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。

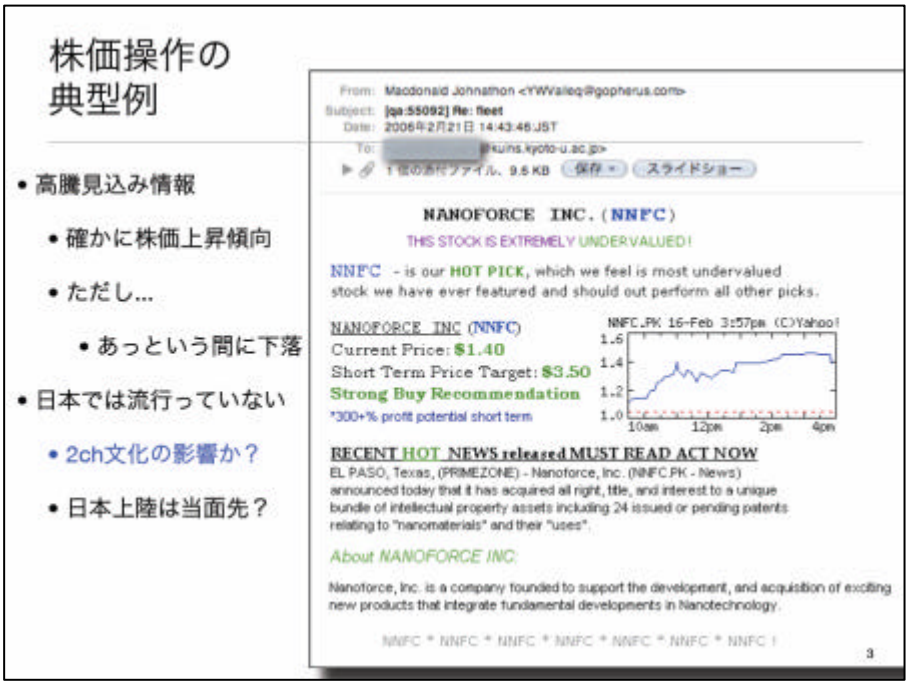
一方、受信者は、膨大な spam メールの中から、必要なメールのみを選別する作業に相当の時間を費やさざるを得ない。この作業を目視で行うと、本来読むべきメールまでも破棄してしまう事故が多発することとなる。

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)。



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を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 Phising 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)。

