ビジネスにおける電子メールの活用と最近の法制の関係その3
－メール活用時の問題解析－

Current Status of E-mail Usage in Business and Related Laws, Part 3 - Problem Analysis for Mail Usage

奥山　徹
Tohru Okuyama

前2回の報告[1,2]においてビジネスにおける電子メールの有効性と危険性について議論し、電子メールビジネスと関連する種々の法律について解説した。また、種々のビジネスシーンごとに、メールビジネスにおいて、陥りやすい問題点についても詳細に調べた。今回は、独自ドメインによるメールサービスを始めるための問題点やSPAMメールなどの発生メカニズムなどについて考え、実際の活用場面での問題点を掘り下げる。

1. はじめに

日本政府は2005年度のe-Japan2の終了を受け、次なる5ヵ年のためのu-Japan構想を打ち上げている。u-Japanは従来のe-Japanをさらに進めて、ユビキタス社会の到来を看過した、新しい社会像を模索するための集中施策と受け取ることが出来る。そして、ICタグを中心とした新しい情報通信デバイスがどのような役割を演じるかについて分析を行っている。また、一般消費者にとり、電子メールがいかに重要な役割を演じるかについて述べている。また、日本の電子メール利用の特殊性(利用者の半数が携帯電話からであるという事実)について述べ、日本が先進国に先駆けて、急激なユビキタス社会に変貌する可能性を示唆している。一方、ビジネスにおいても、電子メールはいまや普遍的なツールとして定着した感がある。それらの概要は、前々回の報告[1]および前回の報告[2]としてまとめた。文献[1]では2000年から2002年の少し古いデータであるが、電子メール利用の現状についても分析している。また、文献[2]では、ビジネスシーン別の問題点を指摘し、その回避策について議論した。今回は、電子メールの更なる活用を目指して、ビジネスにおける独自ドメイン名の運用の意義とSPAMメールなどの迷惑メール対策について議論する。主な内容は次の通りである。

(1) **独自ドメインの意義と運用**:ビジネス戦略の一つとして、独自ドメイン名を取得することの意義についても述べる。

(2) **SPAMメールの発生メカニズム**:SPAMメールとは、世に言う「迷惑メール」のことである。いまや、迷惑メールは電子メールユーザにとって非常に厄介にものとなっている。このような迷惑メールが発生するメカニズムについて述べ、SPAMフィルタなどによる対抗策について概観する。

2. 最近の電子メール利用の動向

はじめに、総務省の情報通信白書[3]からいくつかの統計情報を引用して、電子メールの利用の動向について述べる。その前に、日本におけるインターネットの利用人口と普及率を図1に示す。この図に示すように、利用人口は平成15年において、既に8,000万人に迫っており、現状では既に越えていると思われる。これは、人口普及率に直すと 60%に達し、既に日本国民の二人に一人以上が何らかの形でインターネットを利用していることになる。

また、インターネットを利用する目的について、2003年度（図2の中では「2年前」と記載）と2005年度を比較したデータがあるので紹介しておく。ただし、このデータは個人利用の場合のものであり、企業の利用者のデータについては異なった数値となることが予想される。しかしながら、このデータは個人消費者のインターネット上での利用動向を把握するためには重要なものである。

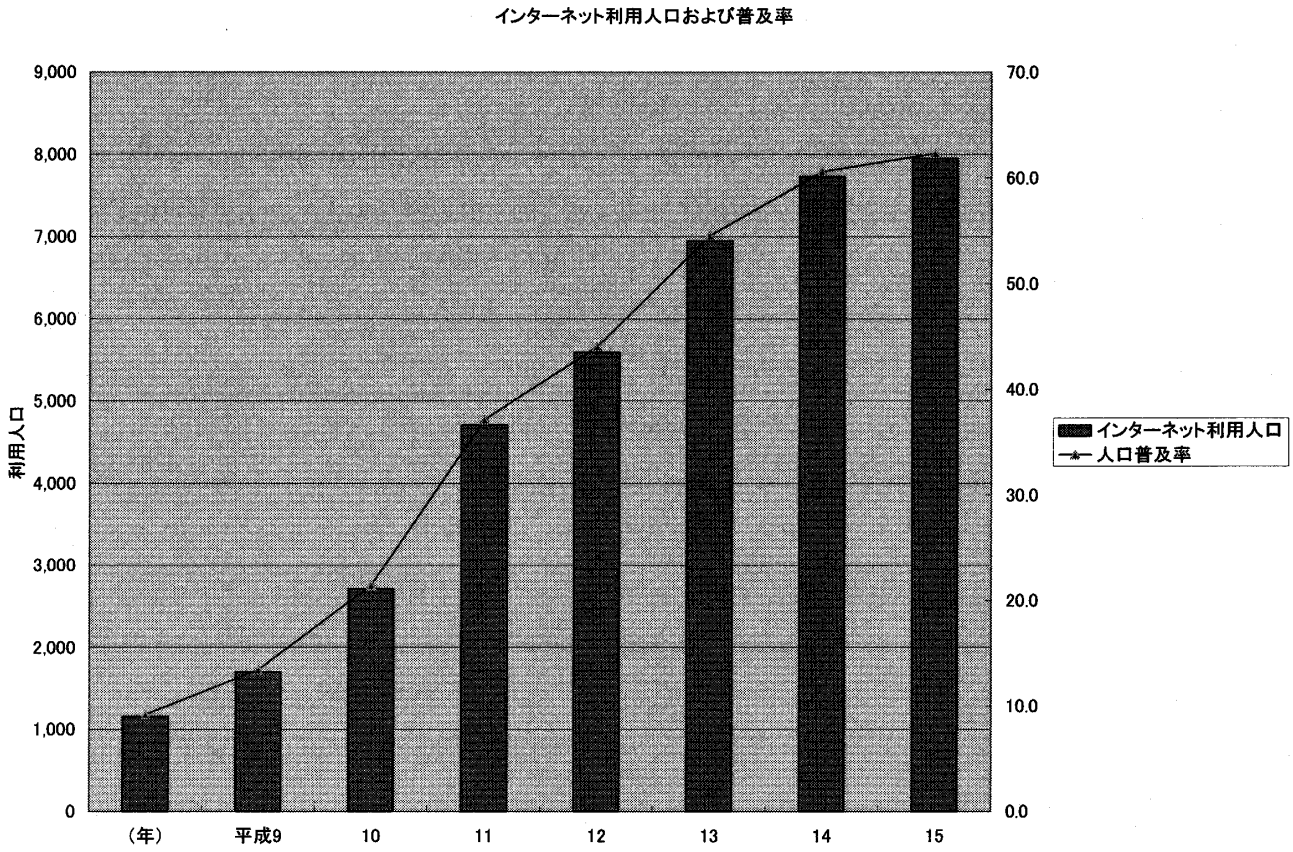

図1. インターネットの利用人口と人口普及率[3]

