

「大学における電子メールを再考する」パネル討論 京都工芸繊維大学における運用事例

梶田秀夫
京都工芸繊維大学情報科学センター

概要：大学だけでなく多くの組織において、電子メールサービスは基本的なサービスとして提供されている。電子メールサービスは、古くから基本的なアーキテクチャが変わっておらず、運用方法は確立されているようにも思われるが、使われ方の変化により、運用方法を適応させる必要があり、各組織においていろいろなポリシーや運用体制が取られている。本稿では、比較的昔からインターネットに接続された5000人規模の大学組織に於ける電子メールサービスの現状について報告する。

キーワード：電子メール、ユーザアカウント、ウィルス対策、SPAM対策

1 はじめに

本稿は、「大学における電子メールを再考する」というパネル討論に於いて、『「電子メールシステムの運用」に関わるお話をいただければと存じます。』という依頼をうけて発表した内容をまとめたものである。

京都工芸繊維大学は、表1に挙げたように、1学部 3学域で構成される国立大学法人である。インターネット接続が開始されたのは、1990年頃で、PI (Provider Independent) なIPv4アドレスを持っており、非常に古くから電子メールサービスが使われている。

著者の属する情報科学センター (CIS) は、学内共同利用の基幹コンピュータシステムの運用管理^[1]と、学内情報ネットワーク (KITnet) を活用する基盤情報技術に関する教育研究を行う学内組織であり、教授1、准教授1、助教1の合計3名の教員と、技術専門職員2、技術専門職員 (再雇用) 1の合計3名

の職員で構成されている。

主な業務は、以下のようなものが挙げられる。

- ・教育用計算機システムの運用管理
- ・ネットワークの運用管理
- ・アカウント管理 (発行)
- ・仮想Web、MLのサーバの運用管理
- ・サブドメインのDNS
- ・キャンパスライセンスの管理

以降、CISで提供している電子メールサービスについて述べる。

2 サービスの内容

2.1 サービス対象

CISでは、すべての学部生・大学院生に対してアカウント (教育ドメイン) を提供している。ユーザ名は、学籍番号をベースに自動的に生成する為、事前に作成し入学時にすぐに配布できるようにしているが、学部から大学院前期課程、大学院後期課程と進学すると、学籍番号が変更されるため毎回変更となる。また、教職員に対しては、センターのシステムを使用したい場合に申請書を提出して貰うことによってアカウント (研究ドメイン) を作成して提供している¹。ユーザ名は、8文字以内という制限の中ではあるが、申請をベースとし、重複チェックのみ実施している。

2.2 メールアドレス

これらのアカウントに対して、教育ドメインについては、LOGINNAME@edu.kit.ac.jp、研究

表1： 京都工芸繊維大学 (KIT) の概要
工芸科学部 (2006年4月～)

生命物質科学域	応用生物学課程 生体分子工学課程 高分子機能工学課程 物質工学課程
設計工学域	電子システム工学課程 情報工学課程 機械システム工学課程 デザイン経営工学課程
造形科学域	造形工学課程
総学生数	約 4500 人
教職員数	約 500 人

1 利用負担金が必要である。

ドメインについては、LOGINNAME@kit.ac.jp という電子メールアドレスが使用可能となっている。さらに、研究ドメインについては、二次電子メールアドレスという形で、ログイン名とは異なるユーザパートを持つメールアドレスを使用できる。

2.3 送受信プロトコル

メールの送受信プロトコルは、POP3S (995/tcp)、SMTPS (port 465/tcp) を基本とし、SSLをベースとしたホスト認証と通信路暗号化を施している。その上で、送信時に於いては、SMTP AUTHを用いたユーザ認証を実施している。ただし、2006年度導入のシステム^[1]以前からのユーザへの利便性のため、学内からのアクセスに限り、POP before SMTPやAPOPを共存させている。

