さらに進んだ インターネット・セキュリティ

サーバー構築/運用術

第10回 電子メール(前編)

迷惑メールがついに社会問題になりました。電子メールが誕生してから30年，迷惑メールに悩まされるようになってから10年弱，社会問題化するほどメールが深く人々の生活に密着するものになったわけで，感慨深いものがあります。

(ケイ・ラボラトリー　仙石 浩明)

2001年10月29日の報道によると，NTTドコモのユーザーあてに大量の迷惑メールの送信を行っていた事業者に対し，横浜地裁が送信を停止する旨の仮処分命令を下しました。続いて10月31日，東京都が2002年7月から迷惑メールを条例で規制する予定とのニュースも流れてきました。迷惑メールは許されないという常識が広く浸透することを願ってやみません。

今回問題となったのは携帯電話に対する迷惑メールで，通常のインターネット上の迷惑メールと比べると，少々事情が特殊であるようです。例えば，

(1) 単一のドメイン(@docomo.ne.jp)に数千万のユーザーがいる
(2) 対象が日本在住の携帯電話所持者に限定されていて宣伝効果が高い
(3) 有効なメール・アドレスか否かの確認が容易

というように，迷惑メールを送る側(以下，スパマー[*1]と呼ぶ)からすると極めて有利な特徴があります。スパマーはランダムに生成したメール・アドレスを片っ端から試してみて，有効なメール・アドレス・リストを作成することができます。ひとたびリストに加えられてしまえば，ランダムな文字列からなるアドレスであっても，迷惑メールが頻繁に送られてくることになるでしょう。

さらに，迷惑メールを受ける側からすると，

(4) 通信費を迷惑メールの受信者が負担しなければならない
(5) 常に持ち歩いている携帯電話に直接着信する

といった迷惑感を倍増させる事情が重なって，ついに迷惑メールが社会問題化したと言えます。

しかも今回の場合，NTTドコモにとっても，

(6) ユーザーからのクレームに対応するコストの増加
(7) あて先が有効なメール・アドレスでなければ課金できない
(8) メール・サーバーの負荷の増大に伴うメール配送の遅延
(9) スパマーを特定することが可能だった

＊1　無差別に送りつけられる迷惑メールは，ネット・ニュースのスパム(spam)と類似点が多いため，スパム・メールと呼ばれることもあります。そしてスパムの送信者はスパマー(spammer)と呼ばれます。

```
    ozenji:/home/sengoku % telnet mx.gcd.org smtp
    Trying 210.145.125.162...
    Connected to mx.gcd.org.
    Escape character is '^]'.
 1  220 asao.gcd.org ESMTP
 2  HELO ozenji.gcd.org
 3  250 asao.gcd.org
 4  MAIL FROM:<postmaster@gcd.org>
 5  250 ok
 6  RCPT TO:<sengoku@gcd.org>
 7  250 ok
 8  DATA
 9  354 go aheado
10  Subject: test
11  From: postmaster@gcd.org
12  To: sengoku@gcd.org
13  Date: Sat, 01 Jan 2000 00:01:02 +0900
14
15  仙石です。これは SMTP 説明用のテストメールです。
16
17  #5403.                                              仙石 浩明
18  http://www.gcd.org/sengoku/         Hiroaki Sengoku <sengoku@gcd.org>
19  .
20  250 ok 946177353 qp 13960
21  QUIT
22  221 asao.gcd.org
    Connection closed by foreign host.
```

図1　SMTPによるメール送信例

という事情があって，迷惑メールを排除する方向に動かざるを得なかったのだろうと想像しています。

迷惑メール

迷惑メールは，今日のように携帯電話メールが普及する以前からありました。日本発の迷惑メールは，1995年のインターネット元年ごろから増えてきたように思います。当時は，(1)単一のドメインに多数のユーザーがいるわけではなく，迷惑メールのあて先アドレスの収集にはネット・ニューズ*2を用いるのが一般的でした。

つまりニューズ・サーバーに蓄積された記事を片っ端から調べて，From: フィールドなどからメール・アドレスを収集していた*3ようです。このため何か記事を投稿すると，数日後に迷惑メールが届くといった具合になります。

