

はじめに

search.ombudsman.jp で管理している、

- ombudsman.jp
- *.ombudsman.jp

のドメインについて、どのような spam 対策を行っているのか述べましょう。あと、すこし余談も。

spam 対策のなかみ

spam 対策というと、スコアリング or 統計処理によるフィルタを想像しますが、そういったものはありません。

2004/7/25 より、主に spam をできるだけ受け取らないようにするという目的で、適切な接続元のみメールを受け取るようにしています。現在では、

- HELO/EHLO コマンドのチェック
 - 文法が不正な場合、拒否
 - 引数のホスト名について、FQDN でない場合、拒否
 - 引数のホスト名について、DNS 上に A または MX レコードがない場合、拒否
- From のチェック
 - From が FQDN でない場合、拒否
- RBL のチェック
 - 相手の IP アドレスが、relays.ordb.org に登録されていれば、拒否
 - 相手の IP アドレスが、sbl-xbl.spamhaus.org に登録されていれば、拒否
 - 相手の IP アドレスが、zen.spamhaus.org に登録されていれば、拒否
 - 相手の IP アドレスが、all.rbl.jp に登録されていれば、拒否
- Graylisting
 - Rgrey。S25R に一致するホストからの接続時に graylisting（一時拒否 -> 配送遅延）を起こし、spam を減らす手法。
- その他のチェック
 - こちらが spammer と判断したメールアドレスから発信されていれば、拒否
 - こちらが spammer と判断した IP アドレスから発信されていれば、拒否
 - たいへんよくみかける spam の Subject であれば、拒否
 - Yahoo が Open Relay だとして拒否するメールアドレスから発信されていれば、拒否
 - Yahoo が偽装アドレスだとして拒否するメールアドレスから発信されていれば、拒否
 - Yahoo がメールボックスがいっぱいだとして拒否するメールアドレスから発信されていれば、拒否
 - その他、業務に差し支えがあるものや、要望があれば、拒否

というポリシーを、受信するアドレスによって適宜適用するという運用になりました。

この他、ML については、別に添付ファイルなどの制限があります。[search.ombudsman.jp で運用する ML の各種制限について](#)を参照。

spam とは？

spam とは、UCE(Uncolicited Commercial Email) とか、UBE(Unsolicited Bulk Email) とも称されます。search.ombudsman.jp における spam の基本的な考えとしては、<http://www.spamfaq.net/spam-evils.shtml> の「2.1.1 What are UBE and UCE? What is SPAM?」にある定義とほぼ同じ考えです。ようは内容ではなく、実態ってことです。

拒否って？ 届いたメールを見ずに捨ててるってこと？

いいえ。一般に電子メールはだいたい下記のように届きます。

出す人のパソコン -> 出す人のプロバイダのメールサーバ -> 受け取る人のメールサーバ -> 受け取る人のパソコン

「拒否」とは、「出す人のプロバイダのメールサーバ」から「受け取る人のメールサーバ」のところで、「受け取る人のメールサーバ」がメールの受け取り自体をしない、ということです。

たとえば、郵便小包を届けに郵便局からきても、小包の荷札をみて、受け取りませんといって、持って帰ってもらう、という感じです。

でも、誤って spam じゃないメールを拒否して、届かなくなるメールってないの？

はじめのころは、制限を全てのアドレスにかけたところ、メールが届かなくなる問題がおきました。特に、HELO のチェックの「引数のホスト名について、DNS 上に A または MX レコードがない場合、拒否」でひっかかるサイトが続出しました。そのたびごとに、ホワイトリストに追加してきましたが、業務に差し支えるようになってきたため、2005 年 6 月中旬より、jp ドメインについては、この制限のみ外しました。

しかし、事務局の要望もあり、2005/9/21 より、

- office [at] ombudsman.jp
- info [at] ombudsman.jp
- police [at] ombudsman.jp

など(他にもありますが、)業務アドレスについては、制限をほとんどかけない運用となりました。しかし、spam の増加傾向に対応するため、現在では、最初に説明したアドレス単位のポリシー適用の運用となり、現在に至っています。

現在では、届かなくなるメールはまずなくなりました。

届かないぞ！

- なんとか @ombudsman.jp
- なんとか @ なんとか .ombudsman.jp

宛のメールで、届かない場合、お手数ですが、isihara [at] ombudsman.jp 宛にご連絡下さいませ。その際、どのアドレスから (From)、どのアドレスへ (To)、送ろうとして遅れなかったかご連絡頂けると、幸いです。

届かなくなる原因で多かったものは？

先にもちょっと書きましたが、HELO のチェックの「引数のホスト名について、DNS 上に A または MX レコードがない場合、拒否」でひっかかるサイトが多かったです。特に、官公庁(特に lg.jp がつくドメイン)でひっかかる例が、やたら目につきました。(電子政府云々いっているなかで、ちょっとはずかしいですね。)

もし、あなたが、官公庁の人（特に lg.jp がつくドメインのメールアドレスを使っている人）であれば、一度チェックして、HELO の引数をちゃんとしたほうがいいと思います。メールサーバの管理をしている業者 or 部内の人に、「メールサーバの SMTP プロトコルの、HELO コマンドの引数って、ちゃんと FQDN になっている？ あと、DNS でその引数ちゃんと引ける？」とつつこんで、直される or チェックすることをおすすめします。

効果は？

SMTP の接続数でみれば、コンスタントに 1 割～3 割ほどはじけています。いちばん数が多いものは、下記で説明している Yahoo filter で、とても有効に機能しています。

Graylisting や Tarpit はしないの？

ともに、whitelist の管理が不可欠であり、それだけ手間をかける必要があります。残念ながら、それだけかけられないのです。

あとは、いまのところ、受信後のベイジアンフィルタによる排除でなんとなくなっている、という理由もあります。

あまりにも spam が増えてきたので、Rgrey の導入に踏み切りました。ただし、全てのメールアドレスが対象ではなく、あくまでも厳しいポリシーを適用したアドレスだけです。

更新記録

2006/6/18

必要が生じたので、いくつかのアドレスを Yahoo のアドレスに転送しています。すると、いくつかの spam とおぼしきメールが 421 ではじかれ、受け取ってもらえません。どうも、それらのメールは毎度毎度しつこくくる spam に該当することがわかりました。なので、Yahoo で 421 で特定の理由付きはじかれたメールアドレスからくるメールは、次回から転送することなく、拒否するようにしました。これは、全てのアドレスが対象です。

2006/12/29

ORDB が活動を停止したので、利用を停止しました。長い間ありががとう、ORDB。

2007/2/6

Yahoo に 553 ではじかれているメールのうち、特定の理由付きではじかれたメールアドレスからくるメールは、拒否するようにしました。

2007/2/9

sbl-xbl.spamhaus.org の利用を止め、zen.spamhaus.org の利用に切り替えました。

2007/3/18

Rgrey を導入しました。