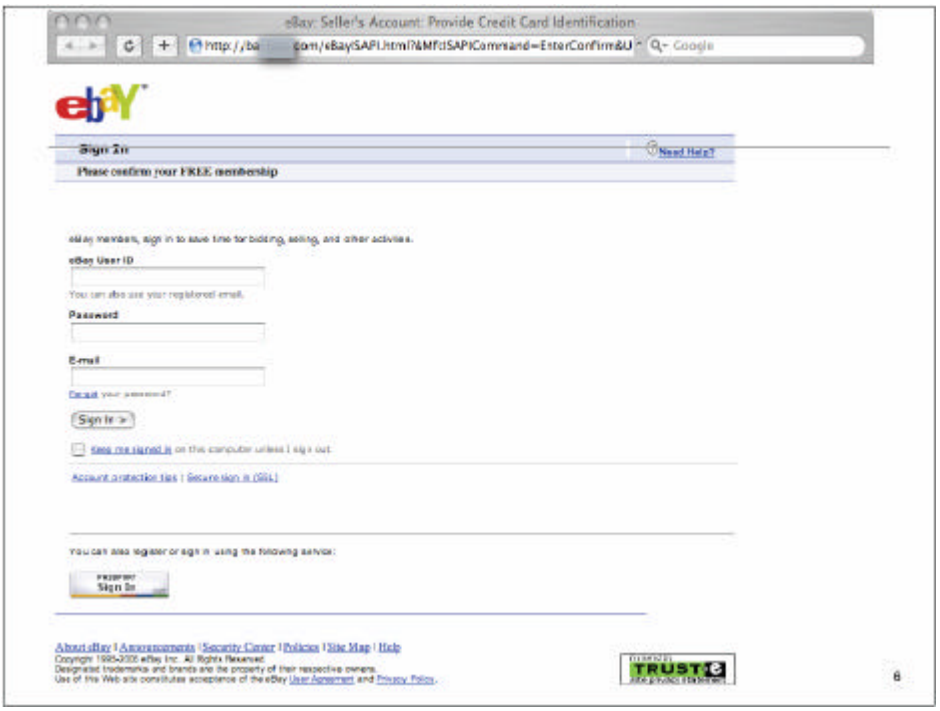
講演資料 4

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。

Phising 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。

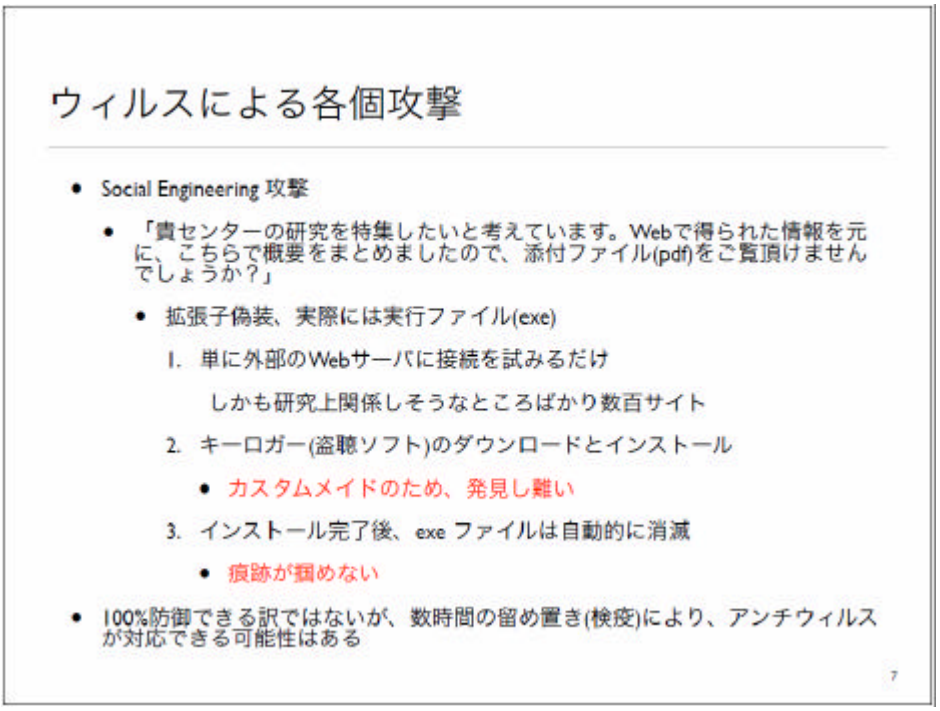
講演資料 5



講演資料 6

4.ウィルスによる個人情報取得

Social Engineering[1] 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。



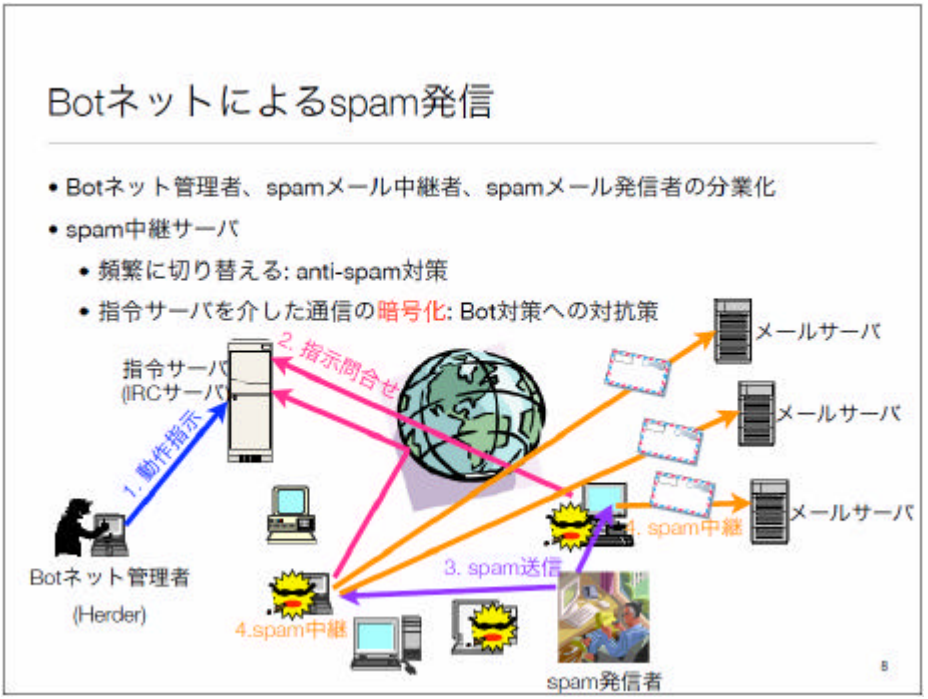
講演資料 7

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。

[1] 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。

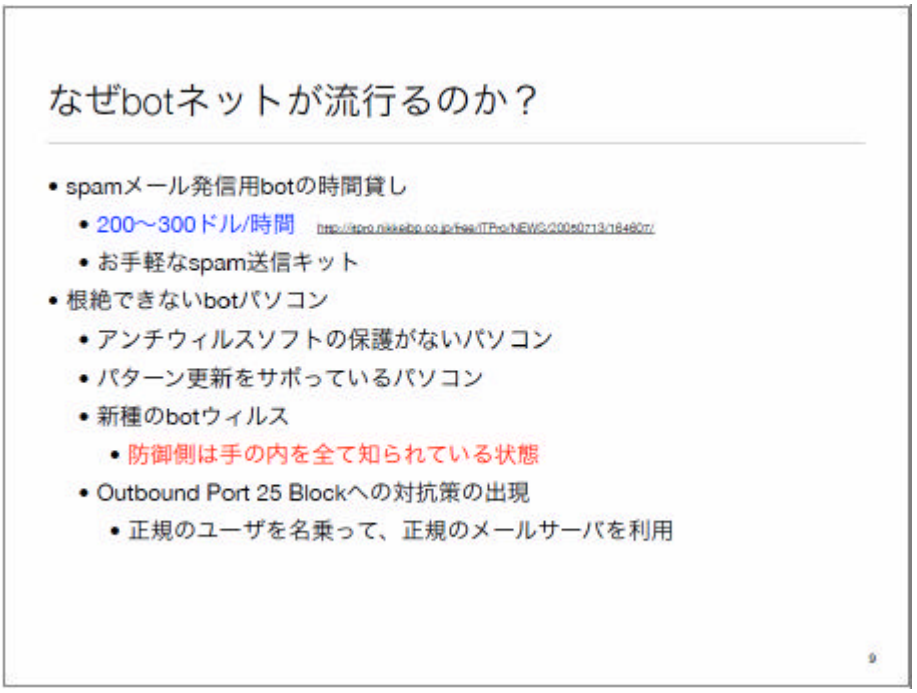
5.bot ネットを利用した spam 発信

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[2])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。



