

メールゲートウェイにおける spam 対策について

吉田 和幸[†]

†大分大学総合情報処理センター 〒870-1192 大分市旦野原

E-mail: †yoshida@csis.oita-u.ac.jp

概要 近年,いわゆる spam メールに加えて,大量のメールを送るマスメール型と呼ばれるコンピュータウイルスやフィッシング詐欺を狙ったメールが増えている.これらの対策のため,大分大学では学内と学外との境界に置いたメールゲートウェイで,2003年2月に統合メール管理システム,2003年11月に spamassassin,2004年4月に greylisting を導入し,2005年1月から sendmail の新たな機能である greet pause 機能を用いて spam メールを拒否するようにしている.本稿では,spam メール対策の方針,および greet pause 機能を中心に運用経験について述べる.

キーワード spam 対策,メールゲートウェイ, sendmail

Measures Against *spam* on Mail Gateway

Kazuyuki YOSHIDA[†]

† Information Processing Center, Oita University DannoHaru, Oita, 870-1192 Japan

E-mail: †yoshida@csis.oita-u.ac.jp

Abstract In recent years, the number of spam mails is increasing rapidly. Mails with computer viruses called mass mail type and mails which are watching for phishing attacks are also increasing. As measures against these spam, we introduced a Mail Account Management System on February 2003, spamassassin on November, 2003 greylisting on April, 2004 and greet pause feature for sendmail in January 2005, and combining them with sendmail on border mail gateway between Oita University's LAN and the Internet. In this paper, I describe the plan of the measure against spam mail, and employment experience.

Keyword measure against spam, mail gateway, sendmail

1. はじめに

近年, spam の増大が問題になっている. spam は,受信者の興味等に関係なく無差別に送られてくる受け取りたくないメールのことで, UCE (Unsolicited Commercial E-mail), UBE (Unsolicited Bulk E-mail)とも呼ばれる. この中には, phishing 詐欺を狙ったものも増えている. さらに, マスメール形のコンピュータウイルスがばら撒くウイルス付きのメールも spam に含めることも多い. spam の送信者アドレスは, 一般に偽装していることが多いため, spam を一旦受信してしまうと, エラーメールを返すことができず, あるいは, エラーメールを送信できたとしても, 実際の送信者ではなく, 関係ない第三者に送られることになる. spam 送信者側からみると, メール配送が成功したことになり, 再度同じアドレスに spam を送ってくるかもしれない. このように spam は, 受け取ってしまったら負けとなる.

大分大学では, ウィルスを検出・除去するためのメールゲートウェイを導入し, 学内 LAN とインターネット

との間を行き来するメールについてウィルスの有無を検査している^{1),4)}. そのメールゲートウェイ上で, (1)送信メールサーバの IP アドレス, およびメールヘッダの形式の検査¹⁾, (2)統合メール管理システムによる学内各メールサーバのアカウントの有無の検査^{1),2),3),4)}, (3)spamassassin⁵⁾によるメールの内容の検査⁶⁾, (4)greylisting^{7),8)}による送信メールサーバの検査^{9),10)}, (5)sendmail8.13¹¹⁾の新しい機能である greet pause 機能を組み合わせて, spam メール侵入を防いでいる.

本稿では, これらの spam メール対策の概要, 運用方針, 運用経験について述べる.

2. spam 対策

2.1. メールヘッダの検査

spam メールは, ヘッダ情報が不完全なものも多いので, まずは, 以下のようなメールの形式検査により, spam メールを受信しないようにしようと考えた.

(1) Message-ID:, From:各ヘッダの形式が <ローカル部@ドメイン部>の形式になっていないメールは拒否

する。

(2) 送信元、あて先の各メールアドレスのドメイン部(「@」より右側の部分)について、DNSを検索して存在しない、あるいは、検索した結果が127.0.0.1である場合は拒否する。

(3) ORDB¹²⁾等の不正中継サーバ、spamメール送信サーバのBlack List(Blocking List)を参照し、送信メールサーバのIPアドレスがこれらのDBに登録されていれば受信を拒否する。