2.4 メールボックスと容量制限

メールボックスについては、UNIX上のQuota機能を用いた容量制限を実施しており、soft quotaを200MByte、hard quotaを300MByteとし、soft quotaを越えた状態を30日間以上継続した場合にはメールの新規受信が出来なくなるようにしている。また、メールの送信時には、メッセージ一通あたりの最大値を10MByteに設定している。

2.5 メール転送

通常の利用者は、メールサーバに遠隔ログイン (ssh) すると、図1のようなメニューにある設定が自由にできる。メール転送は、.forwardを使用しており、追加・変更・削除をCLIでできるようになっている。転送先については、特に制約はなく、ケータイ宛やフリーメール宛であっても設定可能としており、さらに複数の転送先を指定することも可能である。

```
*** Kyoto Institute of Technology ***
Modify and Show your E-Mail Preferences
```

```
Please select number
```

1. Change GCOS field
2. Display contents of .forward
3. Create new .forward
4. Add new address to .forward
5. Delete an address from .forward
6. Change APOP password
7. Delete APOP Password
8. Display quotas

9. Quit

```
Enter the number on above (1-8,9) >
```

図1: メールサーバのメニュー

2.6 ウイルスチェックゲートウェイ

学外から本学宛のメールのMXは、基本的にFsecure Anti-Virus Gatewayの稼働する2つのサーバ (inbound) が担っており、ウイルスチェックをした上で、MBOXを持つメールサーバへの転送を行っている。本学外宛のメールについても、上記とは異なるサーバ (outbound) 上で動作しているF-secure Anti-Virus Gatewayでウイルスチェックをした上で必要なMX に向けてメールの配送を実施している。これにより、学外にウイルスつきメールを配布してしまうリスクを減らし、また、inboundが過負荷状態、つまり学外から大量のメールを処理している状況に陥ったとしても、outboundでウイルスチェックをした上で学内のMBOX宛のメールを配送できるため、学内で閉じたメールの配送の遅延を避けることが可能となっている。

表2: CISの迷惑メール(SPAM)についての見解

迷惑メール対策に関して種々の研究・技術が知られていますが、100%の精度で完全に迷惑メールを排除することは不可能とされています。確かに、ある設定されたルールの下で迷惑メールを高い確率で判定できる技術もありますが、迷惑メールであるかどうかの最終的な判断基準は各利用者の主観性に強く依存します。したがって、企業などルールを一律的に導入できる組織と異なり、個人の自由裁量が大きい大学などにおいては、その導入は本質的に馴染みません。

従いまして、情報科学センターのメールサーバで迷惑メール対策を一律に実施することは時期尚早と判断しております。

現時点で個別に実施できる迷惑メール対策は、以下の通りです。

1. 基本的には電子メールアドレスを、Webなどで不用意に公開しない。
2. 公開によって迷惑メールが到着するようになった電子メールアドレスの使用を取り止める。
 - 公開されたメールアドレスは機械的に収集される危険性が高く、収集され第三者のデータベースに取り込まれたメールアドレスを、そこから削除することは事実上不可能です。
3. 迷惑メール対策のできる(あるいは迷惑メール対策機能を装備した)メールソフトを使用する。
 - 一般に広く利用されているメールソフトにも、このような機能が備わっているのをそれを利用する。参考までに、メールソフト Thunderbird の機能を確認して下さい。
 - その場合でも誤検出に備えて、迷惑メールと判断されたメールを定期的にチェックすることを強く推奨します。

URL: <http://www.cis.kit.ac.jp/index.cgi?page=E-Mail#p22>

2.7 メーリングリスト

メーリングリストは、教員からの申請により開設している²。メーリングリストドライブとしては、基本的にmailmanが利用可能となっているが、以前からの継続性の為にmajor-domoの利用も可能としている。

2.8 SPAM対策

CISとしては、表2に挙げた理由でSPAM対策サービスは原則として提供していない。

しかしながら、配送メールの内容に踏み込まないものは徐々に導入中であり、inboundウイルスチェックサーバの前段にpostfxサーバをはさみこみ、HELO/EHLOチェック、逆引きチェック、Greet Pause、VRFYチェック(MBOXサーバ上で有効なアドレスであるかをチェックする)といった機能を導入している^[3]。

