博 士 論 文

統一認証と迷惑メール対策による
利用者ネットワークの安定性・セキュリティ確保の研究

Sustaining Stability and Security of User Networks through the Introduction of Unified Authentication and SPAM Mail Filtering

平成２３年３月

久 長 穣

山口大学大学院理工学研究科

論文要旨

インターネットや携帯電話の普及に伴い，利用者数及び通信量が急増し，ネットワークの利用形態も多様化している。利用者にとっては，こうしたネットワーク環境が常に快適で支障なく維持されていると考えがちであり，またその前提で通常業務が行われている。ネットワーク環境の安定性，高速性，安全性を保つためには，各利用者PCやそれらが接続するサーバというローカルな対応では不十分であり，ネットワークのシステム全体で対応する管理・運用技術が必要となる。この意味で，企業とは異なるネットワークポリシを持つ，大学等の情報センターの役割は年々重要となっている。

ネットワーク利用において，利用者を認証することはセキュリティ確保上最も重要な対策の一つである。大学のような組織において，複数部署で管理・運用される利用者認証では，それぞれの管理ポリシが異なり，それぞれの担当者のもとで異なる認証システムが管理・運用されるため認証が形骸化し，その継続が困難となる場合が多い。利用者認証を有効に保つためには，ユーザ名・パスワードが適切かつ統一的で継続的に管理・運用され，利用者にとっても利用しやすい認証システムであることが必要である。我々は，大学の情報センターの運営を任されている視点から，利用者が頻繁に利用する基本的なアプリケーション(①ネットワーク利用の認証，②電子メール環境の認証，③Webページ環境での認証）に対して，利用者を誘導する仕組みを考案し，時間をかけて大学組織全体の統一認証の導入に取り組み，結果的に他部署が提供するアプリケーションも含む統一認証システムを実現した。

近年，迷惑メールの増加で，電子メールの埋没，配送遅延，サーバ過負荷等，各種業務に支障をきたす状況が発生している。最も基本的な通信手段である電子メール環

境を適切に維持するためには，迷惑メール対策及びこれに付随する配送遅延対策が必要である。数多くの迷惑メール対策手法が提案されているが，いずれも少なからず誤判定を発生させる。こうした迷惑メール対策を大学等の自由な利用環境にそのまま一律に適用すると，利用者にとって重要な電子メールが不達となる（False Positive）等の問題が生じる。これらの不利益が生じたとしても，大学組織が責任を負うことは困難である。また，迷惑メール対策を導入する場合，学生を含めた全構成員に対するライセンス等のコストが必要となる問題も生じる。

そこで本研究では，利用者毎の電子メールの状況を確認することで，希望者のみに迷惑メール対策を実施した場合でも，利用者及び大学として有効な迷惑メール対策が実施できることを示した。すなわち，多くの利用者は迷惑メールを受信しておらず迷惑メール対策は不要であり，迷惑メールを受信している利用者はわずかであり，希望者のみへの迷惑メール対策でも全体として十分な対策が得られることを明らかにした。また大学においては，各部署において運用が適切に行われていないメールサーバが多数あり，その影響で電子メールの配送遅延が生じていることも明らかとなった。そこで，個々のメールサーバの運用が不適切であっても，大学全体としてメールの配送を適切に管理することで配送遅延を激減できることを示した。さらに，迷惑メール対策の過程の中から，比較的自由なネットワークポリシを保ったまま，今後増大する迷惑メールへの対応方法や大学における電子メールの取扱いを検討し，希望者が望む効率的な電子メールの配送技術など，新たなシステムの提案・導入を含め一定の方向性を示した。

ところで大学ネットワークは，学外部分及び業務部分を除き，利用者の利便性のため一つの利用者ネットワークとして運用されている。自由な環境を重視する大学内のネットワークでは，構成員が各自の管理するPCを接続し，インターネット利用，学

内利用，高度のセキュリティ対策が必要な利用など，セキュリティレベルの異なる利用が共存している。一旦，学内にウイルスや不正アクセスが発生すると全域に拡大し，通信障害，さらに個人情報の漏洩の恐れがある。そのため，各サーバや利用者PCでの対策が必要であるが，それぞれの対策を徹底することは困難であり，不完全・不注意による障害も見られる。利用者の注意や個人的な対策に任せるだけでは，全体として十分な対策を講じることはできない。不適切なサーバや利用者PCが持ち込まれた場合においても，ネットワーク全体とし安全性を維持する仕組みが重要である。

そこで本研究では，統一認証・迷惑メール対策の導入過程の成果のなかで，①大学内に接続されているサーバや利用者PCの利用者･利用場所･利用状況を把握する利用者ネットワークの提案と構築，製品化，②異なるセキュリティポリシが共存できる利用者ネットワークの提案と構築を行った。すなわち，多様化したネットワーク環境の安定運用とセキュリティの維持は，全体として一つの方法ではなく，ネットワークの物理構成，論理構成，アプリケーション及びその利用状況のそれぞれへの対策を総合して実現する必要があることを示した。

Abstract

The spread of Internet access and cellular phones has brought about a rapid increase in the number of users and the volume of network traffic. Users, however, tend to believe that this network is always maintained in an optimum condition. Moreover, users conduct their routine duties on the assumption that the network is always stable. The operating system technology of the network is more important for maintaining stability, high-speed performance, and safety of the network services, than the local management of the server and user PCs. Regarding this point, network management policies in university information technology centers are quite different to those in companies, as the information center is expected to play a role in managing the increasing risks on the network.

User authentication is one of the most important measures for network security. In many cases, user authentication is managed by individual departments with different policies. Maintaining effective user authentication in a university requires a uniform network policy, continuous management, a plain user interface, and the appropriate management of user and password data. As a member of the information technology center at Yamaguchi university, the author has been involved in developing a method for user authentication for the following basic applications: (1) network use, (2) e-mail, and (3) Internet access. Through this method, we have constructed a unified user authentication system in our university. This system has brought about stability, safety, and a user-friendly interface for the network.

In recent years, however, the volume of spam mail has increased exponentially. The huge volume of spam mail has resulted in difficulties in finding relevant mail, mail delivery delays, overload of the mail server, and interference of university activities. Consequently, it is necessary to introduce countermeasures against spam mail and mail delivery delays to maintain the safety and security of the mail environment. Although several methods for spam mail filtering have been proposed, it is hard to avoid false judgments, which can result in serious problems when important mail fails to be delivered to users (False Positive). Since the university cannot take any responsibility for this problem, it is difficult to introduce strict and indiscriminate measures against spam mail in universities.

In this study, we propose an effective mail spam filter for users in universities. Having analyzed the current state with respect to user mail, we set out to introduce spam mail filtering only for requested users. In other words, since many users do not receive spam mail, spam mail filtering is not necessary for them. Not many users receive large volumes of spam mail. It thus seems practical and effective to filter spam mail only for users requesting the service. In universities, many uncontrolled mail-server systems may be introduced by individual departments and laboratories. Under poorly managed conditions, these mail-servers often cause delivery delays in the mail system. In this study, we demonstrate that the mail delivery delay can be reduced by managing the mail gateway server properly under the control of the university information center. We discuss an effective and ideal method for

spam mail filtering in universities and in research institutes under the free policy of the mail environment.

By the way, considering user accessibility, the university network is constructed as a single user's network. In this type of user network, there is much traffic across different security levels, for example, Internet use, internal use, high-level security use, and so on. If a certain type of computer virus is introduced into the network, the virus will spread throughout the whole network, causing communication failure and information leaks. Under these circumstances, it is difficult to secure the management of each server and user PC as each administrator belongs to a different department. Sometimes failures are caused by careless and imperfect management. In this case, it is necessary to introduce a safety maintenance method throughout the whole network.

In this study, in the process of introducing unified user authentication and spam mail filtering, we propose several methods to realize a stable and secure user network. The resulting network system has the following useful characteristics: (1) an authentication network to identify the network user, computer, location, and the use situation, and (2) a coexisting network with different security policies. Consequently, to maintain a stable and secure environment in such a multipurpose network, we demonstrate the need for considering synthetic measures for the physical network, logical network, applications, and utility situation.

目次

第 1 章

序論

1.1 研究の背景

インターネットや携帯電話の普及に伴い，利用者及び通信量が急増し情報通信技術は発展，多様化している。当初（1960 年代）インターネットは軍事ネットワークとして研究開発が進められてきたが，その後，大学等の研究機関を結ぶ世界的ネットワークに展開していった。山口大学においても，1993 年にほぼ全域でインターネットが利用できる環境が整っている。1990 年代は、一般の方々が利用する商用目的のネットワークへと展開した時期で，我が国では 1995 年頃から商用のインターネットプロバイダが設立された。その当時の回線速度は 9.6kbps ～ 150Mbps と，現在と比較して低速であり，利用者も少なかった。反面，不正利用，コンピュータウイルス，迷惑メール等もなく，安全でかつ自由なネットワークであった。

インターネットの進展に伴い，利用者の増加，利用量の増大，利用方法の多様化が進んできた。情報通信白書平成 22 年度版[1] によると 1997 年に 1,155 万人(人口普及率 9.2%）であった利用者が，2009 年では 9,408 万人（同 78%）とほぼ国民全員が利用する状況となっている。特に 10 代から 40 代の利用者は，95%を超えている。また，当初はパソコンでの利用であったが，2009 年では，パソコン利用者が 8,514 万人であるのに対して，携帯電話などのモバイル端末からの利用者が 8,010 万人（利用者全体の 85.1%)と利用形態も多様化してきた。

インターネットの普及に伴い利用者の意識も変化し，以前は不安定なものと考えられていたインターネットが，現在では，安定し，快適に利用ことのできるツールと考えられている。具体的にはモバイル端末の普及により，利用者が利用したい時，いつでもどこでも利用できる（ユビキタス性）。また，通信技術の技術開発によりネットワークの通信速度は 3 年で 10 倍になるほどの高速化が実現され，映像などの大容量，

多数のデータであっても，高速に（瞬時に）通信することが可能となった（高速・大容量性）。

一方，利用者数の増大，利用者の多様化に伴い，不正利用，コンピュータウイルス，迷惑メール，ストーカ等の被害が増加している。インターネット利用において最も多い被害が迷惑メールの受信で，次いで，コンピュータウイルスの感染，架空請求を含む詐欺，不正アクセス等となっている。これらに対する対策を行わなければ，安全で自由なネットワーク，高速で快適なネットワークを損う恐れがある。現状においては各々の利用者の対応に依存しており，対策を行っていない利用者も多く存在する。そのため現状において，安全でかつ，高速で自由なネットワークを維持するためには，各々の利用者に対策をまかておくだけではなく，全体として適切な対策を施すことが必要であり，そのための運用技術及び適用技術が重要である。

1.2 研究の目的

本研究では，ネットワークの安定運用・セキュリティ維持を行うため典型的なネットワーク利用技術である，

(1)各システムが用いるユーザ名・パスワードによる全学統一認証の推進，

(2)迷惑メールを適切に排除しメール環境を安定させる運用手法の確立，

(3)利用者ネットワークの安定運用とセキュリティ対応の確立，

について，現実的な運用技術及び適用方法を提案し，実際の導入経緯から得られた知見について考察する。

誰でも匿名で自由に利用できるインターネットであるが，個人情報や金融や業務等の重要な情報を保護し，利用者を適切に把握し，利用者に応じたサービス・情報を提供する必要がある。他人のユーザ名・パスワードを悪用する不正利用が増加し，個人

情報流出，機密情報流失，金銭的被害を受ける事案が発生している。これらの被害から利用者を守るために，厳格な利用者認証が必要とされ，サービスや情報毎に異なるユーザ名とパスワードを用いるなどネットワーク利用の際の手順が複雑化している。そのため，単純で必要十分な認証技術とその適用技術が必要とされている。利用者１人に対して，ひとつのユーザ名とパスワードを割り当てることで，多くのシステムを利用できる統一認証が模索されている。その試みが大学でも進められているが，自由なポリシーのもと各自が独自にサーバを構築し，サービスを提供しているため，なかなか統一認証が進んでいない。また，認証技術の厳格さを求めるあまり認証方法が複雑化し，利用者が敬遠することで，利用者認証が形骸化することが多い。そのため，利用者にも受け入れやすく，利用者を適切に把握できる統一された認証技術とその適用技術が必要である。

電子メールにおいては，利用数の増加に伴い，ネットワーク及びサーバの負荷が増大し，サービスが利用できない状況が発生している。電子メール数の増加原因は，適切なメール利用の増加に加えて，迷惑メールの増加が顕著なためである。山口大学では１日に配送される電子メール数は約３０万通に達し，配送処理数に至っては約３００万件に上っている。この状況下では電子メール配送に数時間に上る大幅な遅延を生じさせ，電子メールの受信が不能になる事態が発生している。実際に配送される電子メールの８割以上が迷惑メールであると想定される。そのため，迷惑メールを適切に判定し，迷惑メールの配送を削減すること，及びそれによるメールの配送遅延を抑制し，必要な電子メールのみを配送することができる，迷惑メール対策及びメールの配送制御技術とその適用技術が必要である。

携帯可能な端末の普及に伴い，利用場所が多様化し，自宅，ホテル等の組織外での利用，学内のネットワークに携帯端末を接続しての利用が増加している。これに伴い，

大学外部のネットワークからの脅威に加えて，大学ネットワーク内部からウイルス感染，不正利用，個人情報漏洩等の脅威が発生している。各々の利用者端末での対策が求められているが，対策を行わない利用者や，対策を行ってもメンテナンスが不十分の利用者もおり，対策が徹底しないため障害や脅威が発生している。そのため，各々の利用者の端末の対策に依存するだけでなく，ネットワーク全体として学内に接続される端末の管理，利用者の把握，利用者に応じたサービスの提供など，不正利用を未然に防止するネットワークの管理及び運用技術が必要である。

以上のような状況に対応し，ネットワーク環境の安定性，高速性，高セキュリティ性を保つために，各利用者が利用する端末や，それらが接続する各サーバのみならず，ネットワーク全体として対応する必要があり，それらを支える運用技術が重要となる。

1.3 論文の構成

第2章では，一般的な運用技術と適用技術について述べ，これまでの研究の流れと，現実的な技術の必要性について述べる。

第3章では，大学でのネットワーク利用において，ネットワークに接続された学内の情報システムが利用する認証を同じユーザ名・パスワードを用いることにより，ユーザ名・パスワードによるセキュリティを高める方法として，全学統一認証の導入方法と認証のあり方について述べる。

第4章では，情報交換の最も基本となる電子メールを安定的に運用するため，特に迷惑メールへの対応や電子メール数の増加による配送遅延への対応について，利用者の利用状況を分析するとともに，解決方法及び対策のあり方について述べる。大学等における電子メール利用者の利用状況は一定ではなく，利用方法，目的も異なるものがあり，利用実態も一定でない。電子メール配送遅延対策において，一律で厳格なポ

リシーを適用するのではなく，電子メール利用者の個別事情に配慮し，各対策を利用者が希望する範囲において，全体としての電子メール環境の健全性を保つ運用的手法の提案と，その試行により得られた知見を述べる。

第 5 章では，利用者ネットワークにおいて，利用者及び利用場所を適切に把握し，利用者の利用目的に応じた，ネットワーク利用が行えるようネットワーク全体としてセキュリティを高める手法とその導入について述べる。

第 6 章では，各々の利用者の端末の利用方法やセキュリティ対策が不十分であっても，ネットワーク全体として適切に対応することで，ネットワークの安定運用及びセキュリティを高めることができることをまとめ，今後の研究課題について述べる。

第２章

ネットワーク運用技術の現状

2.1　統一利用者認証

ネットワークが導入された当初（1990 年代）は，学部等でシステムに詳しい教職員・学生が独自のサーバを構築し，サービスを提供するのが一般的であった。そのような状況では，サーバ間やサーバ管理者間の連携のないまま，サーバ毎に独立した利用者認証が提供されていた。それでも，サービスの範囲が学部内や一部の興味のある利用者にとどまり，また，サービスの量も少なかったため，サーバ利用者が複数のユーザ名とパスワードを使用する状況は少なかった。

しかし，ネットワークが普及し，多くの構成員がネットワークに接続可能な端末を有するようになると，全学構成員を対象とするサーバやサービスが増え，それらの利用者はそれぞれのサービスを利用するため，複数のユーザ名とパスワードを記憶する事が必要となった。このため，サービス利用者は複数のユーザ名とパスワードを手帳に記録したり，ディスプレーなどに貼り付けるなど，サービス利用者によるパスワード管理が不十分な状況が発生してきた。一方，サービスを提供し，ユーザ名とパスワードを発行する管理者は，発行後のメンテナンスを行わない利用者や，パスワードを忘れる利用者への対応何など，管理・運用の負担を避けるため，ユーザ名とパスワードが同一なもの等，簡単なものを発行する場合が多い。例え，厳重な利用者認証で守られた情報システムを構築しても，サービス利用者のユーザ名とパスワードが適切に管理・運用されていないのであれば，認証機能を導入していないのと変わらない状況である。

この状況を解決させ，利用者認証を適切に運用するためには，サービス毎に異なるユーザ名とパスワードであったものを共通化させ，サービス利用者が記録しなくても記憶できる等，利用者自身が管理できる数に絞ることが重要ある。そのためには，大

学内の特定部局が認証情報を一元的に発行・管理し，全学の他のシステムで利用できる統一認証の仕組みを構築する必要があり，各大学においても統一認証の導入が進められてきている[2-7]。

法人化した国立大学においては，トップダウンで統一認証を導入することも可能となってきているが，セキュリティ確保を目指すあまり，複雑な手続きやパスワードを必要とする情報システムを構築する場合が多い。この場合，利用者は情報システムの利用を敬遠し，逆に各部局で独自の認証を立ち上げてしまう問題点が生じる。また，大学の構成員の把握が各部署で閉じており，全体として構成員が適切に把握されていないため，他部署の構成員の認証情報を設定できない場合もある。統一認証が全学で定常的に利用されるには，必要なセキュリティを確保した上で，全構成員を対象とし，利用者にとって利用しやすいものであり，かつ提供側（管理者）にとって提供しやすいものである必要がある。

情報のセキュリティレベル，利用者や提供者のセキュリティに関する認識の度合い，認証の技術レベル及び，クライアントやサーバソフトの対応状況などを総合して，適切な利用者認証を設定する必要がある。山口大学メディア基盤センターにおいてはこの点に着目し，それぞれの時期で利用者・提供者の立場に立った利用者認証を提供することで，自然に全学での統一認証が構築されるように配慮してきた[2]。

当初，情報システム構築に興味のある構成員のいる学部，学科や研究室等において，独自の認証を持つメールサーバが稼動していた。こうした状況下では，管理組織の責任体制や広報の不十分さが生じ，利用者がサービス内容や認証情報の不明な点等の問合せ先が分からなくなる事態が多々起きた。また，当初，情報システム構築者が離籍等を行い，管理者不在，または，引継ぎが不十分なまま運用し続けられるサーバが存在し，障害が発生する場合があった。このような場合，困った利用者は，とにかく大

学の中央機関としての情報系センターに問い合わせればよいと考えがちである。ただ，各大学の情報系センターであっても，管理していないサーバに対する問い合わせに対しては返答できない。また，問い合わせされているサーバの存在さえ知らない場合もあった。

山口大学においても，各種の情報システムにログインできない場合や，ユーザ名やパスワードを忘れた場合などには，まず山口大学メディア基盤センターに問い合せられる場合が多かった。山口大学メディア基盤センターではこの点に着目し，利用者を山口大学メディア基盤センターが導入しているネットワーク接続，電子メール，及びWebサービス等の主要サービスに，以下の段階で，新規利用者及び困っている利用者を誘導することで，統一認証の導入に先進的に取り組んできた。