ネット・ニューズが廃れてくると，こんどはメーリング・リストのメンバ一覧や，Webページから収集したりと，あの手この手の収集*4が行われていたようです。メール・アドレスを収集されるのを恐れるあまり，不特定多数に知らせるメール・アドレスと，知人のみに教えるプライベート・メール・アドレスを使い分けることが推奨されるようになりました。

しかしながら，メール・アドレスは大勢の人に知ってもらってこそ役に立つものでしょう。迷惑メールを恐れるあまり，知人以外から届いたメールを排除して見知らぬ人とのコミュニケーションの可能性*5を捨ててしまうのは，本末転倒と言わざるを得ません。

もちろん，懸賞に応募するときやアンケートに答えるときにまで普段使っているメール・アドレスを記入する必要はないでしょう。懸賞やアンケートはユーザーの嗜好とアドレスをセットで収集することができるわけで，得られるリストを用いれば，極めて(2)宣伝効果の高いダイレクト・メールの発行が可能になります。

一般に，1つの業者に大量のメール・アドレスが集まることは好ましくありま

＊2　ネット・ニューズについては，本連載2001年10月号～同年12月号を参照してください。
＊3　スパマーにアドレスを収集されるのを防ぐため，From: フィールドに偽のアドレスを記入して投稿することが一時流行しました。しかし，From: フィールドには有効なメール・アドレスを記入するというルールがあるので，このような対策は採用すべきではありません。
＊4　アドレスはどこで収集されるか分かりません。例えばフリー・メールを使っている人にメールを送ると，当然フリー・メールの管理者はそのアドレスを収集できますね。友人にフリー・メールの利用者がいる場合は，注意するべきかもしれません。
＊5　ソフトウエアや論文などを発表するときは，著者の連絡先としてメール・アドレスを記入しておけば，さまざまな人から意見をもらえます。

```
RCPT TO:<sengoku@gcd.org>
250 OK
RCPT TO:<green@gcd.org>
550 No such user here
RCPT TO:<stone@gcd.org>
250 OK
RCPT TO:<yellow@gcd.org>
550 No such user here
```

図2　有効なアドレスか否かの確認

せんし，大量のメール・アドレスを管理している業者は，アドレスのリストが外部に漏れないよう，厳重に管理してほしいものです。

そして，携帯電話キャリアや大手プロバイダ等の事業者は，大量のメール・アドレスを抱えているのですから，第三者によって(3)有効なメール・アドレスか否かの確認が容易にできてしまうことは避けなければいけません。有効なアドレスか否かの確認が容易であれば，それを繰り返すことにより有効なメール・アドレスのリストを作成できてしまうからです。

アドレスが有効か否かの確認

現在のメール配送の大部分は，宛先サイトのメール・サーバーにSMTP*6で接続することにより行われています。例えば，sengoku@gcd.orgあてにメールを送るときには，あて先サイトgcd.orgのメール・サーバーであるmx.gcd.orgにSMTPで接続して，**図1**に示すような通信*7を行います。

3桁の返答コードから始まっている行が，あて先サイトのメール・サーバーからの返信で，それ以外の行が送信です。4行目であて先アドレスのsengoku@gcd.orgを指定しています。その次の行の返答コード250はあて先アドレスが有効であるということを示しています。

もし，指定したあて先アドレスに何らかの理由で配送することができない場合は，百の位が5の返答コードを返すことになっていて，例えば550は指定したアドレスが存在しないことを示します。このSMTPの取り決めを悪用すると，**図2**に示すように，「RCPT TO:<アドレス>」を「アドレス」を変えつつ何度も送信して，それぞれのアドレスが有効であるか否か確認することが可能になります。図2の場合であれば，「sengoku」と「stone」は有効で「green」と「yellow」は無効であるということが分かります*8。