2.2. 統合メール管理システム

メールゲートウェイには、一般にユーザを登録しないので、インターネットから受け取ったメールの宛先が実在するかどうかは、受け取った時点では、わからず、ウイルス、spamの検査後、学内に配送しようとする段階で宛先メールアドレスの有無がわかる。存在しない場合、メールゲートウェイは送信者に対して「User unknown」のエラーメール(bounce mail)を送る。spamメールでは、送信者アドレスの欄を偽装していることも多い。そのような場合、無関係な第三者に bounce mail を送ることになり、結果的に spam 送信を助長することになる^{4),20)}。そのため、LDAPサーバを用いて学内のメールアカウントを集中管理する統合メール管理システムを導入し、メールゲートウェイからもLDAPサーバにメールの宛先が実在するかどうか問い合わせができるようにした^{1), 2), 3),4)}。

2.3. Spamassassin

spamassassin⁵⁾は、メールヘッダやメール本体を解析することによって、spamメールを検出するフリーソフトである。その検出方法の概略は以下のとおりである。

(1) メールの received:ヘッダにあるメール中継サーバのIPアドレスが、OpenRelayサーバ、OpenProxyサーバ、spam送信サーバ等のリストに載っているかどうか、Subject:ヘッダについては、字種はASCII文字のみであるか、あるいは特定の単語を含んでいないか、といった規則を適用し、適合した規則に対応するスコアを与える。

(2) スコアの合計が、あらかじめ決めた値以上になると、spamメールであると判断する。

規則の中には、spamメールに出てくる単語、spamでないメールに出てくる単語をそれぞれ蓄えておき、検査すべきメールの単語と、それらと比較してBayesian確率を計算し、スコア値に換算する規則もある。

大分大学では、以下のような運用方針で、2003年11月から試験運用し、同年12月から本格運用に入った

6)。

(1) spamassassinが、spamメールだと判断しても、実際には拒否せず、spamメールであることを示す"[SPAM]"をSubjectヘッダに追加して、宛先に送る。廃棄するかどうかの判断は、受信者が行なう。

(2) spamメールは、送り手アドレスを詐称していることが多く、一度、受け取ってしまうと、エラーメールを送ることもできず、送り手に受け取らないことを伝えることができない。そのため、「spamに間違いなし」と確信がもてる場合には、送信元に対し、「spamメールなので拒否」のエラーコードを戻す。ただし、そのメール自身は、配送するspamassassinのmilterインターフェースであるmilter-spamcの機能を使用している¹⁰⁾。

(3) spamでないメールに対して、spamと誤検出(false positive)することは、影響が大きいので、なるべくこのような誤検出は避けるようにする。逆にspamメールの検出漏れ(false negative)は、ある程度、許容する。

2.4. Greylisting

spamメールを送信するメールサーバは、特定の個人に確実にメールを送りたいというよりは、大量のメールを短時間に送信したいため、送信先のメールサーバの一時エラーに対しては、たぶん、再送処理を行なうより、他のメールサーバにメールを送ることを優先している。Greylistingは、このことを利用して、内容を見ないで、spamメールと通常のメールを分ける方法の一種である^{7),8),17)}。

Greylisting方式では、メールを受信すると、まずメールサーバのIPアドレス、送信者、受信者のメールアドレスの3つを一組にして記憶し、(本文を受け取る前に)一時エラーを返して、再送を要求する。すぐに、再送されるメールは、spamの可能性が高いので、さらに、一時エラーにする。通常は、15分から1時間経過後に再送されるので¹⁸⁾、先ほど記憶していたIPアドレス、送受信者のメールアドレスと照合して、再送されたメールであれば、通常通り受信する。このように、一旦受信すれば、信用できるメールサーバとして、しばらくは無条件で受信する。この時間関係を図1に示す。現在は、再送受付開始を7分55秒、greylist状態時間切れを24時間、autowhite状態時間切れを14日間としている。適当に流量があるメールリストでは、常にautowhite状態を維持し、遅れ無しに受信することができる。

大分大学では、2004年4月から試験的に導入し、6月から本格的に運用している^{15),16)}。

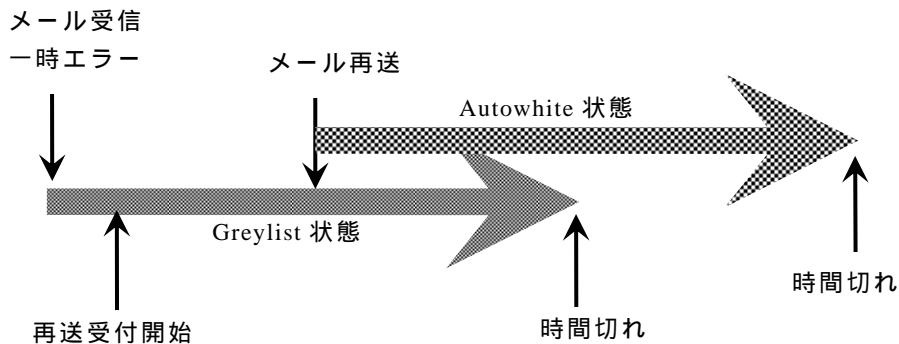


図 1 Greylisting の時間パラメータ

220 ajimu.net.oita-u.ac.jp ESMTP Sendmail 8.13.4/050401; Tue, 5 Apr 2005 12:20:29 +0900