第1フェーズ　ネットワーク接続におけるユーザ認証の統一

第2フェーズ　メールサービスにおけるユーザ認証及びメールアドレスの統一

第3フェーズ　Webサービスにおけるユーザ認証の統一

2.2　迷惑メール対策とメールの配送遅延対策

情報化社会の進化に伴い，大学等の教育研究機関においても，電子メールは教育・研究及び社会貢献上の業務連絡や情報交換の必要不可欠なツールとなっており，利用者数や利用頻度も年々増加している。その一方，学外からのメールの約８～９割が迷惑メールと推定されている[9]。その結果，利用者にとって重要な電子メールの見落としや配送遅延等が生じ，大学等の業務に不利益を生じさせる場合がある。このため，迷惑メール対策の技術的手法及び対策システムが提案され，大学等への適用方法が検討されている[9-20]。迷惑メール対策を行う対象として，メールサーバの配送経路をメールゲートウェイ経由とし，学内の全メールサーバ宛のメールに対して実施する場

合や，情報系センター等の特定のメールサーバ宛メールに対して実施する場合等がある。いずれの方法も該当サーバの全メールが対象とされている。

一方，迷惑メールの判定手法としては，１）メールヘッダの不正な記述に着目した方法，２）配送方式や配送遅延処理に着目した grey　listing, greet　pause [10]，３）メールに含まれるキーワードを分析する Spam Assassin [14]，及びこれらを組合せた判定方法等が用いられている。判定の結果迷惑メールとされた場合は，A）受信拒否，B）Subject などのメールヘッダに情報を付加し注意を喚起（タグ付け），C）配送保留（隔離），及びこれらを組合せた方法で処理される。いずれの対応も該当サーバ宛の全メールを対象とし，複数の判定方法を組合せている。迷惑メール判定手法のうち，1），2）の判定方式により迷惑メールと判定された場合は受信拒否されるため，正常なメールが迷惑メールと誤判定された場合には，正常なメールを受信できなくなる。キーワード分析を適用する場合は，メールを一旦受信後に判定するため，「タグ付け」または「隔離」の方法で処理される。「隔離」されたメールの中には正常メールが含まれている場合もあり，隔離メールを確認し配送する必要がある。こうした場合，利用者自身が確認し配送することのできるシステムが構築されている。結果的には，機械により迷惑メールと判定されたメールは誤判定されていないか確認する必要があり，確認しない場合は，受信漏れにつながる。完全に迷惑メールのみが駆除できる仕組みは，現在のところ存在しないため，多くの場合，メール受信者に受信不能，受信漏れへの対応を強いていると考えられる。

迷惑メール判定方法１）で用いられる方法の一つに，学外のメール送信サーバが DNS（Domain Name System）逆引き登録にない場合，迷惑メールと判定する方法がある。山口大学の事例では，迷惑メール対策の導入に向けたログ解析において，DNS 逆引きが未登録な送信サーバから受信したメールの差出アドレスが「jinji@会社

名.co.jp」等とあり就職情報であるように思われた例があった。これが迷惑メールと判定された際の受信拒否の可否について議論があり，賛否が分かれた。また，若干のヘビーユーザからは，迷惑メール対策そのものに対する強固な反対意見があった。

大学等における電子メールは，教員では論文投稿や共同研究等で利用され，事務員では省庁や他大学及び業者等との連絡業務等，学生においては講義等に関する情報交換，単位取得・履修確認，及び就職活動等の重要な情報の通信手段として利用されている。現実に，電子メールの不達や遅延の影響により，不利益を生じる場合が発生している。また，電子メールは「通信」のひとつとして，「通信の自由」，「通信の秘密」や「通信の公平性」を有して欲しいと望む利用者もいる。こうした状況は一般企業とは大きく異なる。大学における電子メールの利用方法は，大学組織から一方的に規定されるのではなく，大学構成員の要望と合意に基づいて決定されることが望ましいと考えられる。 すなわち，一般企業とは違い，大学等においては一律なポリシーの適用は難しいと考える。もし一律の対策を適用する場合，それに伴い発生するリスクは，電子メールの受信者が受けることになり，組織として保証できるものではない。これらのことから，利用者の利用状況と希望に応じた迷惑メール対策が必要と考えられる。

これまで迷惑メール対策を導入している多くの大学では，導入の単純性，対策の網羅性などから，一律な迷惑メール対策が導入されて来た。組織としてリスクを許容しても一律に迷惑メール対策を実施する必要があるのか，または，希望者のみへの対策で十分なのかについては，従来ほとんど検討されていない。

利用者の対策希望に基づく，大学等における迷惑メール対策のあり方を提案して来た[19,20]。一律なポリシーを適用するのではなく，電子メール利用者の個別事情に配慮し，既存の迷惑メール対策方法を利用者が希望する範囲において選択でき，全体としての電子メール環境の健全性を保つことができた。また，自由な電子メール環境の

保証を必要とする大学等において，利用者と管理者の双方にとってストレスの少ない迷惑メール対策である。

2.3　ネットワークの安定運用とセキュリティ対応技術

ネットワークの利用の多様化と利用者数の増加に伴い，一つの端末を用いて，インターネット利用，成績等の個人情報の利用・処理，会計等の機密情報の利用・処理など，セキュリティポリシの異なる処理やそれぞれに対応した情報システムへアクセスする場合が増えてきた。一方，インターネット環境は不正アクセスによる端末の不正利用，ウイルス感染による個人情報漏洩，迷惑メールや架空請求被害など，適切なセキュリティ対策を実施していない状態の端末を利用することは大変危険な状況になっている。しかし，危険であってもインターネットを利用しないことはありえない状況にある。

大学においては，ノート PC の高性能化と普及に伴い，学生，教職員が，それぞれの自宅と大学との間で，個人のノートＰＣを携帯し，それぞれのネットワークに接続し，ネットワークを利用する状況がある。また，スマートフォンの普及に伴い，携帯電話でも自宅及び大学の無線 LAN 環境に接続する状況が起こってきている。そのため，自宅でノート PC を使ってインターネット利用を行っている時にウイルスに感染する事があり，そのウイルス感染したノート PC を大学ネットワークに接続し，大学ネットワークへウイルスを感染拡大させる場合がある。この場合，大学で個人情報等の処理をし，その個人情報をノートＰＣに保存した状態で自宅に持ち帰り，ウイルス感染等が原因でインターネットへ個人情報を公開してしまう等の事態に繋がる。各自がノート PC のソフトウェアやウイルス対策ソフトのアップデートを適切に処置している場合は，危険は少なくなると思われるが，アップデートを行わない場合やウイル

ス対策ソフトをインストールしていない端末が存在する。

また，利用者の不注意により情報流出が発生することがある。例えば，学生の成績が記録されたファイルが含まれるフォルダの全ファイルを Web ページにアップしてしまう事，初めは非公開用フォルダに保存していたが，フォルダごと誤って公開フォルダに移動させてしまう事などが考えられる。つまり，インターネットも大学ネットワークも各々の利用者の対応に任せていただけでは，高い危険性を有してしまうことから，ネットワーク全体及び大学全体としての対策（リスク管理）が必要である。

これまで，明らかに機密情報や個人情報を扱うサーバや端末は，インターネットとは物理的に独立したネットワーク，端末，サーバで構成し，インターネットとの通信はファイアウォールを経由し必要最低限の通信制限を設定し，インターネットの危険性から防御してきた。例えば，病院業務システムや大学事務システムがこれにあたる。厳密に限られた利用場所，利用者での利用が前提である。実質的に複数のネットワークを構築していること，それぞれのネットワーク用に端末を設置していることなどを考えると重複投資となり，コスト高となっている。

例えば，教務システムを単に事務職員が利用する場合は，専用ネットワークでもよいが，学生が履修登録・成績確認に，教員がシラバス入力・成績登録などを行う場合などに，利用者や利用場所が厳密に限られない状況があり，専用ネットワークを構成することが出来るとは限らない。このような状況においては，インターネットに接続されるネットワーク及び端末を使わざるを得ず，個人情報を扱うシステムがインターネットからの脅威にさらされている状況にある。インターネットと個人情報を扱うシステムがネットワークを共有する。このような状況の中でも，安全に利用できるネットワーク構築が必要である。

安全なネットワークの構築方法としては，次のものが知られている

(1) ファイアウォールによる通信制御

ファイアウォールによる通信制御を行うのが一般的であり，通常インターネットと学内 LAN などのまとまった単位での制御を行う。インターネットからの不正アクセス等から学内 LAN を守るために，ファイアウォールはインターネットから学内への通信を遮断する機能を持っている。学内からインターネットを利用する際には，その通信を記録しておき，記録した通信のインターネットからの返信パケットを通過する機能を有している。最近では，学内 LAN の各部局の入り口に対してファイアウォールを設ける場合がある。

(2) 利用者特定による通信制御

ファイアウォールでは，利用者個々の PC に対しての制御が行えない。山口大学メディア基盤センターでは，1998 年より，利用者が PC を接続しネットワークを利用する際に，利用者のユーザ名とパスワードを入力させることで利用者を権限のある利用者に特定する認証ネットワークを提案・構築した[21]。その後，他大学においても同様な認証ネットワークの研究や導入が行われてきている。利用者によって，ネットワークの利用資格を制御するものであり，当初は，有資格者が学内 LAN を利用できるようにするものであった。最近では，利用者に応じて利用できるネットワークを制御する機能を付加している。例えば，利用者が学内者の場合は，学内 LAN が利用でき学内資産にアクセス可能とさせるが，学会等で参加している学外者にネットワークを利用させる場合では，学内 LAN の利用は制限し，インターネット利用のみを許可する機能がある。山口大学においては，2007 年より学会等の学外者に対して，ユーザ名・パスワードを発行し，インターネットの利用のみを許可するネットワークを構築し，提供している。

利用者の特定には，利用者認証のほか，PC の MAC アドレス認証や，IP アドレス

認証，さらにはデジタル証明書等がある。これらは，利用者が利用しているPCを認証しているとも言えるため，利用者本人を容易に認証する手法として，ユーザ名・パスワードが用いられる場合が多い。

(3) 不正利用・ウイルス感染の制御

いかに利用者が気をつけていたとしても，不慮にウイルスを持ち込んだり，意図せず不正利用したり，知らず知らずのうちにウイルスを感染している場合がある。ネットワーク内の多くのＰＣがウイルスに感染すると，感染拡大行為をするだけではなく，ネットワークの通信障害に至る場合がある。このような場合，不正利用・ウイルス感染の拡大防止のため，これらが利用する通信ポート（プロトコル）を利用できないよう制御する方法がある。例えば，2003年に猛威を振るったMS BLASTというウイルスは，windows OSが，サーバとの通信を行うためのRPC(Remote Procedure Call)通信を利用していた。一般的にWindows OSで感染するウイルスはこの方法を用いる場合が多い。このRPCは，Windowsサーバと通信する際に用い，通常，端末同士では通信する必要はないにもかかわらず，端末同士の通信できる状態であるためにウイルス感染が拡大する。そこで，ウイルスの感染拡大を防止する方法として，サーバとのRPC通信のみを許可するように制御する方法がある。

通常の情報システムでの通信はクライアント・サーバ間での通信であり，サーバと端末間の通信のみが行われ，端末間での通信は行われない。この場合，端末間での通信は不要となることから，端末間の通信すべてを遮断することが出来る。端末同士の通信を遮断していることから，仮にウイルスに感染した端末をネットワークに接続したとしても他の端末に感染することはない。このように端末間での通信を遮断し，サーバと端末間でのみ通信を許可されるネットワークをマルチプルVLANという。

また，利用者PCがウイルス等に感染した事をネットワークが感知し，該当PCへ

の警報を出力する方法や，通信を遮断する方法がある。これを検疫ネットワークという。山口大学では 2003 年に，講義室・図書館等に設置した学生用ネットワークで導入した。導入以前は，端末のウイルス対策が完全でないことが多く，講義中のウイルス感染拡大やネットワークの通信障害が多発した。導入後は，検疫ネットワークがウイルス感染した多くの PC に対して警報を発生し，通信障害を減少させた。

自由で安全なネットワーク環境を提供するためには，仮に何らかの不正アクセス等の異常があったとき，それを感知し，追跡でき，該当部分のみの対応が行える必要がある。例えば，インターネットの掲示板への不適切な書き込みに対する対応としては，事実を確認し利用者に対して適切な対応を取る場合，認証ネットワークは単に利用者を制御するだけでなく，各々の利用者がどこから・いつ・どのようにネットワーク利用しているかの記録としても重要である。仮に，この追跡性が機能していない場合は，1)疑わしい部分のすべてに対処し大きな影響を与えてしまう，2)結果的に追跡できず適切な対応が取れない恐れがある。

ネットワークの利用目的，また，セキュリティレベル等のポリシーに応じて，1 つの組織であっても，ポリシーの異なったネットワーク利用が複数存在している。一般に，ポリシーの異なるネットワークへのアクセスに対しては，セキュリティを保つために IP アドレスによるフィルタやファイアウォール等を設置し，アクセス制限をかけて運用されている。

このような環境では，次のような問題点があげられる。

1．利用者は，ネットワークの利用目的に応じて，そのネットワークに接続されている異なる端末を利用しなければならない。

2．利用可能なサービスが限定される。例えば，Web やメールは利用できるが，それ以外のネットワークサービスを利用して外部との通信ができないなど。

３．管理者側において，ネットワーク毎に端末を設置しなければならないため，端末の設置場所や維持するための経費が余分に必要となる。

４．誰がいつ，どこから，どのような端末を用いて，どのネットワークを利用しているかを，統一的に管理することが困難な状況である。

ひとつの端末，ひとつのネットワークを複数ポリシで共有し，それぞれのセキュリティレベルを保ちつつ，統一的に利用できれば，これらの問題は解決される。

第3章

ネットワーク利用環境における統一利用者認証の導入

3.1 統一利用者認証の導入方針

他部署が管理・運用する情報システムであっても，ログインできない場合や，ユーザ名やパスワードを忘れた場合などには，まず山口大学メディア基盤センターに問い合せられる場合が多かった。山口大学メディア基盤センターではこの点に着目し，利用者を山口大学メディア基盤センターが導入しているネットワーク接続, 電子メール, 及び Web サービス等の主要サービスに，以下の段階で，新規利用者及び困っている利用者を誘導することで，統一認証の導入に取り組んできた[2]。

第1フェーズ　ネットワーク接続におけるユーザ認証の統一

第2フェーズ　メールサービスにおけるユーザ認証及びメールアドレスの統一

第3フェーズ　Web サービスにおけるユーザ認証の統一

すべての構成員を適切に把握することは不可能であり，それでも完全なものを目指すことは，関係部署の協力が得られなくなり，統一認証を進めることができなくなる。そのため，当初は，すべての構成員を把握することはあきらめ，必要に応じて構成員情報を取得する方針とした。

3.2 ネットワーク接続における利用者認証

3.2.1 学部新入生に対するメディア基盤センターのアカウント発行

山口大学メディア基盤センターでは情報処理教育用に希望の部署の教員及び学生に対して演習用パソコンの提供を行なっていた。全員ではないが多くの学部で情報処理教育が行なわれだしたこともあり, 1997 年度から全入学者を対象に山口大学メディア基盤センターの ID とパスワードの発行を開始した。こでは，入学学生情報の取得方法，ＩＤとパスワードを利用者に伝える方法について，関係部署との調整・整理が必

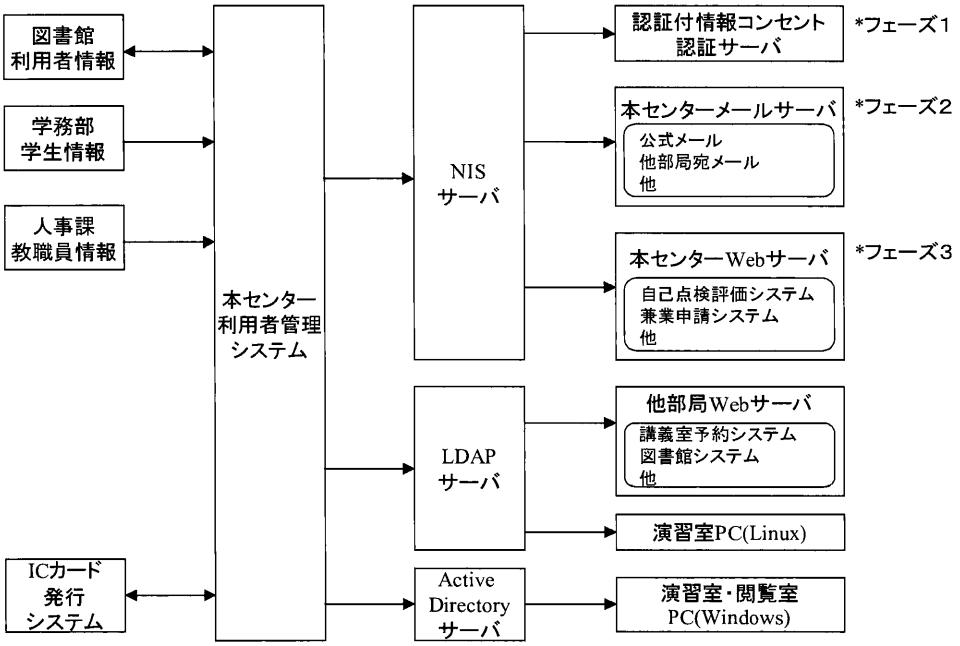


図 3-1 認証システムの概要

要であった。入学者確定後，学務部から入学者リストを取得し，それに対して機械的に ID と初期パスワードを割り当て，当初は A4 用紙サイズの登録証に ID と初期パスワード及びパスワードの運用・変更方法を記載して，各学部で行われる新入生オリエンテーションなどで配布・説明する方法とした。

学生がパスワードを忘れた場合は，山口大学メディア基盤センターにおいてパスワードを初期化（初期パスワードに変更）した。入学時に配布した登録証を紛失した学生が多かったため，学生証により本人確認を行った後にではあるが，初期パスワードも教える必要もあった。そこで，2000 年度からは，登録証を A4 用紙サイズではなく，携帯し易い学生証と同一サイズ（カードサイズ）で配布・説明することにした。

年次進行の結果，学部学生においては，2000 年には全学部学生が山口大学メディア基盤センターの ID とパスワードを取得している状況になった。

3.2.2 認証付き情報コンセント

ノートPCが普及をはじめつつあり，DHCP（Dynamic Host configuration Protocol）[22,23]によるPCのネットワーク設定の自動設定が可能になったことで，図書館等にノートPCをネットワークに接続できる環境を整備する要求が出てくるようになった。しかし，当時DHCPにはユーザ認証機能が存在せず，接続すれば誰でも利用できるという問題があった。大学内でのサービスであることから，単に誰でも匿名で使える情報コンセントでは，サービス責任・教育責任が果たせないとともに利用者責任が明確とならない問題があった。

1998年に図書館等に，先駆けて認証付情報コンセントを整備した[21]。接続にあたっては，利用者の認証とWebページやメールへのアクセスログの保存が必要であると考えた。ノートPC接続後，Webブラウザを起動し，認証ページにてIDとパスワードを入力してもらうことでユーザ認証を行い，ネットワークが利用できるユーザ認証システムを独自に構築した。その認証に山口大学メディア基盤センターのIDとパスワードを用いた。図書館等限定された場所に整備されること，サービスの提供主体が山口大学メディア基盤センターであること，対象が主に学生であったこと，また，学生は全員登録となっていることを背景に，このシステムの導入を試行した。全学ネットワークの構築当初より山口大学メディア基盤センターが全学ネットワークを管理し，サービスを提供してきたこと，認証付情報コンセントの整備がはじめてであったこと，などからシステムの導入が比較的容易に進められた。

認証方法は次のとおりである。

① ノートPCを認証付情報コンセントに接続するとDHCPによるIPアドレス等が自動設定される。

② Web ブラウザを起動すると，認証サーバに接続され，認証ページが表示され，

そこに山口大学メディア基盤センターのIDとパスワードを入力する

③ 認証サーバは，メールサーバに接続しIDとパスワードの確認を行い，正しければネットワーク利用を許可するフィルター設定を追加する。

教職員からは認証付情報コンセントが使えないなどの問合せがあったが，メディア基盤センターのIDとパスワードを取得してもらうことで対応した。この時点で，ネットワーク接続におけるユーザ認証は山口大学メディア基盤センターのIDとパスワードに統一できたと考える（1998年）。