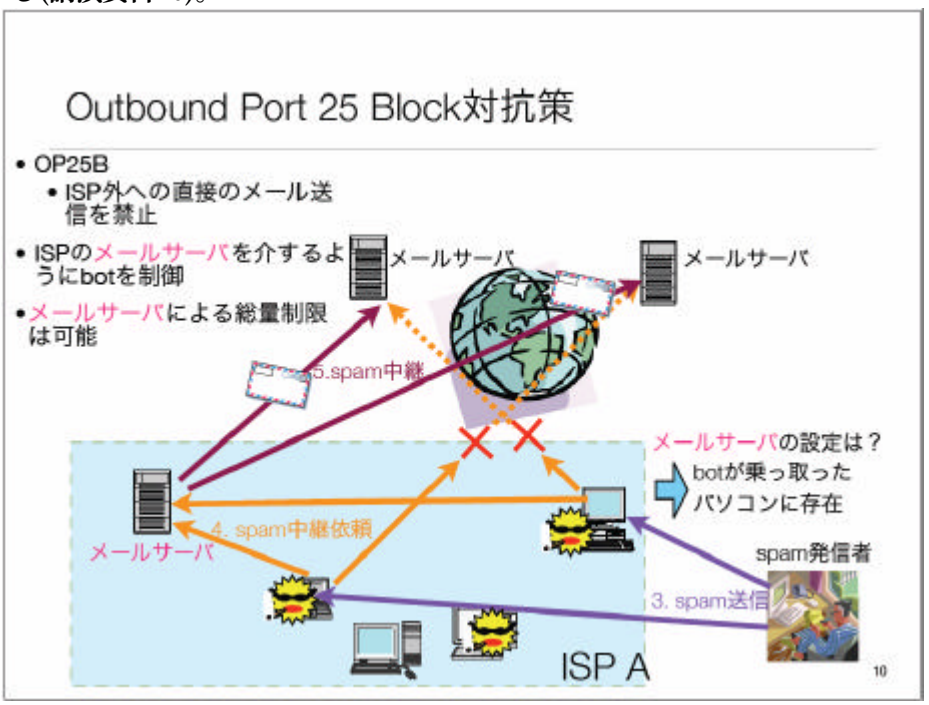
講演資料 9

bot 感染が根絶できない理由はいくつかある。従来は、アンチウィ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

[2] malware : 一般に不正プログラム全般を指す。

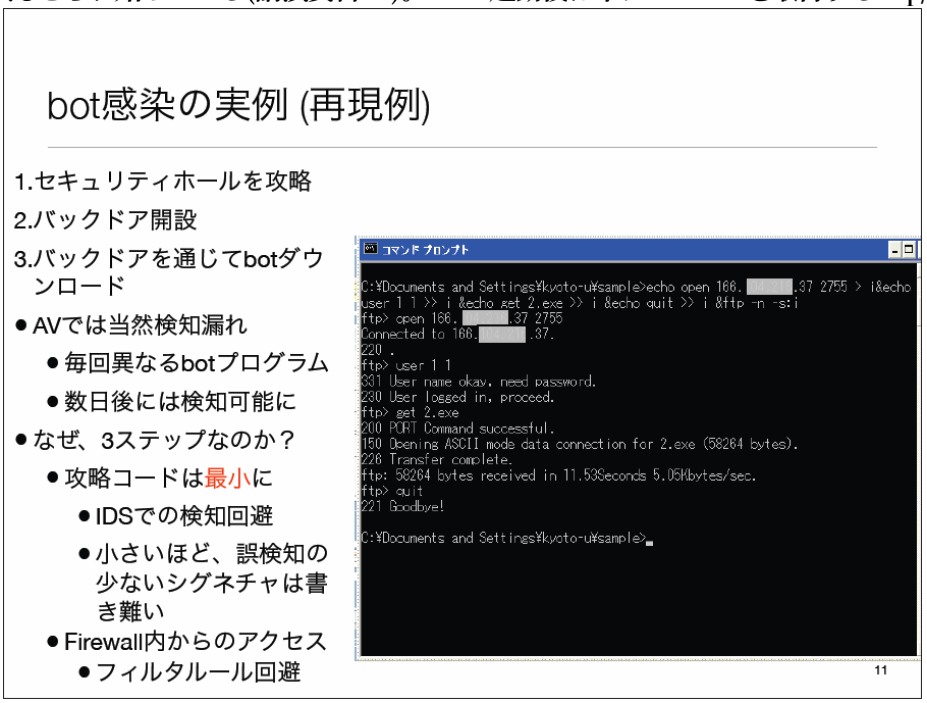
の感染が多かった。しかし、最近では、未知の bot の感染事例が増えている。一般的な防御策は、攻撃者側でも検証可能であり、これを回避する細工を講じていると考えられる。

bot による spam メール対策として、多くの ISP[3]等において、Outbound Port 25Blocking (OP25B)[4]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)。



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 等の脆弱性をついて 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[5]コマンドを実行する。