図 2 . greeting message

554 S.D.U ESMTP not accepting messages

図 3 . error message from greet_pause

2.5. greet pause

Greylisting と同様に、内容を見ないで、spam メールを送信するメールサーバを見分ける方法である。大量のメールを短時間に送信したい spam 送信サーバは、宛先のメールサーバの応答が遅い場合、応答を無視してメール配送の手順を進め、あるいは、メールの配送をあきらめて、接続を切断する。sendmail の greet_pause 機能は、このような通常のメールサーバの動作¹⁸⁾とは異なる動作を検出し、spam の受信を拒否しようとする機能である。

greet_pause 機能では、メールサーバ間で TCP コネクションが、確立した後、受信側のメールサーバが図 2 のような greeting message を送る前に指定された時間待つ。greeting message を送る前に、送信側メールサーバから、SMTP コマンド等、何らかのデータが送られてきた場合、図 3 のようなメッセージを送り、それ以降のメールの配送を拒否する。

sendmail は、相手のメールサーバの IP アドレスとドメイン名を用いて、greeting message を送るまでの時間を決める。

現在以下のように設定している。

- (1) whitelist を検索する。見つかると、800 ミリ秒待って、応答をする。whitelist に存在する正常なメールサーバに対しても、少し待つようにしているのは、メールマガジン等同時に多数の受信者に送られてくるメールに対して、受信メールサーバが過負荷にならないように文字通り throttling するためである。
- (2) 外部のデータベースを利用して spam 送信者らし

いサーバ、ダイナミック IP アドレスを検索し、見つければ、それぞれ 60 秒(6 万ミリ秒)、50 秒待って、応答をする。さらにドメイン名の部分が [IP アドレス] の形式になっているかどうか検査している。この形式になっていれば、逆引きが DNS に登録されていないアドレスである。このようなメールサーバに対しては、50 秒待つ。

- (3) その後常時接続らしいいくつかのドメインの検査をし、50 秒ほど待つ。
- (4) すべてに失敗すると普通のメールサーバである。IPv6 では、10 秒、IPv4 では 6 秒待って、応答する。greet pause 機能では、受信側で拒否をすることはない。50 秒待ったとしても、以降正常な SMTP の手順が進めば、メールは受信される。20~30 秒程度の待ち時間で、正常なメールサーバと異常なものとを分離できるとの情報もある。

3. 運用

3.1. 適用順序

いろいろな spam 対策を組み合わせる際にそれらを適用する順序によって、spam 検出時に発生するエラーが異なるため、適用順を考慮する必要がある。「User unknown」といった、メールアドレスの有無に関するエラーは、なるべく発生させないようにしたい。内容検査のように CPU パワーを必要とするものは、なるべく後回しにする。greet pause 機能は、当然最初に適用することになり、各ヘッダが送られてくると、それに対する検査が直ちに行なわれる。そのため、現在のところ、greet_pause、送信メールサーバの検査 (Blocking List の参照)、送信元メールアドレス(DSN)、