現在では，認証付情報コンセントは，図書館，遠隔講義室，各地区講義室，TV会議室等に整備し，講義，会議等で活用できるようになっている。また，研究室学生へのネットワーク提供の一つとして，指導教員が研究室に認証付情報コンセントを導入するケースも増えてきた。特に，文系の指導教員に希望が多いのが特徴である。各研究室内に認証付情報コンセントを導入することは，利用者認証やログ管理はもちろん，ウイルス対応，ネットワークの不正利用，掲示板を利用した誹謗中傷等への対策の管理を，指導教員が教育的立場で行うのであるが，技術的な点に関しては山口大学メディア基盤センターに依頼することができ，指導教官のネットワーク管理への負担が軽減される効果がある。

3.3 メール環境における利用者認証

3.3.1 メールサーバの集約

山口大学メディア基盤センターの主要サーバであり，学内構成員の多くが利用する可能性の最も高いものは，メールサーバである。1995年以降，文部省からの連絡も，ファックスからメールに変わり，教員だけなく，事務系職員もメールの活用機会が増加し，メールの公的な利用は当然の状況となってきた。しかし，当初は，各部局や研

究室等で独自のメールサーバが運用されていたため，認証情報の統一はもとより，メールアドレスの共有すら進んでいなかった。

メールサービスを利用したい教職員に対して，山口大学メディア基盤センターのメールサービスを利用してもらえるようにすることで，学内構成員が山口大学メディア基盤センターのメールアドレス及びその ID とパスワードを統一して持つことになると考えた。

山口大学メディア基盤センターのサーバを利用してもらえるように，学部学科などで運用されるメールサーバよりも，山口大学メディア基盤センターのサーバの方が，安定であり，メールやフォルダのサイズ等の利用制限もなく，IMAP（Internet Message Access Protocol）サービスの提供など，利用者にとって利便性，安定性が良く，管理者にとって管理コストがなくなるように努めた。このメールサービスの提供を安定運用するため，SMTP（Simple Mail Transfer Protocol），POP3（Post Office Protocol Version 3），及び IMAP のサービスのみを提供する専用サーバを構築した。

IMAP の特徴として，各利用者の受信箱やフォルダが全てサーバ側に保存される。利用者は，異なる場所から，異なる端末を使っても，同じ状態で，メールにアクセスできるといった点で POP3 に較べて優れている。学生や教員などは，学校で使用する PC と自宅や出張先で使用する PC が異なる場合が多い。また，異動の多い事務職員にとっても，メールがそのまま引き継げ，設定変更が容易であることから，利用者が増加している。Web メールサービスとの連携も行い易い。

3.3.2 公式メールアドレスの運用

事務連絡や業務連絡等がメールで行われるようになり，学内構成員のメールアドレスを各部署で把握する必要が出てきた。当初は，事務系職員が学部や学科の教職員の

メールアドレスを調査し，メールアドレスのリストを作成していたが，学部や学科サーバ，理系学部等においては，研究室サーバなどあり，メールアドレスの調査は困難であった。また，最新情報に保つことも困難であった。特定の学部や学科内で教職員のメールアドレスのリストは作成できたとしても，他学部や全学を対象としたメールアドレスのリストの作成にいたっては，ほとんど不可能であった。

そのため，2001 年 12 月 18 日付けで，当時の広中平祐学長の判断で，

1) 山口大学メディア基盤センターのメールサーバに登録があるメールアドレスを公式メールアドレスとすること，
2) 全教職員がメールアドレスを取得すること，
3) メールアドレスの一覧を山口大学ホームページの学内限定版に掲載すること，

を文書にて通知頂いた。この背景としては，

1) 医療系や文系の多くの教職員，及びおおむね全学生が，山口大学メディア基盤センターのメールサーバを利用していた，
2) ウイルスメール対策が実施されていた，
3) 全学へのメールサービスを提供しているのは山口大学メディア基盤センターのみであった

こと等による。これにより，形式的には，大学の教職員及び学生全員が山口大学メディア基盤センターの ID とパスワードを取得することとなった。登録方法は申請制をとったので登録しない教職員も若干いるため，登録のない教職員にはメールによる連絡が取れない等の問題があり，その後の課題となった。

また，通知文書の中に「E メールアドレスを山口大学ホームページの学内限定版に掲載する。」としたことで，学内の全教職員のメールアドレスの一覧表が作成できた。すなわち，学内の教職員の全リスト（個人情報）について人事課から山口大学メディ

ア基盤センターへの流れができた。しかし，人事課にとってのメリットが少なかったため，データの更新が迅速に行えなかったなどの問題点が課題となった。以後，この課題は，人事課を主体としたサービスとの連携を計ることで解決していった。この時点で，山口大学メディア基盤センターのメールサービスにかかる経費は，大学が負担することとなり，利用者への負担としていた課金制度は廃止された。

3.3.3 メールサーバ移行のためのセンター外メールサーバ宛メールの転送

メールサービスの利用者が増加する一方，学部や学科で運用されているサーバは，メールサーバを立ち上げた教員が転勤，あるいは経年によるサーバに障害が生じるなどで，安定運用が困難な状況になっていた。こうしたメールサーバが不調になると，まず山口大学メディア基盤センターに問合せがくるが，山口大学メディア基盤センターでは対応できないという事例が増えてきた。そこで，山口大学メディア基盤センターに問合せがあった際，「山口大学メディア基盤センターのメールサーバを利用していただければ，すぐ対応できるので，可能でしたら，山口大学メディア基盤センターのメールサーバのご利用を検討ください。」と回答することとした。また，山口大学メディア基盤センターのメールサーバへ移行する際の，メールアドレスが変更することを嫌う利用者が多いく，メールアドレスが変わる点が大きな障害であった。そこで，2003年４月より，メールの転送機能を提供することで解決した。山口大学メディア基盤センターのメールサーバへの移行を希望する利用者に対して，学部や学科のサーバ宛のアドレスに送られたメールが，新しい山口大学メディア基盤センター設置のメールサーバのメールアドレスに転送されるよう設定した。こうして，メールサービスの利用者がサーバ移行に伴う大きな障害を回避することができた。

図 3-2 に示すように，山口大学のメールは，学外から学内へ，及び学内から学外への，いずれであっても全てのメールは山口大学メディア基盤センターが設置したメールのウイルスチェックサーバを通過後，配送サーバを経由して学内外に配送されるように構築している。すなわち，山口大学に関する全てのメールは配送サーバを通過する。この配送サーバに転送設定することで，オリジナルのメールアドレスを山口大学メディア基盤センターのメールアドレスに変換して，メールを転送することができる。なお，メールのウイルスチェックサーバの導入は 2001 年，メールの配送経路を統一したのは 2002 年当初である。これらにより，山口大学メディア基盤センターのメールサーバが全学メールサーバとして，名実ともに認知され，メールサービスにおけるユーザ認証が山口大学メディア基盤センターのものに統一される流れが確立した(2003 年)。

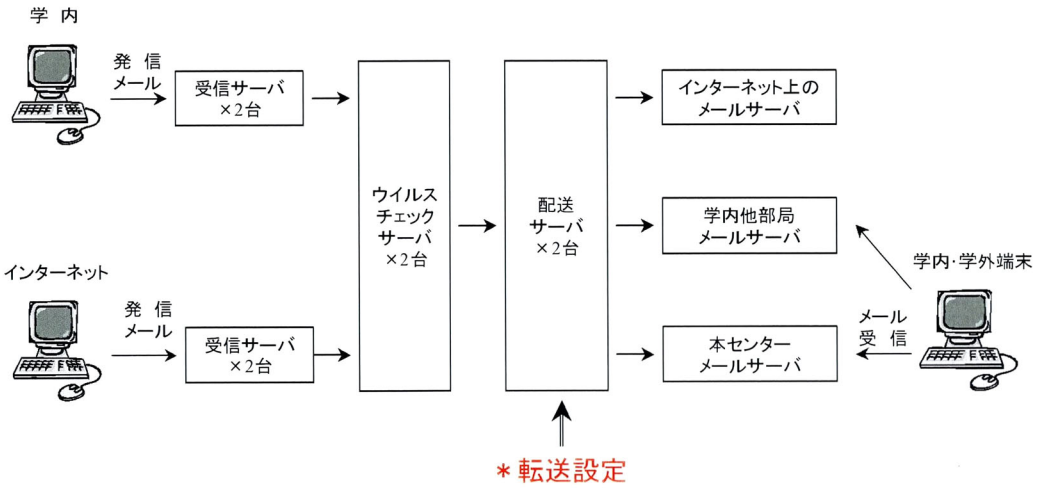


図 3-2　メールの配信経路と転送設定

3.4 Web 環境における利用者認証

3.4.1 Web ページ提供者への利用者認証機能の提供

2000年11月より山口大学メディア基盤センターの利用者であってWebサーバを用いてWebページを作成しようとするWebページ開設者に対して，山口大学メディア基盤センターのユーザ認証を提供するサービスを開始した。山口大学メディア基盤センターのメールサービスにおけるユーザ認証は山口大学メディア基盤センターのNIS（Network Information Service）サーバと連携した。このユーザ認証もNISサーバと連携することで実現した。メールサービスと同じ認証を提供することから，po-login（Post Office login）認証と称している。山口大学メディア基盤センターのWebサーバを利用すれば，山口大学構成員であれば誰でもWebページの作成ができる。またpo-login認証を用いれば，Webページ開設者は，山口大学メディア基盤センターのIDとパスワードによる認証するページを容易に作成することができる。po-login認証はWebサーバの基本（Basic）認証を用いて実現している。Basic認証はそのままでは，ユーザ名はパスワードを暗号化されずにそのまま送られるという欠点があるが，通信を暗号化するSSL（Secure Socket Layer）と組み合わせることで解決できる。

Webページ開設者は，Webページ閲覧者のユーザ認証後のIDを取得できる（ページ開設者が環境変数からIDを取得するCGI（Common Gateway Interface）プログラムを作成した場合）が，パスワードを取得できない。すなわち，Webページ開設者は不正にWebページ閲覧者のIDとパスワードのリストを作成することができない。こうすることで，山口大学メディア基盤センターのWebサーバを用いてページ開設者が，ユーザ認証を必要とするWebページを自由に作成することができるようになった。Webページを作成する側からも，山口大学メディア基盤センターのユーザ認証を容易に利用できる独自の仕組みが提供された。使い方は次のとおりである。

① Webページ開設者は認証を必要とするページのファイルをpo-loginという名前のフォルダ内に置く。

② Webページ閲覧者がpo-loginのフォルダ内のファイルを閲覧する際，webサーバのBasic認証が実行され，認証のためのダイアログがブラウザに表示される。

③ Webページ閲覧者が山口大学メディア基盤センターのIDとパスワードを入力し，その認証が正しければ，Webサーバは該当ページをブラウザに送信する。

単にユーザ認証機能を利用するだけであれば，CGIプログラムを作成する必要もなく，フォルダを作成し，その中にファイルを置くだけである。特に，特定の利用者のみに閲覧を許可したい場合，po-login フォルダ内に .groupfile というファイルを作成し，閲覧を許可したい利用者のユーザ名を列挙することで実現できる。

さらに，2004 年からは PHP（PHP: Hypertext Preprocessor）言語及び Perl（Practical Extraction and Report Language）言語によるCGIプログラムを利用できる機能を提供した，また，許可を得る必要はあるが，Webページ閲覧者の職員情報を取得する機能を提供した。2001年から山口大学評価委員会において導入された自己点検評価（YUSE）システムも，独自サーバで運用されていたが，2005年から山口大学メディア基盤センターの Web サーバ上に移行し，この認証機能を利用するようになった。

3.5 利用者情報の取得

3.5.1 兼業申請システムによる人事情報との連携

山口大学保健管理センターは全学構成員に対して，定期健康診断サービスを提供しており，全学の構成員にサービスを提供している点で，山口大学メディア基盤センターと同じ立場である。全学構成員のリストと各構成員のデータを有する必要がある。

データの質や内容は異なるものの，1)全学構成員のリストとデータを保有する点，また 2)全学構成員のリストを作成するためには，学務部及び人事課の協力が必要である点，では山口大学メディア基盤センターと同じである。1999 年から，保健管理センターでの定期健康診断の自動計測システムの構築に当初からかかわり，健診から証明書発行までのシステム構築を支援した[8]。これにより，全学構成員の個人情報取扱いのノウハウを蓄積した。

2003 年 10 月から，人事課が担当している兼業申請のための Web 申請システムについて，協力して新しくシステム構築をすることとした。これのシステムを実現するためには，次の理由などにより人事情報との連携が不可欠であり，今後の統一認証を進める上で大変有効であると判断したことによる。

1) 多くの教職員が申請している

2) 最新の職員情報が必要

3) 人事課が協力してくれる点

このシステムの利用者認証に人事課の同意のもと，山口大学メディア基盤センターの ID とパスワードを用いることとした。2004 年 2 月からサービスの提供を開始した。システム構築以前は，申請書類の処理に 2 ヶ月以上必要であったが，現在では数日で対応できるようになった。このシステムが稼動後，年度が替わる頃にはほぼ全教員が公式メールアドレス及び山口大学メディア基盤センターの ID とパスワードを取得することとなった。このことにより，利用者認証を提供するために必要な職員情報の提供が人事課より迅速に行えるようになった。

3.5.2 教職員 IC カード

2005 年 4 月より，全教職員の名札としての IC カードを総務課，人事課と連携し導

入した。ICカード導入は総務課が主幹し，山口大学メディア基盤センターは技術的支援及びシステム構築を行った。IC カードは名札の他，入退室管理，複合機利用管理，図書館利用証等に用いている。新規採用や異動の情報は，人事システムに入力された後，山口大学メディア基盤センターの認証サーバ用のデータベースに連携される。このデータベースの情報と写真データを組み合わせて IC カードを発行し，データベースに必要な情報を書き込む。ICカードは全教職員に渡される。このデータベースは図書館システム，入退室システム，複合機利用管理システム等と連携している。人事システムには登録されていないが，大学の業務を行っている構成員にも，ICカードを発行する必要があり，人事課の情報だけでは不十分であるが，他のシステムとも連携することで対応している。

3.5.3 LDAP認証の提供

山口大学メディア基盤センターはLDAP(Lightweight Directory Access Protocol)による認証を，山口大学メディア基盤センターが管理する演習用PCのLinux OSの認証のため整備していた。2004年に学務部及び施設部が導入した講義室予約システムに対して，LDAP認証の提供を開始した。各部局等でのサーバが，山口大学メディア基盤センターが提供する LDAP サーバと連携し利用者認証を行うことが一般的である。しかし，山口大学メディア基盤センターの Web サーバ上でシステムを作成する場合，1)システム構築及び管理が容易である，2)標準で利用者認証機能が利用できるため，現在，多くの Web システムが，個別サーバを構築するのではなく，山口大学メディア基盤センターのWebサーバ上で稼動している。

3.6 評価・議論

山口大学メディア基盤センターの利用者認証機能は計算機利用の認証から始まった

表 3-1 メディア基盤センターの利用者認証統一の経緯

1995 年	文部省からの連絡がメールに変わる
1997 年	学部新入生に対するメディア基盤センターのアカウント発行
1998 年	図書館に認証付き情報コンセントを整備
	ネットワーク接続におけるユーザ認証の統一
1999 年	保健管理センター定期健康診断自動健診システムの構築
2000 年	カードサイズの登録証の配布
	全学部学生メディア基盤センターのアカント取得
	メディア基盤センターWeb サービスの提供開始
2001 年	メールウイルスチェックサーバの導入
	公式メールアドレスの運用開始
2002 年	メール配送経路の統一
2003 年	**メールサービスにおける認証の統一**
	人事課兼業申請のための Web 申請システムの構築
	人事情報の提供の仕組みが確立
2004 年	Web サービスにおける CGI 機能提供
	LDAP 認証の提供
2005 年	全教職員 IC カード名札の発行
	自己点検評価システム (YUSE) がメディア基盤センターWeb サーバへ移行
	教職員ポータル (Web システム) の提供
	Web によるユーザ認証の統一

が，この数年間，ネットワーク接続における利用者認証，メールサービスにおける利用者認証，及び Web サービスにおける利用者認証と連携させることで，概ね大学としての統一認証が実現できた(図 3-1，表 3-1 参照)。ID 登録のための個人情報は当初図書館と連携するだけだったが，学生部の学生情報，人事課の教職員情報とをそれぞれ連携することで，大学関係者の概ね全ての情報を保有することができ，山口大学メディア基盤センターの利用者認証は大学の標準認証としての地位を確立してきた。このことは，今後，デジタル証明書等の新しい利用者認証システムなどを導入する際にも抵抗なく実施できることを保証している。

山口大学メディア基盤センターが運用する主要サーバ，特にメールサーバ，Web サ

ーバに利用者を誘導することで，サービスの集約化ができ，統一認証に進んだ。また，サービスの質，セキュリティ向上のため山口大学メディア基盤センターが主導する立場となっている。現在は，人事情報の個人番号をもとに利用者認証サービスを提供している。職種によっては，非常勤職員から常勤職員へ，また，逆に常勤職員から非常勤職員に変更する場合がある。変更の際には，個人番号が変更になり，人事システムのデータ上は別人と扱われている問題点がある。実際，人事システムのデータ上は旧個人番号の職員は退職として扱われている。個人番号が変更されると，これまでのサービスが受けられなくなる。IC カードも個人番号が変更された時点で無効となる。

上記のように個人番号が変更された場合は，2006 年 4 月より，次の方法で，対応付けを行うこととした。

① 個人番号が変更した職員は大学情報機構に IC カードを提示する。

② IC カード情報を旧個人番号から新個人番号に変更する処理を行う。旧個人番号と新個人番号の対応付けを行う。

③ 山口大学メディア基盤センターの ID とパスワードは新個人番号に対応づける。

なお，この問題の根本的解決には，人事システム内での検討が必要である。

また，非常勤講師の場合，同一人物でありながら，講義を行う学部毎に異なる個人番号を有している場合がある。ユーザ登録されていない非常勤講師の ID の発行や，IC カードの発行を行うには，どれか特定の一つと関係付けることが必要である。現状では，非常勤講師の申請により発行しているので，申請時，個人番号を選んでもらうようにしている。利用者認証で用いる本人を特定するための情報は，教務システム及び人事システムに頼らざるを得ない。認証を進める上で，これらのシステムに必要な改善を行う必要がある。現状のデータを移行しなければならないこれらのシステムでは，対応が難しいかもしれないが，新システムでは，個人と番号の対応関係が例外な

く一対一になるように構成されることを期待したい。また，山口大学メディア基盤センターとしても，支援しなければならない。IC カードの発行は平成 20 年度までは教職員に限られていたが，平成 21 年度からは学生にも学生証兼用で発行された。今後展開すべきサービス等の整理を行っていく必要がある。

山口大学メディア基盤センターが提供するネットワークサービスに集約したことで，シングルサインオンの機能を実現できているが，今後，サービスが多様化し，サーバの複数化に対応するためサーバ間で連携するシングルサインオンの機能を提供する必要がある。現状では，ID とパスワードの組み合わせによる利用者認証が一般的であるが，よりセキュリティの高い認証方式が必要となってきている。たとえば，学外から非常勤講師が担当講義科目の成績を入力するなどといった場合，ID とパスワードの認証だけでは不十分である。入力者を特定するためにデジタル証明書等を用いた利用者認証方式を導入していく必要がある。デジタル証明書の運用については，技術的には可能であっても，実際の運用を想定したときに，公開鍵や秘密鍵の運用管理，システムの運用等をスムーズに行う仕組みを考えていく必要がある。

3.7 まとめ

山口大学メディア基盤センターでは，この数年間，統一認証の実現が自然に行えるよう取り組んできた結果，おおむね大学としての統一認証が実現できた。また，山口大学メディア基盤センターが提供する基本サービスの一つである利用者認証サービスは，全学の標準の利用者認証と位置づけられ，全学の利用者認証の管理をする部署は山口大学メディア基盤センターという認知を得ることができた。事務システムについは，文部省(導入当時)が指導するシステムが稼動しているので，個別の認証であり，システム連携も行えない状況である。国立大学法人化後，大学独自のシステムへの移

行が検討されている。山口大学メディア基盤センターが所属する大学情報機構の情報化推進課と連携して，これらのシステム改変の際に，認証の統一や他システムとの連携などの機能を組み込む必要がある。

