2015 年度神戸大学におけるウイルスメールの受信状況

ネットワーク基盤研究部門・CISO 補佐 鳩野逸生

1. はじめに

近年, アンチウイルスソフトウェアの検知率が低くなってきていることと [1], 感染拡大機能, 遠隔操作, 自動更新機能などコンピュータウイルスが高度化していることにより, 様々な悪事のツールとして用いられるようになってきている. 一旦コンピュータウイルスに感染すると, アンチウイルスソフトで検知されないので長期間感染に気が付かない, 遠隔操作機能により様々な犯罪に利用される, 情報漏えいを引き起こす, などコンピュータウイルス感染によるリスクはますます高くなってきていると言える [2].

本稿では, 神戸大学におけるウイルス付メール対策と 2015 年度に神戸大学に送られるコンピュータウイルス付メールの状況について述べる.

2. 神戸大学におけるウイルス付メール対策

神戸大学に対しても, 従来より, 多くのコンピュータウイルス付メールが送られてきている. 現在, 情報基盤センターのサービスとして運用しているメールの配送は, すべてウイルス/迷惑メールスキャナー (McAfee 社製) を経由するように設定されている. 本装置は, (1) ウイルスメールの検知・除去, (2) SPAM メールの検知除去, などの機能を持っている. 本装置におけるメールの処理状況を Fig. 1, Fig. 2, および Fig. 3 に示す. Fig. 1, Fig. 2, および Fig. 3 は, それぞれ, 正常配信も含めた処理状況, ウイルスおよびスパム等も含めた検知状況, およびウイルスメールの検知状況を示している. Fig. 3 からもわかるように 2015 年度末にかけて検知したウイルス付メールが急増していることが分かる.

