+abmail
迷惑メール対策サービス

迷惑メール判定プログラム「abmail」による
スパム対策の導入のすすめ

株式会社あいはら 研究開発チーム
山田 泰司

迷惑メールの傾向

- 本文における文字列判定、統計的判定を回避
  - 希有なエンコーディング、画像スパム
- 画像スパムのシグネチャマッチング等を回避
  - ノイズ付加された画像、機械難読化された画像
- ボットとして操られているパソコンから送信
- 脆弱性をもつ各種サーバ、ネット家電から送信
- インターネット発展途上国から大量に送信
- greylisting, tarpitting の回避
  - 再送要求、遅延応答に対応したスパム送信エンジン

迷惑メールの現状
１．正当なメールが一日に８０通ほどのユーザの場合

- メーリングリスト、メールニュースを多用
- メールアドレスが公知
- ウイルス付きメールも多量に混在

2006/11/02～
2007/02/15　　105日間のメール受信ログ

	受信数	受信数/総数	受信数/日数
ウイルス	24462	0.398	232.971
スパム	28904	0.470	275.276
その他	8075	0.131	76.905
総数	61441	1.000	585.152

- **９割近くものメールが迷惑メール！**

迷惑メールの現状
２．正当なメールが一日に２０通ほどのユーザの場合

- いくつかのメールニュースを利用
- メールアドレスが公知
- ウイルス付きメールは比較的少ない

2006/06/13～
2007/02/15　　247日間のメール受信ログ

	受信数	受信数/総数	受信数/日数
ウイルス	237	0.007	0.960
スパム	27526	0.821	111.441
その他	5760	0.172	23.320
総数	33523	1.000	135.721

- ８割以上ものメールが迷惑メール！

迷惑メールの現状
3．よく使われるアカウント名（例：webmaster@～）の場合

- メーリングリスト等は未使用
- メールアドレスが公知
- ウイルス対策をメールサーバにて実施

2006/11/02～
2007/02/15　　105日間のメール受信ログ

	受信数	受信数/総数	受信数/日数
ウイルス	6771	0.734	64.486
スパム	1991	0.216	18.962
その他	459	0.050	4.371
総数	9221	1.000	87.819

- **９割以上ものメールが迷惑メール！**

迷惑メール対策の必要性

- 一日に２０通以上の迷惑メールを受信しているユーザは、迷惑メール対策の導入が必要かと…
  - 返信すべきメールを読まずに放置してしまう、読まずに棄てるべき迷惑メールに騙されてしまう危険性に対する**注意力を日々維持するのは困難**
- 既に既存の迷惑メール対策を導入していても、やはり一日に２０通以上の迷惑メールがすり抜けてくるユーザは、別の迷惑メール対策の検討が必要かと…
  - 既に導入している迷惑メール対策ソフトの管理コストや判定能力は、**システム環境やスパムの本質に適合していますか？**

迷惑メールの特徴
1．偽装したEHLO/HELOで送りつけるスパマー

- EHLO/HELOで送り先ドメインを名乗る

Return-Path: <woman_lovely@mail.goo.ne.jp>
Received: from aihara.co.jp (unknown [219.147.232.208])
　　by mailhost.aihara.co.jp (Postfix) with SMTP id 600CD81578
　　for <taiji@aihara.co.jp>; Sat, 3 Feb 2007 22:07:56 +0900 (JST)
MIME-Version: 1.0
Message-Id: <20070203130756.600CD81578@mailhost.aihara.co.jp>
Content-Type:text/plain; charset="iso-2022-jp"
Content-Transfer-Encoding: 7bit
Subject: 検討して頂けましたか？
From: ハセガワ <woman_lovely@mail.goo.ne.jp>
To: <taiji@aihara.co.jp>

長谷川です。
私の説明わかりにくかったかなと思ったのでもう一度連絡しました！

個別紹介は私が個人的な紹介をするために作ったものだから参加費とかお金は一円も私いらないですからね (^^)
http://www.******** . *** /******** / の説明を見てくれてもわかってもらえると思います。
ただ漠然と紹介するよりちゃんとこういう形で紹介した方が静香さんの事も伝わりやすいと思って作ったんです。

