認証基盤と連携したメールホスティング環境の構築

Construction of Mail Hosting System Based on Authentication Database

土屋雅稔*
Masatoshi TSUCHIYA
豊橋技術科学大学 情報メディア基盤センター
Information and Media Center, Toyohashi University of Technology
441–8580 愛知県 豊橋市 天伯町 雲雀ヶ丘 1–1
1–1 Hibarigaoka, Tenpakucho, Toyohashi-shi, Aichi, 441–8580 Japan

未熟な管理者によって管理されているメールサーバには，大きなセキュリティリスクが存在する．このセキュリティリスクを軽減するには，メールサーバのホスティングサービスを提供することが有効である．本論文では，2 つの特長を持つメールホスティング環境について述べる．第 1 に，認証用 LDAP データベースのツリー構造とアクセス制御リストに基づいて，利用組織の管理者に対する権限委譲を実現する．利用組織を単位とするパスワードではなく，管理者個人のパスワードに基づいて認証を行い，さらに，利用組織毎に独立した管理者名簿に基づいて管理作業を認可する．これにより，本論文のメールホスティング環境では，利用組織の管理者の交替を円滑かつ安全に行うことが可能である．第 2 に，本論文のメールホスティング環境では，利用組織毎のメールボックスは存在せず，容量制限が設定された個人用メールボックスのみが存在する．これにより，利用組織の管理者に対して委譲する権限を少なくすることができ，メールホスティング環境の安全性が高まる．また，利用組織の管理者は，自分自身の組織が利用するメールボックス容量を予測・監視する作業を行わなくても良いという利点がある．

キーワード：メール，ホスティング

There is increasing interesting against hosting service for mail servers in a university network, in order to reduce security risks caused by unskilled administrators. This paper explains a mail hosting system which has two features. The first feature is a delegation mechanism based on the tree structure of the authentication database and its access control list, which makes a domain administrator use his/her own password for authentication and allows administration actions to administrators based on the list of their account names. The second feature is that no mail spool is prepared for domains but mail boxes for users are only prepared. The second feature minimises privileges of domain administrators and makes the mail hosting system secure.

KEYWORDS : Mail, Hosting

* E-mail: tsuchiya@imc.tut.ac.jp

1 はじめに

現代のネットワーク社会において大学教員が研究業務を円滑に遂行するには，安定したサーバ資源が必要不可欠である．特に，自らの研究成果を広く発信するためのウェブサーバ，研究情報を交換するためのメールサーバ，および，それらの基盤サービスとしての DNS サーバの 3 つの重要性は大きい．しかし，学内組織および研究室のサーバは，専門外の職員や学生のボランティア的活動によって維持されている場合が多く，十分なメンテナンスが行われていないサーバが少なくない．また，クラッキングの悪質化と件数の増加，spam 件数の増加など，ネットワークを取り巻く環境は悪化の一途を辿っている．そのため，サーバ管理に係る負担が，ボランティア的活動の限界を遠からず超えることは明らかである．

このような状況を改善するには，各種ホスティングサービスを情報系センターで提供することが有効である．特に，ウェブホスティングは，Apache[*1]の仮想ホスト機能を利用すると容易に実現できるため，東京大学情報基盤センター[*2]や名古屋大学情報連携基盤センター [1]，三重大学総合情報処理センター[*3] など多数の情報系センターで提供されている．

それに対して，メールホスティングを実現するためには，メールアドレスの作成や廃止などの管理を実施する方法についての検討が必要になる．九州大学情報基盤センター[*4] は「ユーザ管理はセンター側で行います」と宣言し，管理作業をセンターが代行する方式をとっている．この方式は，利用組織の管理者のスキルに依存しないという意味では優れているが，センターの作業負荷が過大となるため，利用組織数が多くなるとサービスが継続できなくなる恐れがある．広島大学情報メディア教育研究センター[*5] は，メールサーバに対するウェブベースの管理インタフェース (市販品) を提供することによって権限を委譲している．東京大学情報基盤センターでは，メールサーバのアプライアンス製品を利用し，その製品に備わっている管理インタフェースを提供することによって権限を委譲している [2]．これらの方法では，利用組織 1 つに対して管理用アカウントを 1 つだけ発行して，管理作業の認証と認可を行っている．そのため，大規模な利用組織の場合は，1 つの管理用アカウントを複数の管理者で共同利用することになり，異動や卒業などの理由により管理者が交替した場合には，パスワードを適切に変更した上で複数の管理者に通知する必要がある．このような状況ではパスワード管理が適切に行われず，既に交替した管理者が管理作業を実施できてしまうことが多い．また，これらの方法では，利用組織を単位としてメールボックスの容量制限を行うことが一般的である．しかし，大規模な利用組織にとっては，利用者数が多いだけでなく，個々の利用状況も把握しづらいため，適切な容量を事前に予測することは利用組織の管理者にとっても困難である．

本論文では，2 つの特長を持つメールホスティング環境について述べる．第 1 に，認証用 LDAP データベースのツリー構造とアクセス制御リストに基づいて，利用組織の管理者に対する権限委譲を実現する．利用組織を単位とするパスワードではなく，管理者個人のパスワードに基づいて認証を行い，さらに，利用組織毎に独立した管理者名簿に基づいて管理作業を認可する．これにより，本論文のメールホスティング環境では，利用組織の管理者の交替を円滑かつ安全に行うことが可能である．第 2 に，本論文のメールホスティング環境では，利用組織毎のメールボックスは存在せず，容量制限が設定された個人用メールボックスのみが存在する．これにより，利用組織の管理者に対して委譲する権限を少なくすることができ，メールホスティング環境の安全性が高まる．また，利用組織の管理者は，自分自身の組

