ＬＤＡＰを用いた統合メール管理システムについて

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
Tel. 097-554-7874　Fax. 097-554-7990
yoshida@csis.oita-u.ac.jp

概要

学内に 15 台ほどあるメールサーバのユーザを LDAP 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、spam 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 2003 年 2 月のシステム更新にあわせて、導入した。

キーワード

電子メール、spam メール、コンピュータウィルス

1．はじめに

本学では、 2001 年 8 月に高速キャンパスシステムの一環としてメールのウィルス検出ソフト（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、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「@」より左側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。そこで、2003 年 2 月のシステム更新にあわせて、学内に 15 台ほどあるメールサーバのユーザをＬＤＡＰ(**L**ightweight **D**irectory **A**ccess **P**rotocol)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、spam 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。

2．メールゲートウェイと spam メール

従来のインターネットにおけるメールの配送モデルは、送信サーバから直接受信サーバに送られる(図 1)ため、メールアカウント(メールアドレスの「@」より左側の部分)をランダムにしても、たいていは、送信できなかった。しかし、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わかる。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。

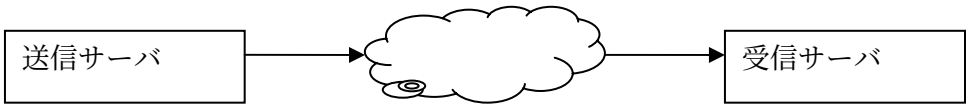


図 1.　従来のメール配送モデル

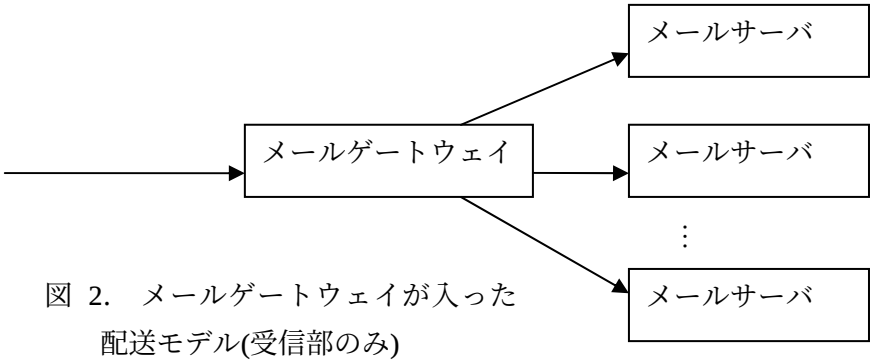


図 2.　メールゲートウェイが入った
配送モデル(受信部のみ)

<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

spam メールは、受け取ってしまったら負けなので、あて先アドレスをチェックする以外にも、以下のような方法で、spam メールを拒否している。

(1) メールアドレスの「@」より右側について、DNS を調べる。
(2) メールの書式(Message-ID, From:の有無)を調べる。(厳密にすると、通常のメールの中にも受け取れなくなるものが出てきた。)
(3) 不正中継サーバ、spam メール送信サーバの Black List(Blocking List)を参照する。大分大学では、ordb[2], jippg[3], spamhaus[4], njabl[5]を使用している。

図 4 に、1 週間にメールゲートウェイが受信したメールのあて先別メール数を示す。この中で、「16344 cc.oita-u.ac.jp」は、cc.oita-u.ac.jp 宛のメールが 16344 通来たことを示す。「Milter:」は、LDAP データベースを参照した結果拒否したメール数である。「ruleset=check_mail」は、From:アドレスについて DNS でチェックし、さらに送信メールサーバの IP アドレスについて BlackList で検索した結果拒否したメール数である。この週は、1/4 ほどのメールを拒否した。

```
   (途中省略)
  677 ac.jp
 1273 arch.oita-u.ac.jp
 1409 ees.ec.oita-u.ac.jp
 2352 ne.jp
 3177 ad.oita-u.ac.jp
 4317 csis.oita-u.ac.jp
 4372 mail.cc.oita-u.ac.jp
 5984 ruleset=check_mail,
10046 Milter:
16344 cc.oita-u.ac.jp
55910  合計
```

図 4.　1 週間のあて先ドメイン別メール数

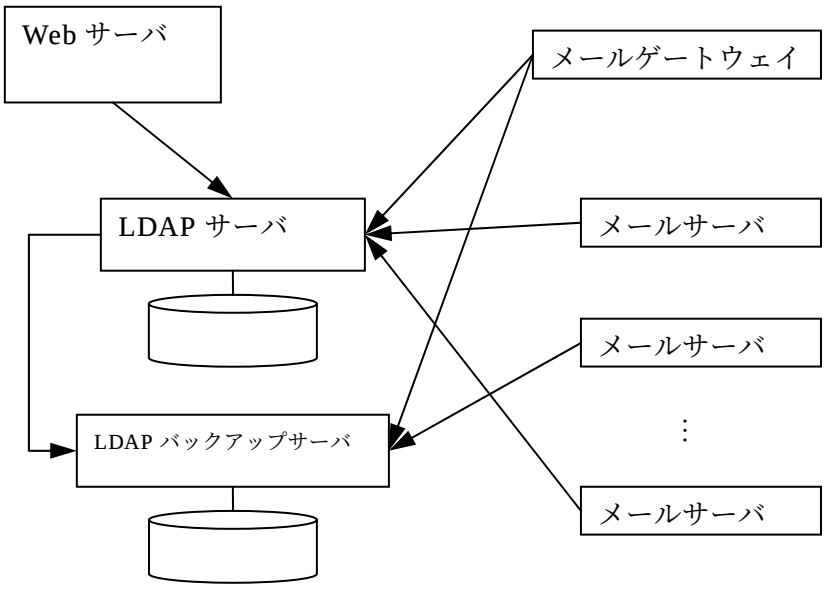
3．LDAP サーバとユーザインターフェース

図 5 に本システムの構成図を示す。2 台の LDAP サーバ[6]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。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からは、メールアカウントの有無だけを 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比較的自由にメールアカウントやメーリングリストの開設を行ってきた。 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、管理者をマスタ管理者と一般管理者に分けた。マスター管理者は、

一般管理者を指名するだけであり、メールアカウントの開設、削除は、一般管理者が行うようにした。更新、パスワード変更は、一般ユーザが直接行える。



4．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、容易に spam メールを拒否できるようになった。学外から内部に侵入しようとするウィルスについては、メールゲートウェイで駆除できる。学内相互、学内から外部へのウィルス送信を止めるために、各メールサーバの管理者に、メール送信の際、無条件にメールゲートウェイに送る設定にするように要請しているところである。

本センターでは、統合メールシステムへのユーザ登録だけでなく、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４つにユーザ登録を行なっている。LDAP のユーザアカウントのデータベースが手に入ったので、これをメールだけに使うのは、もったいない。現在は、UNIX 系の OS(Solaris, Linux)では、このデータベースを用いて、ログイン時のユーザ認証を行なっている。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[7]が、LDAP に対応したらしいので、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今後の課題である。後の２つは、独自のユーザ認証機構を持っていて、LDAP とのインターフェースは、まったく考えられていない。これに関しては、開発元に要望を出していきたい。

参考文献

[1] http://www.trendmicro.co.jp
[2] http://ordb.org
[3] http://blacklist.jippg.org
[4] http://www.spamhaus.org
[5] http://njabl.org
[6] http://www.openldap.org
[7] http://www.samba.org