スパマーにとって，手持ちのメール・アドレス・リストに無効なアドレスがたくさん含まれていると送信効率が落ちますから，有効か否かを確認させてくれるメール・サーバーは大変ありがたい存在と言えるでしょう。つまり，正直に返答コードを返す必要はありません。ユーザー数の多いサイトであれば，有効か否かの確認のためユーザー・データ・ベースを検索するコストも無視できません。(7)あて先が有効なメール・アドレスでなければコストをユーザーに転嫁できませんし，(8)メール・サーバーの負荷の増大に伴うメール配送の遅延につながればメール・サービスの質の低下を招いてしまいます。

従って，「RCPT TO:<アドレス>」に対しては，「アドレス」に対応するユーザーが存在しない場合でも，とりあえず「250」を返してメールを受け取るべきでしょう*9。あて先アドレスが存在しないものについては，後で必要に応じて*10，あて先が間違っていることを差出人に教えてあげれば済む話です。

スパマーの特定

スパマーが，自身が所有するメール・

*6　SMTP(Simple Mail Transfer Protocol)。詳しくは，RFC2821を参照してください。
*7　この例では，telnetコマンドを使って接続していますが，実際のメール配送ではメール・サーバーがこのようなSMTP接続を行います。
*8　gcd.orgは私が運営するサイトですから，もちろんこんな確認はできないようにしてあります。
*9　もちろんアドレスが自ドメインでない場合は受け取りを拒否するべきです。詳しくは後述する不正中継を参照してください。
*10　もし，あて先が間違っている旨，差出人に教えてあげるエラー・メールを，無条件に自動送信するようにしてしまうと，差出人アドレスが偽造されたメールを大量に送りつけられると，その差出人に大量のメールを送り返すことになってしまい，好ましくありません。エラー・メールを返す条件を厳密に設定する，あるいはエラー・メールを返す頻度に上限を設ける，などの対策が必要でしょう。

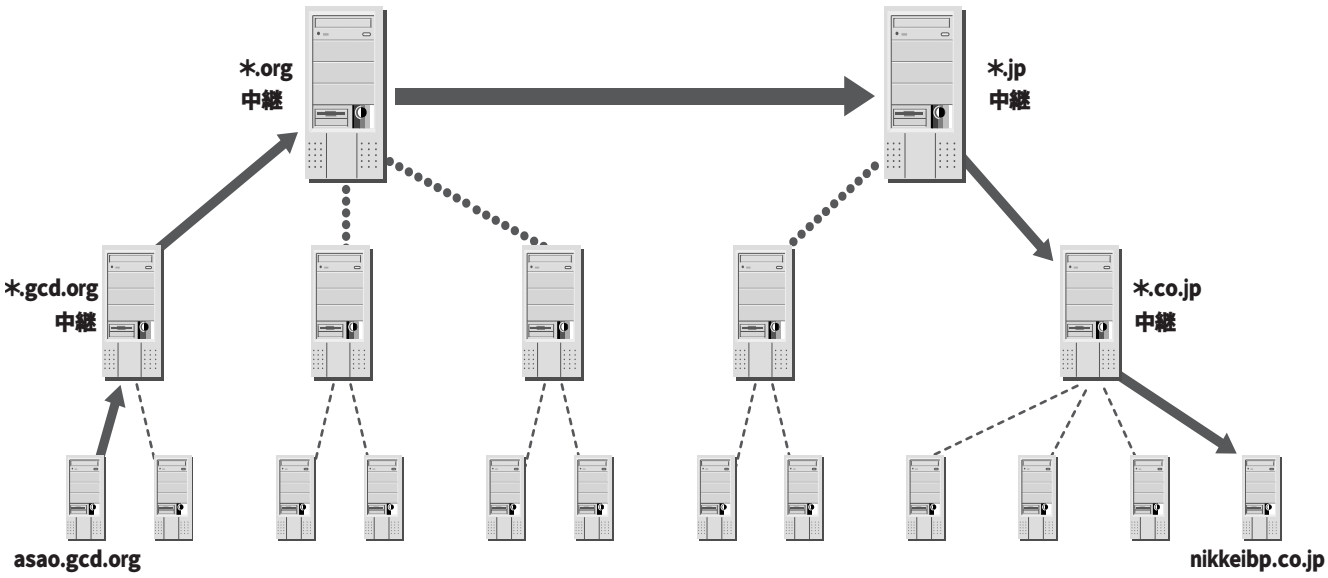

図3　ドメイン名の木構造に沿った配送

サーバーから直接メールを送信すると，受信側で送信元メール・サーバーのIPアドレスが分かります＊11。従って受信者は(9)スパマーの特定ができて，迷惑メール送信の差し止め請求など，法的手段に訴えることができます。