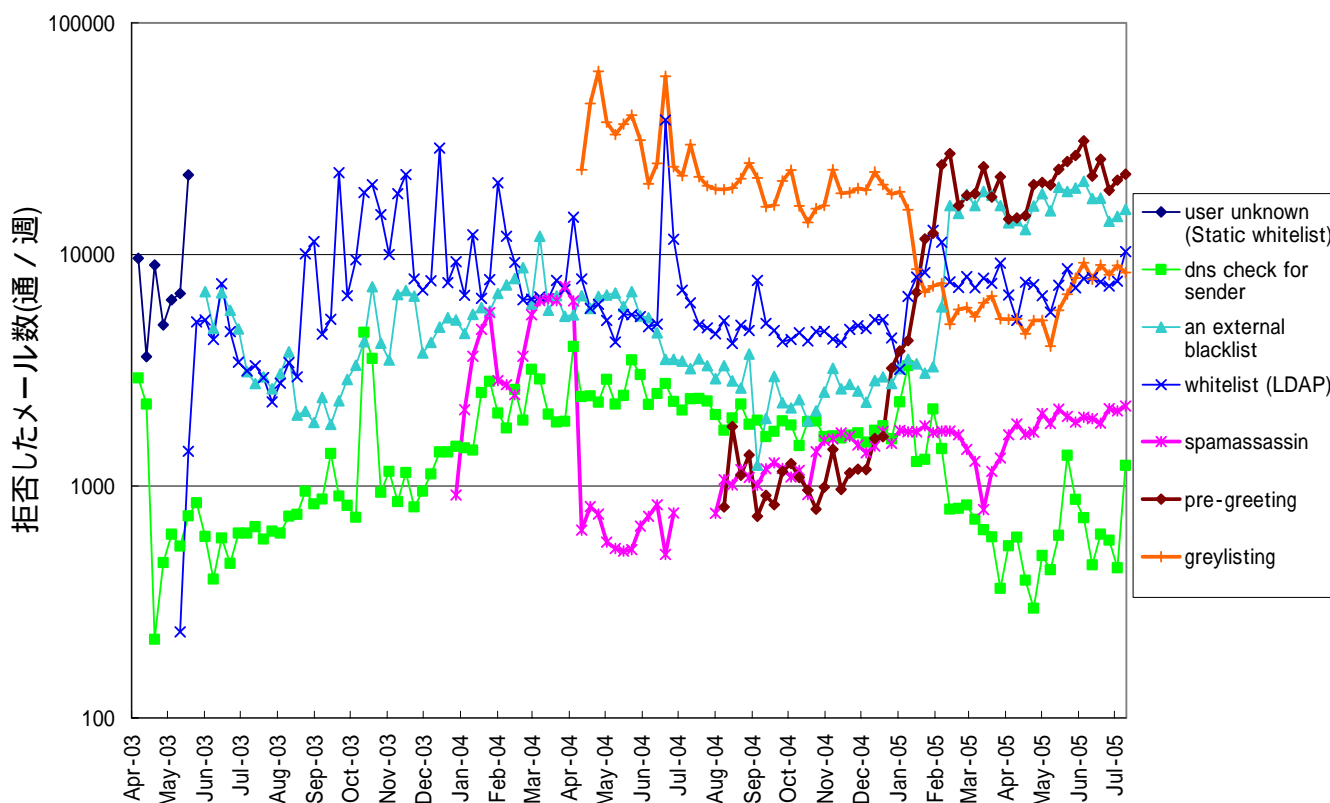


図 4 . 主な spam 対策で受信拒否したメール数

宛先メールアドレス (統合メール管理システム), spamassassin, greylist の順で, 適用している .

3.2. 運用状況

図 4 に主な spam 対策で受信した 1 週間当たりのメール数を示す . 図 5 には , greylist を通過した 1 週間あたりのメール数を示す . 図 5 からは , 毎週 7 万通前後の正常なメールが送受信されていることがわかる . 2004 年 8 月から 12 月までは , greet_pause では , whitelist 検査後 , 一律に 6 秒待つことにしていた . それでも , 毎週 1000 通ほどの spam メールを受信拒否することができた . 2004 年 12 月末から 2005 年 1 月にかけて , greet_pause の設定を修正し , 2.5 節で述べたような設定にした . この過程で greet_pause で検出される spam メール数が 1 週間あたり 2 万通程度に増加し , 同時に greylist の spam 検出数が 6000 通程度に減少した . このことから greylist で検出される「再送処理をしないメールサーバ」の集合と , greet_pause で検出される「greeting message を待つことができないメールサーバ」の集合とは , 大きな共通部分集合を持っていることがわかる .

2 月に spam メール検出のため参照する外部のデータベースの 1 つを xbl.spamhaus.org¹⁹⁾に変更した . このデータベースは , 常時接続の PC で , ウィルス等により

spammer にのっとられた可能性が高いメール送信者 (ゾンビ PC) の IP アドレスを集めたデータベースである . このデータベースを参照することで , spam 検出数が増加する一方 , 同時に , 発信者メールアドレスのドメイン部の DNS 検査 , 宛先メールアドレスの統合メール管理システム (LDAP) での検査で検出される spam 検出数が減少している . ゾンビ PC から送られてくる spam には , 送信者 , 宛先がでたらめなものも多いのであろう .