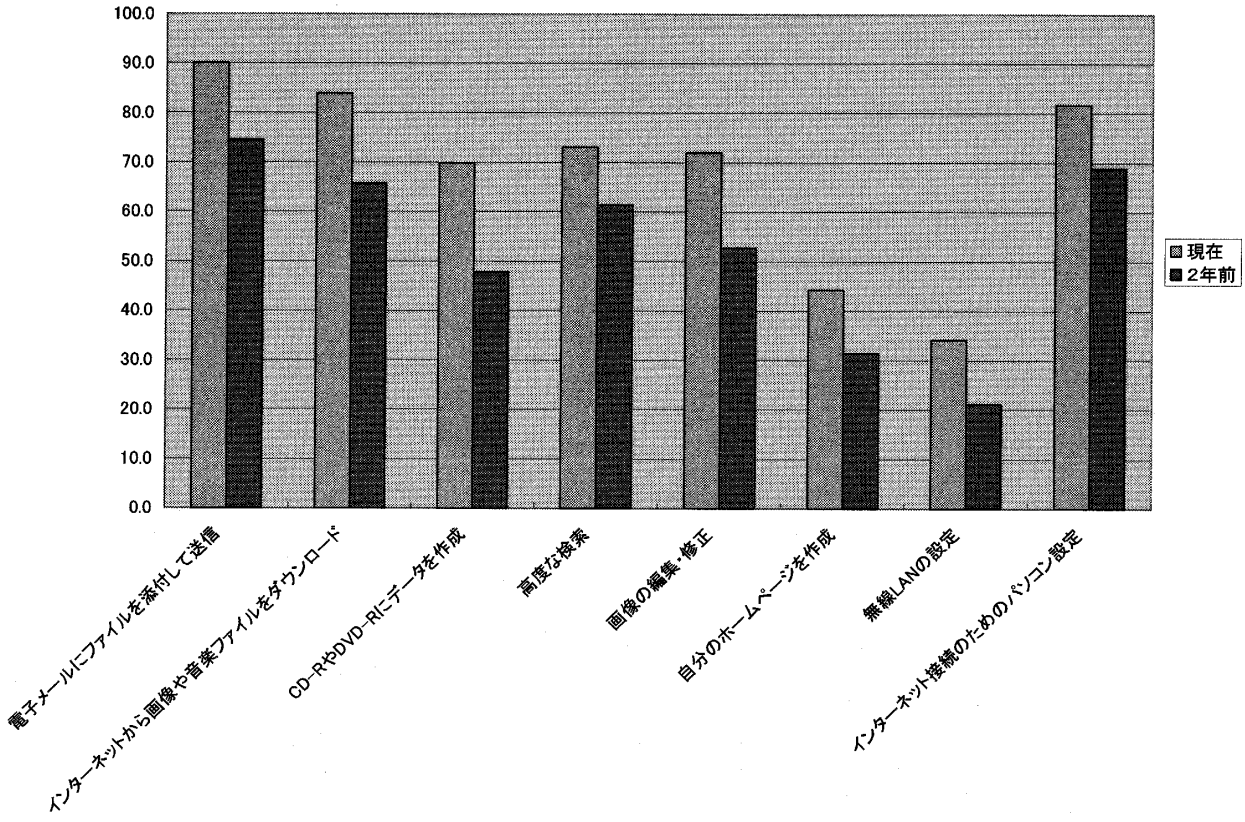

図2. 個人のインターネット利用目的の変化[3]

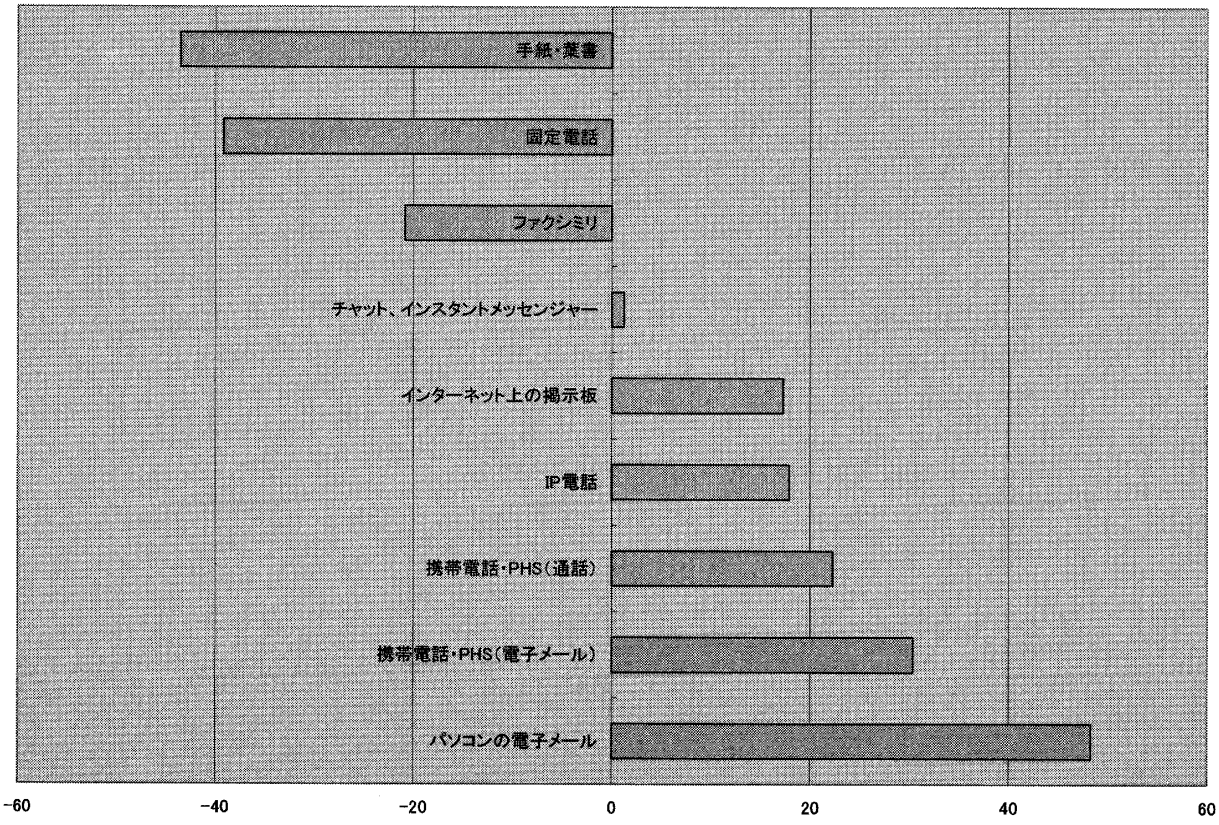

図3. 情報伝達媒体の変化[3]

図2に示すとおり、電子メールによるファイルの交換やダウンロードによるファイルの交換は 2003 年度よりも増加しており、情報伝達媒体として、電子メールが定着していることが伺える。さらに、図3に情報伝達媒体そのものの利用状況の変化を示す。図3に示すとおり、パソコンや携帯電話のメールというものが躍進し、逆に手紙や固定電話の利用が減少していることがわかる。また、電子メールの利用に関して、図4と図5の2つのデータを示しておく。

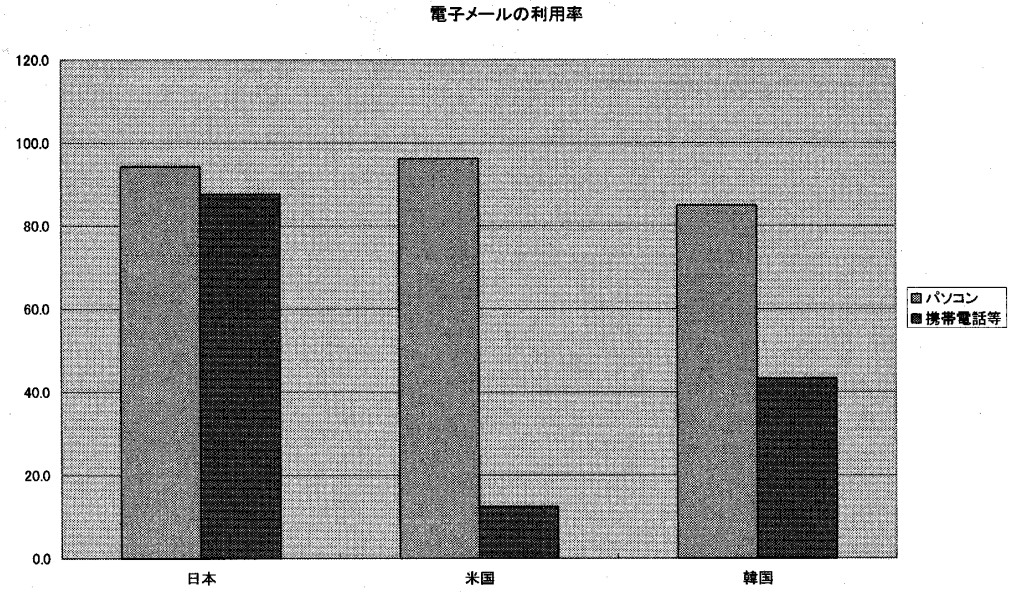

図4. 日米韓における電子メール利用におけるパソコンと携帯電話の割合[3]