静香さんがには個別紹介で待って貰っていますので、連絡してあげてくださいね。
結局不倫の関係になっちゃうからこういう安心って必要ですよね。

メールボックスを作ればすぐ使えるので静香さん自身が望んでる関係なので２，３お話ししてみて話が合いそうだったら
連絡方法を決めてもいいと思いますよ！

なのでまずは静香さんに連絡してあげて下さいね。どうぞよろしくお願いします。

迷惑メールの特徴
2．エンドユーザ空間から直接送りつけてくるボット

- OP25B が世界的に普及しないと…

```
Return-Path: <cruisequiz@hotmail.com>
Received: from mail.hotmail.com (adsl-70-232-22-193.dsl.irvnca.sbcglobal.net [70.232.22.193])
        by mailhost.aihara.co.jp (Postfix) with SMTP id 0C5AC81519
        for <taiji@aihara.co.jp>; Thu, 15 Feb 2007 14:09:02 +0900 (JST)
Received: (qmail 19021 invoked by uid 0); 15 Feb 2007 04:17:38 -0000
MIME-Version: 1.0
Content-Type: text/plain; charset="iso-2022-jp"
Content-Transfer-Encoding: 7bit
Subject: 心ときめく春をプレゼント
From: "DEAR LOVE" <cruisequiz@hotmail.com>
To: "" <taiji@aihara.co.jp>
Date: 15 Feb 2007 04:17:38 -0000

癒しを求め合う男女・日常を豊かに過ごすために
            〜〜特別無料ご招待のお知らせ〜〜

    もしあなたが
    「日常的に小さな不満を持って日々生活している」のであれば、
    小さな楽しみをプレゼント出来ます。

    もしあなたが
    「理想の出会いを求めていてもなかなか見つからない」のであれば、
    小さなときめきをプレゼント出来ます。

    あなたの生活に変化を与えるために、無料で始める
    http://********.***/********/
```

迷惑メールの特徴
3．逆引き不能なIPアドレスから送りつけてくるスパマー

- 正当なメール送信サーバならまずあり得ない

```
Return-Path: <lilicube_28493@yahoo.co.jp>
Received: from pc52 (unknown [222.127.4.237])
        by mailhost.aihara.co.jp (Postfix) with SMTP
        id 4D0ED813B8; Thu, 15 Feb 2007 03:39:17 +0900 (JST)
MIME-Version: 1.0
Content-Type:text/plain; charset="iso-2022-jp"
Content-Transfer-Encoding: 7bit
Subject:  【秘密】必ずご確認下さい
From: lilicube_28493@yahoo.co.jp <lilicube_28493@yahoo.co.jp>
To: undisclosed-recipients:;
Date: Wed, 14 Feb 2007 20:46:24 +0900
Reply-To: <lilicube_28493@yahoo.co.jp>

提携サイト様より、数人の女性の紹介依頼を承っています。
その中であなた様の好みに合いそうな女性を、
今回ご紹介させて頂きたいと思います。

以下ＵＲＬよりアクセス後、ご連絡を望まれる場合は、
メールアドレスの登録が必要となっております。
もし他の女性を希望される場合、今しばらくお待ち下さい。

        http://********.***/********.php
```

迷惑メールの特徴
4．自分は送ってないメールの不到達通知を送る正当なMTA

- 詐称されたメールアドレスによる偽のバウンス

```
Return-Path: <>
Delivered-To: taiji@aihara.co.jp
Received: by mailhost.aihara.co.jp (Postfix)
        id 7578481374; Mon, 29 Jan 2007 18:22:57 +0900 (JST)
MIME-Version: 1.0
Content-Type: multipart/report; report-type=delivery-status;
        boundary="976108135B.1170062577/mailhost.aihara.co.jp"
Subject: Undelivered Mail Returned to Sender
From: MAILER-DAEMON@aihara.co.jp (Mail Delivery System)
To: taiji@aihara.co.jp
Date: Mon, 29 Jan 2007 18:22:57 +0900 (JST)

        :
<joe@aihara.co.jp>: unknown user: "joe"
        :
Received: from aihara.co.jp (unknown [66.36.213.1])
        by mailhost.aihara.co.jp (Postfix) with ESMTP id 976108135B
        for <joe@aihara.co.jp>; Mon, 29 Jan 2007 18:19:07 +0900 (JST)
MIME-Version: 1.0
X-Priority: 3
X-MSMail-Priority: Normal
Subject: Jlcbyjuvsknu
From: taiji@aihara.co.jp
To: joe@aihara.co.jp
Date: Mon, 29 Jan 2007 23:20:56 -0800
Content-Type: multipart/mixed;
        boundary="----=_NextPart_000_0011_F69A8AB6.6B2A41AA"

        :
```