国立情報学研究所が構築を目指している全国大学共同電子認証基盤(UPKI)のような大学間での統一認証への参加にも，学内の統一認証は必要条件となっている。認証の統一だけでなく，学内の情報システムの整備には，山口大学メディア基盤センターが支援・連携しながら進める必要があり，大学の中での山口大学メディア基盤センターの位置づけが重要となっている。

第4章

希望者が選択する迷惑メール対策と配送遅延対策

4.1 迷惑メール対策の構成

4.1.1 山口大学におけるメールの配送方法

山口大学におけるメール環境の整備は，全学で統一したメール環境を用いる方針（2001年当時の学長方針）のもと，メディア基盤センター（以下センターと略す）が運用するメールサーバ（以下全学メールサーバと略す）に利用者を誘導することで始まった。現状では，センターのサーバが全学の公式メールサーバとして認知され，ほぼ全構成員（教職員・学生等）が利用している。しかし，現状においても，学内には各部局・研究室独自のメールサーバがあり，各サーバの管理状況や迷惑メールへの対応が不十分であることを考慮して，以下の諸機能を提供するためメール配送経路を統一している。

（1） 流入・発信するメールに付着するウイルスを防止するため，山口大学宛てのメールおよび山口大学から発信されるメールのウイルスを駆除する機能。

（2） 学内のメールサーバによるOpen Relayを防止する機能。

（3） 差出アドレス偽造メールの送信防止のため，差出アドレスを山口大学ドメインに限定する機能。

山口大学のメールの配送経路を図4-1に示す。また，主要サーバのハードウェアスペックを表4-1に示す。学内および学外から配信されるメールは一旦受信サーバで受信され，ウイルス駆除が行われた後，配送サーバからインターネットおよび学内のメールサーバに配送される。なお，山口大学ではDNSの管理はセンターが統一管理しており，学内のメールサーバのMX（Mail eXchange）は受信サーバに設定されている。利用者は本来，すべてのメールを受信したい，誤って重要なメールを不達にされたくないと希望していることに配慮し，センターとしては原則として全てのメールを

受信者に配送するという方針をとっている。

4.1.2 迷惑メール対策の概要

現時点において完全な迷惑メール対策は存在しないことから，山口大学では対策の有無，対策の方式・パラメータ等を利用者自身が選択できる迷惑メール対策を，2006年９月から開始した[19,20]。迷惑メール対策の対象となるメールサーバは，以下の理由により全学メールサーバとした。

（1） 全学構成員が利用している唯一の全学メールサーバであること。

（2） メールアドレスと全学認証とが１対１に対応していること。（ただし，利用者は複数メールアドレスを取得することができ，保有するメールアドレスごとに迷惑メール対策を希望できる。）

他部局等のメールサーバも独自に運用されているが，今回の対策では他部局のサーバは対象外とした。

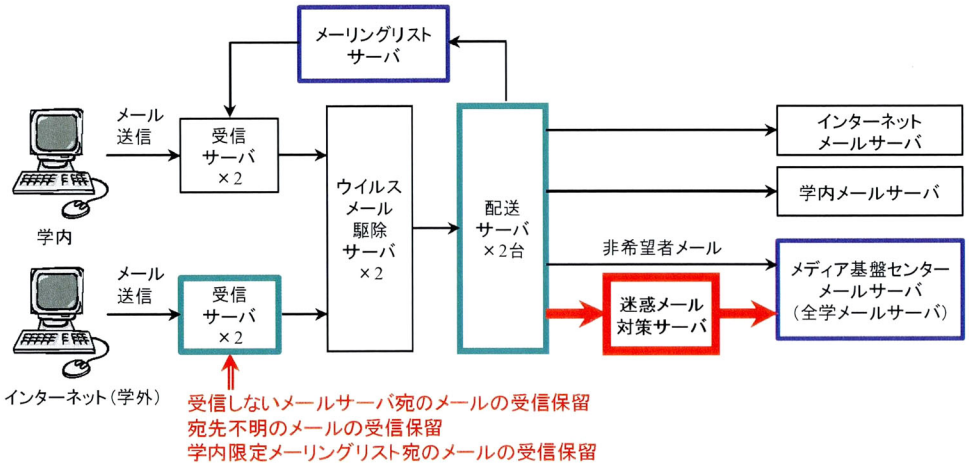


表 4-1 各サーバのハードウェア性能

server	receiving mail server	transmitting mail server	university mail server	mailing list serer
CPU	PentiumIII 1GHz	PentiumIII 1GHz	PentiumD 3.40GHz	Pentium4 2.53GHz
memory	512MB	512MB	3GB	512MB
HDD	40GB	40GB	6TB	80GB
Network	100BaseTX	100BaseTX	1000BaseT	100BaseTX
OS	FreeBSD	FreeBSD	FreeBSD	Linux

利用者自身が各パラメータの選択を行う必要があることから，迷惑メール対策の機器は全学認証システムと連携でき，電子メールの内容に基づく対策が実施できるバラクーダ社製の Spam Firewall 400（現：SPAM & VIRUS FIREWALL 400）[24,25]を導入した。この機器は当初，利用者毎の迷惑メール対策適用の可否を選択できなかったため，可否を選択する仕組みを独自に開発した。図 4-1 の配送サーバの MTA (Mail Transfer Agent)として Postfix を用いており，通常，宛先アドレスに対応したメールサーバにメールを配送する。迷惑メール対策希望者宛てのメールのみを迷惑メール対策サーバに配送することで，迷惑メール対策を実施する仕組みをとった。具体的には配送サーバの Postfix の設定の一つである transport_maps に指定するファイルに，迷惑メール対策希望者のメールアドレスと，配送先である迷惑メール対策サーバの FQDN を登録する。迷惑メール対策希望者自身が，センターの迷惑メール対策を説明する Web ページで，迷惑メール対策の有無を選択することで，自動的にこのファイルに希望者のメールアドレスを登録し対策を有効にする仕組みを構築した。

また，本機器は全学認証システムと連動する場合，認証のユーザ名とメールアドレスのユーザ名が一致する必要があるため，対象外とした他部局等サーバに対応していない。この機器は，山口大学における電子メールの配送経路の中で，ウイルス検査後，宛先メールサーバに配送する配送サーバと全学メールサーバとの間に配置し，迷惑メ

表 4-2 迷惑メール対策利用者 2007 年 9 月 23 日

教職員数	2,122
学生数	10,695
メール利用者数	7,200
迷惑メール対策希望者数（全体）	778
迷惑メール対策希望者数（学生）	78
迷惑メール対策希望者数（隔離設定）	215

ール対策希望者の電子メールのみが通過するように設定した（図 4-1 参照）。 サービスは，以下の手順で提供した。

（1） 迷惑メールと判定されたメールのサブジェクトにタグ文字を付加し配送する機能の提供（2006 年 9 月～），

（2） 迷惑メールの隔離及びパラメータ変更機能の提供（2007 年 3 月～），

（3） 配送遅延への対応のため対策サーバの二重化実施（ 2007 年 7 月～）。

なお，参考のため 2007 年 9 月 23 日時点での全構成員に対する迷惑メール対策利用者数等を表 4-2 に示している。

迷惑メール対策開始にあたり，通常メールが迷惑メールに判定される場合(False Positive)が懸念されることから，迷惑メールと判定された電子メールにはタグを付け，全ての電子メールを宛先に配送するサービスを提供し，迷惑メール対策の実施状況を確認した。迷惑メール判定に用いるスコア値の閾値の設定にあたり，メーカ推奨値（3.5）を用いず，迷惑メールが判定されずにすり抜ける場合（False Negative）が多少増えたとしても，通常メールを迷惑メールと誤判定する場合（False Positive）が少なくなるように大きめの値（6.5）に設定した。メーカ推奨値では日本企業等からのメールマガジンなどが迷惑メールと判定される場合があり，これらの誤判定が少なくなるよう

に少しずつ値を大きくして調整した。この閾値において，手順（1）の開始から 2006 年 10 月 17 日までの間，筆者（久長）宛てに送られた電子メールを分析したところ，迷惑メールの中でタグ付きのもの（迷惑メールと判定）が 1,858 通（86.2%），迷惑メールの中でタグ付きでないもの（通常メールと判定）が 297 通（13.8%），通常メールがタグ付きとされたもの（迷惑メールと判定）が 2 通(0.1%)であった。

4.1.3 電子メール配送遅延対策

希望者のみに迷惑メール対策を提供する一方，非希望者へは全電子メールの配送が必要となる。このため，電子メールをメールゲートウェイ（図 4-1 では配送サーバ）で一旦全てのメールを受信後，希望者と非希望者とで迷惑メール対策サーバに流入する電子メールの制御を行う必要がある。しかし，メールゲートウェイを設けた場合，宛先不明メールを受信した際のバウンスメールが生じ，迷惑メールの中継，及びバウンスメールの送信先となるメールサーバの過負荷等が指摘される[9,11,16]。さらに，メールゲートウェイの配送処理数が増加し，配送遅延が生じ，自組織への影響が発生する可能性がある。山口大学でも，図 4-1 の配送サーバでの一日あたりの配送処理件数が約 250 万件以上にも達したが，実際に配送されている電子メール数は約 1 割の 30 万件程度であり，残りの 220 万件は配送失敗であった。メールゲートウェイを導入し，宛先不明の電子メールを一旦受信してしまうと，配送不能による再送処理に伴い配送処理件数が大幅に増大する。再送処理の時間切れに発生するバウンスの返送処理も同様である。この結果，配送遅延の問題が発生する場合がある。

そこで，学内の各々のメールサーバの適切な管理を呼びかけるとともに，大学全体として，宛先不明の電子メールを学内に取り込まない措置が必要となる。山口大学メディア基盤センターでは，以下のような配送遅延対策を大学全体で実施した。

（1） 配送サーバのログを元にメールサーバの稼働状況の整理と管理の徹底。

（2） 大学全体での一元的な宛先不明メールの受信拒否の実施。

対策(1)は，不適切な管理下にあるメールサーバの排除であり，このための動作不良は発生しにくいと考え速やかに実施した。対策(2)では学内のサーバへ宛先確認を行うため，図 4-1 の学外からの受信サーバの MTA である Postfix の address verify 機能を用いた。address verify は次のような宛先アドレスの有効性を確認する機能である。通常，MTA は他の MTA からメールを受信する際，まず，差出アドレスを受取り，続いて宛先アドレスを受取り，その後本文を受取ることでメールを受信する。address verify 機能を有効にした MTA(以下 MTA①と表す)は，宛先アドレスを受取った時点で，宛先アドレスの最終的な配送先 MTA(以下 MTA②と表す)に対して，その宛先アドレスの有効性を確認する。具体的には，MTA①は MTA②に対して，「MTA①のホスト名」，「MTA①で設定された差出アドレス」，「宛先アドレス」の順に送信する。MTA②は「宛先アドレス」を受信した際に，「宛先アドレス」宛のメールを受信することができる場合は「受信可能」をレスポンスとして返信し，それ以外の場合は「受信保留」または「受信拒否」を返信する。MTA①は MTA②から「受信可能」のレスポンスを受取ることで，宛先アドレスの有効性を確認する。なお，MTA②が Postfix 以外の場合でも，同様の動作を行うので，MTA①は宛先アドレスの有効性を確認することができる。MTA①は，宛先アドレスの有効性が確認できた場合にのみ，メールを受信する。address verify の再確認時間はデフォルト値（3 時間）とした。対策（2）は，実施に伴う動作不良により必要な電子メールへ影響がでないように，慎重に利用者への周知およびシステム試験等を行い，対策(1)の約半年後から実施した。

4.1.4 メーリングリストの迷惑メール対策による配送処理数削減

山口大学では，全学で利用できるメーリングリストのサービスを提供している。メーリングリストサーバ（図 4-1 参照）は，学内及び学外から発信されたメールを配送サーバから受取り，学内用受信サーバを経由し，複数のメンバー宛にメールを複製し送信する。メーリングリストサーバのソフトウェアは mailman を用いている。教職員は誰でも，利用申請を行うことでメーリングリストを開設することができる。メーリングリストの管理は，開設者が Web ページから行うことができる。一律な迷惑メール対策を実施する場合は，メーリングリストの前段で迷惑メール対策が行えることから，メーリングリスト宛の迷惑メールを阻止できる。一方，希望者のみに迷惑メール対策を実施する場合，メーリングリストサーバの後段で迷惑メール対策を行う必要があることから，迷惑メールがメーリングリストにより複製されてしまい，迷惑メール数の急増に伴う配送処理遅延の問題が生じる。そのため，希望者のみの迷惑メール対策の場合，メーリングリストへの迷惑メール対策は，追加対策が必要となる。学内からメーリングリスト宛に到達する電子メールは，1 日あたりわずか 100 通前後であるのに対して，学外からメーリングリスト宛に到達するメールは約 2 万通（全電子メールの 1 割）にも達する。また，ある学部の全教職員に業務連絡を通知するメーリングリストから迷惑メールが配信される例も存在した。すなわち，投稿者管理が不適切なメーリングリストが存在し，迷惑メールを複製していることが予測された。

通常，メーリングリストはその開設者により利用目的や運用ポリシーが明確である。たとえば，学部の教職員の連絡用として開設されているメーリングリストでは，あらかじめその投稿者は当該学部の教職員のみに限定される。学外者から当該メーリングリストへの投稿は想定されないため，このメーリングリストへの投稿を学内からのみと限定しても，希望者のみに迷惑メール対策を実施するポリシーに反しないと考えら

れる。投稿者が学内者に限定されたメーリングリスト宛であるメールのうち，学外から発信されるメールを受信拒否することで，迷惑メール数の削減，及びそれに伴う配送遅延の削減が期待できる。そこで，付加対策として，メーリングリスト管理者へ，メーリングリストへの投稿は学内のみか，または学外も含まれるのかを検討するよう依頼した。その後，学内限定とされたメーリングリストでは，図 4-1 の受信サーバで学外からのメールを受信拒否することで対応した。

4.2 実施と効果

4.2.1 希望者のみの迷惑メール対策の効果

迷惑メール対策を強く要望するメール利用者は「多くのメール利用者が平均的に多数の迷惑メールを受信しており，迷惑メールを受信しないことはまれである。」と考えている。このため，大学全体として一律に迷惑メール対策を適用する方が良いとの判断に陥り易い。一方，文字数が短く推測しやすい電子メールアドレスであっても，迷惑メールを受信しない電子メールアドレスが存在することも知られていた。そこで，迷惑メールの受信状況の実態を把握するために，全学メールサーバが処理した 1 日あたりの電子メール受信数を指標として，宛先電子メールアドレスを分類した。

図 4-2 に 1 日あたりの受信メール数による受信アドレス数の割合の日付による推移を示した。1 日あたりの受信メール数を，10 通未満（青色），10～19 通（紫色），20～49 通（黄色），50～99 通（緑色），100 通以上（濃紺色）に分類した。平日・休日で若干の変化が見られるが，1 日あたり 10 通及び 20 通未満の電子メールを受信しているアドレスが大半を占めていることがわかる。この傾向は調査期間内の時期に依らずほぼ一定である。通常，大学では 9 月末までは夏休み期間であるが，10 月以降の学期期間中と変わらず同様の推移を示していた。そこで，平日の代表的な日として，2007

年 9 月 21 日を選択し，さらに詳細な分析を行った。文献 19 においては，前期授業期間中の日を選定し分析したが，本稿では夏休み中の日を選定し，データの再現性の確認と，さらに詳細な検討を加えた。

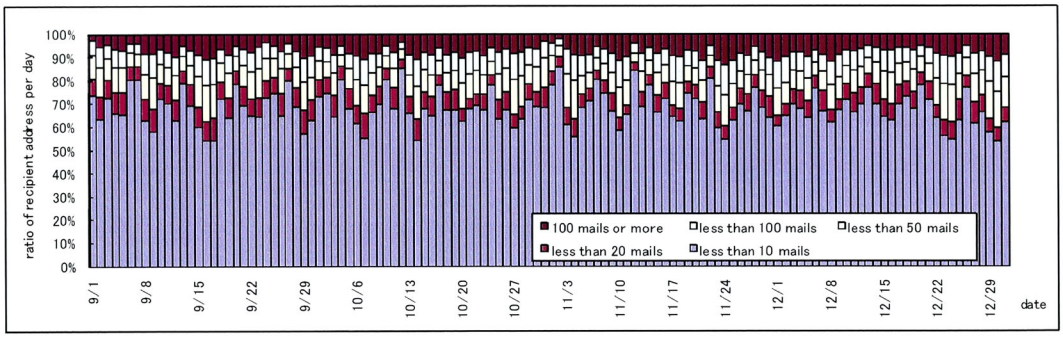


図 4-2 １日の受信メール数に対する受信アドレス数の割合（2007/9/1～12/31）.

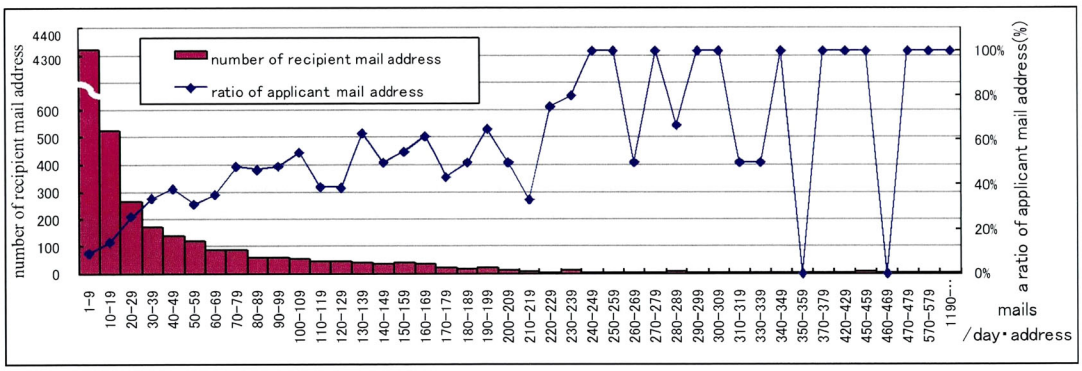


図 4-3 １日の受信メール数に対する受信アドレス数と希望受信アドレスの割合(2007/9/21)

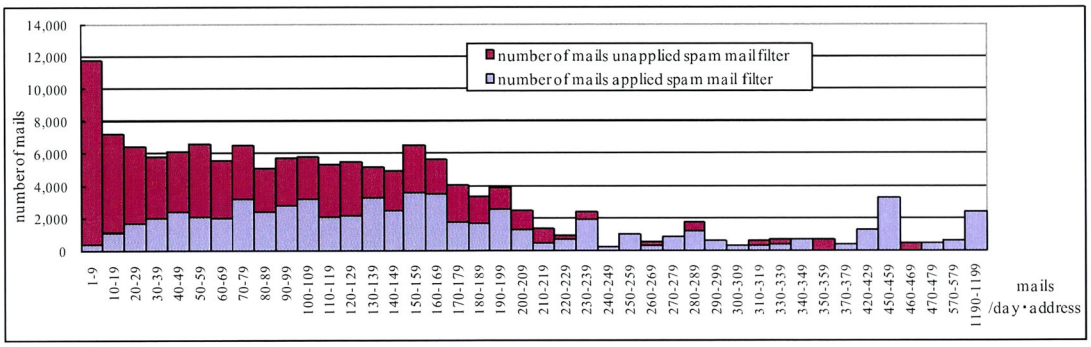


図 4-4 １日の受信メール数に対する対策メールと非対策メール数(2007/9/21)

図 4-3 は，2007 年 9 月 21 日の 1 日中に 1 受信アドレスあたりの受信電子メール数に対する受信アドレス数を示す。受信アドレスによりメール受信数の差が大きいことから，1 日あたりに受信するメール数が 10 通未満の受信メールアドレス数は省略表記とした。また，表 4-3 に代表的な値を示した。この結果から，迷惑メールを殆ど受信しない受信メールアドレスが多く，迷惑メールを数多く受信しているメールアドレスが少ないことが予測できる。メール受信可能なメールアドレス数は約 15,000 個，この日の受信電子メールアドレス数が 6,269 個，そして全電子メール数が 139,918 通であった。1 日あたり受信する電子メール数が 10 通未満の受信メールアドレスの個数が 4,323 個と全受信メールアドレス数の 69%で，その受信メールアドレスが受信する電子メール数の計はわずか 11,722 通（全受信メール数の 8%）となっていた。一方 50

表 4-3 一日あたりのメール受信数, 2007/9/21.