法的手段にまでいかなくとも，迷惑メールを送信し続けるメール・サーバーのIPアドレスのリストを作って，リストに含まれるサーバーからのSMTP接続を拒否するなどの迷惑メール対策が可能になります。

こういった迷惑メールの発信元リストを，サイトごとに作成していると大変ですが，MAPS(Mail Abuse Prevention System＝メール濫用予防システム)RBL(Realtime Blackhole List)が1997年に登場してからは，迷惑メールの送信元となっているメール・サーバーからのSMTP接続を手軽に拒否できるようになりました。

メール濫用予防システム MAPS RBL

MAPS RBLは，迷惑メールの送信元となっているメール・サーバーのIPアドレスのデータベースで，DNS(Domain Name System)を使って特定のIPアドレスが登録されているか否かを確認することができます＊12。例えばIPアドレス「a.b.c.d」の場合，DNSで「d.c.b.a.blackholes.mail-abuse.org」を検索し，もしTXTレコードが登録されていたら，そのIPアドレスがデータベースに登録されていることを意味します。

多くのサイトがMAPS RBLを利用するようになって，スパマーのサイトから送信された迷惑メールのほとんどが受

＊11　SMTPはIP(Internet Protocol)上のプロトコルですから，常に通信相手のIPアドレスを知ることができます。
＊12　残念ながらMAPS RBLは2001年8月1日以降，MAPSと契約した人しか利用できなくなってしまいましたが，http://ordb.org/，http://orbz.gst-group.co.uk/，http://orbz.org/など，いくつかの類似のデータベースが利用可能です。
＊13　電子メールは1971年，Ray Tomlinsonによって発明されました。発明当時，ARPANETには23台のホストが接続されていたそうです。
＊14　ARPANET(Defense Advanced Research Projects Agency Network)。1969年に米国内の5つの軍事研究所の計算機を結んだ実験ネットワークが構築されました。
＊15　USENET(User's Network)。1979年に米Duke大学の大学院生がUNIXマシンをUUCP(電話回線)で結んでメールおよびネット・ニューズを交換することを始めました。ネット・ニューズは多くのユーザーを引きつけ，インターネット・コミュニティの基礎となりました。1990年に電話回線の代わりにNSFNET(National Science Fundation Network, 1986年発足)を利用するようになります。
＊16　BITNET(Because It's Time Network)。1981年に，大学および非営利の研究所の計算機システムを専用回線で接続したネットワークとして発足しました。米ニューヨーク市立大学と米エール大学を中心として，米国や欧州そして日本にも広がりました。