これまでの迷惑メール対策

- 送信者フィルタ型

  詐称可能な情報を判定基準にするのはどうか…

- メール本文検査型
  - ウイルス検知
  - 広告検知、ベイズ推定、シグネチャマッチング

    最近はあまり効果がなく、イタチごっこの様相…

- アドレス管理型、 MTA 検知型
  - RBL(Real Time Black List)
  - greylisting, S25R(Selective port 25 Rejection), Rgrey, tarpitting, taRgrey
  - SPF(Sender Policy Framework), DomainKeys

これからの迷惑メール対策

- **詐称しやすい情報による判定は行わない**

  詐称するコストが高い情報に着目する

- **メール本文も走査しない**
  - ベイズ推定法を回避するスパム…
  - 画像シグネチャマッチングを回避する画像スパム…

  本文を走査しても検査コストが増大していくだけ

- 遅延、受信拒否など**敵に気付かれる手法は排除**
  - メールサーバとしては「来るものは拒まず」
    - スパムは削除、隔離、分類、いずれかの方法でエンドユーザの負担とサーバの負荷を緩和することが肝要
    - スパマーが効果低下に気付くまでの時間を稼ぐ

abmail による迷惑メール判定
1．受信メールの経路情報から判定

- アドレス空間のブラックリスト
  - スパマーやボットの巣窟となるアドレス空間を排除
- ドメイン名のブラックリスト
  - エンドユーザアドレスのボットネットを排除
  - クラックされている MTA 等を排除
- アドレス空間のホワイトリスト
  - 自ドメインやメール転送元となっている MTA
  - 動的アドレス空間上の自前 MTA を救済
- ドメイン名のホワイトリスト
  - エンドユーザアドレスではない正当な MTA を救済

abmailによる迷惑メール判定
2．偽のバウンスにおいても経路情報から判定

- メールに添付されたバウンスレポートのメールヘッダから、詐称されたメールアドレスからの迷惑メールのバウンスメールであることを判定
  - 自分が相手先アドレスを間違って送ってしまったバウンスと偽のバウンスとの判別が可能