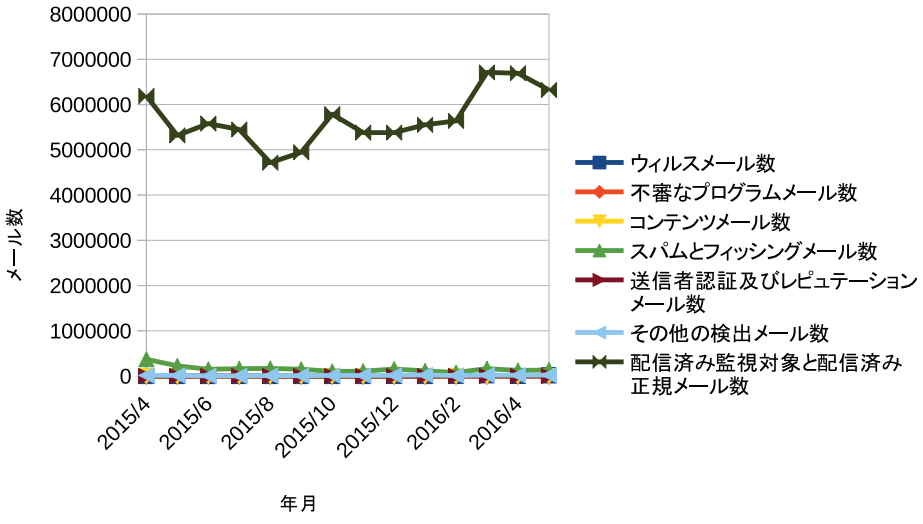

Fig.1: ウイルス/迷惑メールスキャナの全処理状況

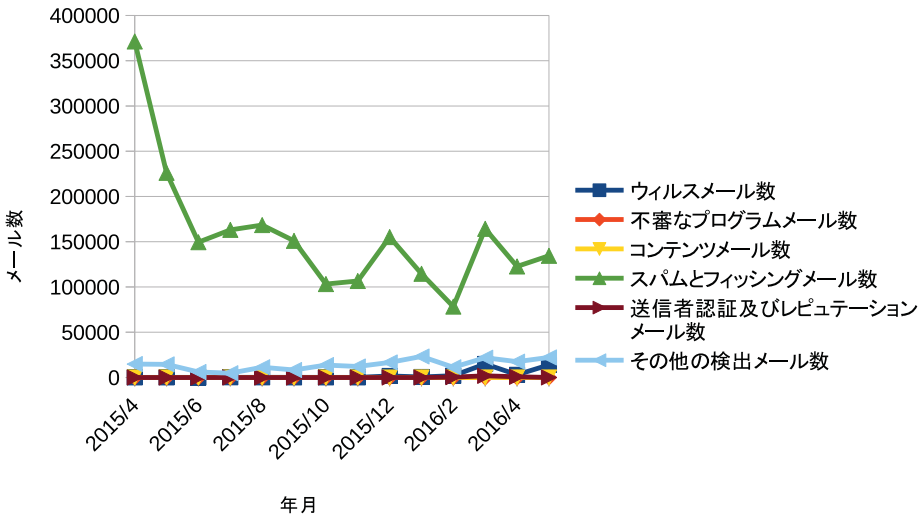

Fig.2: ウイルス/迷惑メールの検知状況

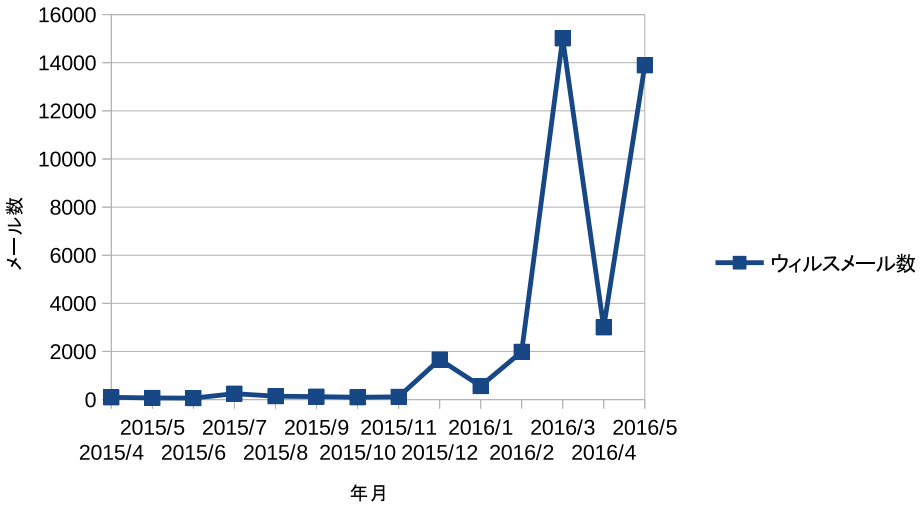

Fig.3: ウイルスメールの検知状況

3. 非検知ウイルス付メールの状況推定

一方で，ウイルス/迷惑メールスキャナーで検知されず，正常メールとして配送されるメールの中に，ウイルスであることが推測されるファイルが添付されていることも多いことが判明している．そのようなメールに添付されているファイルのほとんどは，Windows 実行形式ファイルが zip 圧縮されたファイルであり，ファイル名を，pdf ファイル，ワープロ，表計算，イメージなどと誤解することを狙ったファイル名がつけられている．ファイル名の例を以下に示す．

pdf, ワープロファイルを騙った添付ファイル名の例

```
Doc.scan(1).doc-20.01.2016,PDF.zip
05042016_#751628.doc.zip
jpeg.zip
IMG_&#65288;30561976232&#65289;.JPG.zip
```

本文は，”**iPhone から送信 2016/06/02**”, “**お疲れ様です．自己請求文書を添付し送ります．よろしくお願いします．**” など短いもので添付ファイルを開かせようとするような表現が使われている．一方で，メールリーダによっては

```
iPhone&#12363;&#12425;&#36865;&#20449; 2016/06/02
&#12362;&#30130;&#12428;&#27096;&#12391;&#12377;...
```

のように文字化けして見えることも多い．

ウイルス/迷惑メールスキャナーは，正常，検知にかかわらずすべての通過メール対して処理記録を出力している．本稿では，その記録をもとに，以下のような特徴を持つメールをウイルス付きメールと推定して集計する．本経験則は，著者が受信したウイルス付メールの特徴に基づいている．

ウイルス付メールの特徴

- zip 圧縮のファイルが 1 つ添付ファイルされている．
- 携帯電話メールドメイン，あるいは有名 ISP で利用できるメールアドレスから送付されている．
- 送付元 IP から判定したドメインと送付元メールドメインが一致しない．