1 メールアドレス・1 日あたりの受信メール数	0 通	1 通以上	1~9 通	50 通以上	100 通以上
受信メールアドレス数 (個)	about 9,000	6,269	4,323	844	429
全受信メールアドレス数に対する受信メールアドレス数の割合 (%)		100	69	13	7
迷惑メール対策希望メールアドレス数 (個)		736	77	404	236
受信メールアドレス数に対する迷惑メール対策希望メールアドレス数の割合 (%)		12	2	46	55
受信メール数計 (通)		139,918	11,722	102,680	73,413
全受信メール数に対する割合 (%)		100	8	73	52
迷惑メール対策を適用されたメール数計 (通)		63,792	353	56,367	44,113
迷惑メール対策を適用されたメール数割合 (%)		46	3	55	60

通以上受信している受信メールアドレス数は 844 個（全受信メールアドレス数の 13%），受信した電子メールの総数は 102,680 通（全受信メール数の 73%）であった。また，100 通以上の電子メールを受信している受信メールアドレス数は 429 個（全受信メールアドレス数の 7%）で，受信メール総数は 73,413 通（全受信メール数の 52%）であった。一方で，図 4-3 には記載していないが，約 9,000 個のメールアドレスは電子メールを 1 通も受信していなかった。すなわち，受信メールアドレスのうち，電子メールを受信しない，あるいはわずかな数のメールを受信する受信メールアドレスが大半であり，少数の受信メールアドレスが，大量に電子メールを受信していることがわかる。

図 4-3 の電子メールの受信状況に，迷惑メール対策を希望した受信メールアドレス数の割合（図中折れ線）を重ねると，電子メールの受信数が多くなるにつれて，迷惑メール対策の希望アドレス数の割合が増加していることがわかる。1 日あたり 100 通以上のメールを受信しているアドレス 429 個のうち，迷惑メール対策を希望しているメールアドレスは半数以上の 236 個（55%）であった。また，1 日あたり 10 通未満のメールを受信しているアドレス 4,323 個のうち，迷惑メール対策を希望するメールアドレスはわずか 77 個（2%）であった。迷惑メール対策希望の受信メールアドレスは，大量に電子メールを受信して迷惑メールで困っているメールアドレスである。対策を希望していない受信メールアドレスは 1 日に少数のメールしか受信していないメールアドレスであり，迷惑メールで困っていないと予測される。これらの傾向は前報[19]の結果とほぼ一致しており，対策が必要なアドレスは一日に数多くのメールを受信しているアドレスと考えられる。

ここで，全メールに迷惑メールが均一に含まれると仮定してみよう。例えば，迷惑メールの割合を 80%と仮定する。すると，1 日 10 通未満の受信メールアドレスの 1

アドレスあたり受信メール数は平均 2.7 通となり，うち迷惑メールは 2.2 通となる。一方，1 日 100 通以上受信するアドレスの 1 アドレスあたりの平均は 171 通で，うち迷惑メールは 136.8 通となる。従って，少数の受信メールアドレスは仮に迷惑メールを受信していたとしても，迷惑メールが大量に届き困る状況にはない。この状態でリスクを冒してまで迷惑メール対策を選択することは考え難い。また，実際には 1 日の受信メール数が少ないアドレスは殆ど迷惑メールを受信していないと思われる。

受信メール数に偏りがあることの原因の一つとして，大学構成員における職種などの特殊性と偏りが考えられる。大学等の教員は，研究者情報としてメールアドレスがさまざまな Web ページに記載されており，その他にも問い合わせ窓口用の電子メールアドレス，さらにメーリングリストアドレスが山口大学 Web ページにも記載されている。公開されているとも言えるこれらのアドレスが，迷惑メールの標的になると考えられる。一方，学生，事務職員のメールアドレス，教職員がもつ 2 個目以降のメールアドレスなど Web ページに記載のないメールアドレスは，迷惑メールの送信標的になりにくいと考えられ，このため迷惑メールの受信状況に偏りが生じると推測できる。

希望者のみへの迷惑メール対策の有効性を確認するため，迷惑メール対策希望メールアドレスへの受信電子メールの総数，すなわち迷惑メール対策が適用された電子メール数を調べた。図 4-4 は，2.2 節で述べた迷惑メール対策を実施して 1 年間経過した 2007 年 9 月 21 日の時点における，全学メールサーバが受信した電子メールのうち対策されたもの（灰色）と対策されないもの（黒色）の内訳数を示す。迷惑メール対策が適用された電子メールの総数が 63,792 通，適用されなかった電子メールが 76,126 通であった。迷惑メール対策された受信メールアドレスは受信メールアドレスの 12% であるにもかかわらず，全受信電子メール数の半数近く，46%の電子メールに，迷惑

メール対策が適用されていた。特に，1日あたり100通以上の電子メールを受信しているメールアドレス宛の電子メール数の合計73,413通のうち，60%の44,113通に迷惑メール対策が実施されていた。迷惑メール対策を希望した受信メールアドレス（希望者）のみへの対策により，全体の半数近いメールが対策され，ヘビーユーザでは半数以上の電子メールが対策されることから，迷惑メール対策が効果的に働いていることがわかる。一方，受信した全電子メールのうち半数以上は迷惑メール対策サーバによる処理が必要なく，サーバ負荷の削減に有効となっていることがわかる。こうした傾向も前報の結果とほぼ一致しているが，，前回の調査時点（2007年6月1日）に比べて，約3か月半の間にヘビーユーザ(一日の受信メール数が200件以上のアドレス)の対策への参加が進んでいる事が確認できた。

一方，図4-3に見られるように，大量にメールを受信しているにもかかわらず，迷惑メール対策を希望していない受信メールアドレスがいくつか存在している。もし，これらの受信メールアドレスが一旦受信後，他のメールサーバに転送を設定していた場合には，山口大学メールサーバが迷惑メールの発信源として判定され，山口大学メールサーバが受信拒否サーバリストに記載される恐れがある。また，迷惑メール対策を適用しているが迷惑メールがすり抜ける判定となった場合も同様である。現在，このような障害は顕在化していないが，今後，迷惑メールの増大に伴い顕在化することもあり得ることから，メール転送のあり方についての検討が必要である。

山口大学での迷惑メール対策の導入にあたって，迷惑メール対策の希望を呼びかけたところ，大量に電子メールを受信している殆どの全学メールサーバ利用者が当初から申請した。また，迷惑メール対策導入により重要な電子メールの不達が生じ，迷惑メール対策に対する批判がなされ，対策中止となる事態を防ぐ工夫をした。すなわち，導入から半年間は，迷惑メール対策希望者の電子メールが迷惑メールと判定された場

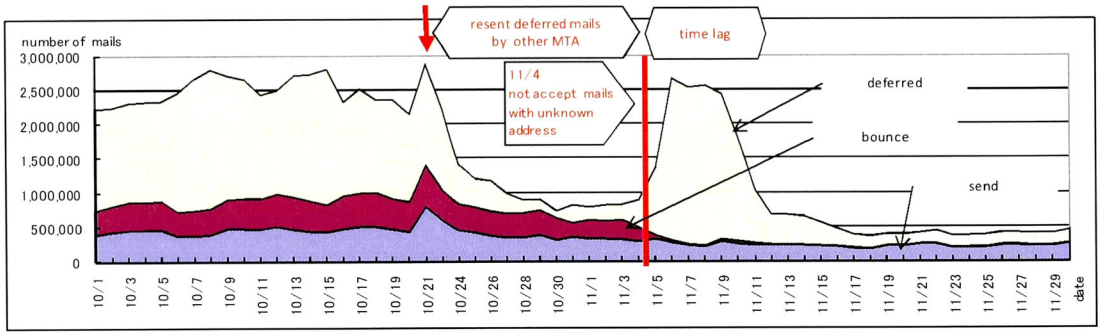


図 4-5　1 日あたりのメール配送処理件数．黄色は配送保留，紫は拒否，青は配送を示す．

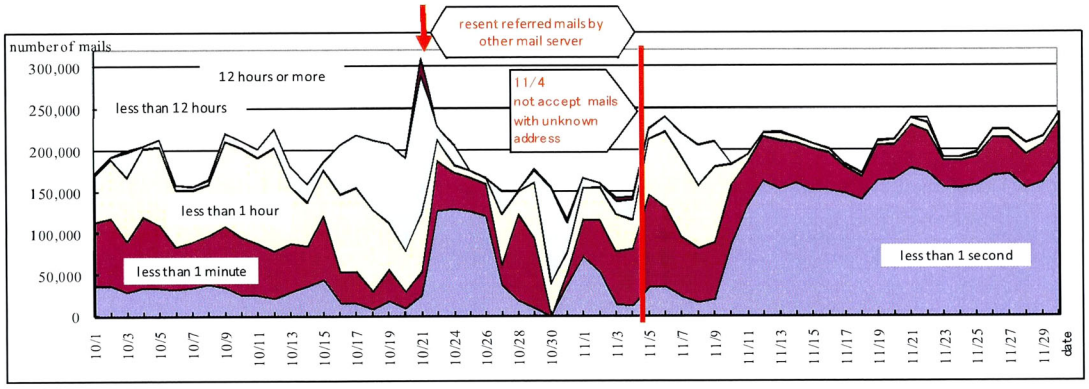


図 4-6　1 日あたりのメール配送遅延時間とメール数．青は 1 秒以内，紫 1 分以内，黄色 1 時間以内の遅延を示す．

合，そのサブジェクトに迷惑メールの可能性を示すタグをつけて配送する措置を行い，その後希望に応じて隔離等の処理を追加した。今後，機能追加する際には，利用者数の推移による対策の影響についての分析が必要であると考える。

4.2.2 電子メール配送遅延対策の効果

迷惑メール対策の導入に伴って発生した配送遅延対策の第一歩(対策(1))として，大学内のメールサーバの稼動状況を調査した。2007 年 4～5 月と 2 ヶ月間分の配送サーバのメール配送ログを分析し，1 通の電子メールも受信していないサーバを「運用されていないメールサーバ」，1 通でも受信したメールサーバを「運用中メールサーバ」

と判定した。明らかに，この条件は緩やかであるが，今回は最低限メールサーバとして受信機能が動作している点に着目し，これを基準とした。緩やかな条件にもかかわらず，学内全体で，運用されていないメールサーバは289台，運用中のメールサーバは63台と判明した。運用中のメールサーバは全体の2割にも満たない。この結果は全く予想外であり，全体の78%ものメールサーバの管理が適切でない状況が明らかとなった。大学組織として，メールサーバの把握・管理の必要性を改めて認識した。

2007年6月3日および7日の2回にわけて，「運用されていないメールサーバ」と判定された289台のメールサーバ宛のメールアドレスを，インターネット用受信メールサーバ（図4-1参照）で，「受信保留」とするよう設定し，メールを受信しない措置を行った。具体的には、main.cfに以下の設定(太字部分）を追加し，deliveryファイルに「運用されていないメールサーバ」289台を登録した。この対応後，メールの配送遅延はわずかに改善されたが，配送遅延の解消までは至らなかった。

address verify機能による配送遅延対策（対策（2））実施前後での，配送サーバの1日あたりの電子メール処理件数を図4-5に，電子メールの配送遅延時間別電子メール数を図4-6に示した。配送遅延対策（2）以前では，9月22日から10月21日の1カ月間の1日平均で2,438,190件の電子メールの配送処理を行っていたが，対策の効果が現れた実施後では，11月11日から12月10日の1カ月間の1日平均は477,143件と80%も減少した。また，対策前後で配送される電子メール数は平均413,705件から225,264件に減少している。これはバウンスメールの配送処理分が削減されたことによると考えられる。対策（2）実施後の処理件数は実際に配送された電子メール数の倍程度にとどまっている。一方，ほぼ瞬時に配送された電子メール数は平均40,443通から158,263通と4倍近くに増加した。また，1分程度以内で配送された電子メール数は，全体の56%から96%に改善した。この状況は，おおむね配送遅延がなくなっ

たと考えても差し支えない状態と理解できる。

対策（2）の開始日（11月4日）から11月9日の5日間，配送処理件数が増加している。配送サーバはメールの配送が保留となった場合は，直ちにエラーとせず，5日間再送処理を繰り返す。このため，対策を行ってから効果が表れるまでタイムラグが生じたと考えられる。

図4-5において，10月21日（図中↓印時点）から対策日（11月4日）の14日間は，一時的に配送遅延が改善しているように見える。これは、，対策（2）実施までの一時的な処置として，次の緊急対策によるものである。迷惑メールの急増に伴い（10月21日頃），配送サーバでの配送処理が急増し，電子メールが配送不能となる障害が発生した。電子メールの配送を継続するために，再送処理を行っている学外宛てのメールの配送処理を急遽用意した別サーバに任せた。これにより配送サーバがこれらの学外宛てのメールの再送処理を行わなくなったことから，配送遅延が減少したと考えられる。

一方，宛先確認を行った後，電子メールを受信したにもかかわらず，1日平均約24万件の受信拒否や再送処理が行われていた。ログを確認すると，宛先メールサーバによっては，差出アドレスのチェックを行うものがあり，差出アドレスが存在しない電子メールを受信拒否，あるいは受信保留していることが主な原因であると考えられる。一般的に，迷惑メールは差出メールアドレスを詐称して送信されるが，差出メールアドレスの返信サーバが存在しない場合がある。この場合は，差出者のメールソフトの設定ミスを除いて，ほとんど迷惑メールであると判定しても差し支えない。研究室等に設置されたメールサーバでは，通常不正な差出メールアドレスの電子メールを受取らないように設定している場合が多い。しかし，センターとしては，発信者が誤った差出アドレスを入力するなど設定ミスのある電子メールでも受信しなければならない

立場にあると考える。このような差出メールアドレスが不正な電子メールがエラーとなり，新たな迷惑メールになり，送信サーバが迷惑メール発信源と誤認される恐れを考えると，このような電子メールへの対策を講じる必要がある。

上記の問題を回避する方法として，以下の対策の変更・追加が必要と考える。宛先アドレスを確認する場合，差出メールアドレスを通知する必要があるが，現在の対策では，受信サーバで稼動しているMTAであるpostfixの制限により，固定した有効な電子メールアドレスを差出メールアドレスとして用いている。これを，学外からの受信メールに含まれる差出メールアドレスを用いるよう変更できれば，前述の問題は発生しなくなる。一方，受信サーバで差出メールアドレスのチェックを行なう回避方法がある。この方法を一律に行なうことは技術的に容易ではあるが，この方法は迷惑メール判定基準のひとつであることから，迷惑メール対策導入の際に行わわれた議論と同様，利用者に適用の有無を選択させることが望ましいと考える。受信メールサーバ上の判定を利用者が選択できる仕組みが必要となる。

4.2.3 メーリングリスト対策による配送処理数削減の効果

配送遅延対策の一環として,メーリングリストの管理者に適切な投稿者管理を行うよう依頼した（2008年10月)。依頼した全652件のメーリングリストアドレスについて，11月末頃までに，42%の275件のアドレスについて回答を得た。そのうち学内限定希望は157件，廃止希望は47件，残りは，学内限定非希望（71件）であった。なお，回答のないものは現状維持，すなわち学内限定非希望として取り扱った。学内限定希望は全体の約24%，廃止希望は約7%となり，学内限定・廃止希望の合計が約31%になった。回答の中には，「意識せず学外投稿を許す状態になっている」や「自宅や出張先から電子メールを出す場合があるので，学内限定にはできない」というもの

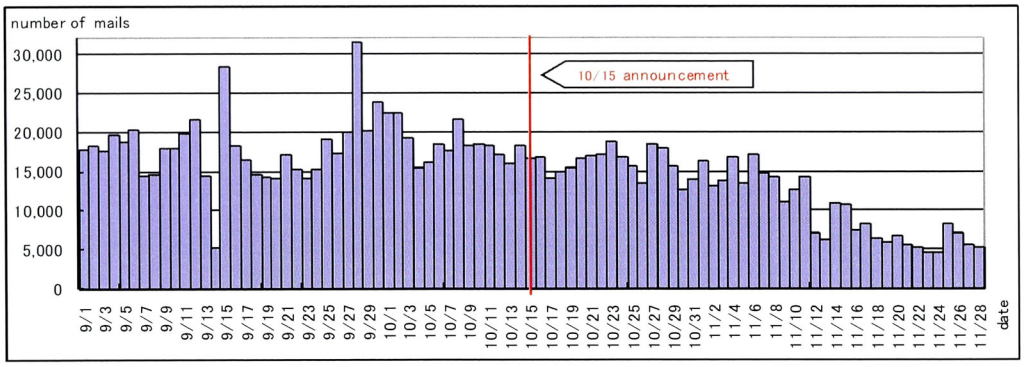


図 4-7 メーリングリストサーバからの発信メール数．縦線は学内限定依頼の送付時点．

もあった。前者に対応するため，メーリングリストの作成時はデフォルトで学内限定とした。後者の場合，学内限定メーリングリストであっても安全に学外から投稿ができる以下の代替手段を説明し，理解・協力を得た。

（1） 送信者認証（SMTP Authentication)の機能を有する SMTP サーバの利用

（2） センターが提供する Web メールサービスの利用

図 4-7 は，メーリングリストサーバから発信された電子メール数の時間変化を示す。学内限定措置及び削除措置を実施した結果（2008 年 10 月 15 日通知），メーリングリストサーバから発信される電子メール数が約 1/3 に減少した（11 月末時点)。すなわち，約 2/3 の配送は不要であり，、迷惑メールを複製し配送していたと考えられる。また，学内限定投稿のメーリングリストは，学外投稿のメーリングリストと比較して，宛先アドレスの登録数が極端に多いため，電子メール数の削減に大きく貢献したと考えられる。結論としては，各々のメーリングリストの運用状況のモニタリングとメーリングリスト管理者への適切な管理依頼を継続していくことが重要であると言える。管理状況によっては，停止又は廃止等の措置も必要である。

4.3 議論

4.3.1 迷惑メール対策と配送遅延対策

大学等の電子メールサービスにおいて一律な迷惑メール対策を適用することは，漏れなく対策が実施できる反面，誤判定によるリスクを許容できない利用者や電子メールの受信量が少ない多くの利用者にとっては，迷惑メール対策は不要であり，自由な電子メール環境への侵害と受け止められやすい。

本研究で用いた迷惑メール対策サーバにおいて，迷惑メール判定の閾値を 6.5（メーカ推奨値の約 2 倍）と大幅に緩やかに設定した場合では，通常メールを迷惑メールと誤判定する確率は約 0.1%であった。通常メールを迷惑メールと誤判定する確率にこの値を用いると，山口大学の調査結果からは，1 日 10 通未満の電子メールを受信している利用者のうち，1 日あたり 461 人中 1 人が誤判定の影響を受ける。電子メールの受信量が少ない多くの利用者にとって，このリスクを冒して迷惑メール対策を行うより，すべての電子メールを受信し目視で対策する方がよいと考えられる。

また，希望者に対してのみ迷惑メール対策を行うことは，利用者自らが対策の有無を選択する際に，迷惑メール対策に伴うリスクを対策選択ページ等で適切に説明されることで，迷惑メール対策によって生じる問題点について確認できると考えてもよい。一律な迷惑メール対策実施時に必要な個別のメール案件への管理者の対応負荷は，希望者のみへの迷惑メール対策では発生せず，管理者の負担は配送サーバ管理のみとなる。実際，「メールが届かない」といった問い合わせの多くは，宛先アドレスの間違いやメール転送設定の間違いによるものであり，迷惑メール対策に起因するものはなかった。すなわち，利用者が選択できる迷惑メール対策を実施することで，利用者にも管理者にも双方に無理なく，対策が実施されると考えられる。