[*1] http://httpd.apache.org/
[*2] http://park.itc.u-tokyo.ac.jp/
[*3] http://www.cc.mie-u.ac.jp/cc/hosting/index.html
[*4] http://www.nc.kyushu-u.ac.jp/hosting/pamphlet.pdf
[*5] http://www.media.hiroshima-u.ac.jp/modules/tinyd0/index.php?id=135

織が利用するメールボックス容量を予測・監視する作業を行わなくても良いという利点がある．

2 メールホスティング環境の設計

2.1 用語

本論文で用いる用語について，以下のように定義する．

プロバイダ メールホスティングサービスを提供する組織 (例えば，情報系センター)．

プロバイダ管理者 メールホスティングサービスを管理する職員．メールホスティングサービスを構成するハードウェアおよびソフトウェア全体の管理を担当する．

プロバイダ利用者 プロバイダを利用する権利を有する全ての人 (例えば，学生や教職員など)．

ドメイン メールホスティングサービスを利用する 1 つの組織 (例えば，学内の部局や研究室)．

ドメイン管理者 メールホスティングサービスを利用する 1 つの組織の管理者．その組織に対応するドメインのメールアドレスの作成や廃止などのドメイン内管理作業を行う．なお，ドメイン管理者は，必ずプロバイダ利用者である．

ドメイン利用者 メールホスティングサービスを利用する 1 つの組織に属する人．なお，ドメイン利用者は，必ずプロバイダ利用者である．

なお，本論文では，各ドメインのドメイン管理者およびドメイン利用者は，必ずプロバイダ利用者であるという仮定を置いている．

2.2 方針

多くのプロバイダは人員および予算に余裕がないので，本論文では，メールホスティング環境の設計上の制約条件として以下の 2 条件を考慮する．

1. プロバイダにとって，必要となる費用が最小であること．
2. プロバイダ管理者にとって，必要となる管理コスト (労力) が最小であること．

第 1 の制約条件 (費用最小) を実現するため，ハードウェアとして一般的かつ安価な IA32 アーキテクチャのサーバを活用し，ソフトウェアとしてフリーソフトウェアを活用する．また，第 2 の制約条件 (労力最小) より，プロバイダ管理者が管理を一手に引き受ける方式は採用せず，ドメイン管理者に適切な権限委譲を図る．

権限委譲にあたっては，(1) 委譲する権限の範囲，(2) 認証および認可の方法，の 2 点について検討が必要である．最初に，委譲する権限の範囲について検討する．一般的なメールサーバにおいて，管理者が行う管理作業には，以下のような作業がある．

(a) ユーザの登録 · 削除
(b) メールエイリアスの設置 · 廃止
(c) ユーザ用メールボックスの容量制限の設定 · 変更

管理作業 (a),(c) を実施するには，ホームディレクトリの作成や quota の設定など，ファイルサーバおよびメールサーバの設定 (の一部) を変更する権限が必要である．よって，ドメイン管理者に管理作業 (a),(c) の権限を委譲するには，ファイルサーバおよびメールサーバに直接ログインすることを許可するか，または，適切な管理インタフェースを提供するか，いずれかが必要となる．いずれの場合であっても，ドメイン管理者のアカウントが漏洩した場合にサーバ本体に危険が及ぶ可能性があるため，多数のドメインをホスティングするには適さない．そこで本論文では，全てのドメイン利用者はプロバイダ利用者でもあるという仮定を利用し，ドメイン管理者に委譲する権限を限定する．具体的には，まず，ドメイン利用者の名簿やドメインに属するメールエイリアス一覧などのドメイン特有の情報を，ファイルサーバやメールサーバからデータベースに分離する (図 1)．その上で，ファイルサーバおよびメールサーバの変更が必要な管理作業はプロバイダ管理者が行い，データベース上のドメイン特有の情報に対する管理作業のみをドメイン管理者に委譲する．

次に，認証および認可の方法について検討する．もっとも一般的で簡単な認証および認可の方法は，利用組織毎に 1 つだけ管理用アカウント (ユーザ名とパスワード) を発行する方式である．しかし，先

に述べた通り，この方式には，パスワード管理が適切に行われなくなる可能性が高いという欠点がある．そこで本論文では，全てのドメイン管理者はプロバイダ利用者でもあるという仮定に基づいて，全プロバイダ利用者が登録された認証データベースの個人用パスワードを用いて認証を行い，ドメイン毎に独立したドメイン管理者名簿に基づいて認可するという方式を採る．

3 メールホスティング環境の実装

本メールホスティング環境の論理構成を図 1 に示す．ドメイン管理者，ドメイン利用者およびプロバイダ利用者などの全てのデータは，LDAP サーバに保管されている．LDAP データベースのツリー構造の例を図 2 に示す．図 2 は，以下のような例となっている．

1. プロバイダは provider.example.net というドメインである．
2. プロバイダがホスティングしているドメインの 1 つは，foo.example.net である．
3. foo.example.net ドメインには，taro と hanako という 2 人のドメイン利用者がいる．ドメイン利用者 taro は，プロバイダ利用者 tx001 である．ドメイン利用者 hanako は，プロバイダ利用者 hy002 である．
4. foo.example.net ドメインには，staff@foo.example.net というエイリアスがあり，これは taro と hanako に転送される．
5. foo.example.net ドメインの管理者は，プロバイダ利用者 tx001 と hy002 である．
6. プロバイダ利用者 tx001 宛のメールは，プロバイダのファイルサーバに蓄積される．
7. プロバイダ利用者 hy002 宛のメールは，外部のアドレス yamada@example.com に転送される．