講演資料 11

[3] ISP : Internet Services Provider

[4] 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

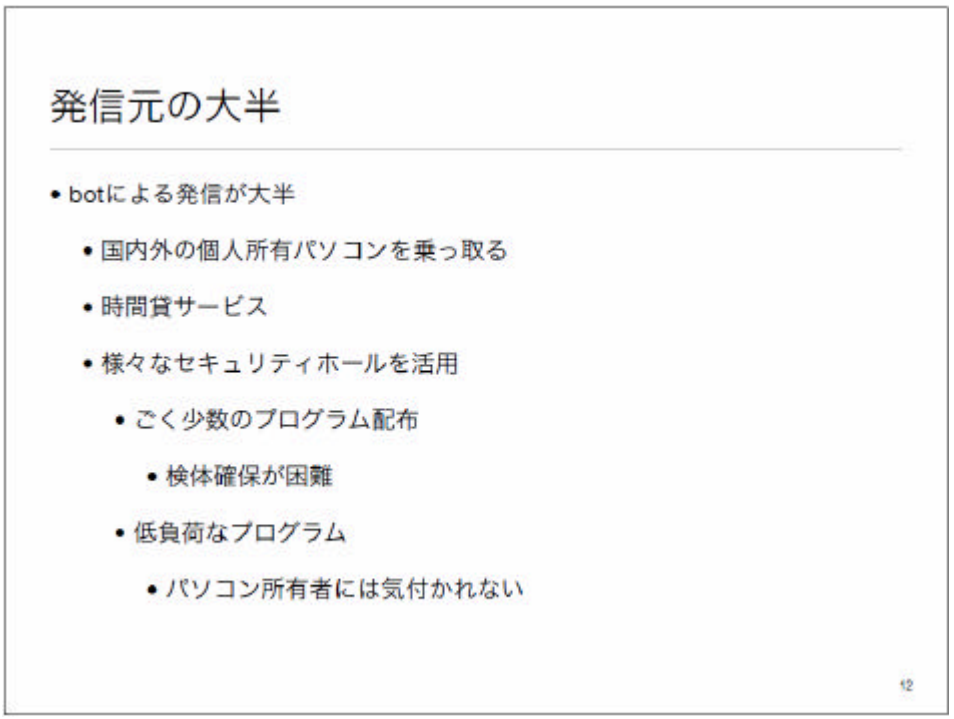
[5] tftp : Trivial File Transfer Protocol , UDP(User Datagram Protocol)を用いてコンピュータ間でファイルを転送するためのプロトコル

感染を試みる malware の大半は、アンチウィ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[6])による検知回避を試みている。IDS では、signature[7]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、アンチウィルスの検知を回避しやすくなる(講演資料 12)。



講演資料 12

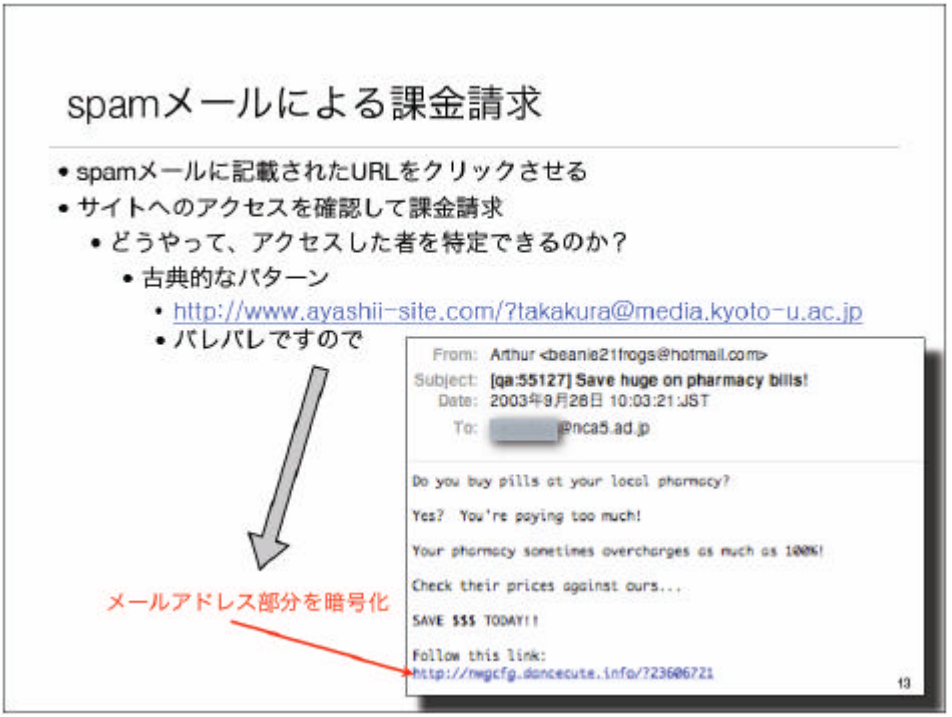
6 IDS : Intrusion Detection System

7 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[8] 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)。



講演資料 13

講演資料 14

[8] 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。

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[9]するのではなく、メール本体のハッシュ値[10]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)。

講演資料 16

[9] 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。

[10] 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 メールの文面を既知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。

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)。

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 発信業者側の苦労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[11]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。