一方，本提案のように利用者が迷惑メール対策の有無やレベルを選択できる状況では，配送遅延の問題が発生する。山口大学のように，各利用者が自由にメールサーバ・メーリングリストを構築できる環境において，適切に運用されていないメールサーバ・メーリングリストの存在は，個別の問題にとどまらず大学等全体の電子メール環境に影響を与え，大幅な配送遅延につながることが明らかとなった。各々のメールサーバ・メーリングリスト構築者自らが責任を持って対処する必要があるが，大学等全体の管理者にとって，各構築者の維持姿勢に任せておいては，配送遅延対策が進まない。そのため，各メールサーバ構築者に対して，教育・研修・依頼等を行う必要があるが，徹底できないのが現状である。こうした観点から，大学等全体として受信メール制御サーバを導入することにより，効果的な対策が実施でき，配送遅延も回避できると考える。

4.3.2 学内・学外発信メール管理

現状の迷惑メール対策は配送経路の都合上，学内から発信されるメールと学外から発信されるメールの両方に対策を実施している。また，配送遅延及びメーリングリストへの対策は，学外発信メールのみに実施したが，十分な効果が得られた。

学内から迷惑メールが配送されることはまれであり，仮に配送されたとしても発信場所が特定でき，再発を防止できると考えられる。たとえば，一般に迷惑メールは差出アドレスが詐称されるため，山口大学では，差出アドレスが山口大学のメールアドレス以外のメールは送信できない対策を実施している（2.1 節参照）。このことから，学内発信メールには迷惑メール対策適用の必要性は低いと考えられる。この意味で，迷惑メール対策希望者へ，学内発メールへの迷惑メール対策を不適用とする選択肢の提供も考えられる。

学外メールを中継し学内に配送するメーリングリストサーバなどが存在する場合は，このサーバから発信された電子メールに対して学内外の判定が明確でなくなる等の問題がある。そのため，学外用，学内用に別の電子メール配送経路を用意するなどの対応が必要である。配送経路を別に用意する場合は，管理情報の共有に注意が必要である。学内発の電子メールには迷惑メール対策を適用しないことで，迷惑メールの誤判定及び配送遅延のリスクを低減できる。

4.3.3 電子メールの効率的な配送・転送管理

本研究において利用者の意向調査を行い，その意向に基づき迷惑メール対策を行った結果，利用者の意向は一律ではなく，幾つかのグループに分類できる事が明らかとなった。現状では，一旦電子メールを受信して，宛先メールアドレスごとに迷惑メール対策を適用する方法を取っている。すでに述べたように，一旦電子メールを受信することは，次のリスクを伴う。

（1） 電子メール配送遅延のリスク。

（2） 詐称された差出メールアドレスへのバウンスメールの返信による再送処理の増加，及び返信メールを迷惑メールと誤認識されるリスク。

（3） 非対策迷惑メールを別組織（例えば商用メールサーバ）等へ転送することにより，山口大学メールサーバが迷惑メール送信サーバとして誤認されるリスク。

また，センターとしては全てのメールを一旦受信しなければならないため，利用者は greet pause，RBL 等の迷惑メール対策が選択できない状況にある。これらのリスクを回避し，迷惑メール対策を効率的に行うためには，一旦電子メールを受信しなくても，適切に管理されている各サーバへ電子メールを配送する仕組みも必要であると考える。あらかじめ迷惑メール対策方法が異なる複数の迷惑メール対策サーバを準備

し，配送元サーバに宛先メールアドレス毎に適切な転送サーバを指示することで，宛先メールアドレス毎に希望の迷惑メール対策を適用することが可能となる。

現状のSMTPには，配送元メールサーバに対して，レスポンスコードにより「251：転送処理を実施したこと」，「551：転送すべきであり受信できないこと」を示す方法は規定されているが，いずれも通知のみで，実際に配送元サーバに転送先を指示して転送させることはできない。配送元サーバに転送先を指示し転送させることができれば，電子メールを一旦受信しなくても配送元サーバによって適切なサーバへ転送させることができる。迷惑メール対策や配送遅延対策だけでなく，さらに，利用者毎に利用メールサーバ（例えば，大学メールサーバ，学外・商用メールサーバなど）を選択させることにも対応できる。これを実現するには，配送元MTAがエラーコード551を受取った後，転送先にメールを配送しなおす機能を実装することで対応できる。一方，インターネット上の多くのMTAにこの機能を実装する困難さがある。今後のシステムの改良が望まれる。

4.4 まとめ

山口大学において，2006年から希望者のみに対し，大学としての迷惑メール対策サービスを開始した[13]。これまでの電子メール管理システムの運用実績を踏まえて，希望者のみへの迷惑メール対策の運用を通じて得られた主な知見は，以下のとおりである。

①受信可能なメールアドレス全体の約87%は，1日あたり10通未満の電子メールしか受信しておらず，実質的に迷惑メールで困っていないと思われる（根拠となるのは，10通未満のメール受信者で対策希望したアドレスは2%未満である：表4-3参照)。電子メール受信数の少ない利用者への迷惑メール対策は，実質的に不要である。

②一部のヘビーユーザ（受信メールアドレス全体の約 12% ） の希望者に対してのみ迷惑メール対策を実施することで，全体として効率的な対策（対策されるメール数は全受信メール数の約 46%）が実施できる。

すなわち，多くの大学では企業と同様に「一律な迷惑メール対策」が実施されているが，上記の知見から判断すると，少数のメールしか受信していない多くの利用者（78%）にとっては「過剰な対策」とも言えよう。

一方，希望者のみへの迷惑メール対策の実施は，配送遅延障害を引き起こした。この主な原因は，

①受信メールを希望者に応じて振り分ける必要があることから，全てのメールを一旦受信しなければならない，

②受信したメール中には宛先不明の電子メールが存在し，配送できず再送処理を繰り返していた（全体の約 9 割），

の 2 点である。宛先不明や，学外から受信する必要のない電子メールの配送を削減することで，効果的に配送遅延を回避できた。宛先不明メールの発生原因としては，

①学部・研究室等で導入され，運用停止状態のまま放置されたメールサーバが数多く存在していた（全体の 78%），

②投稿者管理，運用管理が不適切なメーリングリストが多数存在し（全体の 31%），メーリングリスト経由の多くの電子メール（約 2/3）は迷惑メールであった，

が指摘できる。大学全体として，メールサーバのモニタリング・管理を適切に行うことで，不要なメールの処理を削減することができる。また，メーリングリストの運用管理を適切に行うことで，容易に配送メール数の削減ができ，配送遅延の対策ともなる。

以上により，本論文で提案した「希望者のみに迷惑メール対策を導入する方法」は，

自由な電子メール環境を必要とする大学等にとっては効率的であり速やかに導入できる半面，十分な配送遅延対策を必要とする。特に，迷惑メール対策を希望しないヘビーユーザ宛てのメールに含まれる迷惑メールのエラー処理や転送処理により，配送遅延や迷惑メールの発信源と誤認されるなどの問題が生じる恐れがあり，今後対処が必要である。

本稿で提案した希望者のみに迷惑メール対策を導入する方法は，一旦メールを受信した後，対策の適用・非適用を判定する。このため，greet pause，RBL や不正な差出メールアドレス判定等適用の可否等が利用できない。今後，これらの判定基準を利用者自身が変更できるシステムの導入が必要と考えられる。山口大学ではこれらの対策実施後，現状において十分な迷惑メール対策及び配送遅延対策への効果が得られ，通常メールの利用に支障のない状態にあると考えられる。効果の状況をより定量的に把握するためには，希望者数と効果の関係についてさらに詳しい分析が必要である。

第5章

利用者ネットワーク運用管理とセキュリティ対応

5.1 認証付き情報コンセント

ノートPCの普及が始まり，DHCP（Dynamic Host configuration Protocol）によるPCのネットワーク設定の自動設定が可能になったことで，だれでもがノートPCをネットワークに接続することで，自由にネットワークを利用できるネットワーク環境が広がっていた。山口大学においても図書館等でノートPCをネットワークに接続できる環境を整備する要求が出てくるようになった。

しかし，当時DHCPには利用者認証機能はなく，接続すれば誰でも利用できるという問題があった。大学図書館では学外者の利用が可能であり，研究室でも学外者である共同研究者等が存在している。大学内でのサービスであることから，誰でも匿名で使える情報コンセントでは，サービス責任・教育責任が果たせないとともに利用者責任が明確とならない。

そのため，1998年に山口大学図書館等に，ノートPC接続後，利用者認証を行い，ネットワークが利用できる利用者認証システムを独自に開発し，他大学に先駆けて認証付情報コンセントを整備した[21]。学生の多くは，インターネットは匿名であると考えているが，匿名でないことを認識させる効果もある。導入した認証付き情報コンセントの構成を図5-1に示した。 認証サーバの構成を表5-1に示した。次の手順で利用者は認証される。

(1) ノートPCをネットワークに接続し，電源を投入後，DHCPサーバによりIPアドレスが自動的に割り当てられる。

(2) 利用者はWebブラウザーを起動し，認証ページに接続し，ユーザ名とパスワードを入力する。

(3) 認証サーバはメールサーバに接続し，入力されたユーザ名とパスワードが正しいかどうか確認する。

(4) (3)で正しいと判定された場合，認証サーバは自身の当該ノート PC の IP アドレスに対する通過フィルタを追加する。(利用開始)

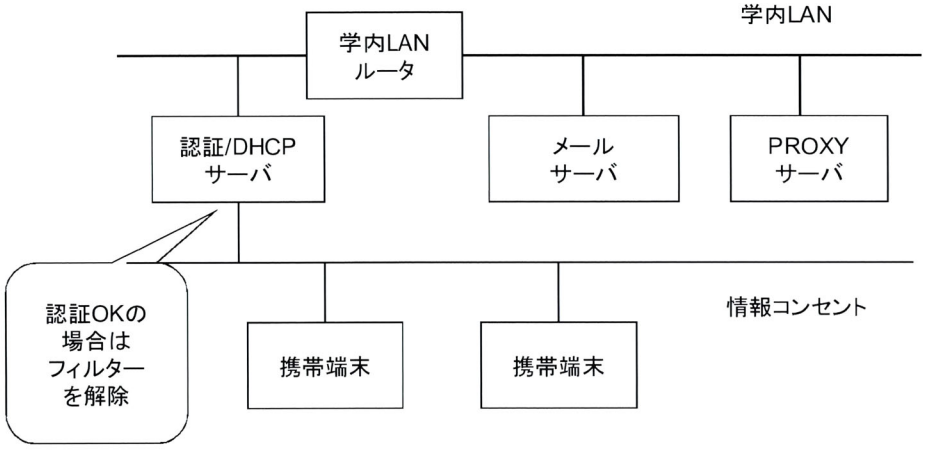


図 5-1 認証付き情報コンセント構成(導入当時：1998 年)

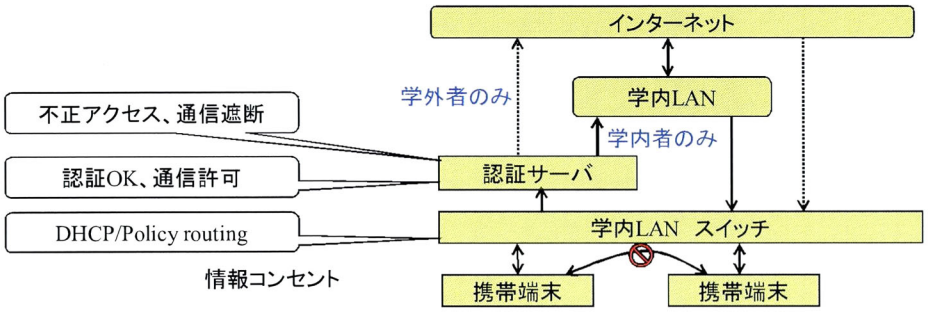


図 5-2 認証付き情報コンセント構成(現状)

表 5－1　認証サーバの構成

CPU	Intel 486DX2 66MHz
OS	FreeBSD 2.2.5
DHCP サーバ	WIDE DHCP server 1.40
WWW サーバ	Apache 1.2.5
ルータ機能	OS 標準機能
IP フィルタ機能	IPFW（OS 標準機能）

(5) 利用期間中は，認証サーバは，利用中のノート PC に，一定間隔で PING により通信確認を行う。

(6) 認証サーバは自身の ARP テーブルを調べ，ノート PC のエントリが存在するかどうか確認し，存在する場合はノート PC が利用されていること，存在しない場合はノート PC の利用が終了したと判断する。

(7) 認証サーバは(7)で利用終了と判断した場合は，ノート PC の IP アドレスの通過フィルターを解除し，通信を遮断する。（利用停止）

山口大学での導入後，他大学でも研究・導入が進められている[26-29]。また，2004 年に端末のネットワーク認証に関する規格 IEEE203.1x が制定された[30]。現在では，各地区の講義室，ラウンジ，閲覧室，会議室及び研究室などで利用でき，おおよそ 8000 個の情報コンセントを設置するに至った。ソフトウェア著作権を山口 TLO に譲渡し，製品化を行った

導入後，利用者・利用量の増加に対応し，安定性・高速性を確保するため，改善を進め，現在の認証付き情報コンセントの構成を図 5-2 に，改善点を以下に示す。

① 認証付き情報コンセントを安定運用し，ネットワーク障害の影響を局在化させるた

め，各建物，各講義室に独立したサブネットを割当てることで，複数の小さなネットワークで構成した。

② 利用者 PC は利用開始にあたり DHCP により IP アドレスを取得するが，DHCP サーバまでのネットワークが不通になると IP アドレスを取得することができない。特に Windows Vista は IP アドレス取得時間が極端に短いため（Vista：6 秒，XP：25 秒），ネットワークが不通ではなくネットワークに遅延が生じた場合でも，IP アドレスが取得できない問題が生じた。そこで，安定的に IP アドレスが取得できるよう DHCP サーバを建物毎に設置した。

③ 講義室では，一度に多くの利用者が一斉に利用することから，ウイルス感染によるネットワーク障害の拡大防止のため，マルチプル VLAN 構成とし，ノート PC 同士の通信を遮断した。また，情報コンセントを個々に制御する機能を導入することで，ウイルス感染したノート PC を特定し，その PC の通信だけを遮断できる構成とした。

④認証付き情報コンセントの認証を制御するため，認証付き情報コンセントから発生した通信は，各建物の棟間スイッチにおいて，認証サーバを経由するように制御する。

⑤ 認証サーバは，認証付き情報コンセントからのパケットを受信すると，未認証の場合は，認証サーバが応答し，自動的に認証画面を表示させる構成とした。認証済みの場合は，そのまま，通信を通過させる。

⑥認証付きの情報コンセント向きのパケットは，通信速度を確保する点から，通常の学内ネットワークと同様とし，制御をしていない。一般的に，アップリンクのトラフィックよりダウンリンクのトラフィックがはるかに大きいことが知られている。通常 TCP/IP は，端末 PC から通信を発生させ，双方向の場合のみ，通信できるこ

とから，認証付き情報コンセント発のパケットを制御するだけで十分である。

⑦認証付き情報コンセントからインターネットのアクセスは，proxy サーバ経由とし，直接アクセスさせない方法を取った。この方法ですべてのアクセスは，proxy サーバにログとして記録される。学内の場合は，アクセス履歴は各サーバに保存され，適切に管理できることから，学内へは直接アクセスできる。

⑧ ウイルスに感染した PC が接続されると，感染拡大行為として特定に通信が大量に発生する。認証サーバは，この通信を感知すると，当該 PC の認証を取り消し，PC のブラウザ上の接続先を警告ページに切り替えて表示させる構成とした。現在の判定条件は，1 分間当たり ICMP， TCP/455， TCP/135 のパケットが 100 個以上と設定している。

⑨学外者が認証した場合は，学内 LAN との通信は遮断したまたとし，学外者用機器に転送させ，インターネットへのみ通信できる構成とした。

研究室学生へのネットワーク提供の一つとして，指導教員が研究室に認証付情報コンセントを導入するケースも増えてた。各研究室内に認証付情報コンセントを導入することは，利用者認証やログ管理はもちろん，ウイルス対応，ネットワークの不正利用，掲示板を利用した誹謗中傷等への対応を指導教員が教育的立場で行うことができる。技術的運用時関は山口大学メディア基盤センターに依頼することができ，指導教官のネットワーク管理が不要となり管理負担が軽減される。

認証付き情報コンセントの導入により，利用者管理を行いつつ，資格を有している誰もが，複雑な手続きなしに，簡単にネットワークを利用できる利便性の効果がある。管理者は，申請・許可･廃止等の処理を削除できる。特に，手続きとしての削除処理はなされないことが多く，認証付き情報コンセントを導入することで，これを防止し，

適切な利用者管理が実施できる効果がある。

5.2 利用者端末運用管理システム

大学の全域で情報コンセントの整備が進み，無線 LAN の普及が進み，移動端末を用いて学内 LAN を利用する運用形態が増えてきた。通常，端末のネットワークはDHCP により自動設定されるか，または，端末の管理者によって手動で設定されるため，端末が学内 LAN のどこから利用されているかは，割り当てサブネットにより大まかな位置は把握できるが，具体的な場所を把握しにくいといった問題がある。そのため，障害発生や不正アクセスがあってもその場所の特定は容易ではない。

そこで，端末の認証だけではなく，該当端末を誰が，いつから，いつまで，どこで利用しているのかを簡単に把握できる利用者端末運用管理システム構築した[31]。

利用者端末には端末固有（物理ネットワークインターフェース固有）の MAC アドレスを有している。このアドレスは，基本的にはネットワークインタフェースを物理的に交換しないと変更できないため，利用者端末固有の情報と見ますことができる。一方，ネットワーク上の通信は DHCP により端末に割り当てられた IP アドレス，または，管理者によって割り当てられる IP アドレスを用いて行われるため，各種サーバには IP アドレスによるアクセスログが保存されている。しかし，IP アドレスは DHCP の割り当て毎に一定でななく，また，利用者が割り当てられた IP アドレス以外のものを用いることができ，端末固有の情報とはみなせない。

LAN 上において，スイッチング HUB(以下 SW-HUB)は MAC アドレスを用いて，宛先端末を特定している。SW-HUB はどのポートにどの MAC アドレスを持つ端末が接続されているかを自動的に学習し，SW-HUB 内のメモリー上に MAC アドレステーブルを作成している。SNMP 機能を有する SW-HUB では，SNMP マネジャー

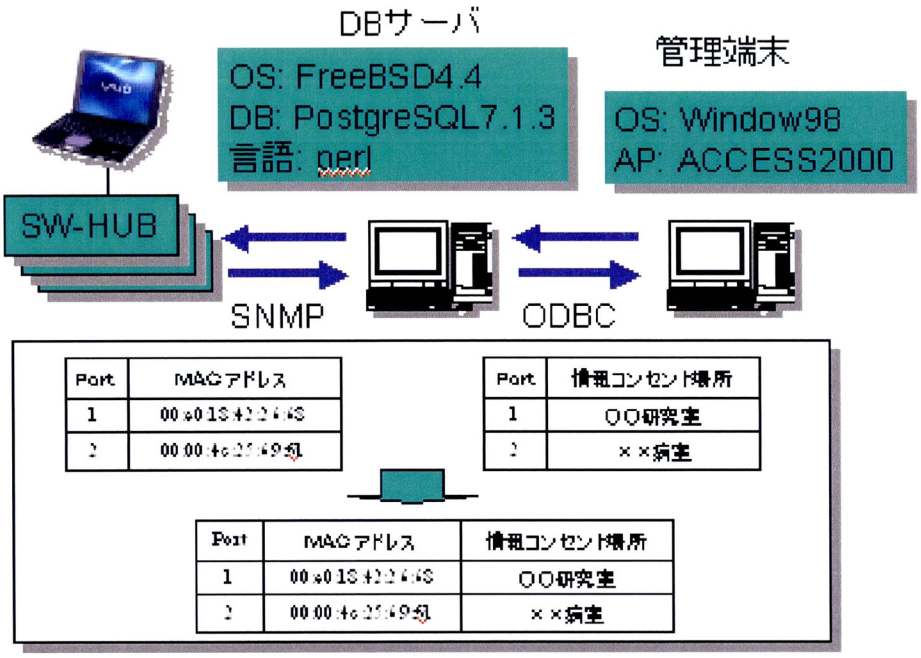


図 5-3 利用者端末運用管理システム

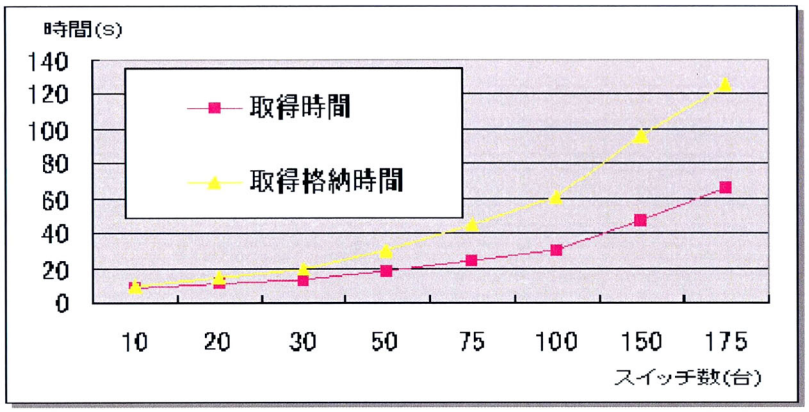


図 5-4 情報収集時間

からこのテーブルの情報を読み出すことができる。(1)ネットワーク内のすべての SW-HUB からこのテーブルを収集し，MAC アドレスを持つ端末がどの SW-HUB のどのポートに接続されているか決定する。