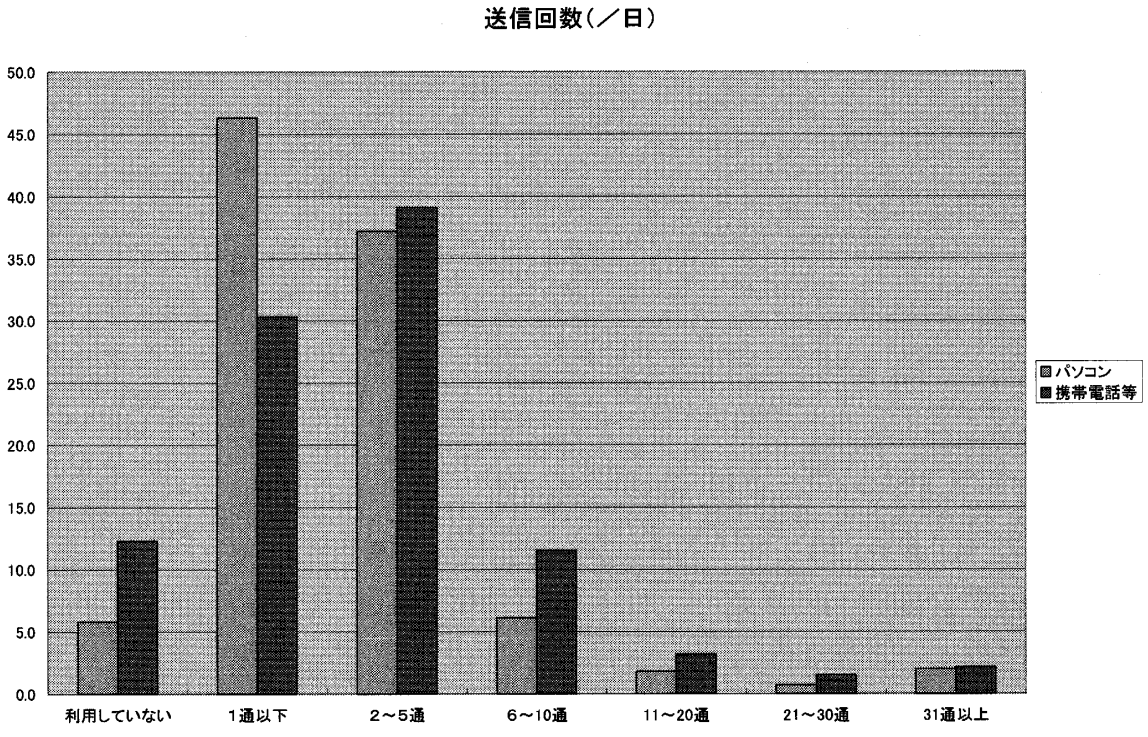

図5. パソコンと携帯電話のメール送信回数（日本の場合）[3]

図4は送信機器別の利用状況であり、日本はパソコンと携帯電話からの利用がほぼ拮抗しているという、世界的に見ても特異な様相を呈している。また、図5に示すとおり１日の送信回数は平均すると2通程度であるが、31 通以上送るユーザも多数存在する。すなわち、日本は、電子メールユーザの多くが携帯電話によるものであり、電子メールを用いたビジネスも、このような日本の特殊性を考慮する必要がある。

3. クライアントーサーバモデル

電子メール配送の概略は、既に前２回の報告[1,2]の中でも述べている。しかしながら、インターネット上のサービスモデルである、クライアントーサーバモデルを概観しておくことは、電子メールの問題点を議論する上では重要なので、ここに概要を示しておく。

図6はインターネットで使われているサービスの実装形態をモデル化したものである。このようなモデルは**クライアントーサーバモデル**と呼ばれている。個のモデルでは、サーバと呼ばれるサービスを行うコンピュータ（及びその上のソフトウェア群）とクライアントと呼ばれるサービスの提供を受けるコンピュータ（及びその上のソフトウェア群）が協調動作することで各種のサービスが実現されている。

- インターネット上にある**サーバ(Server)**は各種のサービスを行うためのコンピュータおよびその上で稼動しているサービスアプリケーションプログラムを指す。
- 一方、**クライアント(Client)**はサーバに対してサービスの**要求(Request)**を出し、サーバからの**返答(Response)**をユーザに返すためのアプリケーションプログラムあるいはそのアプリケーションプログラムが稼動しているコンピュータを指す。

クライアントは、一般的にサーバとの通信制御とユーザインターフェイスの両者を備えている。ここで、サーバとクライアントの間で利用される通信の約束事を**プロトコル(Protocol)**と呼んでいる。また、インターネット上でのサービスを識別するために整数値が使われる。例えば、WWW のサービスなら 80、電子メールなら 25 が使われる。このようなサービスを識別する整数値を**ポート番号(Port Number)**と呼ぶ。例えば、最近話題の W32/MSBlaster というウイルスは135という番号に初期アタックが来ることが知られている。例えば、Personal Firewall の設定で 135 へのアクセスを制限することで MSBlaster の感染を防ぐことができる。

WWW の場合サーバは、Apache[4]のようなWWW サーバプログラムの稼動しているコンピュータとなる。また、クライアントは IE のようなブラウザが稼動しているコンピュータとなる。

インターネット上での電子メールサービスを行うために必要なソフトウェアを考える。電子メールサービスも図7のクライアントーサーバモデルによりサービスされる。したがって、**メールサーバ**と**メールクライアント**が必要となる。図7は電子メールのサービスを行うために必要とされるプログラム群とコンピュータを示したである。図7の説明を行う前に、電子メールが必要としているアドレスについて考える。インターネットで利用される**メールアドレス(Mail Address)**は、次のような形式に統一されている。（実は他の書き方もあるが、それは時間があれば説明する。）

foo@bar.jp

ここで、foo とか bar とかいう書き方はインター

ネット関係者がよく使う単語で、代名詞の変わりである。foo@bar.jp の foo の部分がユーザ ID、また、bar.jp はドメイン名と呼ばれていて、電子メールサービスを行っているメールサーバの名前となる。

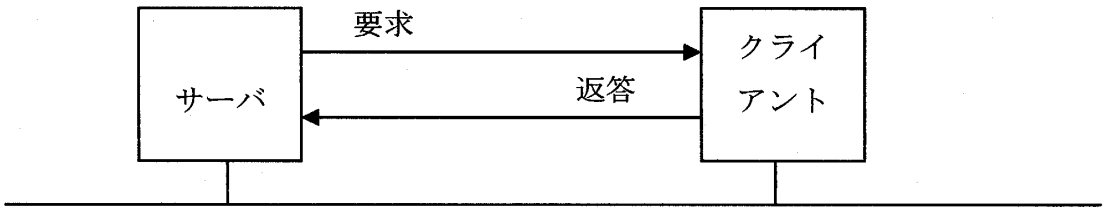

図6. クライアントーサーバモデル

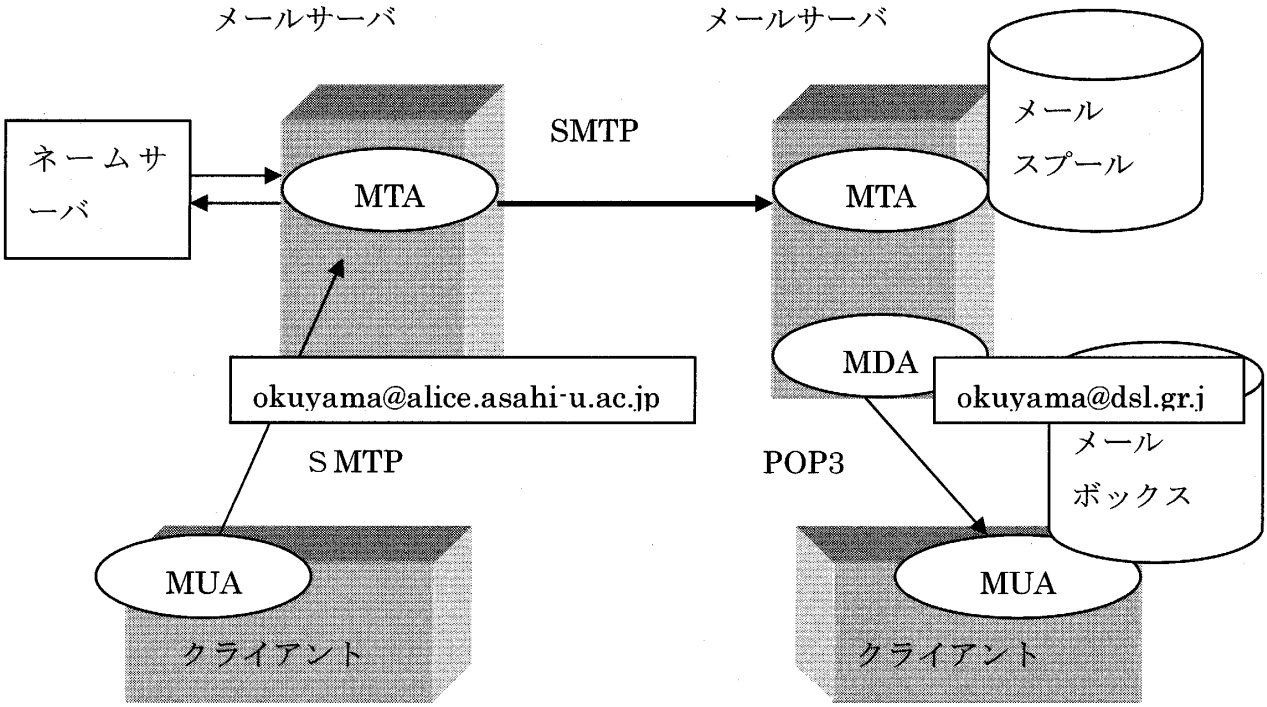

図7. インターネット上のメール配送の仕組み

実は、ドメイン名の部分はコンピュータの名前ではなく、所属しているネットワークの代表名となっている場合がある。例えば、筆者はプライベートな電子メールアドレスとして、

okuyama@dsl.gr.jp

を使っている（大学で使用しているアドレスはokuyama@alice.asahi-u.ac.jp である）。ここで、okuyamaがユーザIDでdsl.gr.jpがドメイン名となる。ただし、これは代表名で省略された書き方で、正確にはokuyama@nsv.dsl.gr.jpとなる。ドメイン名の話は、次の節で改めて述べる。