この他，ac.jp, go.jp, gr.jp および神戸大学内を発信元とするものを除いたものをウイルス付きメールとして集計した[1]. 2015 年度の集計を Fig. 4 に示す．ただし，上記特徴をもつメールの中には明らかに正常と思うわれるものもごく少数混入していることは判明しているが，配送記録だけからでは正確にウイルス付きメールかそうでないかを判定することは困難であるため，明らかに正常と思われるものも除かずに集計している．

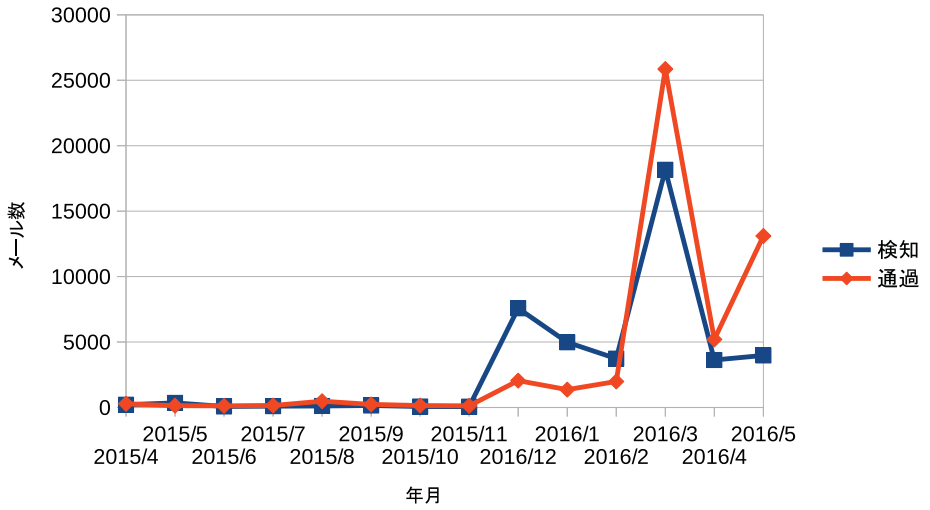

Fig.4: ウイルスメールの推定通過数

Fig. 4 からも分かるように 2015 年末からウイルスメール自体が急増し，特に 2016 年 3 月に多かったことがわかるとともに，相当数のウイルスメールが検知されずに通過していることが推定できる．

[1] ログの予備調査による経験則.

4. おわりに

コンピュータウイルスが非常に多様化して検知自体が困難になっている現在，アンチウイルスソフトの検知率が大きく改善することは考えにくい状況である．このような状況の元では，**添付ファイルは安易に開かない，**という対策を徹底するしかないと思われる．添付ファイルを開く前には，まず，送信元の確認 (思い当たるアドレスであるか), 添付ファイルの中身がなんであるかの確認を慎重に行うしかないと思われる．業務の都合上不特定からのメールを取り扱う必要がある部署は，Windows を利用せず，Mac や Android などの端末を利用することを検討してもよいと思われる．ただし，Mac や Andoroid が絶対的に安全な訳ではないことと状況が変化する可能性には注意が必要である．

また，不幸にしてコンピュータウイルスに感染してしまった場合，アンチウイルスソフトによる除去では多くの場合不完全な除去しかできていない可能性が高い．データをバックアップした上で再インストールすることを強くお勧めする．不完全な状態で放置すると，将来情報漏えいなどが起こる可能性もあり，非常に危険である．

情報基盤センターでは，学内でウイルスに感染した疑いがある PC を通信記録から推定する技術開発を進めている [3].

参考文献

[1] Samuel Gibbs, “Antivirus software is dead, says security expert at Symantec,” *The Guardian*, `http://www.theguardian.com/technology/2014/may/06/antivirus-software-fails-catch-attacks-security-expert-symantec` (2014)

[2] 情報処理推進機構, “情報セキュリティ白書 2015,” 情報処理推進機構 (2015)

[3] 鳩野: HTTP 通信ログ解析を用いた
不正プログラム感染 PC 検知の試み, 2015 年度情報処理学会 IOT シンポジウム講演論文集, 2015.