

abmailsreport

隔離メール報告と再送について

株式会社あいはら 研究開発チーム

山田 泰司

abmailにより隔離されたメール

- アカウントのユーザ権限で日付毎のフォルダで隔離されています
 - `${MAILDIR:-$HOME/Mail}/spam-20070519/*`
- Unix使いなら隔離メールの閲覧は比較的簡単
 - IMAP4対応のメールサーバでも同様
- Windows使い等、一般ユーザが閲覧するには
 - IMAP4の整備、WebMailなどの解決策があるが...
- abmailsreportを使うと便利です
 - Unix使いにとっても、むしろ便利かも

abmailsreport

隔離メール報告及び再送用ツール

- 前日のスパムの一覧をメールで報告
 - cron から呼ぶことを想定
 - abmailsreport は単なるシェルスクリプトで、サマリの作成は abmailc が担当
 - スパムの内容を走査することは、実は簡単ではない！
 - 偽装された文字エンコーディング
 - 不正なMIME、Base64エンコーディング
 - スパムは多様な言語で送られる → 多言語対応
- 隔離メール報告への「返信」で救済したいメールを指定すると所望のメールが再送される
 - この枠組みが悪用されるような脆弱性は許されない！

Subject: [abmails report for \$LOGNAME]

- このようなスパム一覧がメールで報告されます



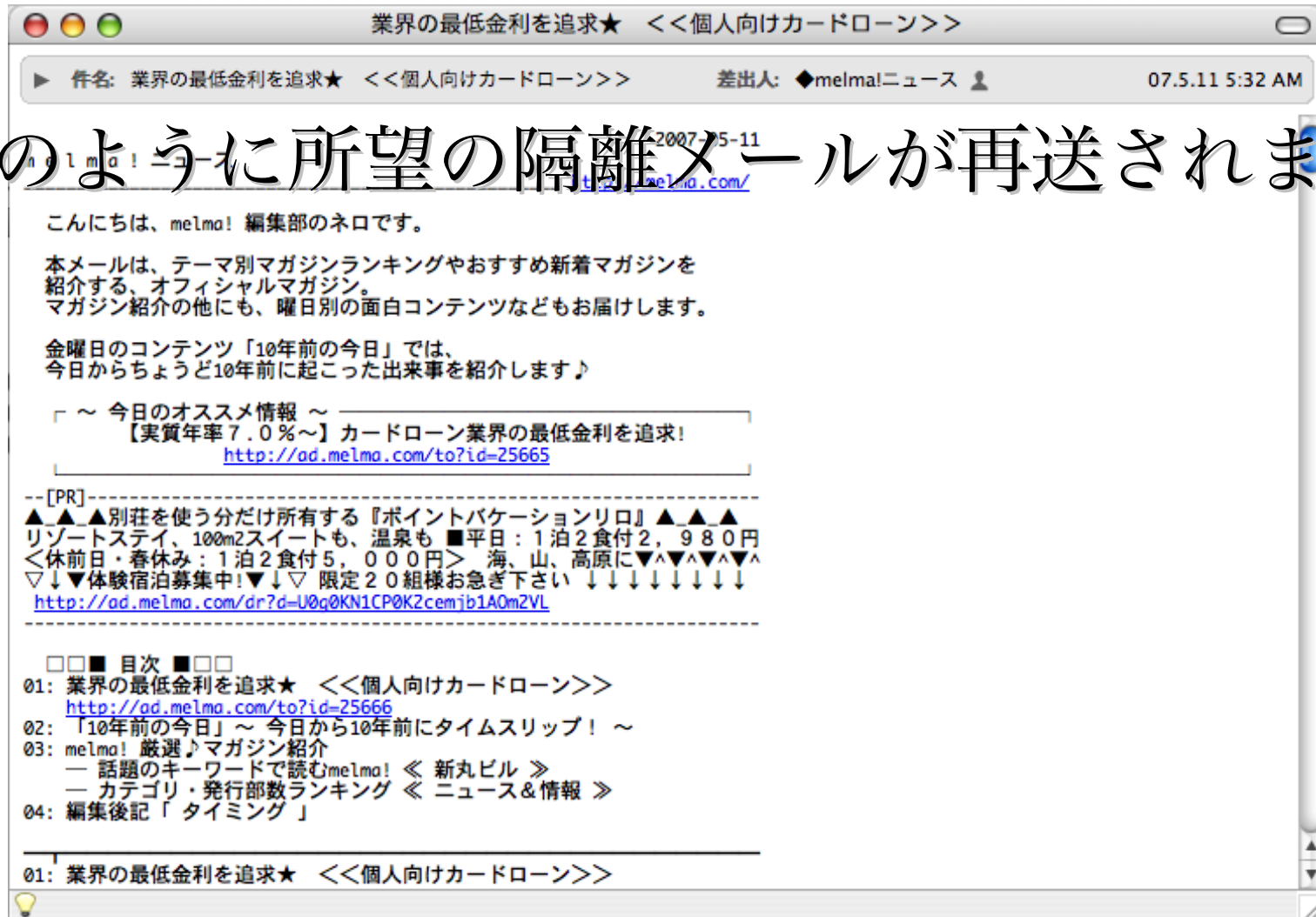
Subject: Re: [abmails report for \$LOGNAME]