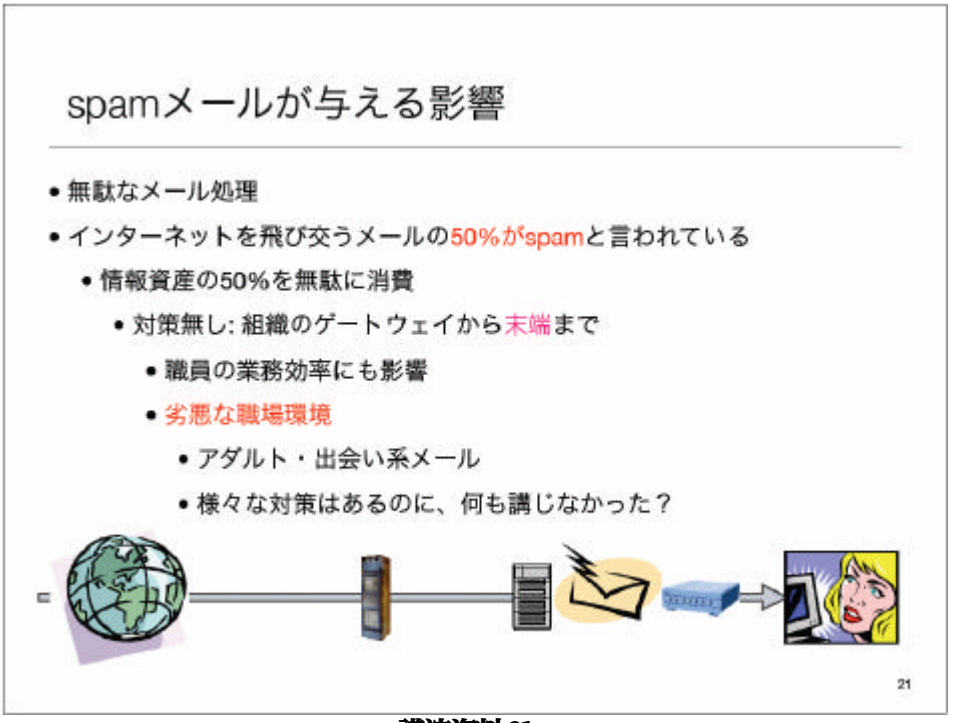
講演資料 20

[11] 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。

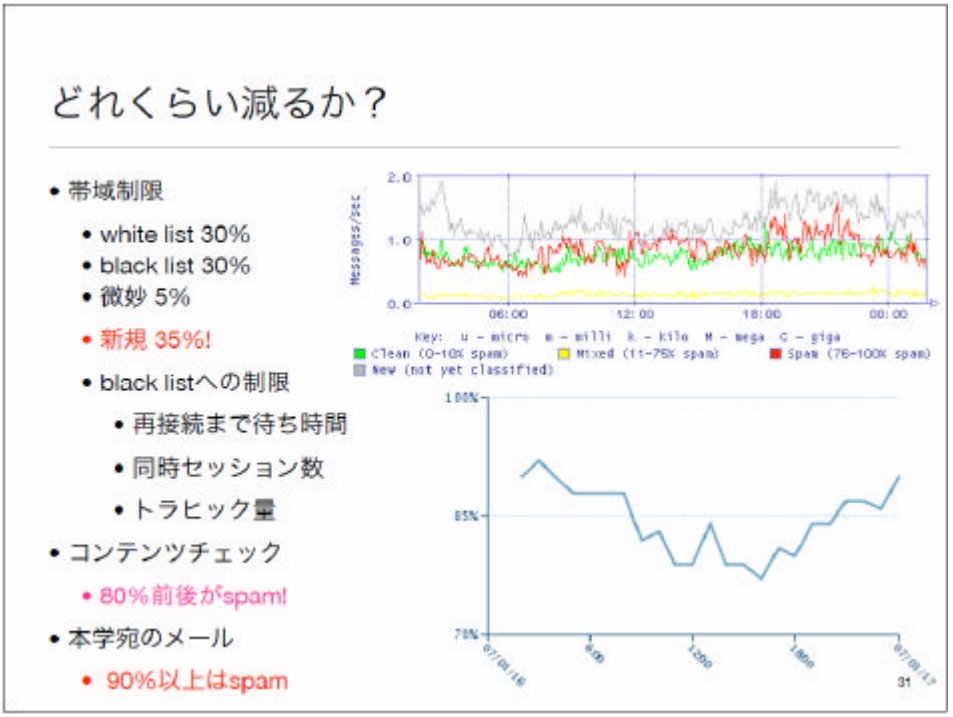
7. spam メールが及ぼす影響

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



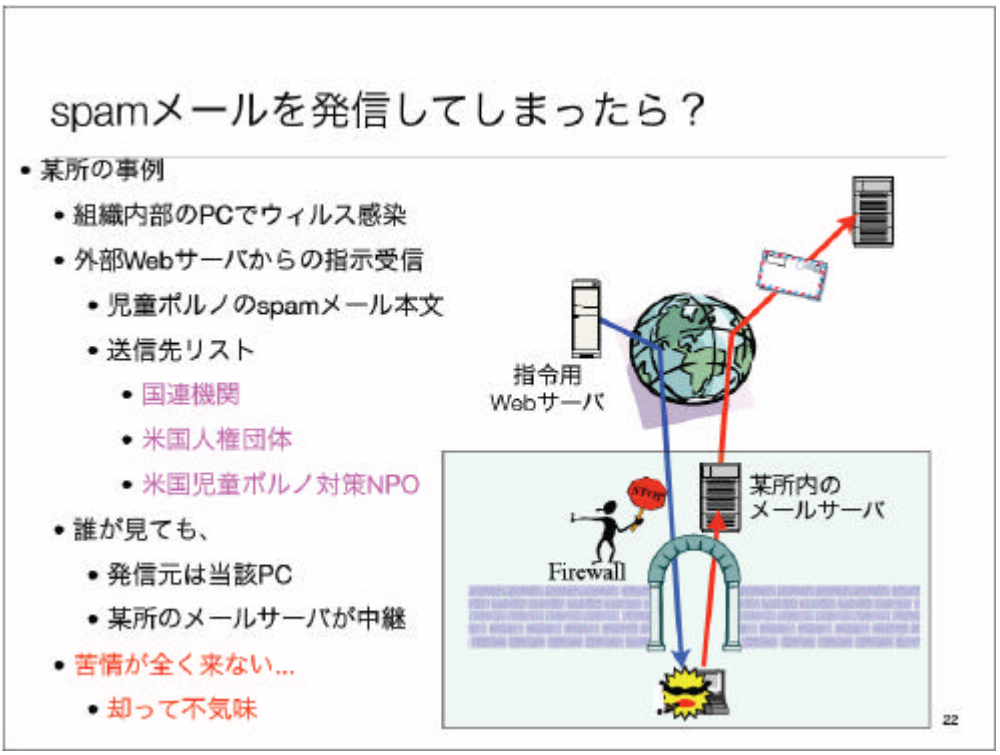
