spamメール対策と統合メール管理システムについて

吉田 和幸†, 矢田 哲二†, 伊藤 哲郎†

ウィルスを検出・除去するメールゲートウェイを導入以来、あて先不明のspamメールによるDoS(Denial of Service)攻撃をしばしば受けるようになった。そのため、学内15台のメールサーバのユーザアカウントについてLDAPを用いて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で、そのLDAPデータベースを参照することにより、あて先不明のメールをメールゲートウェイで拒否することができるようにした。本稿では統合メール管理システムの構成と現在までの運用状況について報告する。

A Measure to Counter *spam* Mail and A Mail Account Management System for Mail Servers

Kazuyuki Yoshida†, Tetsuji Yada†, Tetsuro Ito†

We often have DoS (Denial of Service) attacks by wrongly addressed *spam* mail ever since we introduce a mail gateway against computer viruses. Against that attacks, we introduced a mail account management system for 15 mail servers in OUNET(Oita University computer Network). Referring mail account database in that system by LDAP (Lightweight Directory Access Protocol), it is possible to deny the wrongly addressed e-mail on the mail-gateway. This paper shows the structure and utilization of the system.

1. はじめに

本学では、2001年8月にメールのウィルス検出・除去を行うメールゲートウェイソフトウェア（Interscan VirusWall）[1]を導入した。これにより、以降、学内でウィルスに感染するPCは、ほとんどなくなった。学内宛のメールをすべてチェックできるようにするために、インターネットから来るメールは、一旦、メールゲートウェイに集められ、その後、それぞれの最終的なあて先のメールサーバに送られる。しかし、ウィルスをチェックするメールゲートウェイと最終的なあて先のメールサーバが分離されたため、メールアドレスのローカルパート(「@」より左側の部分)がランダムなあて先メールアドレスをもったspamメールを大量に受信することになってしまった。その後、メールの形式検査(to:, from:, message-id:)を強化し、メールサーバにあるユーザアカウントをメールゲートウェイにコピーして、あて先の検査をするようにしたが、それぞれ、運用上の問題があった。そこで、2003年2月のシステム更新にあわせて、学内に主な15台のメールサーバのユ

†大分大学 総合情報処理センター
†Information Processing Center, Oita University

ーザアカウントをＬＤＡＰ(Lightweight Directory Access Protocol)で管理し、メールゲートウェイでもそのＬＤＡＰデータベースを参照することにより、あて先不明メールを拒否することができる統合メール管理システムを導入した。

本稿では、統合メール管理システム導入以前の運用上の問題点と、本システムの必要性、構成の概要について述べ、現在までの運用状況について述べる。

2. メールゲートウェイ

従来のインターネットにおけるメールの配送モデルでは、送信サーバから直接受信サーバに送られる(図 1)ため、ローカルパート(メールアドレスの「@」より左側の部分)をランダムにすると、たいていは、あて先不明になり送信できなかった。しかし、図 2 のようにメールゲートウェイを間に入れると、メールゲートウェイが一旦受け取り、受信サーバに送ろうとした時点で受信者の有無が判明する。受信者がいない場合、メールゲートウェイから送信者に対して「User unknown」のエラーメールが送られる。spam メールの場合、「From:」アドレスにいい加減なメールアドレスを書いている場合も多い。そのような場合には、メールゲートウェイが、一旦、受け取ってしまうと、エラーメールを戻すことができず、spam メールを送信したメールサーバにとってみれば、送信が成功したようにみえる。そのため、そのメールアドレスに何度も spam メールを送りつけられることになる。統合メール管理システムが検出したメールアドレスの一部を図 3 に示す。明らかにローカルパートが変なアドレスが多い。

図 3 の下線のメールアドレスのように「普通」のメールアドレスに見えるものもある。卒業時に学生が退会手続きを怠ったメールマガジン、メーリングリストから送られてくるものであろう。メールマガジンでは、送信元アドレスに存在しないメールアドレスを書いていることも多い。このような場合も、メールの振る舞いに関しては、spam メールと同様である。卒業してしまった学生あてに送られてくるメールマガジンに対して「User unknown」エラーであることをメールマガジン発行者に対して知らせる方法がなく、いつまでも送り続けられることになる。