一方，(2)ネットワーク内のルータの ARP テーブルを収集することにより，IP アドレスと MAC アドレスの対応表が得られる。この情報も SNMP により取得可能であ

る。最近市販されているL3 SW-HUBでは，この機能を有している

ネットワークを設計・構築する際には，前述した機能を有するSW-HUBを用いてネットワークを構成する。全SW-HUBの全ポートの接続先を整理し，ポートと情報コンセントの位置を対応付けしておく。(3)この情報をSW-HUBポート接続先テーブルという。(1-3)の情報とを組み合わせることで，ネットワークサーバ側に残されたログ情報内のIPアドレス等から利用者端末がどの場所で利用されているか，知ることができる。

こららの機能を実現するため，図5-3に示す利用者端末運用管理システムを構成した。SNMPマネージャとして，AT互換機（OS:FreeBSD)を用いた（DBサーバと称する)。Perl言語で記述されたプログラムによって，SW-HUBのMACアドレステーブルが収集され，データベースに格納される。また，管理の集計・検索等の作業を軽減させるため，DBサーバ上でデータは扱わず，別途用意した管理端末(OS:Windows98)上のACCESS2000データベースソフトを用いることとした。ACCESS2000の豊富なデータベース機能が簡単に利用できる。両データベース間はODBCによってリンクされる。

MACアドレステーブルの収集方法にはいくつかあるが，DBサーバにより数分毎に全スイッチの情報を収集した。過去の状態を調査可能とするため，収集時間も合わせて保存している。

構築したシステムの性能について評価するため，学内にある約175台のSW-HUBからSNMPによりMACアドレステーブルを取得するのに必要な時間を測定した。今回用いたSW-HUBはL3スイッチ機能を有するもので，アライドテレシス社製8624である。SW-HUBの個数ごとに情報収集にかかった時間を図5-4に示す。SW-HUBが100台（ポート数約2000）程度での場合，情報取得時間が1分以下となり，運用

に支障のない実行速度が得られた。SW-HUBが175台では，2分近くかかっている。このようなネットワークは大規模すぎるが，DB サーバを複数台で処理するなどすることにより，改善できる。また，SW-HUB に一時記録される MAC アドレスは一定時間（標準で5分間）利用がない場合は削除されことから，5分間隔で情報を取得することで十分対応できる。

本システムは，不正利用やウイルス感染等が発生した場合，状況を正確に確認するために，利用者だけでなく，発生場所を特定することができる。また，利用者端末にネットワーク障害が発生した場合には障害原因を分析するに必要な情報を提供できる。

現在では，本システムは，山口大学の全ネットワーク機器に対応させ，利用者端末のネットワーク障害に関する問い合わせに対応するため，次の機能を追加している。

(1) 利用者端末が接続されているかどうかを判定するため，各情報コンセントのリンクアップ・ダウンの状況取得

(2) 利用者端末を確認するために，大まかな製造メーカの表示。

取得したMACアドレスに含まれるベンダーコードで製造メーカが推測できる。

(3)利用者端末を利用している利用者を確認するために，認証付き情報コンセントを利用する際に，認証した利用者のユーザ名の表示。

取得した IP アドレスを認証付き情報コンセントの認証サーバに紹介することで，利用者のユーザ名を取得することができる。

(4)ネットワーク障害を確認し，即応するために，障害ネットワーク機器のリスト表示。

これらの機能を利用することで，ネットワークの専門家でなくても，ネットワーク利用者が問い合わせるネットワーク障害へ対応することができる。

5.3 ネットワークループ接続障害対応

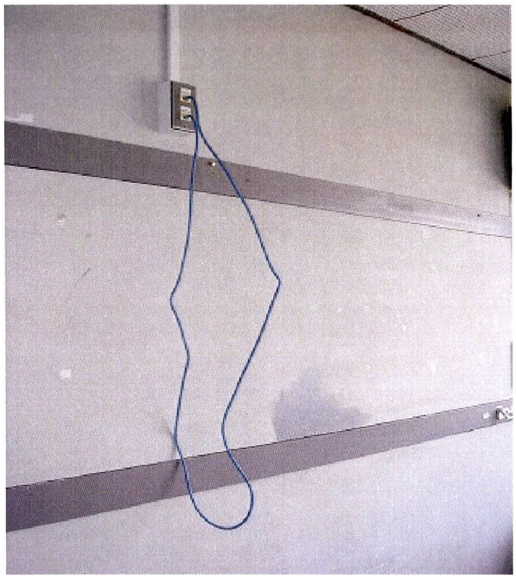
認証付き情報コンセントは誰でも利用できる場所にあり，主に学生が利用することから，思いがけない利用が行なわれる場合がある。例えば，隣り合った情報コンセントに同じケーブルの両端を接続させることがある。学内ネットワークが Ethernet (IEEE802.3)で構成されているため，このようなループ構成にすると，ブロードキャストパケット（または，マルチキャストパケット）が無限に複製され，ネットワーク全帯域を消費し，ネットワーク利用ができなくなる障害が発生する。これをブロードキャストストームという。場合によっては，全学ネットワークに影響を及ぼす場合もある。これを解消するためには，発生場所を特定し，ケーブルの片方を切断する必要がある。一旦ブロードキャストストームが発生すると，同一サブネットの至るところで，ブロードキャストストームが拡大するほか，ネットワークが不通により管理用の通信も出来なくなることから，発生場所を特定することを困難にしている。そこで，以下のブロードキャストストームの対策を講じた。

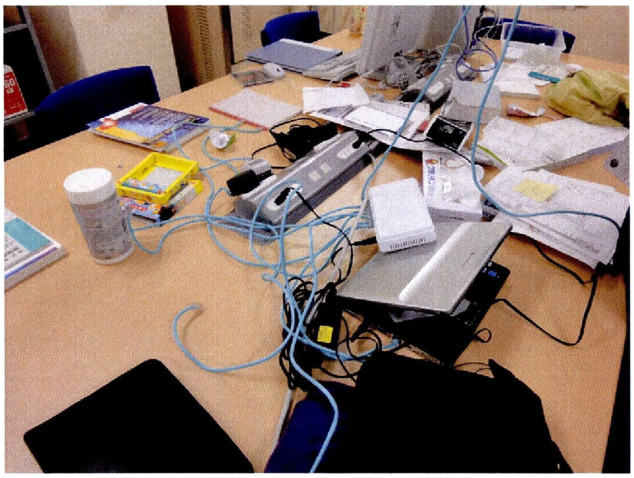
(1) ブロードキャストストームは，サブネットを越えて，パケットを流さないことから，サブネットの範囲を小さくすることで，ブロードキャストストームを一定の範囲に閉じ込めることが出来る。出来るだけサブネットは，講義室単位，又は建物単位でこれを越えないよう最小限のものとし，出来るだけ障害の原因を作った利用者のみ（多少他者を巻き込む場合がある）が影響を受ける構成とした。

(2) 一般的に，ブロードキャスト及びマルチキャストパケットは，通信の支援的機能として利用されているので，全利用帯域のわずかしか利用されていない。仮にブロードキャストストームが発生しても，全帯域を消費することを防止するため，ブロードキャスト及びマルチキャストの帯域をあらかじめ制限した。利用者ネットワークの帯域が 100Mbps であることから，おおよそ，その 1/10 の 10Mbps 以下とした。ただ

し，ネットワーク機器が保持するMACアドレスの接続情報が同時に複数存在し混乱するため，該当ネットワークは不安定又は不通となることは防げない。

(3) ブロードキャストストームの発生場所を特定する方法を構成した。ブロードキャストストームを解消するために発生場所の特定が必要である。一定時間内でのブロードパケットの数が一定値以上を超えた場合は，ブロードキャストストームが発生していると考えてもよい。各ネットワーク機器の各ポートのブロードキャストパケット数を一定時間毎に収集し，前回の値と差分を計算し，閾値と比較し，ブロードキャストストームが発生しているポート及び情報コンセント（キャンパス名，建物名，情報コンセント番号，部屋名等）をネットワーク監視画面上に表示するシステムを構築した。なお，末端の各ネットワーク機器の各ポートは，情報コンセントに一致していることから，ポートの特定は，情報コンセントの特定できる。これまで，ブロードキャスト発生の特定には，トラフィックの分析，疑わしい箇所の通信を切断する方法を用いて数時間程度必要であったが，本システムの導入後，発生時点で特定できるよう改善した。現在の設定値は，収集ポート数は約20,000ポート，収集間隔は約1分間，閾値は500パケット／秒に設定している。障害が発生したときの短期間で情報を取得しなければ，数分後であればネットワークが不通となり情報が取得できなくなる恐れがあることから，1分と短く設定している。





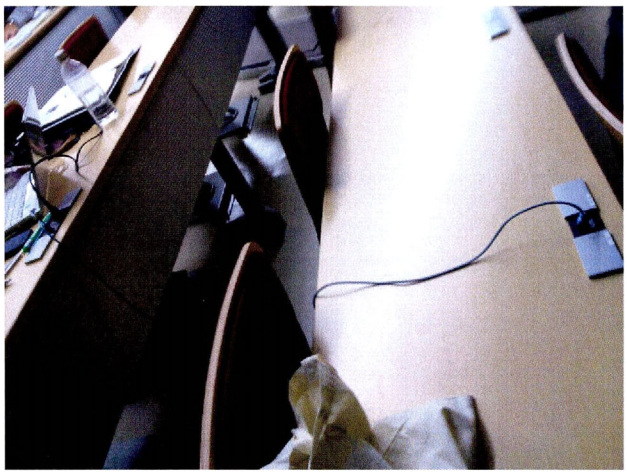


図 5-5 ネットワークループ接続障害の例

5.4 複数セキュリティポリシの切換えネットワーク

一人のネットワーク利用者において，複数のセキュリティポリシーの異なるネットワークを切り替えて利用したい場合がある。たとえば，医療情報ネットワークては，病院業務情報を扱う場合とインターネットを利用する場合などがある[32,33]。このようなセキュリティポリシの異なる複数ネットワーク利用を統一的に利用者が切り替えて利用するネットワークの一手法を図 5-6 のようなシステムにモデル化し構築した[34,35]。ここで，複数ネットワークとして，インターネットのつながる学内 LAN，研究室等で利用される研究用LANおよびもっぱら業務のみで利用される業務LANの3つのセキュリティポリシの異なるネットワークと仮定した。

5.1.1 システムの概要

利用者が希望したネットワークにアクセスするために，以下の3つの認証方式をとった。

個人認証： ユーザ名・パスワードにより利用者認証を行うことで，ネットワークの正規利用者かどうかの判断を行う。

グループ認証： 利用者を学生，研究生，教員，職員等のグループに分け，登録されたグループ属性により利用できるネットワークを制限する。

利用者端末認証： 利用者端末が持つ MAC アドレスにより，あらかじめネットワーク利用が許可された端末かどうか判断を行う。

一つの物理ネットワーク上で複数のネットワークが異なる VLAN となるように論理ネットワークを構成した。システムのハードウェア構成は以下の通りとした。

スイッチングハブ： Cabletron Systems SSR-2000

認証サーバ: FreeBSD4.2

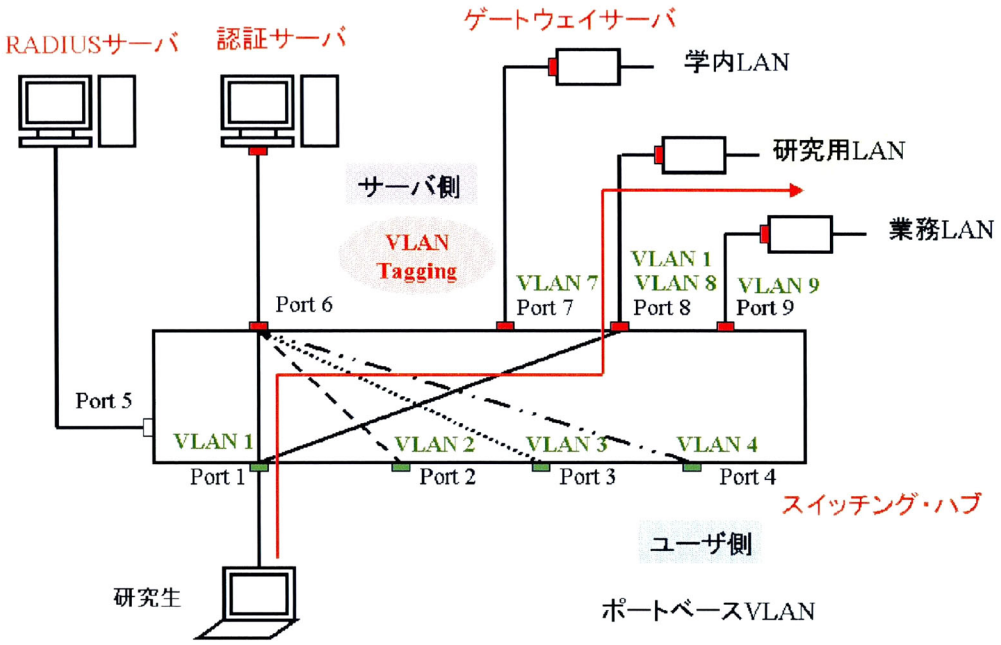


図 5-6　本システムのネットワーク構成

RADIUS [37] サーバ： FreeBSD4.2, Radius-Cistron-1.6.3

DHCP サーバ： ISC-DHCP2.0

Web サーバ： Apache-1.3.4

スイッチングハブには、複数の論理ネットワークを構成できる VLAN 機能，リモートで設定変更できる TELNET [38] 機能，機器の状態を監視する SNMP [39] 機能が必要である。VLAN 方式としてサーバ接続のために IEEE802.1Q [40] を用いた。

図 5－6 にネットワーク概要と VLAN の接続状態を示したあり，Port1 に接続された利用者端末が研究用 LAN を利用し，Port2, 3, 4 は端末が接続されていない状態にある。VLAN の初期状態として，利用者ポートにそれぞれ一つの VLAN を設置，認証サーバにすべての利用者ポートを接続した。

5.1.2 システムの利用手順

あらかじめユーザ名・パスワード及び利用者端末のMACアドレスをRADIUSサーバに登録しておき,

(1) 利用者端末がネットワークに接続されると端末はDHCPによりネットワーク設定が行われる。

(2) 利用者はWebブラウザーから認証サーバに接続し，ユーザ名・パスワード及び利用のネットワークを入力する。

(3) 認証し，正しければ次の処理を行う。

(4) 認証サーバは該当ポートに対してMACアドレスフィルターを施し，利用者端末に限定する。

(5) 認証サーバは利用者が選択したネットワークにVLANを接続する。

以上の処理で希望のネットワークの利用が可能となる。

5.1.3 評価

構築したシステムの性能を測定した。利用開始する前，認証中，利用中，利用終了後のそれぞれについて，VLANの切換え状態を確認し，目的通り切替えられていることを確認した。

複数の利用者が同時に利用開始することを想定し，認証とスイッチングHUBの設定変更にかかる時間を測定した。結果を表5−2に示す。1端末あたり約0.8秒と高速であり，同時利用開始者が8名であれば，7秒以下で処理が終了した。業務や研究等での利用を想定しているので,多くの利用者が一斉に利用開始する事は考えにくく,高々4，5名程度出あるので，事実上十分な速度であろう。この速さはスイッチングHUBの設定に要する時間で占められている。現状では，スイッチングHUBの設定時間が短くなっているので、利用開始時間は改善されている。

表 5-1：通信可能な端末の変化

	他の ユーザ端末	認証 サーバ	RADIUS サーバ	ゲートウェイ サーバA	ゲートウェイ サーバB	ゲートウェイ サーバC
VLAN設定が 行われていない状態	○	○	○	○	○	○
本システムの VLAN設定初期状態	×	○	×	×	×	×
VLAN設定が 切換わった状態	▲	○	×	△	△	△
再びVLAN設定が 切換わった状態	×	○	×	×	×	×

○ :通信可能　▲ :同じ接続先ネットワークを指定した場合のみ通信可能

× :通信不可　△ :ユーザが接続先ネットワークに指定した場合のみ通信可能

表 5-2：ネットワーク利用時における処理時間

処理時間＼接続台数	1台	2台	4台	8台
認証に要する時間(s)	0.08	0.13	0.28	0.51
SW-HUBの設定が 完了するまでの時間(s)	0.71	1.54	3.17	6.41
合計(s)	0.79	1.67	3.45	6.92

利用者端末が同時に複数のネットワークを利用する事はできないため，リアルタイムに利用者端末を中継して別のネットワークに情報が老齢することは不可能である。利用者端末同士の通信は認証が行われるまで利用者端末は認証サーバとしか通信が行えず，端末同士の不正利用を防止できる。また，このシステムでは TCP/IP だけでなく NetBUEI や APPLE TALK 等の任意のプロトコルが利用できるので，サーバと利用者端末間をファイル共有し，常にサーバ上のデータを処理し，データを利用者端末にダウンロードしない運用体制をとることができる。しかし，情報漏洩は別のネットワークに切替えた際に発生する可能性がある。あらかじめ業務ネットワークに接続し，データを利用者端末にダウンロード後に，学内 LAN に接続変更し，データをインターネ

ット等に流す場合がある。データのダウンロードを居あする運用体制では，利用者が故意に行う漏洩はフロッピー（USB メモリ）等でデータを持ち出すとの同じであり防げない。一方，利用者端末に何らかの不正なプログラムを仕掛けられたために起こる故意でない漏洩はウイルス対策ソフトウェアを利用者端末にインストールして不正なプログラムを検査する必要がある。

5.5 議論・展望

前節のネットワークの切り替えは，利用者が利用開始にあたり，手動で切り替えを行うネットワークである。手動で切り替えていたのでは，現在の状態が分からなくなり，ネットワークポリシとは異なる利用を行い，接続不能になる場合が生じる。そこで，利用者利用者端末がサーバあるいはインターネットへのアクセスを感知し，そのアクセス先に応じた自動的なネットワーク切換えを行うことで、利用者の勘違い等による接続不能等の問題は改善される。

5.1.4 多重階層化動的ネットワークの基本構成

動的再構成を行なう多重階層化による高セキュリティネットワークの基本構成を図 5-9 に示す。これまでのネットワークは，インターネット及び特定の業務系ネットワークとの接続に対してファイアウォールを設置し通信を制御するほかは，利用者の利便性を配慮し，一つのネットワークとして運用してきた。このネットワークでは，各種サーバ（学内向・学外向）及び利用者の端末等が共存する状況である。この場合，利用者が持ち込む端末からウイルスやスパイウェアが持ち込まれ，他の機器に感染を拡大させる恐れがある。サーバでは学外・学内の両方にサービスを提供しているものは，インターネットへサービスを開いていることから，インターネットから不正アク

セス等で，不正なプログラムを設置され，または，サーバをのっとり，学内の他の機器への不正アクセスを行なう恐れがある。現に，過去において，これらの状況を発生している。これらを防御するためには，ここの端末及びサーバでウイルス対策ソフトの導入など適切な対応が必要となるが，徹底できているわけではない。そのため，それぞれのネットワーク利用の状況を総合し，必要以上の通信が生じないようにネットワークを機能（利用状況）毎に階層化させる。例えば，次のように分類する。