講演資料 21



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。

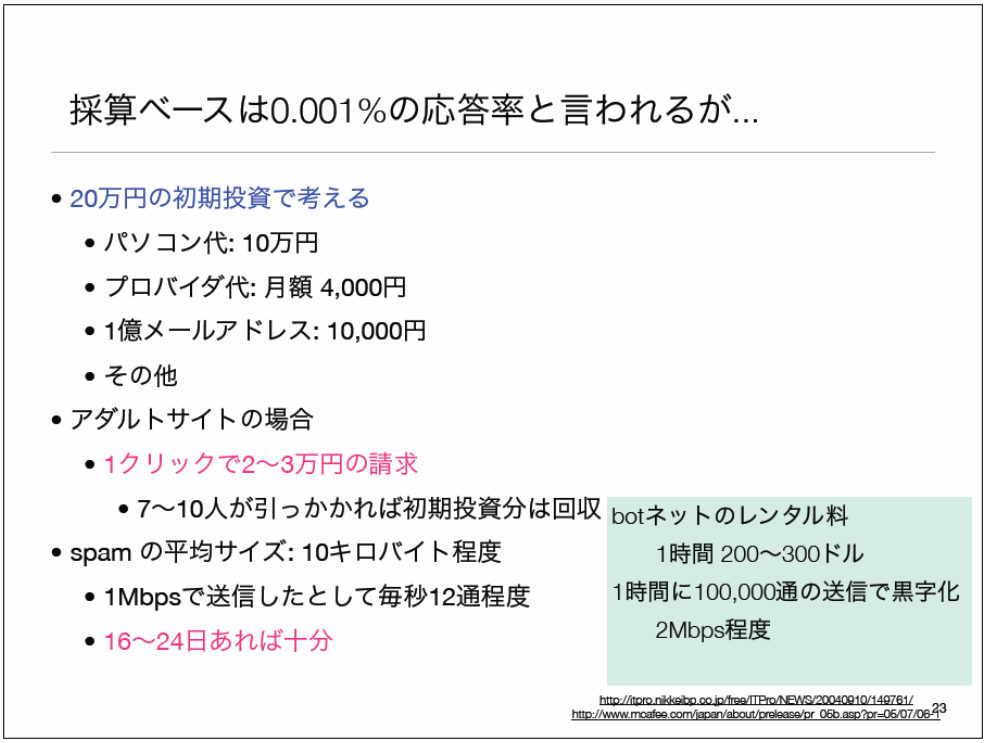
一方、spam メールを発信した場合について考える(講演資料 22)。例えば、組織内のパソコンがウィルスに感染し、外部 Web サーバからの指令で、当該組織のメールサーバを介して spam を発信することが想定される。この場合、当該組織の信用失墜になる危険性がある。