2005 年 3 月 27 日から 1 週間に受け取った全メール (greet pause で拒否したものを除く) の送信メールサーバの IP アドレス , greet_pause , 外部データベース (spamhaus) , spamassassin , 送信元メールアドレスの DNS 検査 , greylisting の 5 つの検査により検出した spam を送信してきたサーバの IP アドレス , greylisting を通過したメールを送信してきたサーバの IP アドレスそれぞれについて DNS を逆引きし , そのトップドメインで分類した結果を図 6 に示す . 受信したメールのうち 2/3 程度は , jp ドメインのメールサーバからであり (図 6(a)) , greylist を通過した (正常な) メールのうち 8 割程度は , jp ドメインからのものであった (図 6(f)) . greet_pause では , 設定で , 逆引きできない IP アドレスを持つメールサーバに対して , 厳しいルールを課し

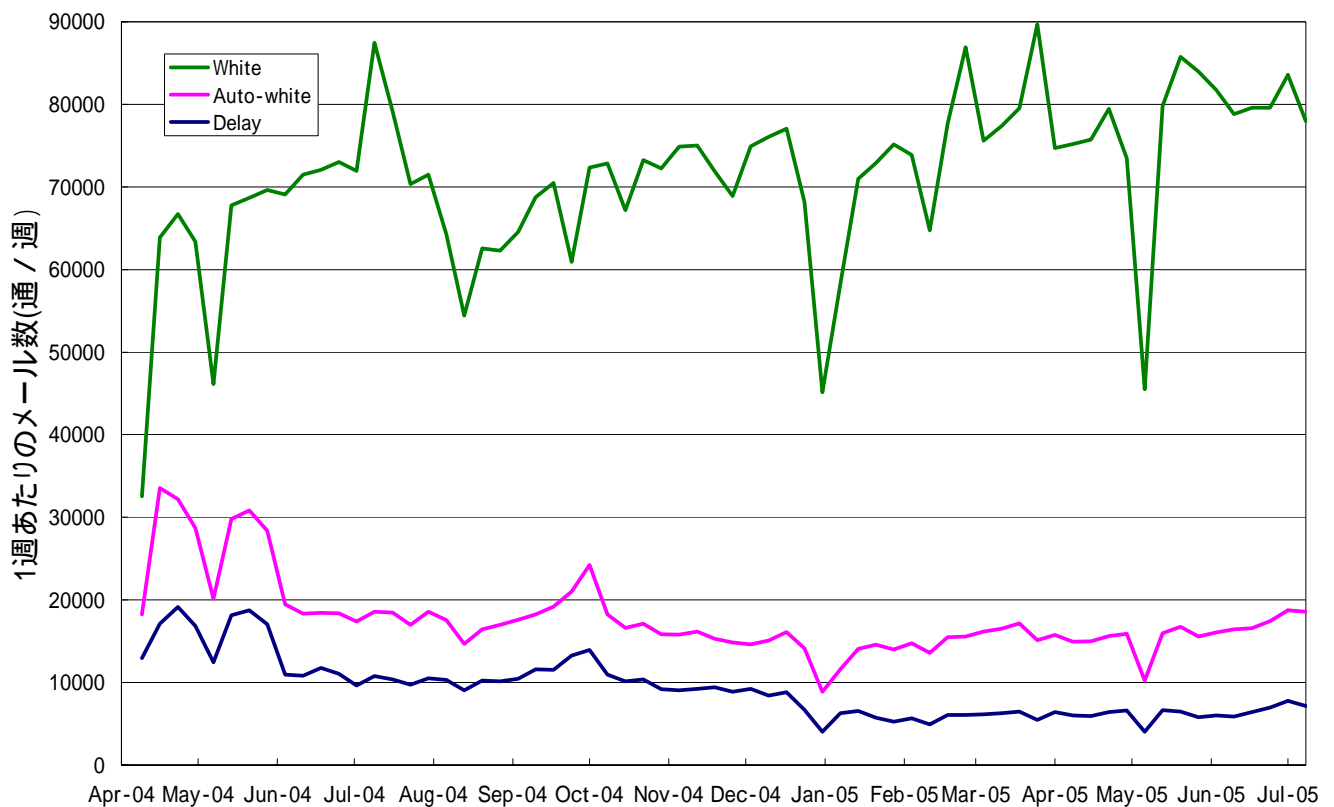


図 5 . Greylist を通過したメール数

ている . このため逆引きできない IP アドレスの spam 送信者の検出数も多くなっている (図 6(b)) . spamhaus による spam 検出でも逆引きできない IP アドレスを持つ spam 送信者が多い (図 6(c)) . これら 2 つで逆引きできない IP アドレスを持つメールサーバからの spam を抑制しているので greylis t で検出した spam 送信者は , 逆引きできないものは少なく , jp ドメイン , com ドメイン , net ドメインに分散している (図 6(f)) . これらに対して , spamassassin による内容検査 , 送信元メールアドレスの DNS 検査で検出される spam の送信者は , jp ドメインが 2/3 ほどあり , 逆引きできない IP アドレスを持つメールサーバの割合は小さい (図 6(c) , (g)) . これらに現れているメールサーバは , spam 送信者というよりは , 中継サーバであろう . 中継を誰にでも許可している open relay なサーバばかりでなく , メールングリストサーバ , 利用者が行なう forward による転送等も含まれる . 中継サーバを経由したメールに対しては , greet_pause , greylis t は , 無力である . このように中継サーバを経由する spam の検出にはヘッダの検査や spamassassin による内容の検査が必要である .