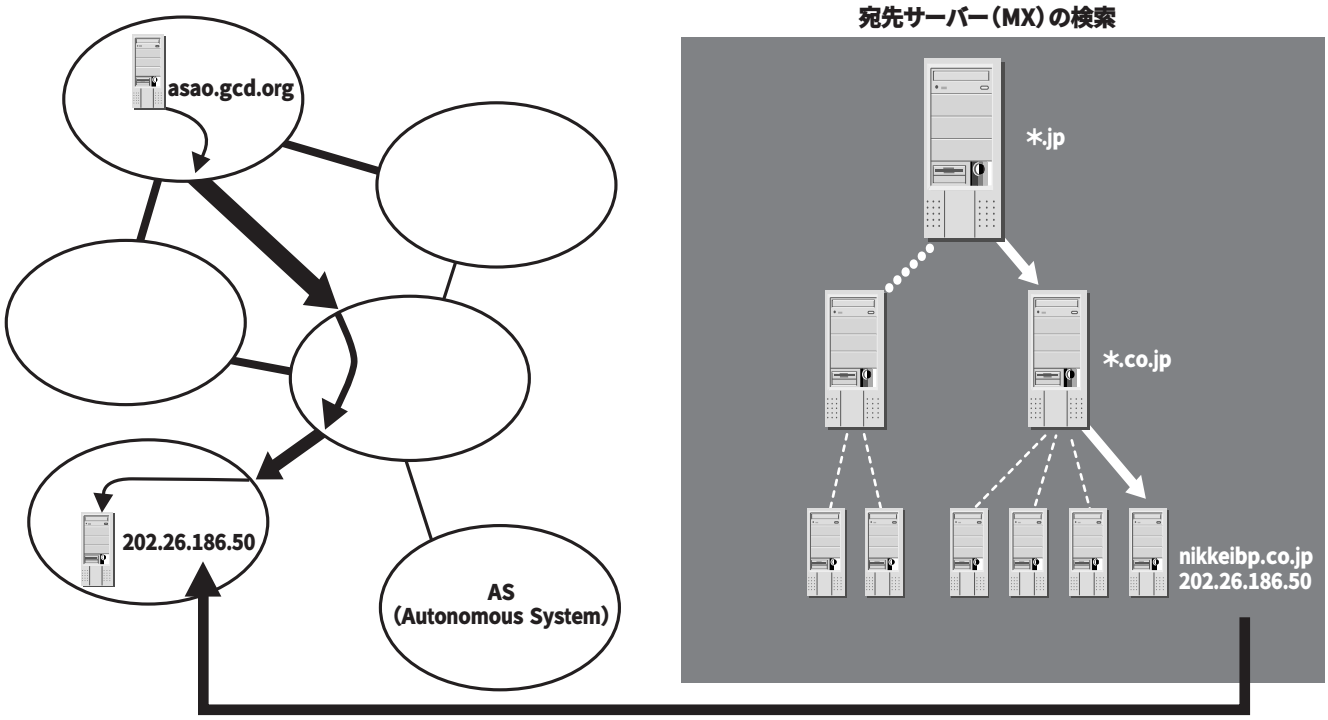

図4　インターネットの構造に沿った配送

信拒否されるようになると，迷惑メールをあて先メール・サーバーへ直接送信するのではなく，別のメール・サーバーに中継させて迷惑メールをばらまくようになります。これが不正中継です。

不正中継

電子メールが誕生*13して以来1995年前後辺りまで，電子メールは中継すべきものでした。1980年代，ARPANET*14，USENET*15，BITNET*16，CSNET*17など，それぞれ異なるプロトコルで構築されたネットワーク間でメールを交換するためのゲートウエイが設置され，メールはゲートウエイで中継されていましたし，それぞれのネットワークも木構造のトポロジを持っており，各メール・サーバーは未知のアドレスあてのメールは上位サーバーに中継してもらうのが普通でした。

ところが1990年代になってTCP/IPによるネットワーク，つまりインターネットが一気に優勢になります。その他のネットワークはインターネットの末端にぶらさがる従属的なネットワークになっていったのです。

その結果，ほとんどのメールはDNSを使ってあて先のメール・サーバー（MX，MailExchanger）を検索して，あ

＊17　CSNET(Computer Science Research Network)。1981年に，NSFがARPANETへのアクセスができない大学の科学者にメール等を提供するために拠出した資金を基に構築され，1989年にBITNETと統合しました。

```
azabu.klab.org % telnet 212.72.XX.51 smtp↵
Trying 212.72.XX.51...
Connected to 212.72.XX.51.
Escape character is '^]'.
220 server.aes.nt Microsoft ESMTP MAIL Service, Version: 5.0.2195.2966 ready at  Sat, 10 Nov 2001 12:11:47 +0400
HELO asao.gcd.org↵
250 server.aes.nt Hello [210.156.250.240]
MAIL FROM:<test@gcd.org>↵
250 2.1.0 test@gcd.org....Sender OK
RCPT TO:<postmaster@gcd.org>↵
250 2.1.5 postmaster@gcd.org
DATA↵
354 Start mail input; end with <CRLF>.<CRLF>
From: test@gcd.org↵
To: postmaster@gcd.org↵
Subject: test↵
↵
This is a test mail, sorry.↵
.↵
250 2.6.0 <SERVERyF1BcI3Em6kwV00000903@server.aes.nt> Queued mail for delivery
QUIT↵
221 2.0.0 server.aes.nt Service closing transmission channel
Connection closed by foreign host.
```