- 救済したいメールの引用「>」を外し「返信」



Subject: Re: [abmails report for \$LOGNAME] File: spam-20070511/87

- このように所望の隔離メールが再送されます



abmailsreport の仕組みと安全性

- メールの走査はabmailcが担当
 - 極めて安全かつ高速にサマリを作成
 - 文字コードに偽装があっても文字化けを極力回避
 - 多言語に対応、最終的にUTF-8でサマリを送信
 - 不正なBエンコード、Base64も安全にデコード
- 隔離メールのサマリを送信する際に生成、登録されたユニークかつランダムなMessage-Idへの返信に対してのみ再送要求を受理し、再送
 - この枠組みへのDoSを防御！
- サマリメールが漏洩しない限り悪用は不可能
 - その漏洩も懸念されるなら、さらなる防衛も…

abmailc - (ab)mail converter

\$ abmess ~/Mail/spam-20070428/*

繁体字、簡体字、日本語、韓国語、キリル文字、
UTF-8等々のMIMEメッセージを端末でも！

abmess: abmail+lv+less on xterm, kterm,
mlterm, Terminal.app etc.



```
...st-regression/Mail_spam-20060602-20070428 — less — 80x24
Subject: [debian-devel:16743] Re: Your Vallum Order #9529050
From: "Hung Mcrae" <akira@linux.or.jp>
Message-Id: <HmKqgXDSJWak.ea@ttux.or.jp>
We have everything you need: Cialis Soft T4bs, Viagra
Soft T4bs, Cialls, Viagra, Levitra, Propecia, Vallum, Xan4x, Amblien,
Zub4n, Atar4x, At1wan, Cal1som, Ultr4m, Glucanb4ge,
Lip1u, Mef4d4, 214d4, 14b4sc
We respect your privacy - we guarantee you a total
privacy of your Order.
Visit US He4lthc4re Inc. online at: http://www.trebbiann.com/
.
File: spam-20070428/57
Envelope-From renypxqph@unitel.co.kr
Return-Path: <renypxqph@unitel.co.kr>
Received: from 221.215.169.175 (unknown [221.215.169.175])
        by mailhost.aihara.co.jp (Postfix) with SMTP id BC6AD0817D2
        for <taiji@aihara.co.jp>; Sat, 28 Apr 2007 10:57:27 +0900 (JST)
Subject: 영어발음교정책자 무료로 배송중입니다. 서두르세요.
From: "무료영어" <idfqbajjwd@nate.com>
To: taiji@aihara.co.jp
Message-Id: <HHSILXFTEUQGTIXLZFRGBWS@yahoo.com>
:█
```

abmailsreport の運用方法

- 必要なコマンドとライブラリや設定
 - procmailのformail, perl
 - abmailc, libpcrc, libiconv
 - \$HOME/.procmailrcとcronの設定
- /etc/aliases にて別名に対して一括してabmailでスパムを隔離する場合に必要なもの
 - root権限およびスパム用隔離フォルダ
 - /etc/aliasesとcronの設定

他にもいろいろな運用方法があるでしょう

abmailsreport まとめ

スパムは、毎日数百通も受信している人で、一年溜めておくと1ギガにもなります。

多数のアカウントを抱えていて、かつ、abmailによりスパムを隔離する場合、十分なストレージが必要となります。

環境に合った間隔で、定期的に隔離フォルダを削除するとよいと思います。

毎日数十通以上のスパムを受信している方は、abmailで日々のメール処理の負担が著しく軽くなり、加えて、abmailsreportで稀にあるかもしれない偽陽性の誤判定への対処方法が提供され、その上、スパム対策の効果もユーザに明らかで、「安心・簡単」と好評です。