以下では，図 2 の例を用いて，本メールホスティング環境の実装を説明する．

3.1 メール受信時の処理

メール受信時の処理手順は，以下の通りである．

メールは，最初に，受信用 SMTP デーモンによって処理される．受信用 SMTP デーモンは，(1)spam 送信用ボットである可能性が高いホストからの接続に対して遅延応答 (tarpitting) する，(2) 存在しないアドレス宛のメールは拒否する，という 2 つの処理を行う．前者の詳細は 3.2 節で述べる．アドレスの存在確認には，図 2 のドメイン利用者名簿，ドメインエイリアス表，プロバイダ利用者名簿などを参照する．次に，フリーのウイルス検出ソフトウェアを用いて，ウイルスフィルタリングを行う．

続いて，ドメイン配送処理を行う．ドメイン配送処理は，基本的には，図 2 のドメイン利用者名簿およびドメインエイリアス表に基づくアドレス書き換え処理である．例えば，staff@foo.example.net 宛のメールの宛先アドレスは taro@foo.example.net および hanako@foo.example.net に書き換えられる．また，taro@foo.example.net 宛のメールの宛先アドレスは tx001@provider.example.net に書き換えられる．

最後に，ローカル配送処理を行う．ローカル配送処理に到達する全てのメールは，前段のドメイン配送処理によって，宛先アドレスがプロバイダ利用者に書き換えられているはずである．ローカル配送処理部は，LDAP サーバ上に格納されているプロバイダ利用者の個人設定に基づいて，メールをファイルサーバ上の個人用メールボックスに格納したり，外部に転送したりする処理を行う．なお，プロバイダ利用者毎の個人用メールボックスの容量制限は，メールを個人用メールボックスに格納するプログラム (Mail Delivery Agent) の機能によって実現している[*6]．

3.2 spam メール対策

最近の spam メールの送信手法としては，大量の spam 送信用ボットを用いる手法が一般的である．spam 送信用ボットは，通常の MTA とは異なる幾つかの特徴的な挙動 (例えば，一時エラーに対して再送処理を行わない，RFC に定められた範囲

[*6] 本環境では，MDA として，Dovecot 付属の deliver コマンドを用いる．これは，IMAP サーバの機能によって個人用メールボックスの残容量をプロバイダ利用者に通知するためである．