図5　不正中継サーバーを利用した不正中継の例

て先のサーバーに直接届けられるようになりました。つまり従来，ドメイン名の木構造に沿って行われていた配送（**図3**参照）が，インターネットのネットワーク構造に沿って行われるようになった（**図4**参照）わけです。そしてドメイン名をインターネットのアドレス，すなわちIPアドレスに変換するために使われるのが，DNSというわけです。

DNS自体は木構造のシステムになっています。言い換えれば，メール配送はもっぱらインターネットのパケット配送によって行われるようになった，ということであり，メール独自の中継システムは不要になった，ということです。中継は，サイト内部，あるいは従属的な小規模ネットワークの中でのみ行うだけで済むようになりました。

つまり，インターネットと直接メールをやりとりするメール・サーバーは，

(a) 他サイトから発信された自ドメインあてのメールを受け取り，必要に応じてサイト内部のメール・サーバーへ中継

(b) サイト内部から発信された他ドメインあてメールを，あて先のメール・サーバーへ中継

すれば良いのであって，

(c) 他サイトから発信された他ドメインあてメールを中継

＊18　インターネットの急激な普及でネットワーク管理者が不足したため，メール・サーバーを適切に設定できなかったサイトが多かったというのも理由の1つでしょう。

```
Received: from unknown (HELO server.aes.nt) (212.72.XX.51)
  by asaogw.gcd.org with SMTP; 10 Nov 2001 17:22:07 +0900
Received: from asao.gcd.org ([210.156.250.240]) by server.aes.nt with Microsoft SMTPSVC(5.0.2195.2966);
         Sat, 10 Nov 2001 12:12:52 +0400
From: test@gcd.org
To: postmaster@gcd.org
Subject: test
Return-Path: test@gcd.org
Message-ID: <SERVERyF1BcI3Em6kwV00000903@server.aes.nt>
X-OriginalArrivalTime: 10 Nov 2001 08:13:41.0421 (UTC) FILETIME=[9BA7A5D0:01C169BF]
Date: 10 Nov 2001 12:13:41 +0400

This is a test mail, sorry.
```

図6　不正中継サーバー経由で送られて来たメール

する必要はありません。

不正中継サーバーの弊害

ところが中継が原則不要になった後も，多くのメール・サーバーが(c)の中継を行う設定のまま放置されました＊18。これが不正中継サーバー(Open SMTP Relay)です。

MAPS RBLの普及によって送信したメールの多くが拒否されるようになってしまったスパマーたちは，不正中継サーバーを利用するようになります。迷惑メールの大半が不正中継サーバーを利用して発信されるようになったため，1998年1月にメール・サーバーでの中継拒否を要請するインターネット・ドラフト(draft-lindberg-anti-spam-mta-01.txt)が提案され，1999年にはRFC2505＊19になっています。

不正中継サーバーは，他サイトからのSMTP接続においてあて先アドレス(すなわち，「RCPT TO:<アドレス>」の「アドレス」)が自サイトと関係ないアドレスであったとしてもメールを受け取り，あて先アドレスへ中継してしまいます。例えば，azabu.klab.orgから不正中継サーバーの212.72.XX.51＊20を利用して，postmaster@gcd.orgあてにメールを送信した例を**図5**に示します。postmaster@gcd.org側で受け取ったメールが**図6**です。

図5において，「HELO asao.gcd.org」「MAIL FROM:<test@gcd.org>」などと送信元サーバー名と送信者アドレスを偽造している点に注意してください。図6のヘッダーを見ると，「Received: fromasao.gcd.org」「ReturnPath:test@gcd.org」などとなっていて，一見＊21送信元のメール・サーバーが「asao.gcd.org」で送信者が「test@gcd.org」であるように見えます。スパマーにとって送信元を隠すことができる不正中継サーバーは有難い存在と言えるでしょう。