図中で使われている、MTA、MUA、MDAやプロトコルの解説及びそれらを使った詳細なメール配送の様子は文献[1]に詳しく記したので、ここでは省略する。

電子メールには必ず**メールヘッダ（Mail Header）**と呼ばれるものと**メールの本文（Mail Body）**が存在する。本文は、各ユーザが作成したメールそのものなので、特に問題は無いであろう。メールヘッダは、MTAやMUAがメールを転送する場合に必要とされる情報や各種の付加的な情報が記述されている。例えば、メールの宛て先（通常「To:」というフィールドが使わる）や差出人（「From:」というフィールドが使われる）、表題（「Subject:」）、あるいは日付（「Date:」）などある。ヘッダの情報はメール作成時にMUAが生成する。代表的なメールヘッダのフィールドの意味を表1に示す。

表1．代表的なメールヘッダのフィールドとその意味

フィールド名	意　味
From	MUA で設定された送り主のアドレス
To	メールの宛て先のアドレス
Cc	カーボンコピーの宛て先のアドレスのリスト
Bcc	ブラインドカーボンコピーの宛て先のアドレスのリスト
Subject	メールの表題
Date	メールの発信時刻
Sender	メールを発信した送り主のアドレス
Reply-To	メールに対する返事を送るべきアドレスのリスト
In-Reply-To	どのメールに対する返事かを示す識別子
Message-ID:	メールに付けられた個別の識別子
X-ではじまるもの	利用者定義のヘッダフィールド

ヘッダの情報はMUAで作成される。したがって、多くのMUAは宛て先であるToや表題（Subject）の入力を要求する。しかし、一般的には送り主のアドレスであるFromなどはあらかじめMUAに設定されたアドレスを使う。したがって、MUAの設定を間違えると、間違ったメールアドレスを相手に伝えてしまう可能性がある。また、それを逆手にとって、自分のアドレスとは異なるメールアドレスをFromフィールドに挿入してメールを送ることが可能となる。通常のMUAはユーザインターフェイスの画面で送り主のアドレスを変更することはできないが、MTAとSMTPで直接接続すれば、あらゆるメールアドレスを偽造することができる。

では、偽造されたアドレスであるかどうかを

見破る方法はないのであろうか。電子メールにはユーザが操作できるメールヘッダ情報とは別に、MUA や配送経路にある各 MTA が付加するエンベロープ（封筒の宛名書き）という情報が存在する。したがって、エンベロープにある MTA が付加した From 情報（通常、これを UNIX From とか呼んで、ヘッダの From フィールドと区別する）と From フィールドの情報を付き合わせれば、From フィールド（つまり、送り主のアドレス）が偽造されているかどうかを調べることができる。ただし、UNIX From は通常では表示されない。MUA に「すべてのヘッダ情報を表示する」などのオプションがある場合は、それを使って表示させることができる。

リスト 1-1. 電子メールのすべてのヘッダ（含むエンベロープ）情報

----リスト 1-1 はじまり

From toyo00@inl-au.jp Tue Aug 5 11:52:14 2003

>From toyo00 Tue Aug 5 11:52:14 2003

Return-Path: <toyo00@inl-au.jp>

Delivered-To: toyo00@inl-au.jp

Received: from www.inl-au.jp (ns.inl-au.jp [218.224.200.202])

by ns.inl-au.jp (Postfix) with SMTP id 5E12F888CB

for <toyo00@inl-au.jp>; Tue, 5 Aug 2003 11:52:14 +0900 (JST)

Date: Tue, 5 Aug 2003 11:52:14 +0900(JST)

Message-ID: <20030805115214.240f.toyo00@inl-au.jp>

From: toyo00@inl-au.jp

To: toyo00@inl-au.jp

Subject: Test Mail

MIME-Version: 1.0

Content-Type: text/plain; charset=us-ascii

Content-Transfer-Encoding: 7bit

X-UIDL: S"@!!I1Y"!8<a!![jC!!

X-Mailer: WebMailer Ver0.954 on Apache/1.3.24 (Unix) with Mozilla/4.0 (compatibl

e; MSIE 6.0; MSIE 5.5; Windows NT 5.0) Opera 7.03 [ja]

Status: RO

This is a test mail for myself.

Please, ignored.

Cheers,

T. Okuyama

-----リスト 1-1 終わり

リスト 1-2. 添付ファイルがある電子メール

----リスト 1-2 はじまり

From toyo00@inl-au.jp Tue Sep 9 07:27:40 2003

X-UIDL: dbJ"!%m=!!0`j!!KaZ"!

>From toyo00 Tue Sep 9 07:27:40 2003

Return-Path: <toyo00@inl-au.jp>

Delivered-To: toyo00@inl-au.jp

Received: from 127.0.0.1 (catv-157-053.tees.ne.jp [202.216.157.53])

by ns.inl-au.jp (Postfix) with SMTP id 777AE888CB

for <toyo00@inl-au.jp>; Tue, 9 Sep 2003 07:27:29 +0900 (JST)

Date: Tue, 9 Sep 2003 07:44:41 +0900(JST)

Message-ID: <20030909074441.0cf9.toyo00@inl-au.jp>

```
From: toyo00@inl-au.jp
To: toyo00@inl-au.jp
Subject: Test Mail 2
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="----------PGDbHl83g30GKErg2kkKco"
X-Mailer: WebMailer Ver0.954 on Apache/1.3.27
(Win32) with Mozilla/4.0 (compatib
le; MSIE 6.0; MSIE 5.5; Windows NT 5.0) Opera
7.03  [ja]
Status: RO

This is a multi-part message in MIME format.

----------PGDbHl83g30GKErg2kkKco
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit


This is a test mail for attached file.
Please, ignore.

T. Okuyama
----------PGDbHl83g30GKErg2kkKco
Content-Type: application/msword;
name="=?ISO-2022-JP?B?GyRCJVMlOCVNJTkkSyQ
qJDEk
a0VFO1IlYSE8GyhC?=

=?ISO-2022-JP?B?GyRCJWskTjtIJCRKfSRIJTslLSVlJ
WolRiUjGyhC?=.doc"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
filename="=?ISO-2022-JP?B?GyRCJVMlOCVNJTkkS
yQqJ
DEka0VFO1IlYSE8GyhC?=

=?ISO-2022-JP?B?GyRCJWskTjtIJCRKfSRIJTslLSVlJ
WolRiUjGyhC?=.doc"

0M8R4KGxGuEAAAAAAAAAAAAAAAAAAAAP
gADAP7/CQAGAAAAAAAAAAAAAHAAAAegA
AAAAA
AAAAEAAAfAAAAAEAAAD+////AAAAAHkAAA
B/AAAAgAAAAIEAAACCAAAAgwAAAPkCAAD///
//
```

----リスト 1-2　おわり

ここで、メールサーバとメールクライアント（以下、「メーラ」と記す。）との情報のやりとりの安全性について考える。現在の多くのメールサーバは自分のドメイン名（あるいは同じネットワークプレフィクス IP アドレス）以外のクライアント（メーラ）からのメールの送信を制限している。これは、メールサーバが SPAM メールを発信する踏み台として利用されないための処置である。

しなしながら、このような処置を講ずることにより、例えばモバイル端末の場合、移動先でのメールの送信ができなくなるなどの問題が生じる。そのため、メール送信前にユーザを認証することで、メールサーバの正規のユーザであることを確かめて、電子メールの送信を許す仕組みが導入された。このような仕組みは大きく分けて次の 3 つがある。

