウェアスパムメール	9,627	37.71
スパムメール	2,156,510	13.83

5.2.2　送信先メールアドレスのドメインの分析

メールの送信先アドレスのドメインに着目した比較を行う．送信先アドレスのドメインごとの，マルウェアスパムメールとスパムメール全体に占めるメール数の割合を，各上位 5 ドメインについて表 5.4 に示す．なお，表 5.4 におけるドメイン名は，スパムトラップの設置箇所を隠蔽するために，変数とトップレベルドメインで表した仮の物である．スパムメールでは，トップレベルドメインが jp である d6 に半数近くのメールが送信されている．一方マルウェアスパムでは，トップレベルドメインが com である d1, d3, d4 と，トップレベルドメインが net である d2 と d5 が上位となっている．以上より，マルウェアスパムメールが送信される送信先ドメインは，d2 が一致している点を除いて，スパムメールとは異なる傾向があることが分かる．

また，送信先アドレスのトップレベルドメインごとの，マルウェアスパムメールとスパムメール全体に占めるメール数の割合を表 5.5 に示す．マルウェアスパムメールは約 70%が.com に送信されおり，スパムメールの 25.3%とくらべて非常に高くなっている．さらにスパムメールで最多である.jp が 7%程度しかないなど，送信されるドメインに大きな差があることが分かる．以上より，スパムメールとマルウェアスパムメールの送信先ドメインは異なる傾向があり，.com などの企業系のドメインに多く送信されていることがわかった．

表 5.4: 送信先ドメインごとのメール数の割合

マルウェアスパムメール		スパムメール	
ドメイン名	割合 (%)	ドメイン名	割合 (%)
d1 (com)	14.45	d6 (jp)	40.01
d2 (net)	9.48	d2 (net)	8.10
d3 (com)	9.34	d7 (jp)	6.70
d4 (com)	7.24	d8 (net)	4.89
d5 (net)	6.72	d9 (net)	3.04

表 5.5: 送信先ドメインの TLD ごとのメール数の割合

マルウェアスパムメール		スパムメール	
トップレベルドメイン	割合 (%)	トップレベルドメイン	割合 (%)
com	70.2	jp	48.7
net	22.8	net	25.5
jp	6.98	com	25.3
org	0.00275	org	0.435

5.2.3　メールの到着時間の分析

メールの到着時間の分析を行う．スパムメール，およびマルウェアスパムメールのメールの協定世界時 (UTC) における 1 時間ごとのメール数をそれぞれ図 5.6 および図 5.7 に示す．スパムメールは 1 時間ごとのメール数に大きな変化がないのに対し，マルウェアスパムメールでは 14 時から 17 時のメール数が多くなっている．特に 14 時台のメールは 0 時台に比べて 3 倍以上になるなど，メールの送信時間に大きな差があることがわかる．このことから，マルウェアスパムメールはスパムメールと比較し，送信時間が特定の時間に集中していることがわかった．

