Vol.2009-IOT-7 No.3
2009/10/9

認証基盤と連携した学内メールホスティング環境の構築

土　屋　雅　稔[†1]

本稿では，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．管理者個人のパスワードによって認証し，利用組織毎に独立した管理者名簿に基づいて認可することによって，円滑かつ安全な管理者の交替を実現する．第 2 に，利用組織毎にメールボックス容量を制限する代わりに，個人毎に容量制限されたメールボックスを用いる．この特長により，利用組織の管理者は，自身の組織が利用するメールボックス容量を管理しなくても良い．

Construction of University Mail Hosting System Based on Authentication Database

Masatoshi Tsuchiya[†1]

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 users' private mail boxes are only prepared.

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] 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[⋆3] 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[⋆4] 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

†1 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

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

管理者にとっても困難である．

本稿では，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．管理者個人のパスワードによって認証し，利用組織毎に独立した管理者名簿に基づいて認可することによって，円滑かつ安全な管理者の交替を実現する．第 2 に，利用組織毎にメールボックス容量を制限する代わりに，個人毎に容量制限されたメールボックスを用いる．この特長により，利用組織の管理者は，自身の組織が利用するメールボックス容量を管理しなくても良い．

2. メールホスティング環境の設計

2.1 用　　語

本稿では，以下の用語を用いる．

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 (情報系センターなど)．

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 (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 (学内の部局や研究室など)．

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，本稿では，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

本稿では，プロバイダ管理者の管理コスト (労力) を最小化することを目標として，メールホスティング環境を設計する．そのため，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，ドメイン管理者に必要な権限を委譲する．

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，サーバの設定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，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．そこで本稿では，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，サーバの設定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．そこで本稿では，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．

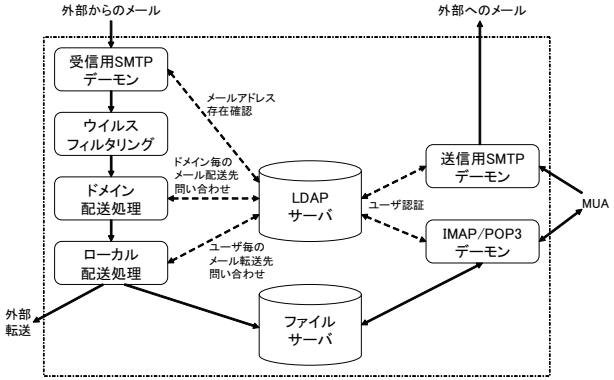

図 1 メールホスティング環境の論理構成
Fig. 1 Logical structure of our mail hosting system

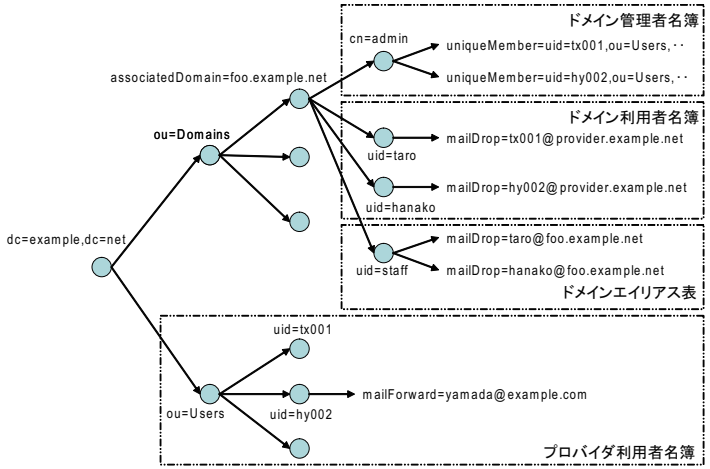

図 2 LDAP データベースのツリー構造
Fig. 2 Example of tree strucure of LDAP database

(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，本稿の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．前者は，spam 送信用ボットの挙動を利用して，spam メールをなるべく受け取らないようにするための対策である[3]．後者は，バウンスメールに対する対策であるが，単純に拒否すると Directory Harvesting Attack を受け易くなるため，拒否応答する前に遅延を挿入している[4),5]．具体的には，Starpit 法[⋆1]を一部変更し，以下のような処理手順としている．

(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) 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，応答するまでに以下の 2 段階の遅延を行う．

- 45 秒遅延する．
- 宛先アドレスについて，ドメイン利用者名簿，ドメインエイリアス表およびプロバイダ利用者名簿 (図 2) を参照して，存在確認を行う．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．