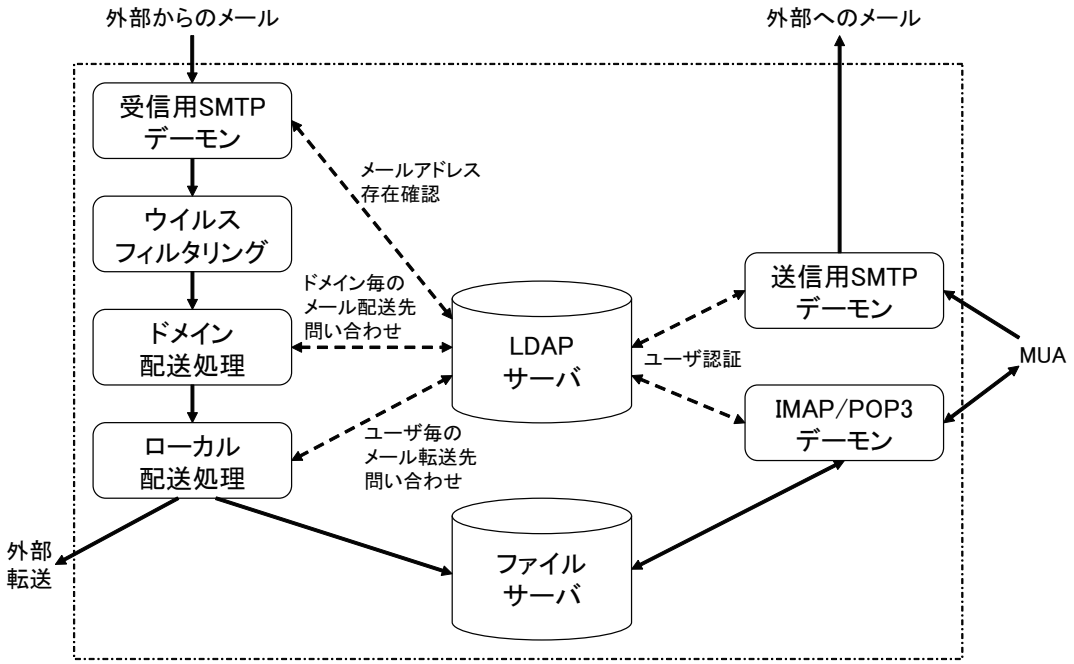

図 1　メールホスティング環境の論理構成

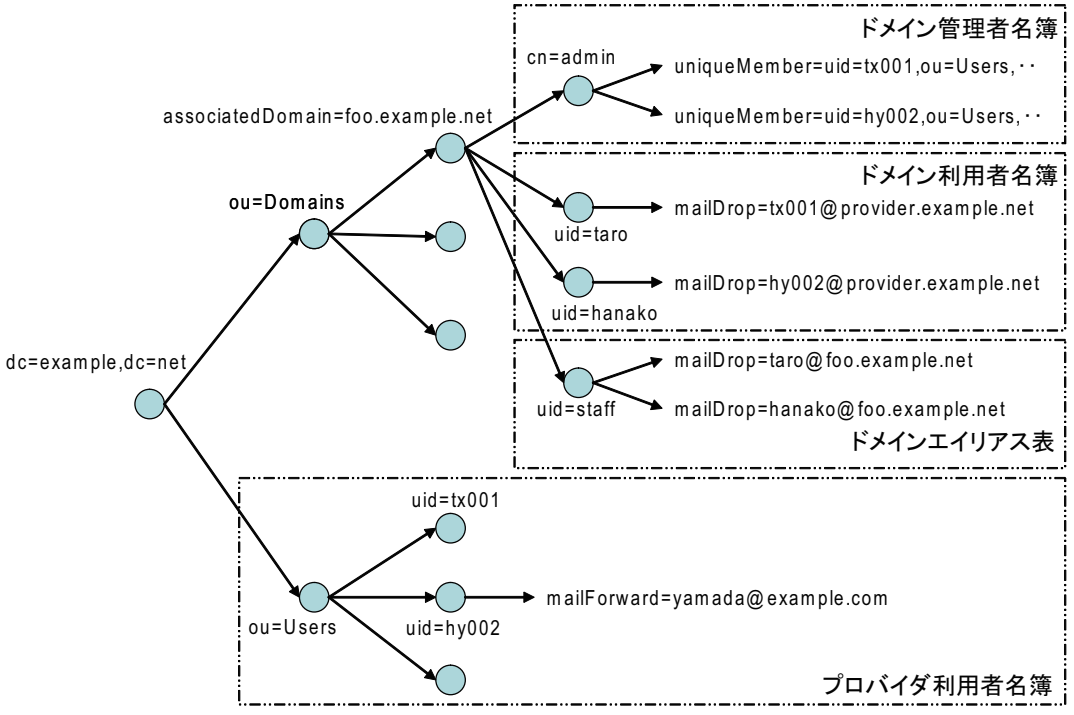

図 2　LDAP データベースのツリー構造

内の遅延であっても接続を切断する，など) を示す．spam メール対策には，(1) spam 送信用ボットの挙動に注目し，MTA の挙動を変更することによって spam メールをなるべく受け取らないようにする手法と，(2) spam メールと通常のメールの内容の違いに注目し，利用者に配送する前に filtering する手法の 2 通りがある [3, 4]．しかし，プロバイダ側でユーザ全員に対して一律の基準で行う filtering には，様々な問題がある．特に，ユーザによって spam の定義が異なる問題は深刻であり，ユーザ単位で fitering を実施するか否かの選択を行わせるなどの対策が必要になる [5]．本メールホスティング環境の実装にあたっては，先述の通り，できるだけプロバイダ管理者の管理コストを低減することを目標としている．そのためには，後者の手法 (filtering) よりも，MTA の挙動を変更する前者の手法が優れている [6, 7]．

本メールホスティング環境では，そのような手法の中でも，最も管理コストが少ない手法として，Starpit 法[*7]を採用した．具体的な手順は以下の通りである．

1. SMTP 接続元の IP アドレスから逆引きを行い，逆引きに失敗した場合，または，機械的に生成された可能性が高いホスト名 (例えば，`ppp1234` や `adsl5678` など) が得られた場合，その接続元は spam 送信用ボットである可能性が高いと判定する．
2. spam 送信用ボットである可能性が高い場合には，SMTP セッションで RCPT を受信してから，応答するまでの間に，185 秒遅延させる．ただし，遅延は以下の 2 段階で行う．
   - 45 秒遅延する．
   - 宛先アドレスの存在確認を行い，存在しないアドレスの場合は，受信を拒否する．
   - 更に 140 秒遅延する．

遅延を 2 段階に分割している理由は，Directory Harvesting Attack 対策である．詳細については，4.3 節で述べる．

3.3 データベースのツリー構造とアクセス制御リストに基づく権限委譲

本メールホスティング環境では，LDAP データベース上の部分木に対するアクセス制御リストによって，ドメイン管理者に対する権限委譲を実現する．本節では，この実装の詳細と利点について述べる．

最初に，ドメイン管理作業を，LDAP データベースに対する操作のみで実現するために 2 つの準備をする．第 1 に，ドメイン利用者名簿やドメインエイリアス表などのドメイン特有の情報を，LDAP データベースに分離する (図 1)．第 2 に，ファイルサーバおよびメールサーバに対する操作を必要とする管理作業 (プロバイダ利用者の作成・削除，およびプロバイダ利用者の個人用メールボックスに対する容量制限設定) はプロバイダ管理者が行うことにする．このような準備を行った上で LDAP データベースのツリー構造 (図 2) を考慮すると，ドメイン管理作業のためにドメイン管理者が操作・変更できなければならない範囲は，LDAP データベース上の部分木に限定される．例えば，`foo.example.net` ドメインの管理者が操作・変更できなければならない範囲 (ドメイン利用者名簿およびドメインエイリアス表) は，`associatedDomain=foo.example.net` ノード以下の部分木のみである．

次に，ドメイン管理作業の認証および認可を実装する．本メールホスティング環境では，LDAP サーバとして OpenLDAP 2.3.30[*8] を採用した．OpenLDAP には，LDAP データベースのツリー構造に対してアクセスの許可・不許可を制御するためのアクセス制御リスト機能が実装されている．アクセス制御リストを図 3 のように設定すると，あるドメインのドメイン管理者名簿，ドメイン利用者名簿，ドメインエイリアス表の修正を，そのドメインのドメイン管理者名簿に登録されているプロバイダ利用者に認可することができる．ドメイン管理者としての認証は，プロバイダ利用者名簿に登録されて

[*7] `http://d.hatena.ne.jp/stealthinu/20060706/p5`

[*8] `http://www.openldap.org/`

```
# associatedDomain=foo.example.net ノードに子ノードの追加・削除を許可する設定
access to dn.regex="^associatedDomain=([^,]+),ou=Domains,dc=example,dc=net$" attrs=children
  by group/groupOfUniqueNames/uniqueMember.expand="cn=admin,associatedDomain=$1,ou=Domains,dc=example,dc=net" write
  by * read

# associatedDomain=foo.example.net ノードの子ノードの内容の修正を許可する設定
access to dn.regex="^[^=]+=[^,]+,associatedDomain=([^,]+),ou=Domains,dc=example,dc=net$"
  by group/groupOfUniqueNames/uniqueMember.expand="cn=admin,associatedDomain=$1,ou=Domains,dc=example,dc=net" write
  by * read
```