図1. 従来のメール配送モデル

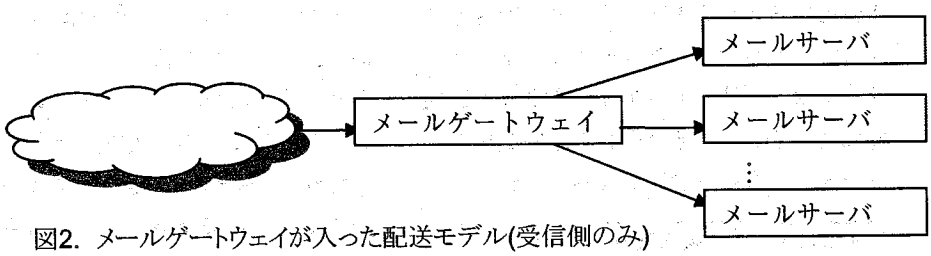

図2. メールゲートウェイが入った配送モデル(受信側のみ)

<abailey@csis.oita-u.ac.jp>,
<abakus@engy.en.oita-u.ac.jp>,
<abbys@eee.oita-u.ac.jp>,
<abe@engy.en.oita-u.ac.jp>,
<abeatty@csis.oita-u.ac.jp>,
<abet@csis.oita-u.ac.jp>,
<abeta@csis.oita-u.ac.jp>,
<abiela@cc.oita-u.ac.jp>,
<ability@csis.oita-u.ac.jp>,
<ablais@csis.oita-u.ac.jp>,
<ablang@eee.oita-u.ac.jp>,
<acct@csis.oita-u.ac.jp>,
<aceventura@csis.oita-u.ac.jp>,
<acmech@engy.en.oita-u.ac.jp>,
<acocheng@engy.en.oita-u.ac.jp>,
<aconner@csis.oita-u.ac.jp>,
<acord@eee.oita-u.ac.jp>,
<acsb@csis.oita-u.ac.jp>,
<actor@engy.en.oita-u.ac.jp>,
<acuff@eee.oita-u.ac.jp>,
<acw@engy.en.oita-u.ac.jp>,
<adah@csis.oita-u.ac.jp>,

図3. spamメールのあて先アドレスの例

3. Spamメール対策

spamメールは、ヘッダー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:各ヘッダーが、ないメールは、拒否する。

(2) Message-ID:, From:各ヘッダーの形式が <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。

(3) 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メールは拒否する。

(4) ORDB[2]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。

これらのうち、(1)に関しては、Message-IDなしでメールを送ってくるISPがあり、エラー通知メールのエンベロープのFrom:は空(<>)になるので受信する必要があり、今は拒否していない。

(4)に関しては、外部データベースを用いずに、独自にブラックリストを作成し、使用することも考えられる[3]が、リストの作成、維持や、リストに載せたサーバからの削除依頼をどのように受付けるかを考慮すると外部のブラックリストを利用するほうがよいと考えた。

しかし、これらの検査((2)～(3))では、メールの規格を満たしているspamメールは、通してしまう一方、規格を満たさない通常のメールを拒否してしまう。

メールのDoS(Denial of Service)攻撃を受けたことをきっかけとして、DoS攻撃が特に激しかった4つのメールサーバのユーザ名の一覧表をもらってきて、メールゲートウェイ上でそのメールサーバ宛のメールについて、あて先のユーザが存在するかどうかの検査を行なうようにした。

このようにするとあて先不明のspamメールは、必ず受信を拒否でき、メールゲートウェイの負荷を軽減できるが、毎年3月、4月に集中するアカウントの登録削除が、

メールサーバとメールゲートウェイとで同期が取れなくなるとメールの受信ができなくなってしまう。2箇所でアカウントの登録削除を行なう手間も大変である。そのため、LDAP[4]で複数のメールサーバのメールアカウントを統一的に管理することができる統合メール管理システムを計画した。本システムは、ユーザ登録数が多い15のメールサーバのアカウントを管理することとした。

4. 統合メール管理システム

図4に本システムの構成図を示す。2台のLDAPサーバとデータベースを操作するためのWEBのインターフェースとからなる。LDAPサーバは、TurboLinux上にOpenLDAP 2.0.27で、WEBサーバは、Windows2000上にApache2.0.47とphpで、それぞれ構築している。メールサーバからは、pop, imap等からpam_ldapを介して、LDAPサーバにユーザ認証情報を要求する。メールゲートウェイは、Sendmail8.12.10からPerlプログラムを通してメールアカウントの有無と有効期限とだけをLDAPサーバに照会する。

従来、各メールサーバの管理者は、ユーザの要望に応じてメールアカウントやメーリングリストの開設を自由に行ってきた。LDAPサーバにメールアカウントを集めるにしても、総合情報処理センターが集中管理する方式では、センターの負荷が大きくなるばかりであり学内にも受け入れられない。

本システムでは、管理者をマスター管理者と一般管理者に分けた。マスター管理者は、本システム全体の管理者ではあるが、一般管理者を指名するだけである。一般管理者は、個々のメールサーバの管理者であり、メールアカウントの開設、削除を行う。更新、パスワード変更は、一般ユーザが直接行える。