バウンスではないスパムとほぼ同等の判定能力

但し、稀に適切なバウンスレポートを添付してくれないMTAが世の中には存在し、判定不能となる

abmail による迷惑メール判定
3．偽装された情報から判定

- EHLO/HELO における偽装
  - 宛先のドメイン名で偽装
  - 宛先のドメインのアドレスで偽装
  - プライベートアドレス空間で偽装

偽装が明らかなので、まず誤判定がありえない

abmail による迷惑メール判定
4．逆引き不能による判定と救済措置

- 逆引き不能な MTA は、まずスパマーである

  たまたま逆引きが不能なケースが、稀にあり得る

  – 隔離されたスパムを時間差で改めて逆引きすることで、誤判定を救済することも可能

  DNS サーバへの負荷を考慮するなら、隔離もしくは分類されたスパムをエンドユーザが確認できる環境であれば、救済措置は必ずしも必須ではない

abmail による迷惑メール判定
5．RBL による判定と救済措置

- RBL を併用するとブラックリストの管理が軽減

  しかし RBL による誤判定も往々にしてあり得る

  – 隔離されたスパムを時間差で改めて検査することで、誤判定を救済することも可能

  DNS サーバへの負荷を考慮するなら、隔離もしくは分類されたスパムをエンドユーザが確認できる環境であれば、救済措置は必ずしも必須ではない

  信頼性の高い RBL を利用し、オープンリレーのまま放置されている管理が不適切な MTA を簡便に排除することが目的

abmail による迷惑メール判定
6．ウイルス対策ソフトとの併用

- ウイルス対策ソフトを併用すると隔離スパムメールボックスの容量が低減

  隔離もしくは分類されたスパムをエンドユーザが確認している場合、その人的コストも軽減

  – 併用しない場合、大部分のウイルスをスパムと判定

  しかし最近は、ウイルス対策ソフト自体の脆弱性を狙われる事態もあり得るので、ウイルス対策ソフトの適切な運用が肝要

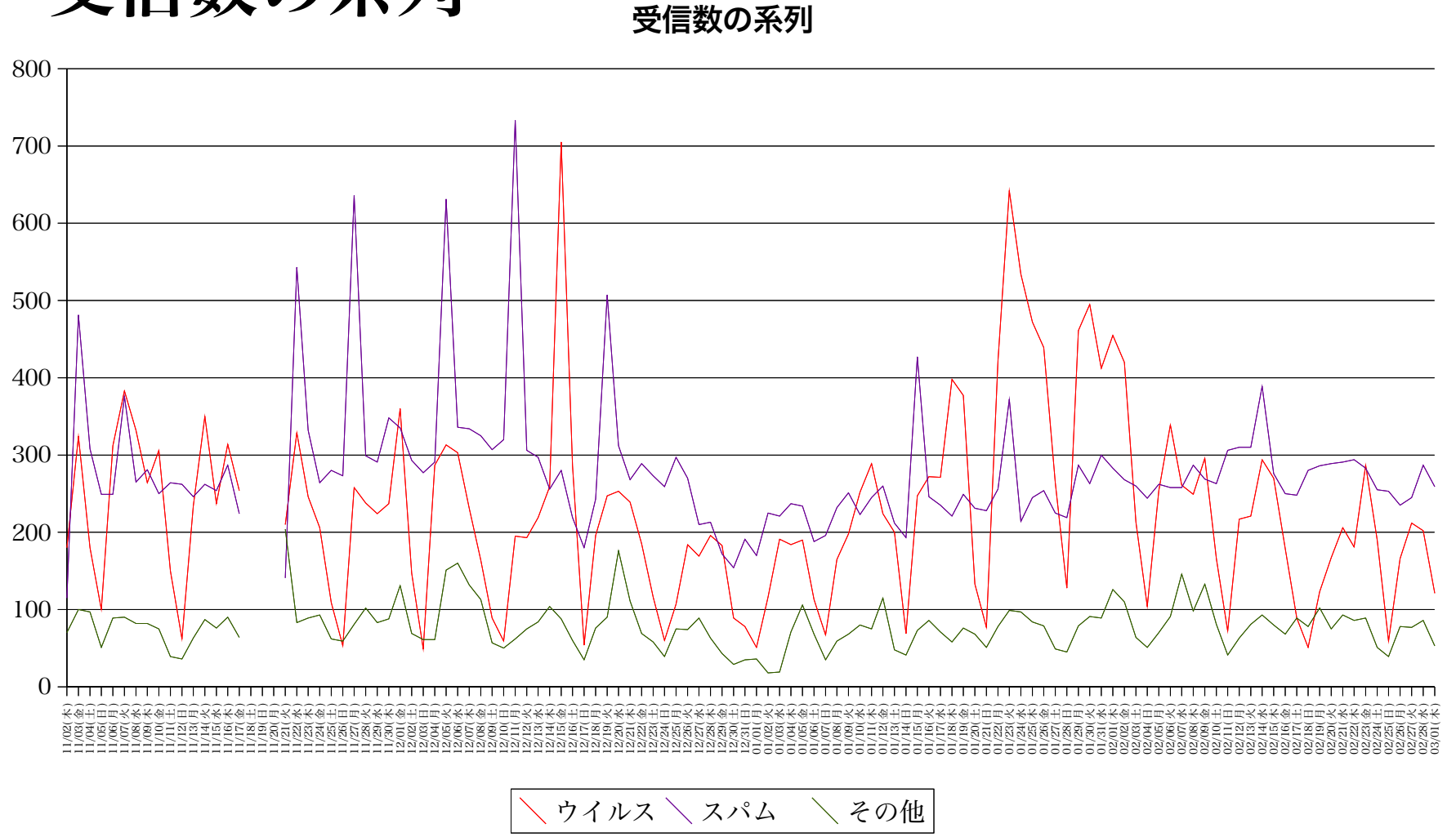
abmail による迷惑メールの現状
１．正当なメールが一日に８０通ほどのユーザの場合

- 105 日間の受信メールの内訳

種類	受信数	受信数/日
ウイルス	24462	232.971
不正なEHLO/HELO	199	1.895
偽装されたEHLO/HELO	6811	64.867
エンドユーザアドレス空間	21603	205.743
信頼できないアドレス空間	13	0.124
RBLに登録されたアドレス空間	190	1.810
不正なバウンスレポート	88	0.838
その他	8075	76.905
総計	61441	585.152