このようにメール・ヘッダーは容易に偽造できますから，送信元サーバー名や送信者アドレスをうのみにして抗議メールなどを送らないよう注意すべきです。送信者アドレスに使われた test@gcd.orgには何の落ち度もなく，もしかすると元々の送信者はtest@gcd.orgに対する攻撃を意図してこのような偽造メールを送ったかも知れないからです。

さらに，図6のような偽造メールにおいてあて先のpostmaster@gcd.orgが存

＊19　http://www.ietf.org/rfc/rfc2505.txtを参照。
＊20　私のサイトにSMTP接続を試みた不正中継サーバーを利用した実例を紹介していますが，なるべく真似はしないでください。同じサーバーにアクセスが集中するのを避けるため，IPアドレスの一部を伏せ字にしています。このメール・サーバーはserver.aes.ntと名乗っていますが，「nt」というトップ・レベル・ドメインは現時点では存在しないようです。
＊21　IPアドレスを見れば本当の送信元サーバーが分かりますが。

在しないアドレスだったらどうなるでしょうか。

不正中継サーバーは，エラー・メールを返信しますが，その送り先は本来の送信者ではなく，アドレスをかたられたtest@gcd.orgになります。

つまり，スパマーが送信者を偽造して不正中継サーバー経由で迷惑メールを大量に送った場合，

- **あて先に届けば，そこから抗議メールが送られてくる恐れがある。**
- **届かなければ，不正中継サーバーからエラー・メールが返ってくる。**

いずれの場合も，アドレスをかたられた側にメールが殺到することになります。特定のアドレスに対する攻撃手段として，かなり有効な方法と言わざるを得ません。

以上をまとめると，不正中継サーバーは，

- **MAPS RBLに登録されてしまったスパマーもメールを中継してもらえる。**
- **スパマーが自身の身元を隠ぺいしつつ迷惑メールを送ることができる。**
- **攻撃対象アドレスを送信者に見せかけた偽造メールを大量に送ることにより，特定のアドレスを攻撃できる。**

という理由から，放置すべきではありません。可能なら管理者に連絡して中継をやめるよう要請すべきでしょう。

不正中継サーバー・データベース ORDB

とは言っても，不正中継サーバーの数は非常に多く，そのすべての管理者に連絡して設定を変更してもらうことは現実的ではありません。いまだに中継を許す設定のまま放置されているのですから，メールなどで連絡しても放ったらかしにされるのがおちです。もしかすると管理者不在のまま運用されているサーバーかも知れません。

そこで，不正中継サーバー矯正システムORBS（Open Relay Behavior-modification System）＊22が登場しました。前述したMAPS RBLとよく似ていますが，MAPS RBLが実際に迷惑メールの配送に使われたメール・サーバーのリストであるのに対し，ORBSは，実際に迷惑メールの配送に使われたことがなくても中継を許可する設定になっていれば，迷惑メールの配送に使われる恐れがあるという理由でリストに含めています。

事実，スパマーの多くは次々と新しい不正中継サーバーを見つけては迷惑メールのばらまきに利用していましたから，実際に迷惑メールの配送に使われたサーバーのリストだけでは，あまり役に立たなかったのです。

ORBSの登場当時は，不正中継サーバーの数が圧倒的に多く，不正中継サーバーからのSMTP接続を拒否すると，多くのサイトからのメールを受け取ることができなくなる＊23ということで不評でした。リストに登録されてしまったサイトの中には，スパマーに荷担していた自身の責任を棚に上げて訴えるところまで出てくる始末でした。

とうとうORBSは2001年7月7日に活動停止に追い込まれましたが，その“遺志”を継いでORDB（Open Relay Data Base=http://ordb.org/），ORBZ（Open Relay Blackhole Zones=http://orbz.org/）などのデータベースが登場しています。

中でもORDBのWebページには，日本語版のFAQや用語解説があるのでお勧めです。

＊22　登場当時は，Open Relay Blocking Systemという名前でした。
＊23　取引先など業務上メールをやり取りする必要があるサイトからのSMTP接続を拒否してしまうケースが多発して，会社などではORBSを利用したくても利用できない状況でした。