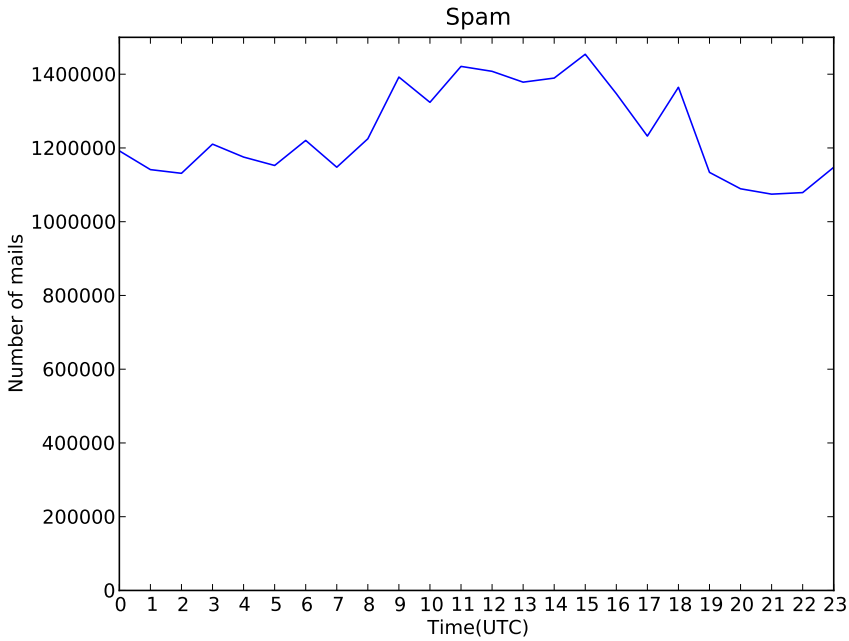


図 5.6: スパムメールの 1 時間ごとのメール送信数

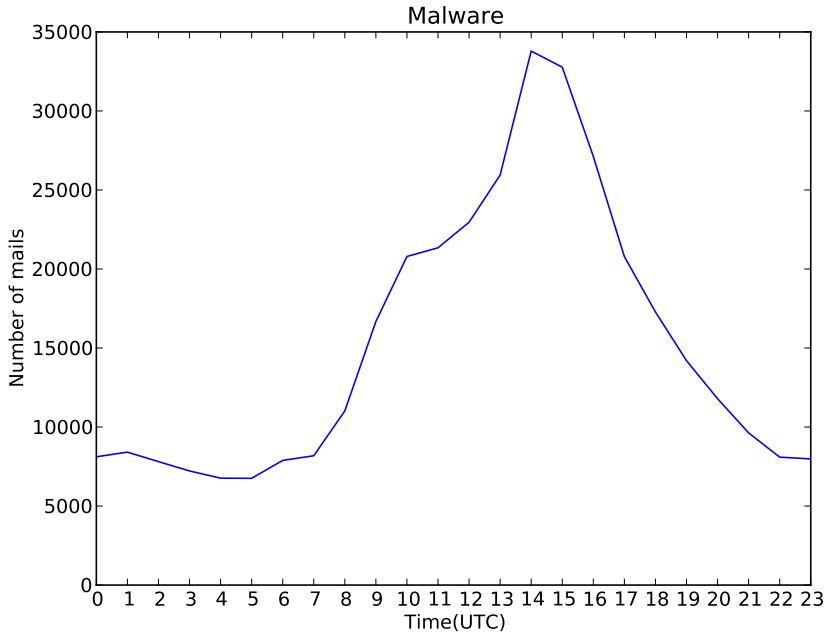


図 5.7: マルウェア付スパムメールの 1 時間ごとのメール送信数

第 6 章

考察

6.1　マルウェアスパムメールの分析結果

マルウェアスパムメールの分析結果について考察する．送信されるマルウェアは，Zip ファイルが主に使われていることがわかった．これは，添付ファイルがマルウェアとして検出されるのを防ぐためと考えられる．メールサービスやメールサーバでは，添付ファイルがマルウェアであるかを検出するためのスキャンを行うことがある．しかし Zip ファイルの場合，実行ファイルなどと比べてスキャンされる可能性が低い [9]．そのため，Zip ファイルがマルウェアとして多く使われていると考えられる．Zip ファイルは観測期間を通じて多くのマルウェアスパムメールが送信されており，マルウェアスパムメールで送信されるファイルの主流になっていることがわかる．また，PDF が一時期のみ多く用いられたり，2014 年 12 月から拡張子が.doc のファイルが急増しているなど，スパムメールを用いたマルウェア感染の手法には流行が見られることが判明した．

6.2　スパムメールとマルウェアスパムメールの比較結果

スパムメールとマルウェアスパムメールを比較した結果について考察する．

スパムメールとマルウェアスパムメールの送信先アドレスのドメインには異なる傾向が見られた．また，マルウェアスパムメールの送信先アドレスはスパムメールと比較して，特定のアドレスに集中していることがわかった．一般的に，スパムメール送信者であるスパマーは，メールアドレスのリスト使用し，そのリストのアドレスを標的にスパムメールを送信する [10]．この結果から，スパムメール送信に使われるメールアドレスのリストと，マルウェアスパム

メール送信に使用されるアドレスのリストが異なると考えられる．また，メールの送信時間でも，マルウェアスパムメールは特定の時間に集中して送信されるなどの差が見られた．これらの原因として，以下のような理由が考えられる．

- メール送信に用いるアドレスのリストや，メール送信の挙動をスパムメールとマルウェアスパムメールで変えている
- スパムメールを送信するスパマーと，マルウェアメールを送信するスパマーが異なる

また，送信先アドレスのドメインでは，スパムメールは TLD が.jp のアドレスが最もメール数が多かったのに対し，マルウェアスパムメールでは.com のアドレスが最も多かった．ここから，マルウェアスパムメールは，企業のメールアドレスを標的に送信される場合が多いと考えられる．以上のことから，マルウェアスパムメールは，一般的なスパムメールとは異なる送信傾向を持つメールだと考えられる．