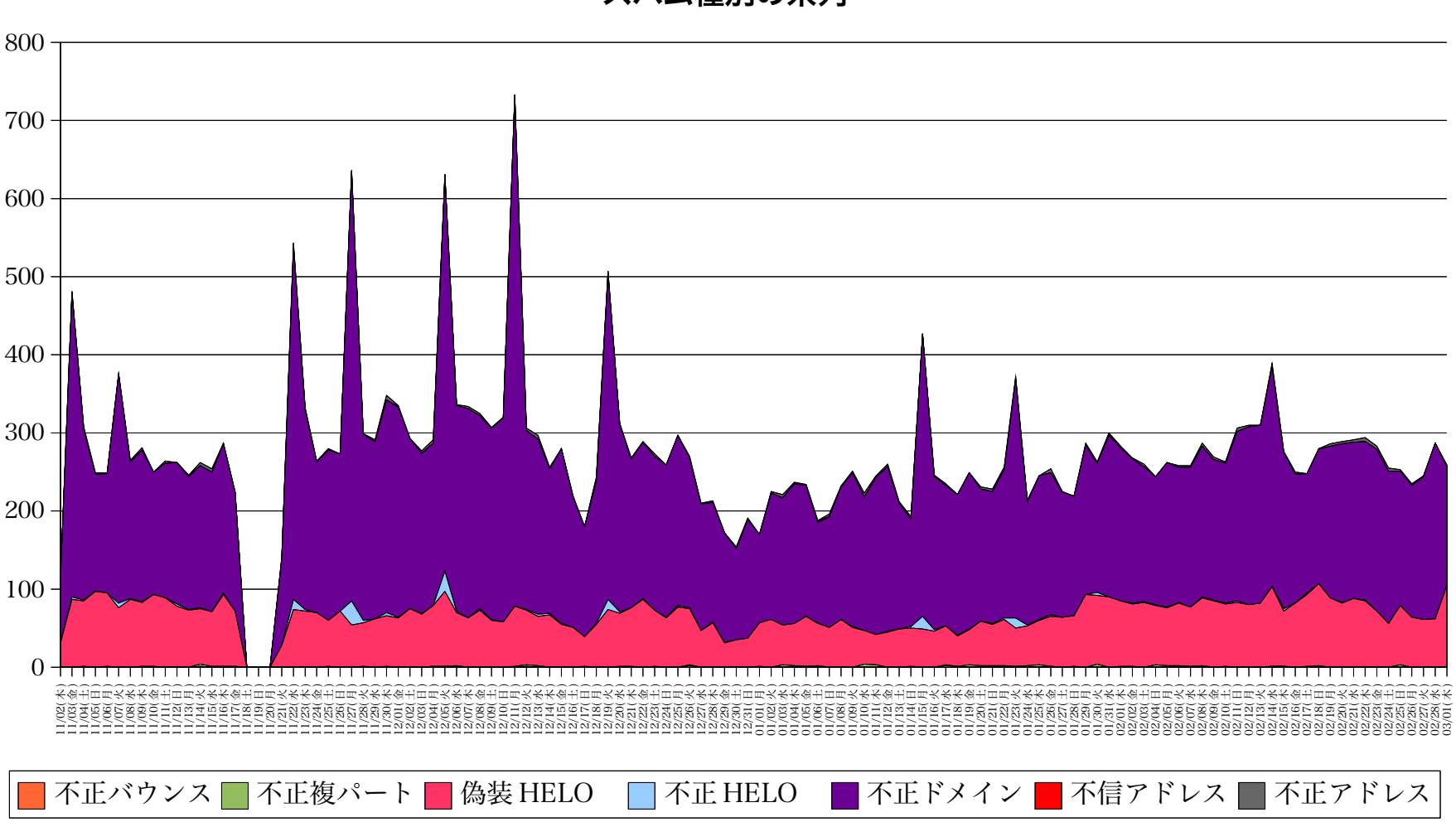
abmail による迷惑メールの現状
１．正当なメールが一日に８０通ほどのユーザの場合（続き）