4. おわりに

大分大学におけるメールゲートウェイでの spam メール対策とその運用状況について述べた . 現時点では , greet pause 機能 , greylis t 方式による spam メールの抑制は , サーバの CPU にあまり負担をかけず , 大きな効果があり , spamassassin が , 検出する spam メールの大部分をあらかじめ拒否できている . このことは , 大部分の spam メールが , spam メール送信専用のサーバから送られてくることを表していると考えられる .

greet_pause と greylis t は , spam 送信サーバが , 大量のメールを送ろうとするため , 通常のメールサーバとは異なった動作をすることに注目して , spam 検出を行なおうとするものである . greylis t は , 一旦一時エラーを送って , 再送を待つ方式である . このため , 再送されるまで 30 分程度多く配送に時間がかかる . さらに , 再送されたメールであることを確認するために , メールサーバの IP アドレス , 送受信メールアドレス , 時刻のデータベースを作成する必要があり , そのデータベースのためのメモリー領域を必要とする . このデータベースの保持期間等 , 設定すべきパラメータが多い . 一方 , greet_pause では , 最初の応答まで待つ時間は , 今のところ最大 60 秒で十分効果があがっている . 設定

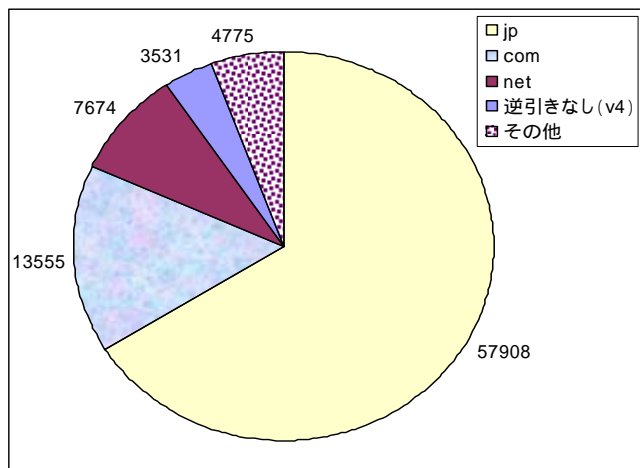
すべきパラメータは、待ち時間のみである。設定すべきパラメータが少ないので、十数行の sendmail.cf への追加で利用可能である。ただし、TCP コネクションを保ったまま待つので、sendmail のプロセス数、TCP セッション数は増えやすい。

検出した spam 送信者の IP アドレスについて DNS の逆引きを検索した結果、greet_pause で検出された spam は、逆引き DSN に登録されていない IP アドレスのサーバから送られてくるものが半分以上を占めていた。一方、spamassassin による内容の検査で検出される spam の送信者は jp, com 等のドメイン名を持つ普通のメールサーバのようであった。メーリングリストサーバや、ISP に持っているメールアドレスから大分大学のメールアドレスへのメールの転送により、spam が来たのだと思われる。このような場合、それぞれのメールサーバの管理者の spam メール対策に期待するほかない。