(1)　POP before SMTP：SMTP でメールを送信する前に、必ず POP あるいは IMAP でメール受信を行う（POP も IMAP もユーザ ID とパスワードでの認証が必要）ことを前提とし、接

続情報（IP アドレス）などを記憶しておき、そのIPアドレスからの電子メール送信を一時的に許可する方法

(2) SMTP AUTH:SMTP 接続をしてメールを送るユーザ専用のIDとパスワードを発行して認証する方法

(3) TLS（SSL）:公開鍵証明書を使ったセキュア接続のための手段であるTLS（SSL）を使いユーザを認証して電子メールを送信する方法

現在の多くのメーラはこのいずれの方法にも対応している。一方、メール送信サーバ側も、(1)から(3)に対応する必要があるが、これらは個別に設定しなければならない。

また、(1)を使うためには、電子メールを送信する前に、必ずメールの受信を行い、利用しているIPアドレスなどの情報をサーバに知らせておく必要がある。このような情報はWatcher と呼ばれるソフトウェアにより管理されており、ある一定期間、メーラからのアクセスがなくなると、Watcher はそのメーラの情報を破棄してしまう。したがって、新着メールの問い合わせ間隔を短縮するなどにより、常にメールサーバとの接続を維持しなければならない。

4. 独自ドメイン名の運用

電子メールのところで既に述べたとおり、foo@bar.jp の「@」の左側はユーザ ID を右側はメールサーバの名前であると同時に、その組織を示すための名前であると述べた。しかしながら、後者の場合は、その組織が独自ドメイン名を運用しえいる場合であり、ISP のドメイン名をそのまま利用している場合や、フリーメールのアドレスの場合はそうとはならない。したがって、ある組織を代表するようなメールアドレスを使用したい場合は、独自ドメイン名を取得して運用することになる。最近では、ドメイン名の運用を請け負うホスティングサービス（電子メールとWWW独立のサービスや両方とも受けられるサービスがある。）が充実してきたので、それらを使用することにより、簡単に独自ドメイン名を運用できるようになった。

組織独自のドメイン名を使いメリットとしては、

【SPAM の語源】1994 年当時「spam」という言葉は、マルチユーザ版のダンジョンというロールプレイングゲームの愛好者間で、「ナンセンスな繰り返し」という意味で使われていた。語源は、ホーメルフーズ社の豚の加工食品「SPAM」であることはよく知られている。spam が「ナンセンスな繰り返し」という不名誉な烙印を押されたのは、イギリスの人気テレビシリーズの『空飛ぶモンティ・パイソン』第 25 話、「スパム・スケッチ」に由来している。なお、この話は、次の URL にて紹介されている。

http://python-airways.cside.com/sketch/25-spamspam.htm

内容は見ればわかるが、要するにこの中で、「スパム」という言葉がくどいほど繰り返されている。そのために、「ナンセンスな繰り返し」となったのである。しかし、実際にはこのネタは spam の a を伸ばして発音すると「sperm」となる下品なものである。そこで、「ナンセンスな繰り返し」からさらに進んで、「不快でくどい」ものということになった。これは、まさにネット上の spam 行為そのものであると言ってよいであろう。

例えば、自社ブランドとして定着している名前を用いることで、ユーザにその組織体を印象付けることができる、などである。なお、日本のおけるドメイン名のレジストリは(株)日本レジストリサービス(JPRS)が担当しており、JPRS の Web ページ[5]から独自ドメイン運用のための各種の情報を得ることができる。

5. spam メールとその対策

日本では「迷惑メール」と呼ばれるが、世界的には「spam メール」と呼ばれるのが一般的である。また、日本の迷惑メールは携帯電話のメールに届くことから、秘匿性が強く、特に青少年の性犯罪に利用されることが多く、そちらの方がより強調されがちである。しかしながら、実際にはインターネット上の spam メールは、各種の問題を引き起こしている。ここでは、まず spam メールとは何かを明らかにし、spam メールの発生メカニズムについて考える。そして、ユーザレベルでの spam メールの対処法として、自分のメーラをカスタマイズして spam 対策を行うことを考える。

spam の起源は IIJ の山本和彦[6]によれば、1994 年にネットニュース(現在の BBS(掲示板)

NO.6 : High Quality Replica
Date : Mon, 12 Sep 2005 07:31:12 +0800
From : "Chase B. Chamberlain" <chamberlain1@powerweb.de>
To : okuyama@dsl.gr.jp
Subject : High Quality Replica
X-Mailer : Microsoft Outlook Express 6.00.2800.1158

Do you want a high quality replica?

In our online store you can buy replicas of Rolex watches and
other brands. They look and feel exactly like the real thing.

- We have 20+ different brands in our selection
- Free shipping if you order 5 or more
- Save up to 40% compared to the cost of other replicas
- Standard Features:
 - Screw-in crown
 - Unidirectional turning bezel where appropriate
 - All the appropriate rolex logos, on crown and dial
 - Heavy weight

Visit us: http://vlew.com/

と思ってもらってよい）に投稿されたのが初めてのものとされている。

電子メールにspamが登場したのは、先の山本の解説によると、1995年のJeff Saltonのメールだと言われている。Slatonはspamメールでところで、「spam」の本家、ホーメルフーズ社は「迷惑メール」にspamという言葉を宛てることを容認しているが、商標登録している「SPAM」と明確に区別するために、全ての小文字の「spam」と使うことを要求している。日本語に翻訳した場合（単に、「スパム」と書かれてしまう！）どうするかは問題であるが、ここでも、ホーメルフーズ社の意向にそって、今後は一貫して「spam」と表記する。

spamメールの定義を行ったが、それでは、具体的にどのようなものがspamメールとして送られてくるのであろうか？spamメールは大きく宣伝した最初の製品が売れたのに気をよくして、spamの配信自体が商売として成り立つと考え、電子メールアドレスを詐称して、自ら「spamキング」と名乗って、spamの配信を宣伝するspamメールを出した。

分けて、次のように分類できる。

- 広告
- チェーンメール
- 架空請求
- メール爆弾
- ウイルス
- フィッシング（phishing）
- 出会い系サイトへの誘導

広告メールは（単なる筆者の見解であるが）、spamメールの王道を行くものであり、もともとのspamメールの起源となったものである。最近の広告メールの例を示す。この例は英文である

```
Return-Path: <chamberlain1@powerweb.de>
Delivered-To: okuyama@dsl.gr.jp
Received: from libero.it (pool-71-102-168-28.snloca.dsl-w.verizon.net [71.102.168.28])
        by sv.dsl.gr.jp (Postfix) with SMTP id 8A52FE08E
        for <okuyama@dsl.gr.jp>; Mon, 12 Sep 2005 08:32:23 +0900 (JST)
Received: from 209.93.96.108 by smtp.powerweb.de;
        Sun, 11 Sep 2005 23:31:38 +0000
Message-ID: <9b9201c5b728$07441216$ca85108a@libero.it>
From: "Chase B. Chamberlain" <chamberlain1@powerweb.de>
To: okuyama@dsl.gr.jp
Subject: High Quality Replica
Date: Mon, 12 Sep 2005 07:31:12 +0800
MIME-Version: 1.0
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2800.1158
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1165
```

が、最近では日本語のものも数多く見られるようになった。

このメールのヘッダとエンベロープの情報を次に示す。ここで、下線で示した2つの UNIX From に注目する。最終的にメールを受け取った MTA は、sv.dsl.gr.jp にあることがわかり、そこにメールを送った MTA は libero.it であることがわかる。しかしながら、実際の送り主の MTA はその次の UNIX From で示された、smtp.powerweb.de であり、送り出した MUA は、209.93.96.108 とう IP アドレスからであることがわかる。209.93.0.0/16 は INFONET 社というカナダの ISP に割当てられたアドレスブロックであり、実際に誰が使用しているかは、これ以上追及できない。また、ppowerweb.de はドイツの ISP であり、ここのメールサービスが使われたらしいことはわかるが、実際に From メールアドレスに記載されているユーザが実在するのか、単に踏み台にされたのかは不明である。あるいは、サーバをたくみに使ってメールアドレスを偽造しているのかもしれない。いずれにしても、広告メールはこのような巧妙な接続パスを使って送られてくることが多い。