図 3　アクセス制御リスト

いる管理者自身のパスワードを用いて行う．

この実装方式には，幾つかの利点がある．第 1 に，ドメイン管理者に対しても，各種サーバにログインすることを許可しなくて良い．仮に，ドメイン管理者にファイルサーバへのログインを許可していると，ドメイン管理者の認証情報が漏洩した場合には，ファイルサーバにクラッカーが侵入して権限上昇を行い，他ユーザのメールを盗み読むなどの被害が生じる可能性がある．第 2 に，ドメイン管理者の認証は，ドメイン管理者自身のパスワードによって行われるので，ドメイン管理用パスワードのようなものは存在しない．さらに，ドメイン管理者は，自分自身の権限と責任において，新たなドメイン管理者を追加したり，削除したりすることができる．これにより，ドメイン管理者を，容易かつ安全に交代させることができる．第 3 に，管理作業の認証および認可には OpenLDAP の機能を利用しているため，プロバイダ管理者は認証および認可を行うプログラムを実装しなくて良い．管理作業の認証および認可は，セキュリティ的に非常に重要な処理であり，この処理を自力で実装しなくても良いということは，セキュリティホールの発生を未然に防ぐ上で大きな意味がある．

実際には，ドメイン管理者が直接 LDAP データベースを操作することは難易度が高いので，管理用 CGI を作成した．この管理用 CGI では，`/etc/passwd` および `/etc/aliases` の編集と，ほぼ同じ作業によって，ドメイン利用者の追加・削除およびエイリアスの設定が行えるようになっている．

3.4　ハードウェア構成

本メールホスティング環境は，図 4 の通り，メールサーバ 2 台，DNS サーバ 2 台，ファイルサーバ 2 台からなる．なお，図 4 には物理サーバ (4 台) も含まれているが，これらのサーバは，ウェブホスティングを行うために用意したサーバ群であり，メールホスティング環境とは直接的な関係はない．ただし，ドメイン管理者向けの管理用 CGI などは，このウェブホスティング環境上で動作している．

メールサーバ (2 台) は，基本的に同一の構成であり，受信用 SMTP デーモン・ウイルスフィルタリング・ドメイン配送処理・ローカル配送処理・IMAP/POP3 デーモン・送信用 SMTP デーモンの処理を行っている．この 2 台のサーバに対する IP アドレスの割り当ては，図 5 のようになっており，2 台のサーバが正常に動作している場合は，DNS ラウンドロビンによって負荷を分散している．メールサーバ 1 に故障が発生した場合には，メールサーバ 1 に割り当てられていたサービス用 IP アドレスをメールサーバ 2 が引き継ぎ，メールサーバとしての応答性を維持する．これを実現するソフトウェアとして，Postfix 2.3.8[*9], Dovecot 1.0.15[*10], ClamAV 0.95.2[*11], Heartbeat 2.0.7[*12] を用いた．

プロバイダ利用者の個人用メールボックスは，ファイルサーバ (2 台) に接続された RAID アレイ上に保管されている．ファイルサーバは，稼動系・待機系からなる冗長構成を取っており，異常発生時

[*9] http://www.postfix.org/
[*10] http://dovecot.org/
[*11] http://www.clamav.net/
[*12] http://www.linux-ha.org/

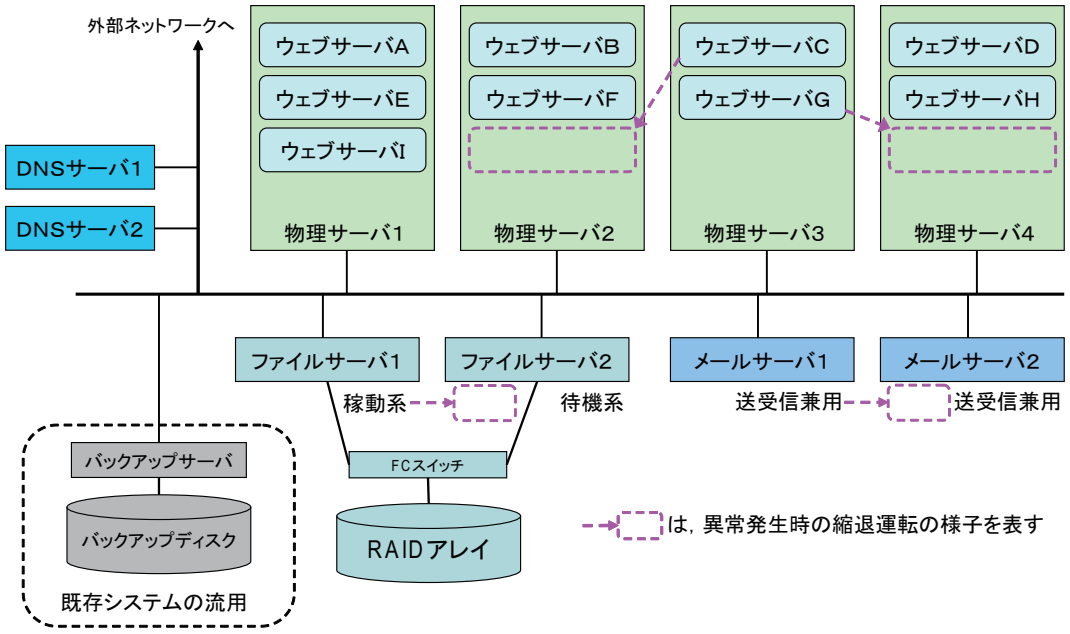

図 4　メールホスティング環境のハードウェア構成

		メールサーバ 1	メールサーバ 2
実 IP アドレス		10.0.0.1	10.0.0.2
サービス用 IP アドレス	正常時	10.0.1.1	10.0.1.2
	故障時	—	10.0.1.1, 10.0.1.2