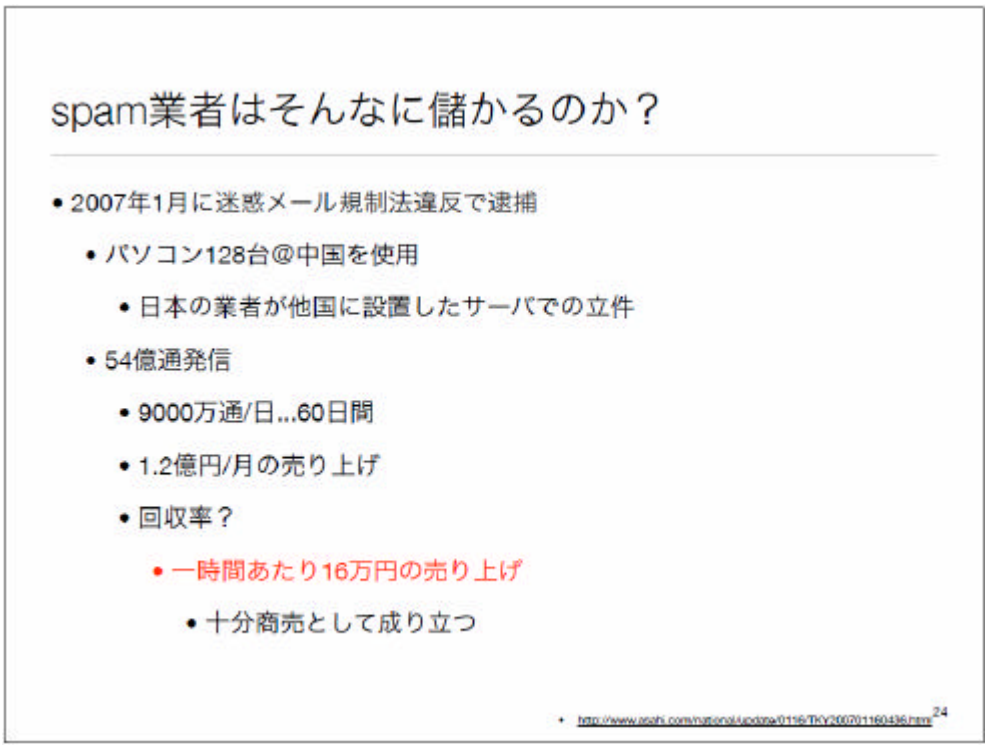
講演資料 22

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。



講演資料 23

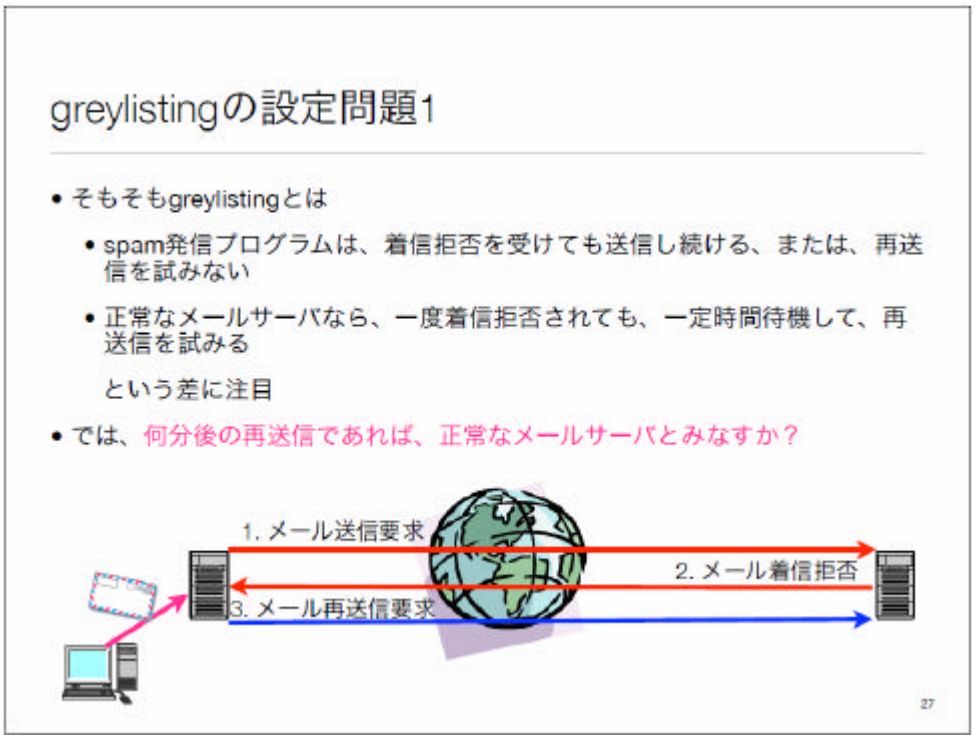


講演資料 24

9. 京都大学の対策

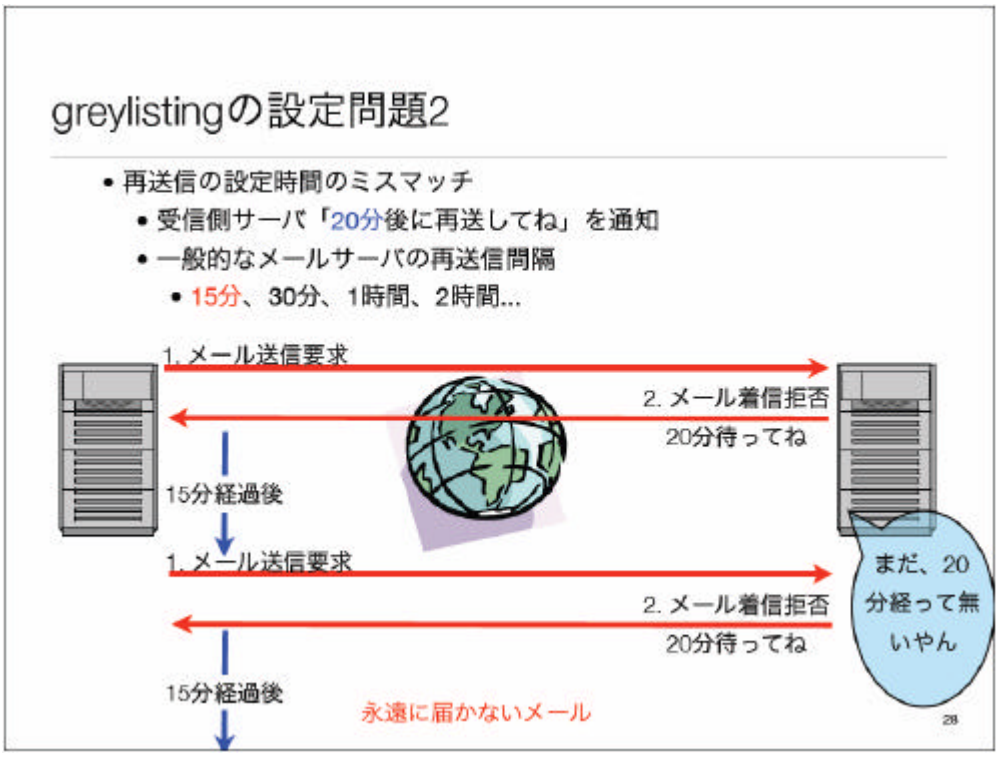
9.1 greylisting

当初は greylisting[12] (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。



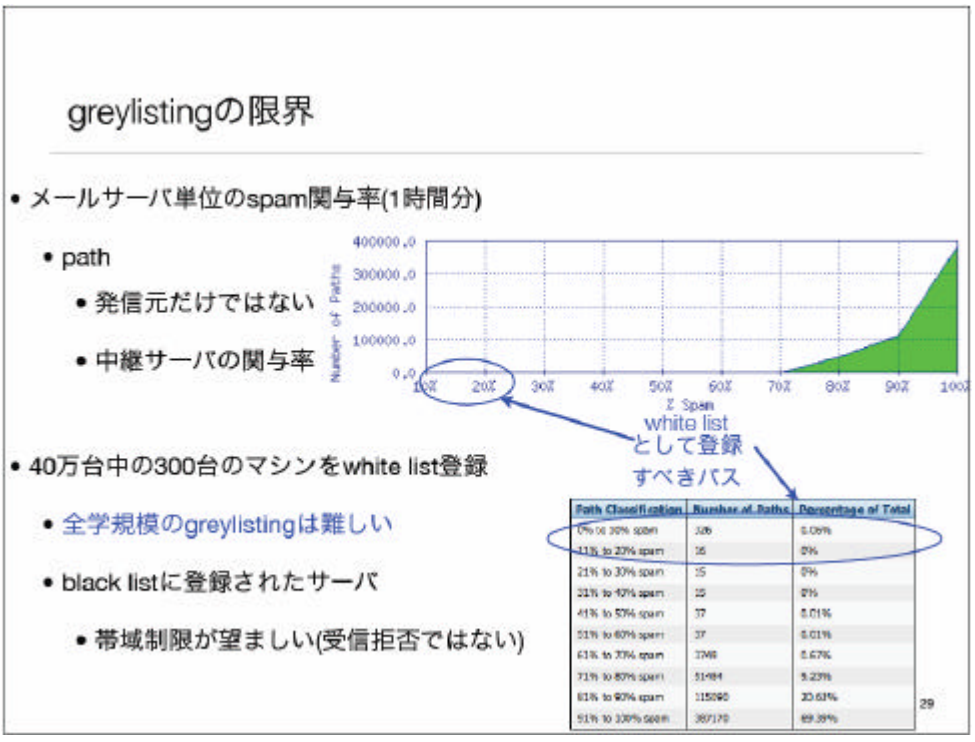
講演資料 27

[12] 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、エンベロープ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。



講演資料 28