通常、広告主と spam 業者は別であり、spam 業者は電子メールアドレスを偽り、広告主 から依頼された内容を本文に入れて送信する。興味を持ったユーザが電子メール内のリンクをクリックするか、あるいは読むだけで Web ページにアクセスしてしまうようなメールリーダを使っていれば、Web ページへのアクセス数が増える。これによって spam 業者は、広告主への義務を果たしたことになる。

広告の内容は、アダルトサイトや出会い系サイト、あるいは強壮剤などが圧倒的に多い。出会い系サイトの問題は別項目として取り扱う。また、対策としては spam フィルタを使うのが有効であるが、それについては後に詳しく説明する。

チェーンメールの代表的なものは不幸の手紙である。例えば、『あるメールと同じ内容のメールを知り合いのメールドレス 5 名に送らないとあなたは不幸になる』、といった人間の心理的な不安を突くメールである。もし、このような非科学的な誘惑に負けて、メールを送ると、それが無限連鎖となり、大量の無意味なメールを誘発するとこになる。

前述の山本和彦の解説には、脅迫メールとは別の観点でメールが止まらなくなった事件として有名な「ドラえもんの最終回」について、が示されている。少し長いが、ここに全文を掲載する。

---引用はじめ

脅迫まがいの内容ではないが、メールの連鎖がなかなか止まらない事件もあった。有名なのは「ドラえもんの最終回」であろう。「のび太が植物人間になる話」と「のび太が技術者になる話」の 2 種類に大別されるようだが、著者が頻繁に受け取っていたのは後者である。

ドラえもんの電池が切れて動かなくなる。ネコ型ロボットの補助電池は耳であり、耳がないドラえもんの電池を交換しようとすると記憶をなくす。ドラえもん の設計者は秘密であり、助けを求めることができない。のび太はドラえもんを押し入れに保管し、必至に勉強を開始する。技術者となったのび太は、ドラえもんを修理することで、実はドラえもんの設計者になった。

---引用おわり

その他では、例えば善意の発露からチェーンメールとなるものがある。例えば、インド洋の大津波の時、大津波の義捐金を募集するためのメールが大量に流れた。この中には、容易にチェーンメール化する表現を使っていたものがある。例えば、

――引用はじめ
『あなたの善意でたくさんの人が救われます。この活動に同意された方は、Web サイトにアクセスしていただくと同時に、このメールの内容をあなたの友人にフォワードしてください。これにより、より多くの方々がこの活動に参加していただけるようになるでしょう。』
――引用おわり

原文は英文なので、正しく訳せているか疑問もあるが、問題点は下線を引いた部分である。こ

弊社は信用調査会社・コンテンツ業者からの依頼に基づいて各種の料金等支払遅延者リスト（ブラックリスト）を一括管理している（株）帝国データーリサーチと申します。

この度は貴殿が使用されたプロバイダー及び電話回線から接続された有料サイト利用料金について運営業者より利用料金支払遅延に関して料金等支払遅延者リスト（ブラックリスト）掲載要請を受けました。

これまで貴殿のネットワーク利用料に付きましては、コンテンツ事業者様及び債権回収業者が再三のご連絡を試みてまいりましたが、未だ入金の確認がとれず、また貴殿より誠意ある回答も遺憾ながら本日に至るまで頂いておりません。

以上のような理由から個人信用情報調査会社を経由して弊社に貴殿の個人情報を料金等支払遅延者リスト（ブラックリスト）に掲載する要請が届きました。

貴殿の個人情報に関しましては既に調査対象メールアドレスから、プロバイダ・ISP 業者・個人信用情報調査機関からの情報開示を受け、既に貴殿の住所・氏名・勤務先等の情報は判明しております。

個人信用情報機関のブラックリストに掲載されますと、各種融資・クレジット契約・携帯電話の購入および機種交換他・就職先制限等の様々な貴殿信用情報に今後大きな支障が発生する可能性があります。

れは意図的なので無意識なのかわからないが、明らかにチェーンメールを誘発する表現となっている。これと同じようなメールは世界的に大きな出来事があると、必ずといっていいほど流れてくる。例えば、「イラク戦争」、「アメリカの同時多発テロ」などであり、最近では「ハリケーン被害救済」というものも受け取った。
また、より深刻なチェーンメールとして無限連鎖講（いわゆる「ねずみ講」）を誘発するものもあるが、最近ではあまり見かけなくなった。

このように、チェーンメールには種々のパターンがあるが、いずれにしてもむやみにメールを増殖させるのに手を貸すことは避けるべきである。例えば、第三の例のような人道的な支援についても、自身が賛同すればよいことであり、それを他人に押し付けてはならない。

架空請求も大きな社会問題化している。残念ながら（というか幸いにして、と言うべきか）、筆者は架空請求のメールをいまだ受け取ったことがない。そこで、ここでも山本和彦の例を引用する。

このような架空請求を不特定多数に送りつけることで、受信者の中には身に覚えがないのにも関わらず不安にかられる人がでてくる。架空請求のミソは、それが払えない金額ではないというところになる。そのため、不安を取り除くためにお金を振り込んでしまうのである。
自分の身を守るうえで重要なのは、架空請求をしてきた人とは関わらないことである。相手は受信者のことは何でも知っているフリをしているが、まず間違いなく、電子メールアドレス程度の個人情報しか知らない。そのため、家に押し掛けてくることは絶対にない。これ以上の個人情報を渡さないことが重要であり、架空請求は、単に無視するのが一番であるが、最近では、制度上の弱点を巧妙についた架空請求も現れてきているので、心配なら消費生活センターなどに相談するのがよい。（国民生活センターhttp://www.kokusen.go.jp/から相談窓口を探すことができる。）以下に、山本のページにある架空請求の例文を示す。

メール爆弾とは、大量のメールを送りつけることで、ユーザやサーバのメール領域を飽和させてサービスを妨害する攻撃である。このような攻撃を受けた場合、個人では対処しようがない。そこで、速やかに利用している ISP に相談すべきである。

ウイルスつきのメールに関しては、いまさら照会する必要もないであろう。現在、ウイルスの感染経路として、もっとも重要なものの一つとなっている。最近では、メールサーバ上にウイルス対策が施されている ISP も多くあるが、クライアント（MUA）の稼動しているコンピュータには、必ずウイルス対策ソフトウェアをインストールしておくべきである。
しかしながら、ゼロタイムウイルス（未知のセキュリティホールをついて蔓延するウイルス）やパターンファイルの対応の遅れなどを考えた場合、覚えのないメールは開かないことが重要である。

フィッシングメールという問題もある。これは、電子メールを使った詐欺行為である。特に、電子メールを使った詐欺行為の中でも、電子メールを入り口として、特定の Web ページに誘導して、利用者の個人情報などを不正な方法で入手する行為をさす。日本では、最近多くな

っている（例えば、UFJ カード事件や Yahoo Japan のアドレス収集詐欺など）が、アメリカでは既に数年前から流行しており、多額の被害が報告されている。

フィッシングの典型的な手口を紹介すると次のようになる。なお、実例は講習の中で示す。

(1) 特定業者を偽って電子メールにより緊急の連絡が必要であるというメールを送る
(2) その中に、業者の Web ページに告示したアドレスを載せた偽ページを用意する
(3) 用意されたページにより、利用者の個人情報を搾取する

フィッシング被害にあわないもっとも良い方法は、疑わしきは罰するという方針を貫くことである。つまり、少しでも疑わしいメールであるなら、そのメールの内容を直接メール以外で当該業者に問い合わせることである。このことが、フィッシング被害を事前に防ぐことが出来る最大の防止策となる。

フィッシングメールかどうかを判断する方法はいくつかある。フィッシングについて、最近では非常によく解説したサイトがいくつか存在する。ここでも、その中の１つを使って、フィッシングについての更なる解析と、防止策について述べていく。参照するページは次のとおりである。これらについては、Web ページにリンク集を設けておくので、そちらを参照して欲しい。

- eaxyfox の Firewall&Forest のフィッシング詐欺ページ
  (http://eazyfox.homelinux.org/Security/Security21.html)
- Anti-Phising Working Group（英文）
  (http://www.antiphishing.org/)
- フィッシング詐欺の擬似サイトと対策（判定の方法）を行うページ
  (http://eazyfox.homelinux.org/Security/special/Security24.html)

フィッシングに引っかからないためには、2つの側面から考える必要がある。一つは到着した電子メールの信憑性の判断であり、他の一つは表示された Web ページの信憑性の判断である。しかしながら、もっともよい防御策は、先に書いたとおり、ネットワーク的な手段以外で相手に連絡を取ることである。