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

⋆1 http://d.hatena.ne.jp/stealthinu/20060706/p5

```
# 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
Fig. 3 Example of access control list

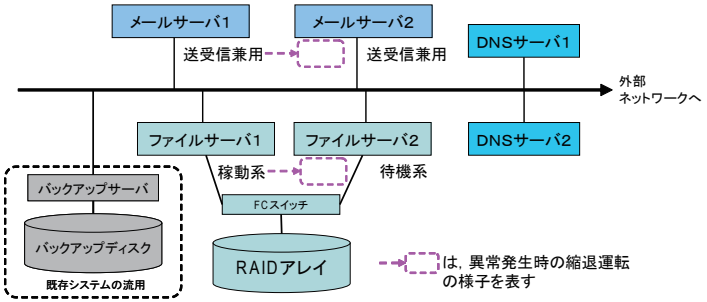

図 4 メールホスティング環境のハードウェア構成
Fig. 4 Hardware structure of our mail hosting system

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[⋆1]．

3.2 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

本稿では，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[⋆2]に限定される．

次に，ドメイン管理作業の認証および認可を実装する．本稿では，LDAP サーバとして OpenLDAP 2.3.30[⋆3] 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，ドメイン管理者がファイルサーバにログインできるとすると，ドメイン管理者の認証情報が漏洩した場合，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，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．

⋆1 本稿では，Mail Delivery Agent として，Dovecot 付属の `deliver` コマンドを用いた．
⋆2 `foo.example.net` ドメインの管理者の場合は，`associatedDomain=foo.example.net` ノード以下の部分木．
⋆3 `http://www.openldap.org/`

3.3 ハードウェア構成

本稿の環境は，**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．

2 台のメールサーバは，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．両方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．どちらかのサーバが故障した場合には，故障したサーバに割り当てられていた IP アドレスを他方のサーバが引き継ぐ．ソフトウェアとしては，Postfix 2.3.8[⋆1], Dovecot 1.0.15[⋆2], ClamAV 0.95.2[⋆3], Heartbeat 2.0.7[⋆4] を用いた．

プロバイダ利用者の個人用メールボックスは，稼動系・待機系からなる冗長構成のファイルサーバに接続された RAID アレイ上に保管されている．全てのメールは，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 回バックアップされる．

4. 利 用 状 況

7 ドメインを対象として，2007 年 10 月に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．利用しているドメインは，2009 年 7 月時点で 35 ドメインである．

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 5** 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 5 より，ドメイン利用者数とドメイン管理者数の間には相関関係は存在せず，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分かる[⋆5]．ドメイン管理者の平均人数は 3.1 人である．

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 だったが，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 6** 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，本稿の手法では，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．

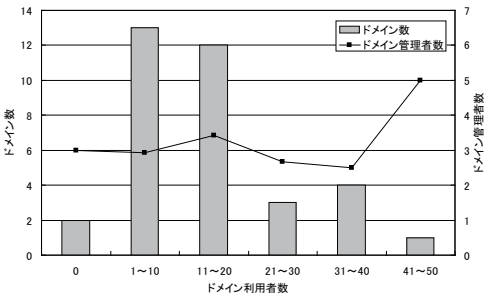

図 5 ドメイン利用者数別のドメイン数・ドメイン管理者数
Fig. 5 Numbers of domains and numbers of their administrators

表 1 メールボックス使用量
Table 1 Quantity of mail boxes

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

2008 年 12 月 7 日から 2009 年 6 月 6 日までに外部から受信したメールの処理状況を**図 7** に示す．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%)，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．

⋆1 http://www.postfix.org/
⋆2 http://dovecot.org/
⋆3 http://www.clamav.net/
⋆4 http://www.linux-ha.org/
⋆5 ただし，(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) 学生をドメイン管理者に追加しても良い，というホスティング利用規約の影響が考えられる．

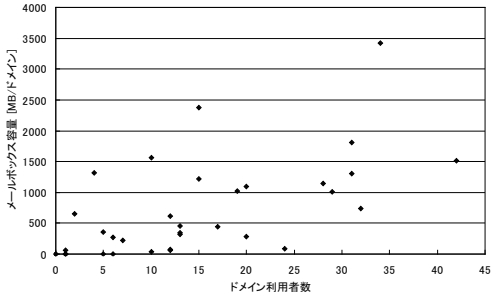

図 6 ドメイン毎のメールボックス使用量
Fig. 6 Domains and their using mail box quantities

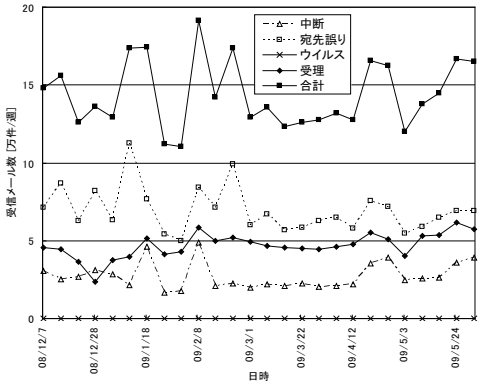

図 7 外部から受信したメールに対する処理
Fig. 7 Process against mails recieved from outer network

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

この spam ブロック率はけっして高くはないが，本稿で採用した 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．

5. 結　　論

本稿では，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，利用組織の管理者に対する権限委譲を実現した．具体的には，管理者個人のパスワードによって認証し，利用組織毎に独立した管理者名簿に基づいて認可する．この特長により，ドメイン管理者は円滑かつ安全に交替できる．第 2 に，利用組織毎にメールボックス容量を制限する代わりに，個人毎に容量制限されたメールボックスを用いた．この特長により，利用組織の管理者は，自身の組織が利用するメールボックス容量を管理しなくても良い．

最近は，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が増えている．この時，各大学の事情に合わせた綿密なカスタマイズを行うと，カスタマイズ費用がかさみ，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．本稿のシステムは，そのようなラッパーシステムとしても有用である．この場合，受信用 SMTP デーモンとドメイン配送処理を行うサーバ (稼動系 · 待機系) を用意すれば良い．

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) 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).
5) 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.