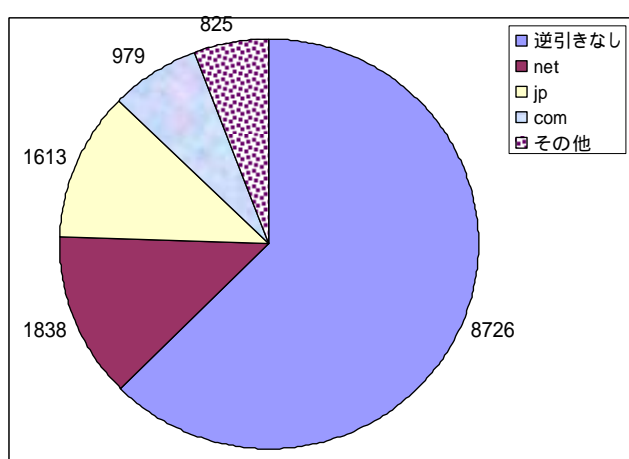
文 献

- [1] 吉田, 矢田, 伊藤: “spam メール対策と統合メール管理システムについて”, 情報処理学会分散システム/インターネット運用技術シンポジウム 2004 論文集, pp.37-42(2004)
- [2] 吉田: “LDAP を用いた統合メール管理システムについて”, 学術情報処理研究 No.7, pp.55-59 (2003)
- [3] 吉田: “統合メール管理システムとその使用経験について”, 大学情報システム環境研究, Vol.7, pp.47-52(2003)
- [4] 吉田, 矢田, 原山, 伊藤: “spam メール対策と統合メール管理システムについて”, 情報処理学会論文誌, Vol.46, No.4, pp.1035-1040(2005)

- [5] Apache Spamassassin Project: “Spamassassin”, <http://www.spamassassin.apache.org>
- [6] 吉田: “メールゲートウェイにおける spam メールの検出について”, 情報処理学会 DICOMO2004 シンポジウム論文集, pp.493-496(2004)
- [7] Emmanuel Dreyfus, “Milter-greylis”, <http://hcpnet.free.fr/milter-greylis/>
- [8] Evan Harris, “greylisting white paper”, <http://projects.puremagic.com/greylisting/whitepaper.html>
- [9] 吉田: “greylisting の運用について”, 学術情報処理研究, No.8, pp.57-62(2004)
- [10] 吉田: “greylisting による spam メールの抑制について”, 情報処理学会分散システム/インターネット運用研究会, 情報処理学会研究報告 2004-DSM-35, pp.19-24(2004)
- [11] sendmail, <http://www.sendmail.org>
- [12] open relay data base, <http://ordb.org>
- [13] J. Klensin, Ed.: “Simple Mail Transfer Protocol”, RFC2821, <http://www.ietf.org> (2001)
- [14] TrendMicro (株): “InterScan VirusWall”, <http://www.trendmicro.co.jp>
- [15] P. Resnick, “Internet Message Format”, RFC2822, [http://www.ietf.org/rfc.html\(2001\)](http://www.ietf.org/rfc.html(2001))
- [16] Anthony C Howe: “milter-spamc”, <http://www.milter.info/milter-spamc/index.shtml>
- [17] spam 対策, <http://moin.qml.jp>
- [18] R. Braden, Ed.: “Requirements for Internet Hosts -- Application and Support”, RFC1123, [http://www.ietf.org/rfc.html\(1989\)](http://www.ietf.org/rfc.html(1989))
- [19] The Spamhaus Project, <http://www.spamhaus.org>
- [20] 山井: パウンスメール対策, 情報処理, Vol.46, No.7, pp.762-766(2005)