図 5　IP アドレスの引き継ぎ

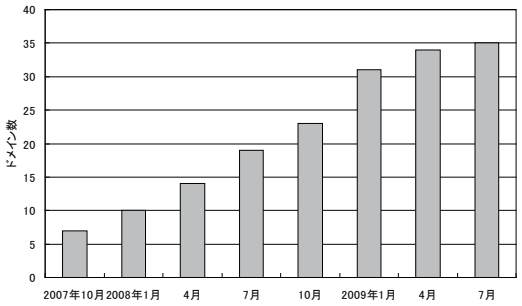

図 6　ドメイン数の推移

には自動的に切り替わるように設計されている．また，全てのコンテンツおよびメールは，既存の研究教育用システムの一部を流用したバックアップディスクに，毎日 1 回バックアップしている．

4　利用状況

4.1　ドメイン毎の利用状況

2007 年 10 月に，メールホスティング環境が本論文で述べた通りの構成となったので，7 ドメインを対象としてプレサービスを開始した．半年ほどの実運用により，概ね安定していることが確認されたので，2008 年 7 月に正式サービスを開始した．ドメイン数の推移を図 6 に示す．利用しているドメインには，プロバイダ自身やグローバル COE プログラム「インテリジェントセンシングのフロンティア」事務局[*13]などがある．

ドメイン管理者の人数によってドメインを分類した時のドメイン数と平均ドメイン利用者数を図 7 に示す．なお，ドメイン管理者数が零のドメインは，プロバイダが直接管理しているドメインである．最も多い分類は，ドメイン管理者が 2 人いるドメインで，9 ドメイン存在する．ドメイン管理者の平均人数は 3.1 人である．実際のドメイン管理者を見てみると，教員に学生を加えている場合が多い[*14]．つ

[*13] gcoe.tut.ac.jp
[*14] ホスティングの利用規約は，(1) ドメイン管理者には教員を必ず 1 名以上登録すること，(2) ただし，学生をドメイ

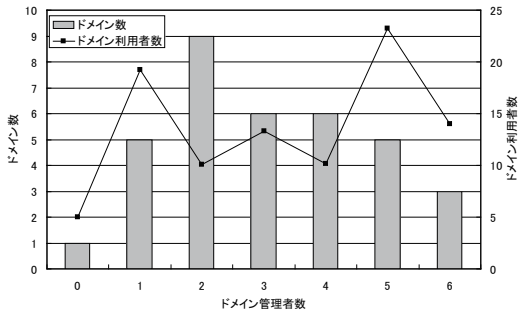

図 7　ドメイン管理者数別のドメイン数・ドメイン利用者数

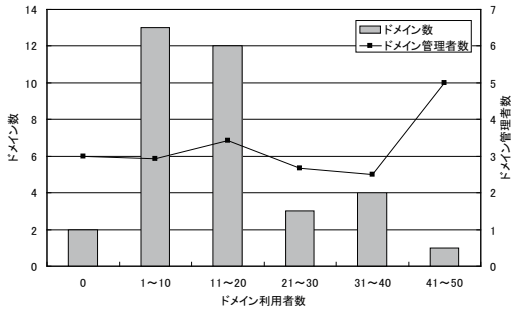

図 8　ドメイン利用者数別のドメイン数・ドメイン管理者数

まり，ドメイン管理者の交代・追加が容易であるという本論文の環境の特長によって，ドメイン管理者を担当する教員の管理コストが低減されている．

ドメイン利用者の人数によってドメインを分類した時のドメイン数と平均ドメイン管理者数を図 8 に示す．なお，ドメイン利用者数が零のドメインは，メールの転送のみを行っているドメインである．ドメイン利用者の平均人数は 14.0 人である．図 8 より，ドメイン利用者数とドメイン管理者数の間に明らかな相関関係があるとは考えられず，小規模なドメインであっても 2 人以上の管理者を置いていることが多いことがわかる．

2009 年 6 月末時点でのプロバイダ利用者のメールボックス使用量を表 1 に示す．プロバイダ利用者 1 人あたりの平均メールボックス使用量は 6.4MB だった．ただし，表 1 より，メールボックス使用量

ン管理者に追加しても良い，としている．

表 1　メールボックス使用量

メールボックス使用量	プロバイダ利用者数
1MB 未満	3887 人
1MB 以上 -10MB 未満	296 人
10MB 以上 -100MB 未満	224 人
100MB 以上 -1GB 未満	64 人
1GB 以上	1 人

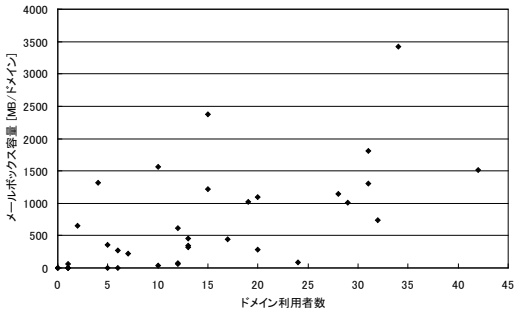

図 9　ドメイン毎のメールボックス使用量

は利用者によってかなり異なっている．ドメイン利用者の個人用メールボックスが使っている容量をドメイン毎に合計した値を図 9 に示す．ドメイン利用者数のばらつきと，ドメイン利用者 1 人あたりのメールボックス使用量のばらつき，という 2 つのばらつきがあるために，1 つのドメインあたりのメールボックス使用量を予測することは難しいことが分かる．そのため，ドメイン毎にあらかじめメールボックス使用量の上限を設定しておく従来手法では，ドメイン管理者は，ドメインのメールボックス使用量を定期的にチェックしなければならない．それに対して，本論文の手法では，プロバイダ利用者単位でのメールボックス使用量の上限によって管理されており，ドメイン管理者の管理コストが低減される．