【電子メールの信憑性を考える】

電子メールは、先に示したとおり、ヘッダと本文があり、ヘッダはさらに通常のヘッダとエンベロープに分かれる。これまでの議論ではエンベロープの書き換えはほとんど不可能であるようなことを述べたが、最近では経由する MTA 自身が乗っ取られていたり、あるいは別のサーバであったりするような巧妙な例が増えてきた。もちろん、このような場合は、エンベロープも偽造メールの判断の決め手とはならない。しかし、現状ではエンベロープとヘッダの情報の不一致を見ることが、偽造アドレスからのメールであるかないかを判断する重要な情報源となる。

【Web ページの信憑性を考える】

Web ページの場合、ページソースとページのプロパティが一つの判断材料となる。ページソースの表示は、IE ならば、「表示」メニューの

「ソース」を使ってみることが出来るようになっている。しかしながら、JavaScript や他のスクリプト系の言語などを使っている、必ずしもソースが見えないことがある。スクリプト系言語は、今では多くのページが利用しており、昔のように安易にスクリプト系言語の実行を禁止すればよい、とはいえなくなってきてしまっている。もちろん、そのようなサイトを利用するのを控えるのは、賢いユーザの選択肢の一つである。しかしながら、実際にはインターネット上でアクセスできるサイトを極端に狭めることとなる。Web ページを作成する場合、逆にこのようなスクリプト系言語を使わなくても、十分効果的なページを作成することは可能なので、安易にスクリプト系言語に頼りことは避けるべきである。

Web ページに対する第二の情報源は、Web ページの種々の情報を表示させることである。IE であるならば、表示されているページ内で右クリックし、「プロパティ」で表示させることができる。例えば、以下は Web メーラの ID をパスワードの入力画面であるが、これに対して、次に示したような情報を得ることができる。

出会い系サイトへの誘導に関して、最近は巧妙になってきて、一見すると出会い系サイトへの誘導であると思わせないものがある。通常のパターンとして、例えば次のようなメールがやってきて、リンクをクリックすることで、出会い系に誘導するというパターンである。

この例では、着信拒否アドレスがあるだけ親切な例であり、多くの場合、法的な規制があるにも関わらず、件名の記載や着信拒否アドレスや責任者の明記がないままに送られてくる。このようなメールは無視するのが一番である。

ところで、最近は個人名を使って、あたかも手違いやどこかで連絡先を知ったようなパターンのメールが送られてくることがある。山本の示した「黒川京子」という個人名を使った出会い形サイトへの誘導（何度かメールをやり取りしているうちに、会いたいといって出会い系に誘導するパターン）は有名な話である。最近、筆者は次のようなメールを受け取った。残念ながら、というか、幸いにしてというか、筆者はエキサイト（Excite）の掲示板は使ったことがなかったので、まるっきり心当たりが無かったが、これが、通常使っているポータルサイトやブログサイト、あるいは、Yahoo と言われると信じたかもしれない。

今回の地域紹介が逆￥限定ですので、希望女性会員の数により、男性様へのご紹介は人数限定と致しまして、長時間経過してもご返答のない方は自動破棄と判断し他の方に移行させて頂く事も有りますので、予めご了承下さい。

□紹介会員(女性)：三沙子　さん(32)

■簡単なメッセージ直送→

「はじめまして、三沙子です。
　今回の紹介申し込みは彼氏じゃなく、お互い都合いい時に会える人（大人の関係!?）を探してみようかと思っているからです！一応結婚している(主婦？笑い)ので、主人にばれないような協力をして欲しいです、その代わりに出来る範囲なら感謝代は私がだします。プロフィールの写真は見れるはずなので、良かったら返事を下さい。宜しくお願いします。
　わがまま書いてしまって申し訳ないです。」

三沙子さんへ返信→　http://www.tirol-festival.net/?k4sv01　（登録無料）

□　今回の【紹介料】【入会費用】は全て無料です。登録後発生する事なども一切有りません。
□　逆援助希望女性は最低３万円以上が確定されている方のみご紹介致します。
□　一発で成立ならなくても、最新情報を随時更新後紹介させて頂きます。
□　写真、電話番号、プロフィールなど女性会員情報一覧を観覧できます。

ご入会の方は　http://www.tirol-festival.net/?k4sv01

□重要□
上記【ページ】が表示されなかった場合は〔権利終了〕となっておりますので、一般入会ページ【】をご利用下さい。その代わりに貴方様の〔逆￥特別権利〕次の男性様へと「権利が移行」してしまいますので予めご了承下さい。
□さらに、電話番号確認された皆様に漏れなく￥8.000円分の無料ポイントをプレゼントいたします□

拒否
iranai@tirol-festival.net

はじめまして！真知子です！
来月で24歳になります…。
時間が経ってしまったのでちゃんと届くのか心配ですが(i-i)
このメールを送るのにかなり勇気が…。

わかってるとは思いますけど、エキサイトの掲示板を見てメールしましたヨンコミ
私は既婚者なんですが…真剣な恋愛希望です！
家庭の事情と言うか主人が出張が多くてほとんど相手してくれないんで
時間と欲求と…いろいろ持て余しています(汗)

まだ全然大丈夫ならお返事下さいね♪
間に合ってるよ！って事ならこのメール削除しちゃってください(i-i)

淋しいから勝手に送って勝手に待ってるだけですので(汗)

このメールはどうなるかと推移を見守っていると、連絡を取るための掲示板らしきアドレスがそのうち送れられてきて、それをクリックするといつの間にか出会い系サイトへの登録画面へ誘導されるというものであった。

このメールは yahoo.co.jp の個人名と思われるアドレスを使っていた。フリーメールを利用する友人などがいなければ、yahoo.co.jp からのメールを全てフィルタすることで、この手のメールを迷惑メールとして取り扱うことができるが、そうでない場合は厄介である。特定のメールアドレスのみをフィルタしても、別のアドレスで送られてくるとおしまいである。

6. spam メールの現状と対策

さて、spam メールの現状については、先に紹介した IIJ の山本和彦らの第二回目[7]に詳しく解説されているので、そちらを参照して欲しい。

では、spam 対策として何を行えば良いのであろうか？ユーザにおける spam 対策の基本はフィルタリングである。つまり、spam と思われるメールを検知し、特定のフォルダ(spam フォルダ)に封じ込めてしまう、という方法である。

sapm フィルタリングについては、IIJ の櫻庭秀次が、上で紹介したシリーズの 3 回目[8]として紹介している。

櫻庭の解説[3]によれば、spam フィルタとして、次のようなものが存在している。

- メール本文で使われる単語の使用頻度による「ベイジアンフィルタ」
- メールヘッダ情報などから判断する「ヒューリスティックルール」
- 特定の spam をあらかじめ登録し判断
- 送信元情報から判断する「送信ドメイン認証」
- サーバ接続情報から判断

それぞれの細かい解説は、櫻庭のページにあるので、ここでは省略する。

さて、ユーザレベルにおいて、簡単にできるものは真ん中の「特定 spam をあらかじめ登録して判断」である。最近よく利用されるようになった Thunderbird と呼ばれるメールクライアント[9]にもこのような spam フィルタの設定が可能となっている。

Thunderbird の迷惑メールフィルタでは、あらかじめ迷惑メールフィルタによる処理方法を「ツール」メニューの「迷惑メールフィルタ」により設定しておく。そして、迷惑メールとしたいメールをユーザが手動でチェックすることで、迷惑メールフィルタを学習させる。学習が進むと、フィルタは自動的に迷惑メールと判断して、それをフィルタリングするようになる。迷惑メールとされたメールは直ちに直接ユーザが指定する場合は、『直ちに消去する』という設定もできるが、学習型のフィルタによるものは、いったん「迷惑メールフォルダ」に移される。したがって、定期的に迷惑メールフォルダを検査して、本来は迷惑メールとなってはならないものが含まれていないかチェックする必要がある。

また、最近はヒューリスティックルールを使った学習型フィルタを設定可能なメーラも増えている。このようなフィルタを上手に使うことで、迷惑メールの被害を少しでも減らすことが可能である。

このような機能は、Windows で最もよく利用されている OUTLOOK でも、もちろん利用可能となっている。詳細は、マイクロソフトのページ[10]などを参照して欲しい。

7. サーバ側での対策

ここまでは、ユーザ側の対策を中心として述べたが、最近ではサーバ側で spam メール対策ができるパッケージや、ISP がサーバサイドで spam メール対策を施すことができる場合がある。いずれにしても、これらはサーバ管理者や ISP の担当者によく問い合わせて、どのような設定がされるのか？spam と認識されたメールはどのような取り扱いを受けるのか？など、疑問に思うことを解決した後、積極的に利用していくとよいであろう。