また、greylisting では white list[13]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[14]を施す方が望ましいと考えた。



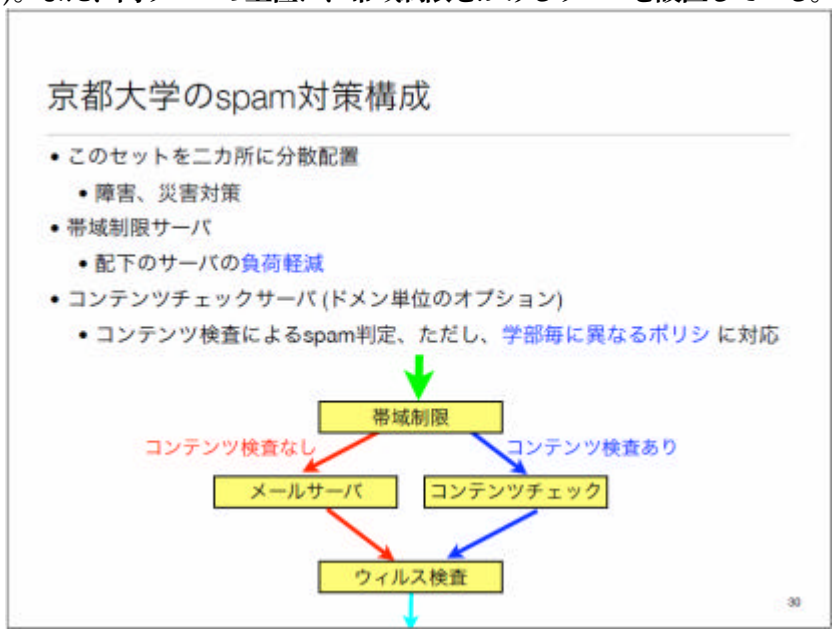
講演資料 29

13 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、配送遅延の原因となる。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。

14 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ことが狙い。

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。



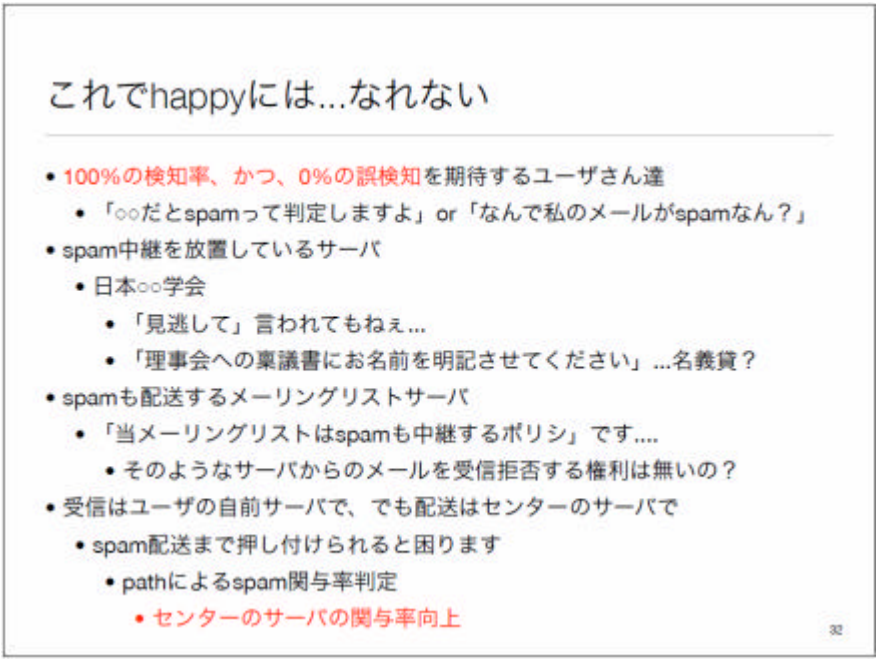
講演資料 30

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。



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/