4.2　全体の負荷状況

2008 年 6 月 1 日から 2009 年 7 月 4 日までの期間に外部から受信したメール数の推移を図 10 に示す．2008 年 8 月から 9 月にかけて大きなピークが現れているが，これは Directory Harvesting Attack によるものである．この時期を避けて，2008 年 12 月 7 日から 2009 年 6 月 6 日までの期間を対象とし

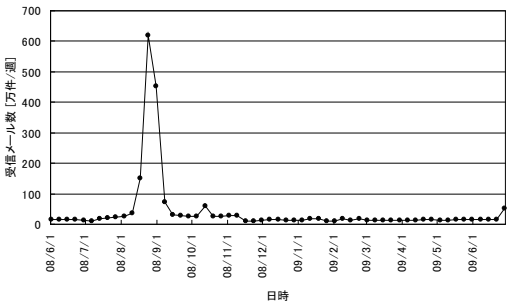

図 10　外部から受信したメール数

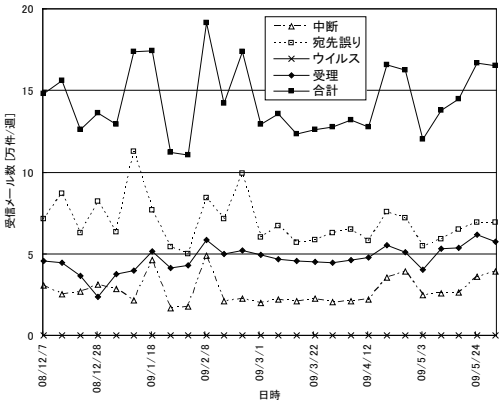

図 11　外部から受信したメールに対する処理

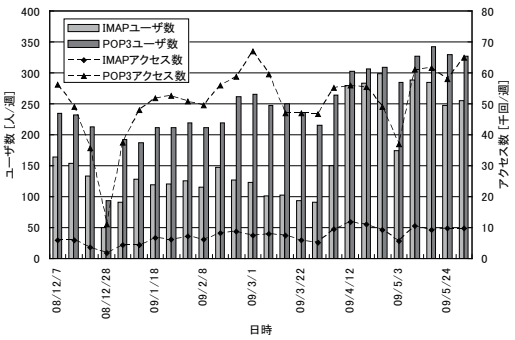

図 12　メール受信数

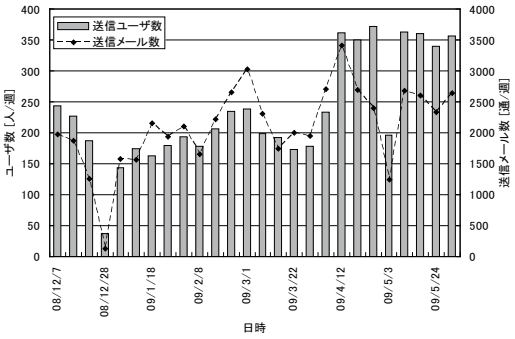

図 13　メール送信数

て，外部から受信したメールがどのように処理されたかを図 11 に示す．図 11 の時期に，遅延応答により接続を中断した件数は平均約 27,000 件/週 (18.8%) だった．また，宛先アドレスが存在しないために，受信を拒否したメールは平均約 69,000 件/週 (48.2%) だった．(1) 接続を中断したメールおよび存在しないアドレス宛のメールは全て spam である，(2) 実際に受理したメール (平均約 47,000 件/週) にも，全体と同じ比率で spam が含まれる，という 2 つの仮定をおくと，本環境における spam ブロック率は次式によって求められる．

$$\frac{27,000}{47,000 \times (18.8\% + 48.2\%) + 27,000} = 46.2\%$$

この spam ブロック率はけっして高くはないが，本論文で採用した Starpit 法がほぼ完全にメンテナンスフリーであることを考えると，やむを得ない値と考える．

図 11 と同じ時期を対象として，プロバイダ利用者によるメール受信アクセス回数と，IMAP/POP3 デーモンによって認証されたユーザ数の推移を図 12 に示す．図 12 より，2009 年 4 月以後に IMAP 利用者数が伸び，POP3 の利用者数に近づいたことが分かる．これは，新入生が IMAP の使い方の授業を受けたことと対応していると考えられる．また，プロバイダ利用者によって送信されたメール数および送信時認証されたユーザ数の推移を図 13 に示す．図 13 より，2009 年 4 月以後については，本環境から外部に送信されたメールは約 2,500 通/週で推移していることが分かる．図 11 より，外部から受信されるメール数は約 15 万通/週であるから，送受信メール数には約 60 倍の違いがある．つまり，メールサーバの設計にあたっては，外部から受信したメールのスループットが重要である．

4.3　Directory Harvesting Attack

実際には存在しないアドレス宛の spam メールを受信すると，その spam メールに対するバウンス

メールを送信しようとして，メールサーバの資源が浪費される問題がある [8]．そのため，最近のメールサーバでは，実際には存在しないアドレス宛のメールは最初から受信しないという対策が一般的である [9]．Directory Harvesting Attack (DHA) とは，この対策を逆用した攻撃手法であり，以下のような手順で行われる．まず，大量のユーザ名候補を格納した辞書と実在するドメイン名を組み合わせて，大量のアドレス候補を生成する．次に，このアドレス候補に対するメール送信を試みて，受信拒否応答 (応答コード = 550) を利用して，実在するアドレスのみからなるリストを作成する．