第 7 章

結論

7.1 まとめ

本研究では，スパムトラップを用いてスパムメールを収集し，マルウェア感染を目的としたスパムメールの特徴を分析した．

マルウェアスパムメールでは，主に Zip 圧縮ファイルが用いられることがわかった．しかしそれ以外の実行ファイルや Word ファイルなどが用いられる場合もあり，使用されるファイルに流行があることがわかった．また，マルウェアスパムメールの標的になりやすいドメインはスパムメールとは異なること，マルウェアスパムメールは特定のアドレスに集中して送信される傾向がある事がわかった．

分析の結果，マルウェアスパムメールはスパムメールとは異なる送信傾向を持っており，標的となりやすいドメインなどに特徴があることが判明した．

7.2 今後の課題

本研究の今後の課題を示す．

7.2.1 分析内容の追加

本研究では，添付ファイルの拡張子ごとの時系列変化や，マルウェア種別に基づいてマルウェアスパムメールの分析を行った．またスパムメールとマルウェアスパムメールとの比較では，メールの送信先アドレス，メールの送信時間といった情報に関して比較を行い，分析を行った．

これらの情報に加えて，メールヘッダに付加された情報や，メール送信に使用されたマシンの IP アドレスなど，さらなる情報を分析対象とすることが今後の課題としてあげられる．

7.2.2　Web 経由のマルウェア配布への対応

本実験では，マルウェアが添付ファイルとして付加されたスパムメールを対象に実験を行った．しかしスパムメールの中には，メール内に記載されたリンクに誘導し，Web 経由でマルウェアを配布するスパムメールも存在する．このような添付ファイル以外でマルウェア感染を引き起こすスパムメールを分析対象とすることが課題としてあげられる．

謝辞

本修士論文を作成するにあたり，日頃よりご指導いただいた早稲田大学基幹理工学研究科の後藤滋樹教授に深く感謝いたします．また，本研究においてご協力とご指導をいただいた早稲田大学基幹理工学研究科の森達哉准教授，NTT コミュニケーションズの畑田充弘氏に深く感謝いたします．最後に，多大なご協力をいただいた後藤研究室の皆様に重ねて感謝いたします．

参考文献

[1] “スパムメールとは,” Kaspersky Labs Japan, Nov 2013. http://www.symantec.com/content/en/us/enterprise/other_resources/intelligence-report-06-2015.en-us.pdfl

[2] “SYMANTEC INTELLIGENCE REPORT JUNE 2015,” Symantec, Jun 2015. http://www.viruslistjp.com/spam/153350526.html

[3] 志村正樹, 畑田充弘, 森達哉, 後藤滋樹, “スパムトラップを用いたマルウェア添付スパムメールの分析,” コンピュータセキュリティシンポジウム 2015 論文集, 2015(3), pp.1243–1250 (2015-10-14).

[4] VirusTotal.
https://www.virustotal.com/ja/

[5] “MYDOOM,” Trend Micro,
http://about-threats.trendmicro.com/Malware.aspx?language=jp&name=MYDOOM

[6] “「UPATRE」による攻撃とは,” Trend Micro,
http://about-threats.trendmicro.com/RelatedThreats.aspx?language=jp&name=Keeping+Up+with+the+Damage+of+UPATRE

[7] “ボットネット「Zeus」、「ZBOT」ファミリ、ボットネット「Kneber」の関係とは,” Trend Micro,
http://about-threats.trendmicro.com/RelatedThreats.aspx?language=jp&name=The+ZeuS\%2C+ZBOT\%2C+and+Kneber+Connection

[8] “Before you enable those macros···,” Microsoft Malware Protection Center,
http://blogs.technet.com/b/mmpc/archive/2015/01/02/before-you-enable-those-macros.aspx

[9] “Right-to-Left Override ’ Aids Email Attacks,” KrebsonSecurity http://krebsonsecurity.com/2011/09/right-to-left-override-aids-email-attacks/

[10] Gianluca Stringhini, Oliver Hohlfeld, Christopher Kruegel, Giovanni Vigna. “The harvester, the botmaster, and the spammer: on the relations between the different actors in the spam landscape,” ASIACCS, 2014.

[11] David S. Anderson, Chris Fleizach, Stefan Savage, Geoffrey M Voelker “Spamscatter: Characterizing Internet Scam Hosting Infrastructure,” USENIX Security Symposium , Aug 2007.

[12] Mamount Alazab, Roderic Broadhurst “Spam and Criminal Activity,” Trends and Issues (Australian Institute of Criminology), Forthcoming., 2014. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2467423

[13] Christian Kreibich, Chris Kanich, Kirill Levchenko, Brandon Enright, Geoffrey M Volker, Vern Paxson, Stefan Savege “Spamcraft: An Inside Look At Spam Campaig Orchestration,” 2nd USENIX conference on Large-scale exploits and emergent threats: botnets, spyware, worms, and more, Aug 2009.