2 利用料金が必要である。

3 サービスの運用ポリシー

本学では、情報セキュリティポリシーは策定済みである^[2]。しかしながら、電子メール限定の話は入っていないのが現状である。

本学に於けるサービスポリシーの決定方法は以下の通りとなっている。

1. センター次長が技術的な側面から基本方針の素案を作成する
2. センター長が決裁をする
3. 必要ならば、情報セキュリティ運営部(情報担当理事+センター長+情報化推進室長)へ上申して審議する

電子メールサービスの運用ポリシーの例は、以下のようなものがある。

- ・ 転送先の設定に制限は設けない
- ・ MLには差出人制限をかける
- ・ 学内組織で独自のメールサーバの運用を

認める

- ・ ウィルスチェックGWを極力経由するように依頼
- ・ 学外からのメールサーバへのアクセスは、暗号化対応のものに限る
- ・ 内容に踏み込むSPAM対策の導入はしない

4 サービス提供上の問題

4.1 SPAM対策の要望

2.8節にある通りの理由でSPAM対策は実施していないが、それでも対策の要望は時おり出てきている。

しかしながら、SPAMの誤検知にまつわるユーザサポートコストの増大が懸念されることもあり、導入には現時点でもなお否定的である。逆に、電子署名付メールの普及といった形で、「正しいメール」を識別しやすくする、ということを啓蒙していきたいと考えている。

4.2 転送先エラーの多発

2.5節にある通り、転送先に特に制限をかけていない運用をしていると、特にケータイ宛の転送先でエラーが目立つ。これは、ケータイメールのアドレスを変更した際に、友人にその旨を伝えることはあっても、転送設定を変更するところまでは気が回らないためと考えられる。転送エラーは、サーバ管理者やメール送信者には分かるが、転送設定をした受信者では基本的に気がつかない為、対策を検討中である^[4]。

4.3 他サービスへの移行

本学では、事務側からの通知には電子メールが使用され、必要に応じて紙による通知を行ってきた。しかし、SPAMの増大により事務通知メールがSPAMに埋もれてしまっているのではないかと、という声があり、業務通知をWeb 掲示（ポータル）に集約する、ということが行われた。

現時点では、業務通知の周知が以前よりも不徹底となってしまう、電子メールでのダイジェスト配送などを補助的に行っているが、やはり、電子メールのプッシュ型ツールとしてのメリットを活かし、必要なメールを安全に目立たせる方法を検討するべきと考えている。

4.4 ウィルス対策サーバの負荷増大

SPAMの増大により、メール配送量自体が増加しており、特に添付ファイルを含むSPAMの増大は、ウィルスチェックの負荷に直結しており、接続待ちが発生することも散見されるようになってきている。

また、通常の電子メール交換においても、パスワード付ZIPファイルの添付が増加傾向にある。これは、内容を暗号化して送りたい場合に、PGPやS/MIMEを使用せず簡易的な暗号化手段としての利用と考えられる。

5 まとめ

本稿では、京都工芸繊維大学における電子メールシステムの運用事例について述べた。

今後の課題としては、電子メールサービスの向上にむけて管理者の負担軽減だけでなく、電子署名や認証スキームの徹底による安全性の向上を目指したシステム運用を行っていきたい。

参考文献

- [1] 榊田秀夫、平田博弘、黒江康明、柴山潔：“京都工芸繊維大学における新情報教育システムについて”，2006PC カンファレンス（2006.08）。
- [2] “京都工芸繊維大学情報セキュリティポリシー”。
- [3] 榊田秀夫、落合優：“メールゲートウェイにおけるバウンスメール発生抑制法とその評価”，FIT2007（2007.09）。
- [4] 石橋由子：“誤った転送設定によるエラーメールを抑制する手法とその評価”，平成19年度京都工芸繊維大学電子情報工学科卒業セミナー報告（2008.03）。