あるドメインに対して，2008 年 8 月末に DHA が仕掛けられた．2008 年 8 月 24 日から 31 日までの 1 週間に，約 546 万通のメールに対して受信拒否応答を行い，10 個のアドレス宛のメールを受信した．よって，546 万アドレスの試行によって，10 個のアドレスが漏洩したと考えられる．このドメインには，実際には 62 個のアドレスが存在しているので，このドメインを網羅するアドレスリストを作成しようとする攻撃者は，約 3390 万通のメールを送り込まなければならない．よって，3.2 節で述べたように，すぐに受信拒否応答するのではなく，わずかな遅延 (本環境では 45 秒) を行うようにすれば，網羅的なアドレスリストが漏洩する危険性はかなり低くできる[*15]．

このように，DHA のセキュリティリスクは小さいが，サービス拒否攻撃としては実害がある．実際に DHA が行われていた期間には，メールサーバが過負荷状態になり，正規のプロバイダ利用者がメールを送信できなかったり，正規のメールの受信が遅延したりした．そのため，同時に実行できるプロセス数の上限値を緩和するなどの対策を行う必要があった．根本的には，受信用 SMTP デーモンを分離するなどの対策が必要となると考えられる [10]．

[*15] 今回の攻撃事例では，第 3 者転送可能なメールサーバが踏み台として使われていた．そのため，spam ボットとして可能性が高いホストとは判定されず，攻撃に気づくまでの間に多数のアドレスについて受信拒否をしてしまった．

5 結論

本論文では，2 つの特長を持つメールホスティング環境について述べた．第 1 に，認証用 LDAP データベースのツリー構造とアクセス制御リストに基づいて，ドメイン管理者に対する権限委譲を実現した．第 2 に，本環境にはドメイン毎のメールボックスは存在せず，利用者毎に容量制限が設定されたメールボックスのみが存在する．これにより，ドメイン管理者の交替を円滑かつ安全に行うことができると同時に，安全性の高いメールホスティング環境を実現した．

最近では，情報系センターは大学構成員全員のアカウントを作成し，全員がメールを利用できる状態を整えていることが一般的である．ただし，その場合のメールアドレスは，機械的に生成されたアドレス (例えば，職員番号や学籍番号など) になるため，あまり利用されていないことが多い．この問題を解決するには，ユーザが希望するメールアドレスを発行することが有効である [11]．本論文のメールホスティングシステムは，ドメイン管理者に対してドメイン利用者が希望するメールアドレスを発行する権限を委譲するシステムと見なすこともできる．そのような目的のためには，図 1 の受信用 SMTP デーモン，ドメイン配送処理，LDAP サーバのみを，既存のメールシステムに追加すれば良い．この場合，2 台のサーバを用意すれば，サービスを開始することが可能である．

また，情報系センターのメールシステムをアウトソースする事例も増えてきている．しかし，各大学の事情に合わせたカスタマイズを行うとアウトソース費用がかさんでしまい，アウトソースの効果が薄れる．そのため，各大学の事情に合わせたラッパーシステムと，アウトソース事業者が提供するメールシステムを組み合わせることが有効である．本システムは，そのようなラッパーシステムとしても用いることができる．

謝辞

研究遂行に際しご指導頂いた元豊橋技術科学大学情報メディア基盤センター廣津登志夫ネットワーク部長 (現在は法政大学情報科学研究科教授) ならびにセンター職員の皆様に深く感謝する.

参考文献

[1] 平野靖. Web ホスティングサービス. 名古屋大学情報連携基盤センターニュース, 2004. http://www2.itc.nagoya-u.ac.jp/pub/pdf/pdf/vol03_01/007_008syoukai.pdf.

[2] 前田光教. ホスティング技術による学内組織向け電子メールサービス. 平成 14 年度東京大学総合技術研究会, pp. 12–14, 2003. http://www.ut-tech.iis.u-tokyo.ac.jp/uttech/5/05-05.pdf.

[3] 鈴木常彦. spam メールの現状と対策の動向:2. 技術的側面から見た spam メール対策 2.2 ブロッキング, スロットリング. 情報処理, Vol. 46, No. 7, pp. 754–757, 2005.

[4] 安藤一憲. spam メールの現状と対策の動向:2. 技術的側面から見た spam メール対策 2.3 フィルタリング. 情報処理, Vol. 46, No. 7, pp. 758–761, 2005.

[5] 久長穣, 杉井学, 長篤志, 三池秀敏. 大学における迷惑メール対応のあり方—利用者毎のオンデマンド対策の効果—. 学術情報処理研究, No. 11, pp. 5–13, 2007.

[6] 鈴木常彦, 後藤邦夫, 山口榮作, 石川雅彦. MTA による spam 対策の実践報告. 情報処理学会研究報告, 第 2004–DSM–034 巻, pp. 61–64, 2004.

[7] 吉田和幸. throttling による spam メール抑制の効果について. 情報処理学会研究報告, 第 2005–DSM–39 巻, pp. 69–73, 2005.

[8] 山井成良. spam メールの現状と対策の動向:2. 技術的側面から見た spam メール対策 2.4 バウンスメール対策. 情報処理, Vol. 46, No. 7, pp. 762–766, 2005.

[9] 吉田和幸. 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. 55–60, 2003. http://www.ipc.ibaraki.ac.jp/ipc2003/jacn7/IPC03-03.pdf.

[10] 三原槙仁, 吉田和幸. Throttling による spam 対策のためのメールサーバの分別について. 電子情報通信学会技術研究報告 (インターネットアーキテクチャ), 第 107 巻, pp. 43–48, 2007.

[11] 江藤博文, 只木進一. 新しいメールアドレスの柔軟な運用に向けて. 学術情報処理研究, No. 12, pp. 98–102, 2008.