- 受信数の系列



abmail による迷惑メールの現状
1．正当なメールが一日に８０通ほどのユーザの場合（続き）

- スパム種別の系列



abmail による迷惑メールの現状
２．正当なメールが一日に２０通ほどのユーザの場合

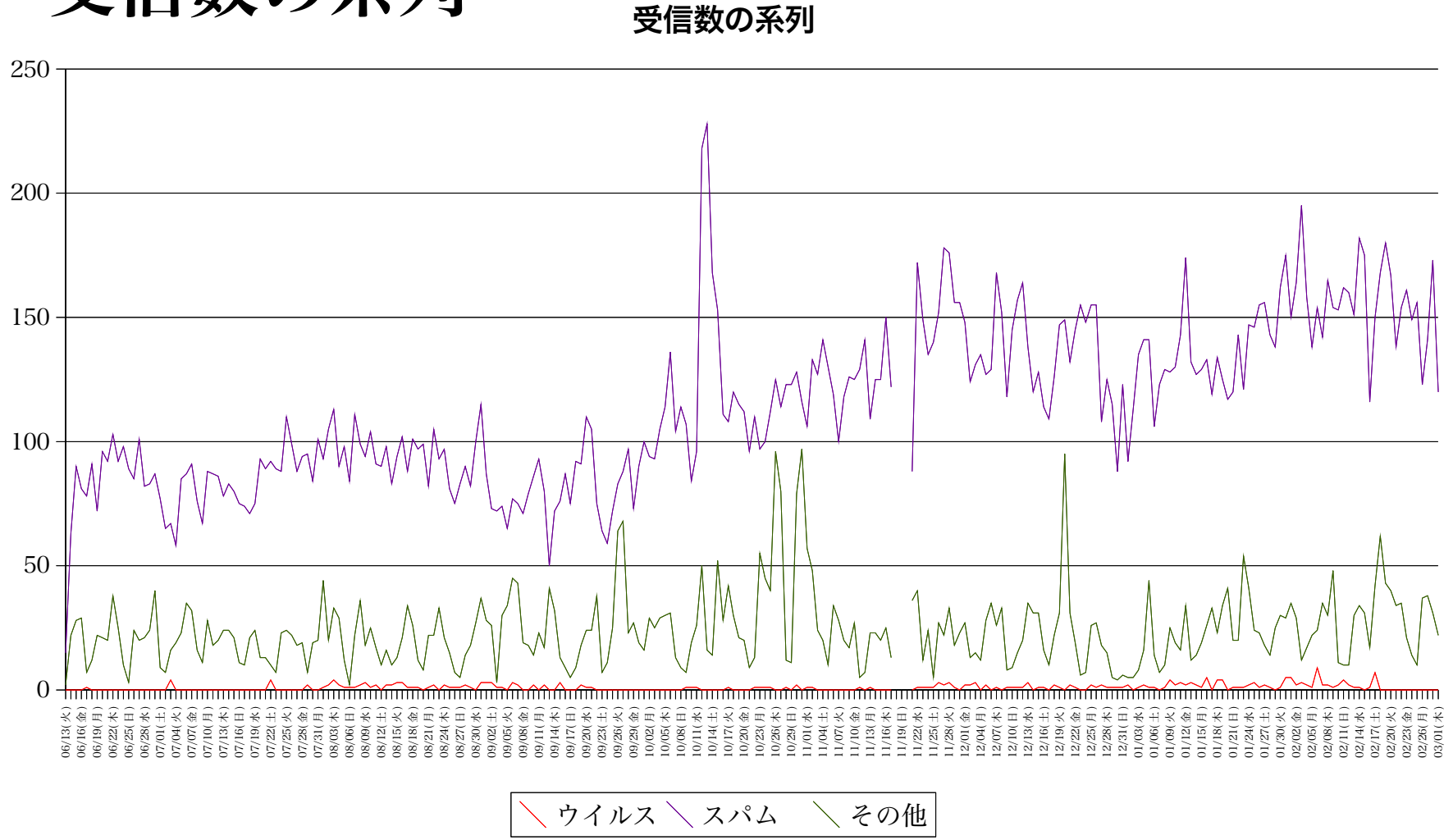
- ２４７日間の受信メールの内訳

種類	受信数	受信数/日
ウイルス	237	0.960
不正なEHLO/HELO	91	0.368
偽装されたEHLO/HELO	7565	30.628
エンドユーザアドレス空間	19470	78.826
信頼できないアドレス空間	142	0.575
RBLに登録されたアドレス空間	257	1.040
不正なバウンスレポート	1	0.004
その他	5760	23.320
総計	33523	135.721