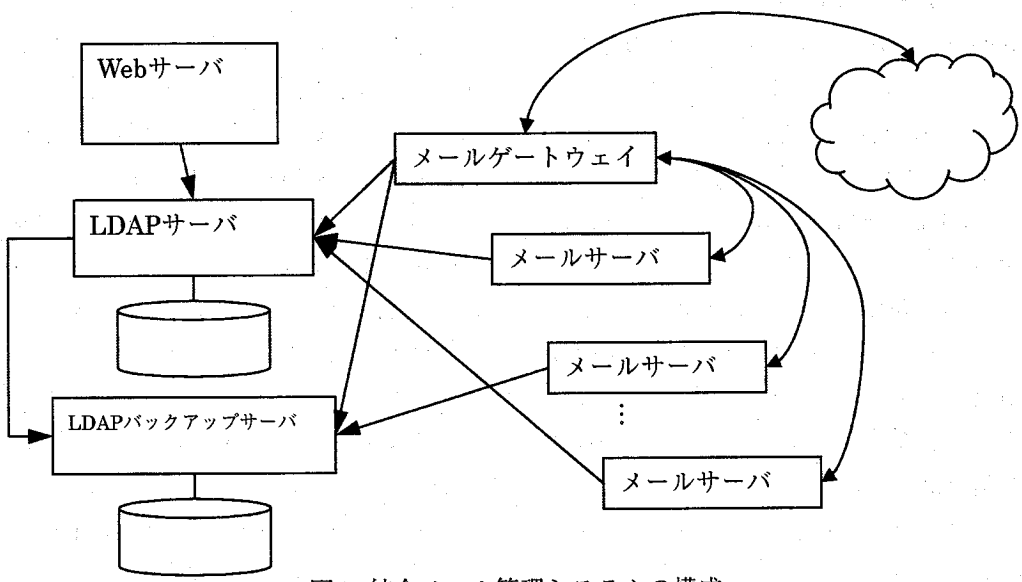

図4. 統合メール管理システムの構成

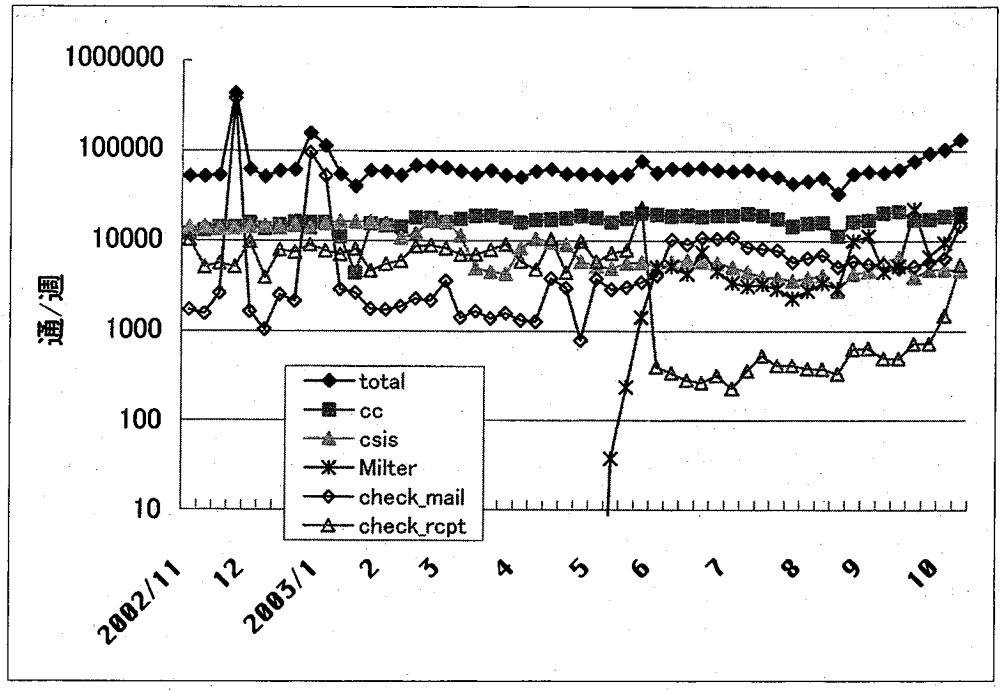

図 5.　一週間当たりのメール受信数

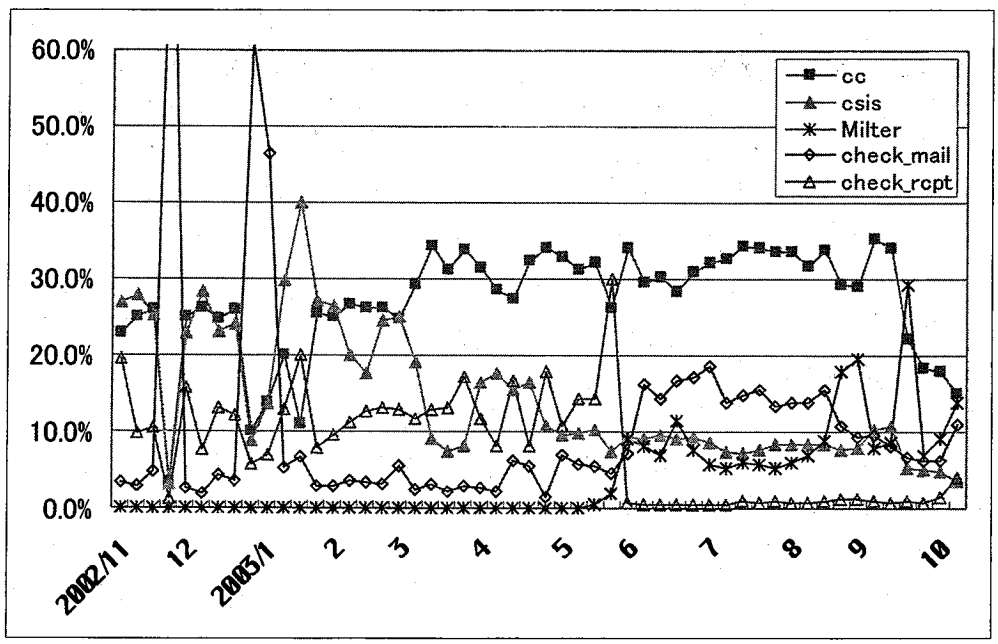

図 6.　一週間当たりのメール受信数の割合

5. 運用状況

図5に最近1年間の各週ごとについて、全体、主な2つのサブドメインのメール受信数、およびLDAP参照、エンベロープのFROM、TOの検査により受信拒否したメール数の変化を示す。図6には、全体に対する図5の各区分の割合を示す。2002年11月、12月にメールのDoS(Denial of Service)攻撃を受けている。このときは、エンベロープ、ヘッダー等の形式的な検査で、受信拒否ができ、事なきをえた。今年8月,9月に「Milter」の小さなピークがありDoS攻撃を受けたようである。LDAPを用いた検査で受信拒否をすることができた。なお、9月後半以降メール受信数が増えているのは、大分大学と大分医科大学との統合により、医学部あてのメールがこのメールゲートウェイを通るようになったためである。

6. まとめと今後の課題

LDAPを用いた統合メール管理システムについて述べた。本システムにより、ウィルス検出駆除のためのメールゲートウェイを使っても、メール本体を受信することなく、spamメールを拒否できるようになった。あて先が実在するspamメールに関しては、spamかどうか判断するために内容を検査する必要がある。MUAの中にはspamかどうか検査する機能を持ったものもあり、spamassassin[5]等のMTA上で内容を検査するシステムもある。これらはユーザ自身が対策をとることができるものである。本システムとこれらとを組み合わせることで、運用管理者、利用者がそれぞれの立場で互いに協力してspam対策を進めていくことが、今後、重要になるであろう。