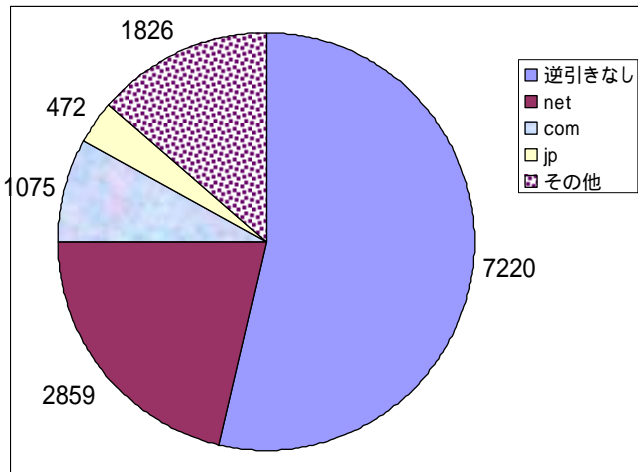


(a) 全メール

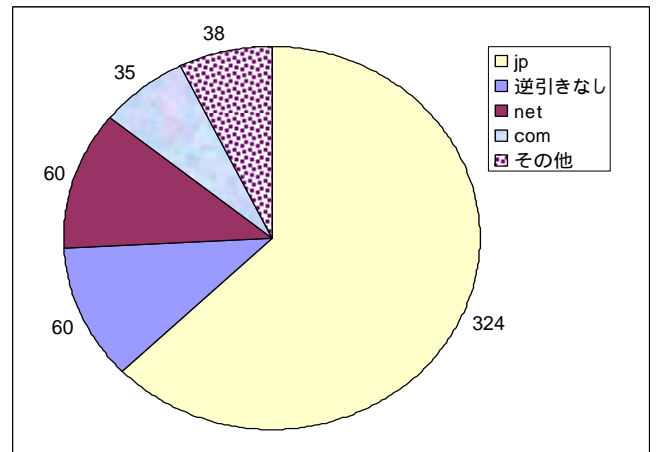


(b) greet pause

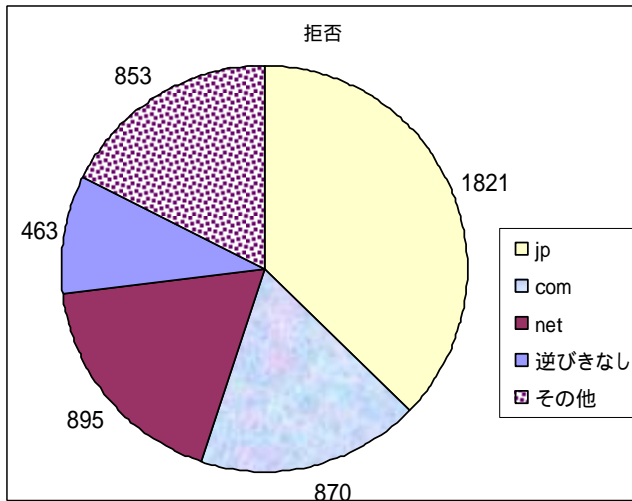
図 6. メール送信サーバの IP アドレスによる分類 (その 1)



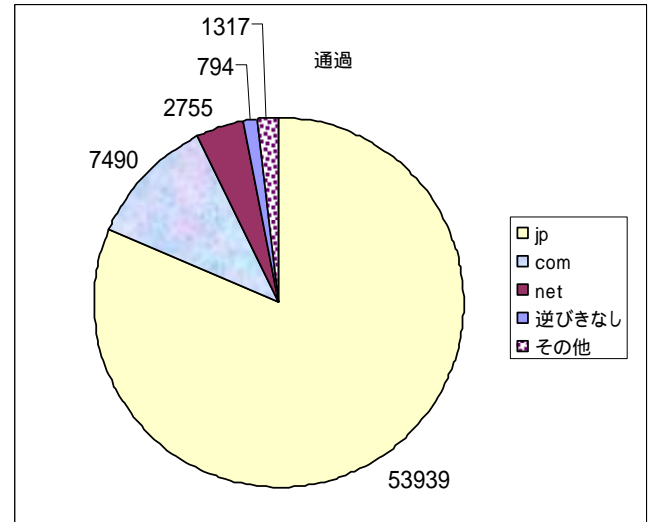
(c) 外部 blocking list(spamhaus)



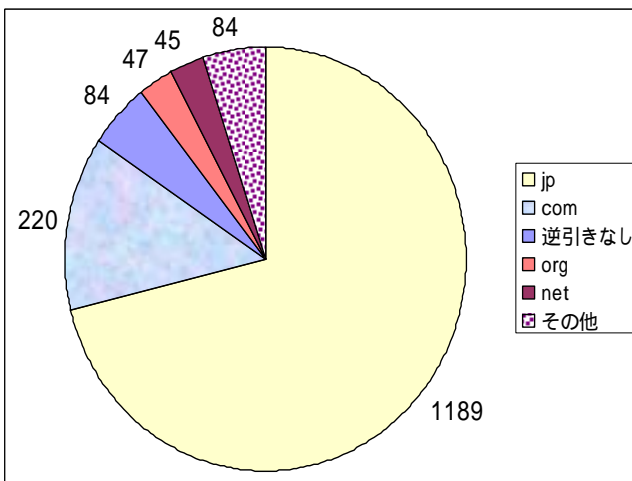
(d) 送信元メールアドレスの DNS 検査



(e) greylist で拒否



(f) greylist を通過



(g) spamassassin

図 6 . メール送信サーバの IP アドレスによる分類 (その 2)