8. 最近の法制との関係

ビジネスに利用する電子メールアドレスを取得し、利用する場合、オプトインとオプトアウトとう 2 つの手法があることは既に紹介した[1]。今回は、これらを含めて、電子メールを適切に運用するために制定された法律である、「特定電子メールの送信の適正化に関する法律」について説明する。

【オプトイン】

Web ページなどを介してあらかじめ、電子メールアドレスを取得し、それを利用しダイレクトメールやメールマガジンの配布に利用する。この際、必ず電子メールの保有者に対して、利用目的、利用方法などを明示して同意を求めなければならない。最近は、これにさらに個人情報の保護に関するプライバシー条項を付加して、メールアドレスを取得することになる。

【オプトアウト】

メールを送信後に、受信者からの同意を取る（とっても、受信拒否通知が来なければ、暗黙の了解として同意したと考えている業者が多い）方法であり、そのメールの内容は「特定商取引に関する法律」や「特定電子メールの送

信の適正化に関する法律」の内容に従わなければならない。

【特定電子メールの送信の適正化等に関する法律(抜粋)】

◆特定電子メールの送信の適正化◆等に関する法律

(平成十四年四月十七日法律第二十六号)

最終改正年月日:平成一七年七月二六日法律第八七号

(目的)

第一条

この法律は、一時に多数の者に対してされる特定電子メールの送信等による電子メールの送受信上の支障を防止する必要性が生じていることにかんがみ、◆特定電子メールの送信の適正化◆のための措置等を定めることにより、電子メールの利用についての良好な環境の整備を図り、もって高度情報通信社会の健全な発展に寄与することを目的とする。

(定義)

第二条

この法律において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

一　電子メール　特定の者に対し通信文その他の情報をその使用する通信端末機器(入出力装置を含む。次条において同じ。)の映像面に表示されるようにする ことにより伝達するための電気通信(電気通信事業法(昭和五十九年法律第八十六号)第二条第一号に規定する電気通信をいう。)であって、総務省令で定める 通信方式を用いるものをいう。

二　特定電子メール　次に掲げる者以外の個人(事業のために電子メールの受信をする場合における個人を除く。)に対し、電子メールの送信をする者(営利を 目的とする団体及び営業を営む場合における個人に限る。以下「送信者」という。)が自己又は他人の営業につき広告又は宣伝を行うための手段として送信をする電子メールをいう。

イ　あらかじめ、その送信をするように求める旨又は送信をすることに同意する旨をその送信者に対し通知した者(当該通知の後、その送信をしないように求める旨を当該送信者に対し通知した者を除く。)

ロ　その広告又は宣伝に係る営業を営む者と取引関係にある者

ハ　その他政令で定める者

三　電子メールアドレス　電子メールの利用者を識別するための文字、番号、記号その他の符号をいう。

(表示義務)

第三条

送信者は、特定電子メールの送信に当たっては、総務省令で定めるところにより、その受信をする者が使用する通信端末機器の映像面に次の事項が正しく表示されるようにしなければならない。

一　特定電子メールである旨

二　当該送信者の氏名又は名称及び住所

三　当該特定電子メールの送信に用いた電子メールアドレス

四　次条の通知を受けるための当該送信者の電子メールアドレス

五　その他総務省令で定める事項

(拒否者に対する送信の禁止)

第四条

送信者は、その送信をした特定電子メールの受信をした者であって、総務省令で定めるところにより特定電子メールの送信をしないように求める旨(一定の事 項に係る特定電子メールの送信をしないように求める場合にあっては、その旨)を当該送信者に対して通知したものに対し、これに反して、特定電子メールの送 信をしてはならない。

(架空電子メールアドレスによる送信の禁止)

第五条

送信者は、自己又は他人の営業につき広告又は宣伝を行うための手段として電子メールの送信をするときは、電子メー

ルアドレスとして利用することが可能な 符号を作成する機能を有するプログラム（電子計算機に対する指令であって一の結果を得ることができるように組み合わされたものをいい、総務省令で定める方 法により当該符号を作成するものに限る。）を用いて作成した架空電子メールアドレス（符号であってこれを電子メールアドレスとして利用する者がないものをいう。第十条及び第十六条第一項において同じ。）をその受信をする者の電子メールアドレスとしてはならない。

（措置命令）

第六条

総務大臣は、送信者が一時に多数の者に対してする特定電子メールの送信その他の電子メールの送信につき前三条の規定を遵守していないと認める場合におい て、電子メールの送受信上の支障を防止するため必要があると認めるときは、当該送信者に対し、当該規定が遵守されることを確保するため必要な措置をとるべきことを命ずることができる。

（総務大臣に対する申出）

第七条

特定電子メールの受信をした者は、第三条又は第四条の規定に違反して当該特定電子メールの送信がされたと認めるときは、総務大臣に対し、適当な措置をとるべきことを申し出ることができる。

2 総務大臣は、前項の規定による申出があったときは、必要な調査を行い、その結果に基づき必要があると認めるときは、この法律に基づく措置その他適当な措置をとらなければならない。

（苦情等の処理）

第八条

特定電子メールの送信者は、その特定電子メールの送信についての苦情、問合せ等については、誠意をもって、これを処理しなければならない。

（電気通信事業者による情報の提供及び技術の開発等）

第九条

電子メールに係る役務を提供する電気通信事業者（電気通信事業法第二条第五号に規定する電気通信事業者をいう。以下同じ。）は、その役務の利用者に対 し、特定電子メールによる電子メールの送受信上の支障の防止に資するその役務に関する情報の提供を行うように努めなければならない。

2 電子メールに係る役務を提供する電気通信事業者は、特定電子メールによる電子メールの送受信上の支障の防止に資する技術の開発又は導入に努めなければならない。

さて、このような法律があるにも関わらず、電子メールアドレスの収集に関しては、種々の問題が発生している。例えば、メールアドレスの売買や横流しは、オプトインでアドレスを取得した業者間でも行われている。実際に購入した電子メールアドレスがどれくらい使えるかという正式な報告はない。（あるほうが困る。）しかしながら、実際に購入したアドレスを試したという報告は、インターネット上にいくつか散見される。それによると、購入アドレスの半数は、購入時点で利用不可となっているという事例が多く見られる。

一方、業者間の横流しもあとを絶たない。例えば、あるポイント制のメール会員に登録したら、それ以外のダイレクトメールも送られてくるようになる、といった例は後を絶たない。また、受信拒否アドレスがあるにも関わらず、そこに通知しても正しく処理されるとは限らない。この場合は、法律により定められている指定法人（例えば、迷惑メール相談センター[11]など）に連絡を取り、改善を要求することになる。

いずれにしても、ビジネスにおける電子メー

ルアドレスの取り扱いに関しては、十分な注意を必要とする。

9. 終わりに

今回は、電子メールにまつわる問題の 3 回目として、現状の電子メールの利用状況を概観した後、spam メールとその対策などを論じた。spam メール対策は、今後ビジネスにおける電子メール利用のための重要な問題となるであろう。

10. 文献など

[1] 奥山徹、種田智哲、「ビジネスにおける電子メールの活用と最近の法制の関係」、『情報学研究－朝日大学情報教育研究センター紀要』、Vol.13、pp.1-25、2004.

[2] 「ビジネスにおける電子メールの活用と最近の法制の関係その2－ビジネス場面別活用事例－」、『情報学研究－朝日大学情報教育センター紀要』、Vol.14、pp.19-40、2005.

[3] 総務省、「平成 17 年度　情報通信白書」、2005.
http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/cover/index.htm

[4] http://www.apache.org/参照.

[5] http://www.jprs.jp/参照.

[6] 山本和彦、「spam からメールを守れ。第一回：spam の歴史と分類」、2004.
http://www.rbbtoday.com/column/spam/20041201/.

[7]近藤学、「spam からメールを守れ。第二回：日本と世界における spam の現状」、2004.
http://www.rbbtoday.com/column/spam/20041220/

[8] 櫻庭秀次、「spam からメールを守れ。第三回：spam のフィルタリング」、2005.
http://www.rbbtoday.com/column/spam/20050113/

[9] http://www.mozilla-japan.org/products/thunderbird/参照.

[10] http://www.microsoft.com/参照.

[11] http://www.dekyo.or.jp/soudan/top.htm 参照.

奥山　　徹　（経営学部情報管理学科教授）