Unix系サーバ(Solaris, Linux)、Radiusを利用するDialUpのユーザ認証はすでに、本システムのLDAPサーバを用いて行なわれている。しかしながら、本センターでは、統合メールシステムへのユーザ登録ばかりでなく、他に情報教育システムのWindows、英語自習システム(e-Learning システム)、CALL(Compter Aided Language Laboratory)の3つにユーザ登録を行なっている。本システムの計画時点では、WindowsのDirectXとLDAPとの互換性が問題になり、今のところ、本システムとは別に情報教育システムのWindowsにユーザ登録を行なっている。最近、samba[6]が、LDAPに対応したらしいので、約300台のPCからなる情報教育システムについてWindowsのユーザ認証を本システムで行なえるようにすることが当面の課題である。

本システムへの移行に当たっては竹内三太郎事務情報係長、原山博文技官をはじめとする学内各メールサーバの管理者の方々のご協力をいただきました。本システムの構想段階から賛同いただき開発を請け負っていただきましたコムネット(株)、納入業者である富士通(株)には、大変お世話になりました。ここに記して謝意を表します。

参考文献

[1] http://www.trendmicro.co.jp
[2] http://ordb.org
[3] 山守、杉浦：ウィルスチェックサーバの導入とメール爆弾対策の効果、大学情報システム環境研究、Vol.5、pp.9-18, 2002.
[4] http://www.openldap.org
[5] http://www.spamassassin.org
[6] http://www.samba.org