abmail による迷惑メールの現状

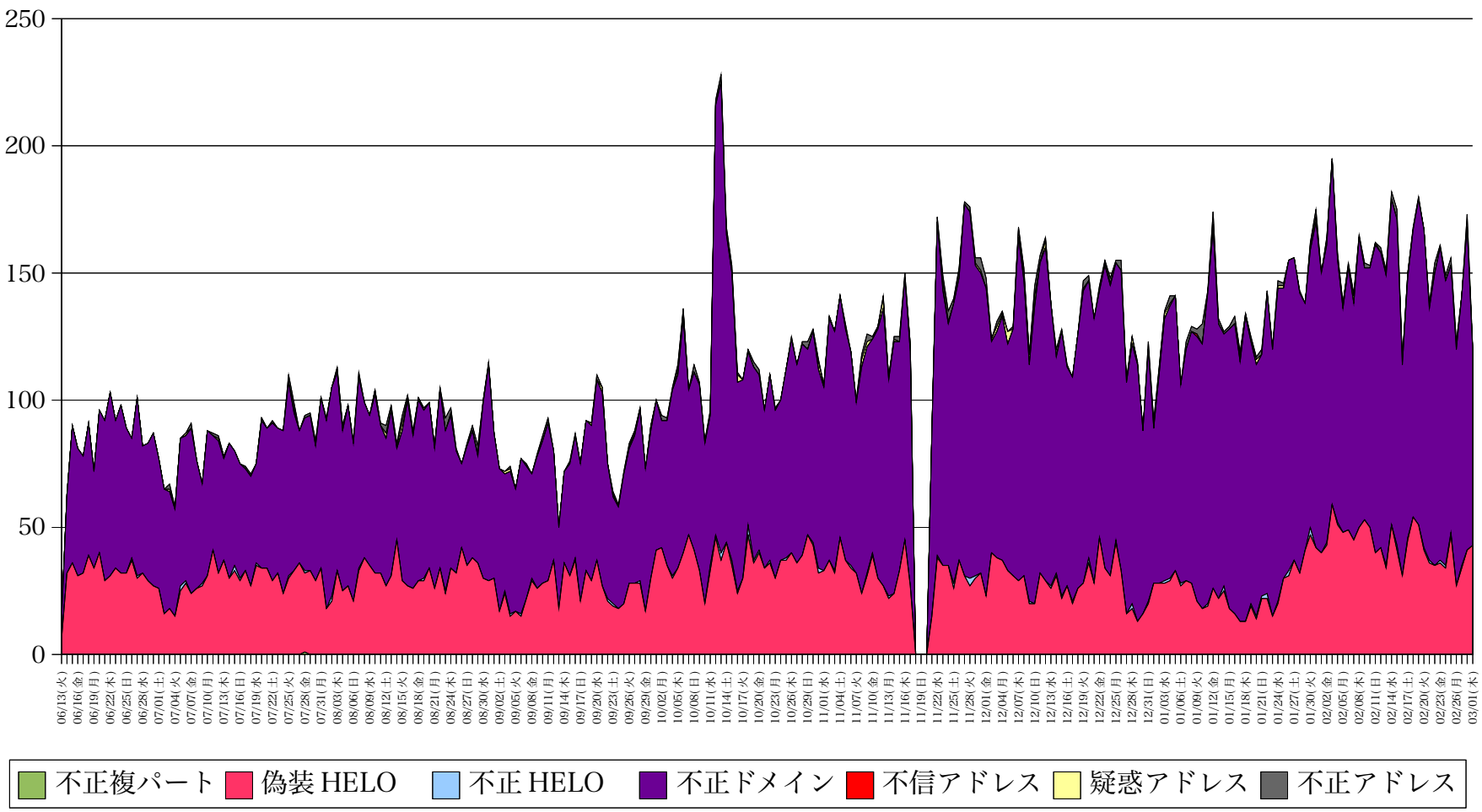
２．正当なメールが一日に２０通ほどのユーザの場合（続き）

- 受信数の系列



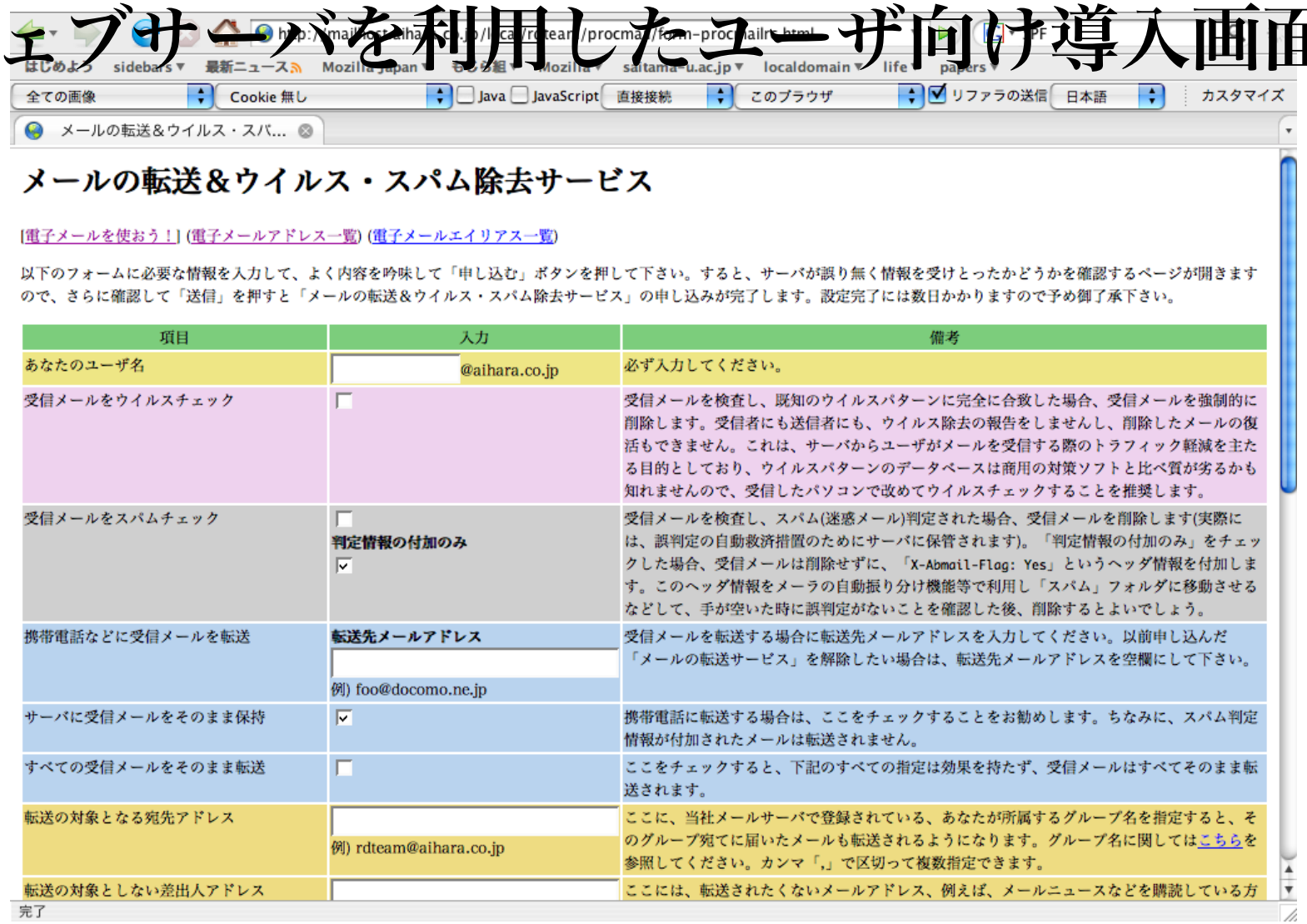
abmail による迷惑メールの現状
２．正当なメールが一日に２０通ほどのユーザの場合（続き）

- スパム種別の系列



導入事例
1．+abmail によるスパム除去サービス

- ウェブサーバを利用したユーザ向け導入画面



導入事例
2．+abmail によるスパム判定サービス

- メーラの自動振り分け機能での利用例

導入事例
3．+abmail によるスパム除去サービス

- メールサーバ管理者向け設定例

  postfix|sendmail+procmail+abmail

```
MAILDIR=$HOME/Mail

:0
* SW_ANTISPAM ?? ^^^^
{
  SW_ANTISPAM=on
}

:0
* SW_ANTISPAM ?? on
{
  ANTISPAMDIR=spam-`date +%Y%m%d`
  :0 HB
  * ? abmail -b -g -d -v; test "$?" = "1"
  ${ANTISPAMDIR}/.
}
```

abmail による迷惑メール判定
7．偽陽性に対する姿勢

- 偽陽性（正当なメールを誤判定してしまう）は極力なくすべき

  しかし、S25R のように送信元の MTA に高負荷を強いてまで偽陽性の緩和をすることは甚だ疑問

  - 実は、隔離されたスパムメールボックスに稀にあるかもしれない「正当なメール」をユーザが見つけることは意外と容易い

    逆に、正当なメールの中から人間がスパムを判別して棄てることは、かなり難しい

- ユーザの傾向に合わせて設定が熟れてくれば、偽陽性をほぼ零にすることが可能
  - 例： 105 日間で偽陽性は 1 通

+abmail のまとめ

- セキュアコーディングされた「abmail」
  - 安全な迷惑メール対策
- 極めて軽量な「abmail」によるヘッダ走査
  - 高速な迷惑メール対策
- 厳格なスパム判定基準に基づく「abmail」
  - イタチごっこになり難い迷惑メール対策

但し、特に初期導入時に、ホワイトリスト・ブラックリストの設定・管理、サーバ環境に応じたチューニングは必要

迷惑メールに困っている方は是非 rdteam@aihara.co.jp へ