・学外サーバエリア

学外へサービスを提供するサーバを設置する。学外又は学内へのサービス提供は，要求に応じて開始し，要求があるまでは，学外及び学内へのアクセスは発生させない。

・学内サーバエリア

もっぱら学内へのみサービスを提供するサーバを設置する，利用者エリアからの要求に基づきサービスを提供する。

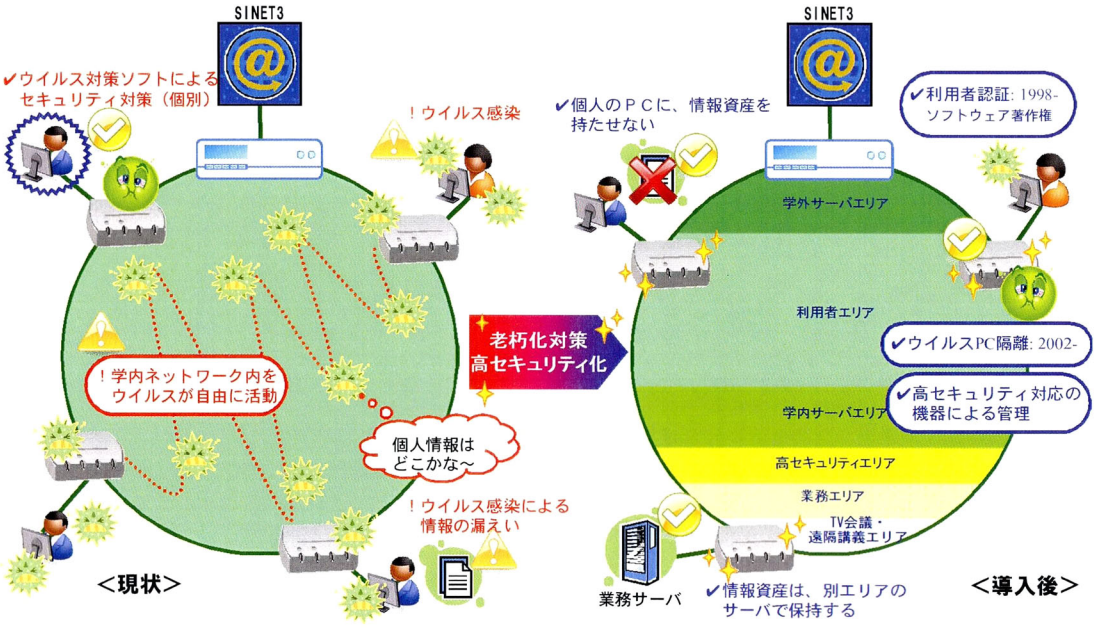


図 5-9 多重階層化ネットワークによるウイルス感染拡大対策

・利用者エリア

利用者端末を接続する。利用者端末はインターネット及び学外サーバエリア，学内サーバエリアの機器と通信をすることが出来る。利用者端末同士の通信は行えないようにすることが望ましい。

・高セキュリティエリア

個人情報・機密情報を有するサーバを設置する。このエリアは，原則他のどのエリアとも接続されない。もし，利用者がこのエリアの情報へアクセスする場合は，他のエリアから一旦切断し，本エリアに接続して利用する。また，原則，利用者端末に，データを保存させない仕組みが必要である。これにより，利用者端末を経由して，個人情報や機密情報が学外等へ漏れることを防止できる。

・業務エリア

病院業務システムや事務システムのように独立して運用することの出来るネットワークエリアである。

これらのエリア間，エリア内の通信を適切に整理・制御することで，ネットワークの安全を確保することを目指す。図 5-9 に多重階層化することで，ウイルスの影響を局在化される状況を示す。

5.1.5 利用者エリアと高セキュリティエリアの動的的切換え

利用者エリアと学内サーバエリア及び高セキュリティエリアの関係を図 5-10 に示す。

通常の状態では，利用者エリアに接続されている利用者端末は，エリア境界でアクセスの資格の確認が行なわれ，学内サーバエリアのサーバへのアクセスは行なえるが，高セキュリティエリアにあるサーバには接続できない。ところが，教員などの場合，

インターネット利用や学内サーバ利用などを行なうほか，高セキュリティエリアに接続されている教務システム等へアクセスし，履修者一覧や成績入力などの業務を行う必要がある。そこで，その場合次の手順で，高セキュリティエリアに接続変えをする。

(1) 利用者端末が，高セキュリティエリアにアクセスすることを感知する

(2) 両者端末は接続されているスイ-ッチのポートを利用者エリアから，高セキュリティエリアに切り替える。

(3)利用者端末は，高セキュリティエリアのサーバに対してアクセスを再送する

一旦(1)の段階で，接続先には接続できないため，アクセスは中断されるが，TCP/IPのプロトコルの性質として，相手からの応答がない場合，再送を試みる仕様であるので，(2)でエリアが切り替わった後の再送により，通信が継続できる。ただし，１度目のアクセスが失敗することから，接続には通常の場合よりも若干遅延が生じることが予測される。

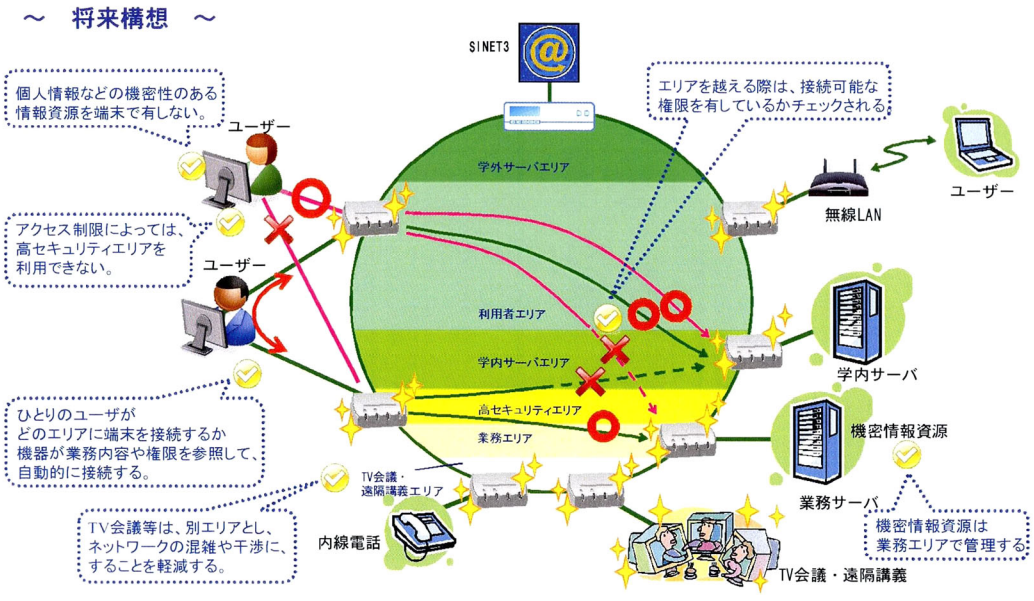


図 5-10　利用者端末の動的切替

5.6 まとめ

ネットワークの安定運用・セキュリティ対応のため，利用者の特定，利用場所の特定できる認証付き情報コンセント等のネットワークを提案し，構築した。不正利用やブロードキャストストームなどの障害が発生した場合に，障害場所の迅速な発見を支援するシステムを提案し，構築し，不正利用の特定ができ，障害対応時間を短縮することができた。VLAN 設定を動的に切り換えることにより，事前に登録された正規利用者と端末のみが，セキュリティポリシに異なる複数ネットワークを切り替えて利用できる環境を構築し，附属病院の研究室において試験的に試みた。また，利用者が選択的に切り替えるのではなく，アクセス先に応じて自動的に切り替える仕組みを提案し，複数のネットワークを運用する一つの方向性を示した。

今後さらに複雑化するネットワーク管理，セキュリティ問題を考えると，異なるセキュリティポリシを持つ複数ネットワークを持つようなネットワーク環境において，本システムのように複数ネットワークを動的に切り替えて利用する環境が重要になる。本システムは一部の研究室で試験的に運用を試みている。

第6章

結論

この数年間，情報システム利用の基本となる，利用者認証の各サーバでの統一の実現が自然に行えるよう取り組んできた結果，大学全体としての統一認証がおおむね実現できた。また，メディア基盤センターが提供する基本サービスの一つである利用者認証サービスは，全学の標準の利用者認証と位置づけられ，山口大学メディア基盤センターが全学の利用者認証管理を実施する部署であること，システムを構築する際には山口大学メディア基盤センターの認証を用いるべきという認知を得ることができた。これにより情報システムの利用者特定によるセキュリティ対応が進んだ。

事務システムについは，文部省（導入当時）が指導するシステムが稼動しているので個別の認証であり，システム連携も行えない状況である。国立大学法人化後，大学独自のシステムへの移行が検討されている。山口大学メディア基盤センターが所属する大学情報機構の情報化推進課と連携して，これらのシステム改変の際に，認証の統一や他システムとの連携などの機能を組み込む必要がある。国立情報学研究所が構築を目指している全国大学共同電子認証基盤（UPKI）のような大学間での統一認証への参加にも，学内の統一認証の実現は必要条件となっている。学内での認証の統一への過去の経緯を考えると全国大学の統一認証は困難であると考えられる。各大学での統一認証を利用し，連携する方法で行うのが現実的と思われる。

自由な電子メール環境を維持する必要のある大学等における電子メール管理システムのあり方や，大学全体として効率的で安全な運用実績で得られた主な知見は,以下のとおりである。

①大学等における，自由な電子メール環境の維持と効率的な迷惑メール対策の実施の両立に当たっては，一律で厳格なネットワークポリシを適用することは困難であり，利用者の希望に応じた迷惑メール対策の導入が有効である。

②利用者に応じた迷惑メール対策を実施するには，対策実施の可否，判定方法や基準の選択を利用者自身が理解し変更できるシステムが必要である。

③実際の運用実績から，利用者の一部（1 日に 50 通以上の電子メール受信者約 13%，100 通以上の電子メール受信者約 7%）のヘビーユーザに対してのみ迷惑メール対策を実施することでも，全体として効率的な対策が可能である。電子メール受信数の少ない利用者（約 70%）への迷惑メール対策は実質的に不要である。

④配送遅延の原因となる，運用されていないメールサーバ宛の電子メールが非常に多く，大学全体として受信メールの制御サーバを導入することで，効果的に配送遅延を回避できる。

⑤メーリングリスト宛の迷惑メールは配送遅延の原因の一つであるが，メーリングリスト管理者に学内限定措置を確認し，④の制御サーバを適切に設定することで，効果的な対策が実施できる。

これらの対策後，現状において十分な効果が得られ，多量の迷惑メールを受信する環境下の電子メールの利用において，支障のない状態にあると考えられる。さらに，迷惑メール対策の適用過程の中から，比較的自由なネットワークポリシを保ったまま，今後増大する迷惑メールへの対応方法，大学における電子メールの取扱いを検討し，新たなシステムの提案・導入を含め一定の方向性を示した。

自由な環境を重視する大学内のネットワークは，インターネットと学内のネットワーク，及び異なるセキュリティポリシが共存している。このネットワーク環境で，安定運用及びセキュリティ対応のため，次の方法を提案・導入することで複数のセキュリティポリシに対応し，一定の効果が得られている。

①認証ネットワーク（認証付き情報コンセント）の提案・導入

講義室，閲覧室に学内でのネットワーク利用を開始する際に利用者認証を行う認証

付き情報コンセントを提案し・構成した。これによって，ネットワーク利用者の匿名性を排除して利用者を特定するとともに，部外者がネットワークを利用することの防止の効果を実現できた。

また，学内外のネットワークを利用しつつ，利用者端末同士のウイルス感染や不正アクセスを防止機能を追加した。このことにより、ウイルス感染拡大を防止し，仮にウイルスに感染した利用者PCが接続されたとしても,100人以上の講義においても,他の利用者は安全に安定運用することが出来る。

②ネットワーク上での利用者 PC の利用者と利用場所のリアルタイム特定機能の提案・導入

利用者 PC の登録情報，認証情報、ネットワーク機器が一時的に記憶している IP アドレス、MAC アドレスを収集・集計することで、利用者 PC の利用者と利用場所をリアルタイムで特定仕組みと支援ソフトをを提案し・構築した。このことにより、ネットワーク障害状況の確認、ウイルス感染・不正利用等の追跡がが可能となり、専門知識を必よとしなくても迅速な対応が可能となった。

ネットワーク管理の最小単位を各居室とし、十分なトレーサビリティー(追跡性)の確保ができた。ブロードキャストストームの発生場所を特定する仕組みを構成することで，ネットワークの不通・不安定な状態を早期に解消できる。限られた管理者が多くの最小規模なネットワークを運用・管理するためには，支援ツールの整備も重要である。

③1 台の利用者 PC が異なるセキュリティポリシを持つ複数のネットワークの利用環境

利用者がネットワークを利用する際に，利用する情報の性質（つまりセキュリティポリシ）に応じて，利用者 PC の通信先のネットワークを適切に切り替ことで，不必

要な通信を遮断でき，高いセキュリティを必要とする通信においても，安全に通信を行うことが出来る。このようなネットワーク利用環境を提案し，医学部附属病院で実証実験を行い一定の効果が上がった。これにより，附属病院の業務 LAN 以外に，研究利用のネットワーク（部門別の習学 LAN 等）の構築に繋がった。

利用者 PC の通信先を常に監視しすることで，通信先ネットワークのポリシに応じて通信先ネットワークを動的に切り替える機能を実装する。このことで，利用者が意識することなく，必要なセキュリティポリシを守ったネットワークの利用環境が構成できる。実際に，この機能を有する物理ネットワークを構成した段階である。今後，このネットワーク上で運用試験を行った後，全学に展開していくことが課題である。

以上のように多様化したネットワーク環境の安定運用やセキュリティの確保は，全体としてひとつのものではなく，ネットワークの物理構成，論理構成，アプリケーション及び利用形態のそれぞれへの対策を，組合わせることで実現できる。特に，各々の対策の完全性を目指すあまり，全体として歪なものになることがある。したがって，各々の対策の完全性よりも，その時々に応じて，他の対策と組み合わせたとき，シームレスな連携が行え，全体としてより効果の高い対策を実現すべきと考える。

謝辞

本研究の遂行並びに本論文の作成にあたり，懇切丁寧な御指導と御鞭撻を賜りました，山口大学大学院理工学研究科 三池秀敏 教授に，厚くお礼申し上げます。山口大学ネットワークの管理・運用業務の中から研究課題を見つけ、論文として纏める手法や考え方について御指導いただきました事に感謝いたします。

また，本論文の作成に際し、副査をお引き受けいただき，本論文に対するご検討と多くの有益なご教授を賜りました山口大学大学院理工学研究科 小河原加久治 教授，多田村克己 教授，松藤信哉 准教授，長篤志 准教授に厚く御礼申しあげます。

本研究の遂行にあたり，セキュリティを確保したネットワークの構築・運用に関する重要な御示唆と御支援をいただきました山口大学大学院医学系研究科 井上裕二教授に深く感謝いたします。

本研究の遂行並びに本論文の作成にあたり，特に多大なご迷惑をおかけしたにも関わらず，御理解と御協力並びに御支援をいただきました，山口大学大学情報機構機構長 纐纈厚 教授，前機構長 阿部憲孝 名誉教授，元機構長 福政修 名誉教授，山口大学大学情報機構メディア基盤センターのセンター長, スタッフの方々, 関係部署の方々に深く感謝いたします。

参考文献

[1] 情報通信白書平成２２年度版, 総務省,
http://www.soumu.go.jp/johotsusintokei/whitepaper/index.html (2010).

[2] 久長穣, 刈谷丈治, 三池秀敏, 山口大学における統一認証の導入事例について, 学術情報処理研究, No.10, pp.55-64 (2006)

[3] 江藤博文, 只木進一, 総合情報基盤センター新システム概要～学内組織との連携強化～, 学術情報処理研究, No.10, pp.75-80 (2006)

[4] 酒井善則, 研究教育を促進する先進的ICTインフラストラクチャ整備, 大学電子認証基盤シンポジウム, pp.67-72 (2006)

[5] 曽根原登, 岡田仁志, 岡部寿男, 島岡政基, 谷本茂明, 峯尾真一, 渡辺克也, 全国大学共同電子認証基盤（UPKI）の構築, 平成１８年度国立情報学研究所オープンハウスシンポジウムー最先端学術情報基盤(CSI)の構築に向けてー, pp.41-46 (2006)

[6] 平野靖, 内藤久資源, 梶田将司, 小尻智子, 間瀬健二, 名古屋大学のユーザ認証基盤の現状, 平成１８年度国立情報学研究所オープンハウスシンポジウムー最先端学術情報基盤(CSI)の構築に向けてー, pp.41-46 (2006)

[7] 馬場健一, 岡村真吾, 寺西裕一, 秋山豊和, 中野博隆, 大坂大学における学内認証基盤の構築, 平成１８年度国立情報学研究所オープンハウスシンポジウムー最

先端学術情報基盤(CSI)の構築に向けて－, pp.41-46 (2006)

[8] 久長穣, 平野均, 平田牧三, 自動入力とデータデース化による Web 連携検診システムの構築, 第 30 回中国･四国大学保健管理研究集会報告書, pp.100-103 (2000)

[9] 松平卓也, 車庫正樹, 井町智彦, SPAM メール対策システムの現状, 学術情報処理研究, No.10, pp.85-89 (2006)

[10] 吉田和幸, メールゲートウェイにおける SPAM 対策について, 学術情報処理研究, No.9, pp.37-43 (2005)

[11] 本田修啓, ウイルス, SPAM 検出機能を持つメール中継システムの構築と運用, 学術情報処理研究, No.9, pp.129-133 (2006)

[12] 広瀬雄二, 大駒誠一, spam 対策に特化した SMTP wrapper, 情報処理学会研究報告, DSM-35, pp.25-30 (2006)

[13] 相馬崇弘, 南弘征, メールヘッダを利用したスパムフィルタとその結果について, 全国共同利用情報基盤センター研究開発論文集, No.28, pp.15-20

[14] "The Apache SpamAssasinProject", http://spamassassin.apache.org/

[15] 杉井学, 松野浩嗣, 機械学習によるスパムメールの特徴の決定木表現, 情報処理学会研究報告, DPS-130, (2007)

[16] 山井成良:「バウンスメール対策」, 情報処理学会, 46巻, 7号, pp。762-766 (2005)

[17] 山井成良, 迷惑メール対策の最新研究, 迷惑メール対策セミナ [福岡], http://www.iajapan.org/anti_spam/ event/2006/

[18] 総務省, 迷惑メールへの対応のあり方に関する研究会最終報告書, http://www.soumu.go.jp/s-news/2005/pdf/ 050722_2_02_00.pdf, (2005)

[19] 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.55-62 (2007)

[20] 久長, 杉井, 王, 長, 三池, 大学等における迷惑メール対策とこれに伴う配送遅延への対応, 電気学会論文誌C, Vol. 131, No. 5, 11p (2011) (印刷中)

[21] 久長穣, 岡田隆, 刈谷丈治, 情報コンセントのユーザ認証について, 学術情報処理研究 No.2, pp.77-81 (1998)

[22] Dynamic Host Configuration Protocol, RFC2131 (1997)

[23] 笠野英松監修, インターネットRFC辞典, アスキー出版局(1998)

[24] Barracuda Spam Firewall Datasheet (日本語), http://www.barracudanetworks.com/ns/ downloads/Datasheets/DS_Barracuda_Spam_Firewall_JP.pdf

[25] Barracuda Spam Firewall Administration Guide (Japanese), http;//www.barracudanetworks.com/ns/downloads/Admin_Guides/AG_Barracuda_Spam_Firewall_JP.pdf

[26] 石橋勇人,山井成良,安部広多,大西克実,松浦敏雄: IPアドレス/MACアドレス偽造に対応した情報コンセント不正アクセス防止方式,情報処理学会論文誌, pp.4353-4361(1999).

[27] 丸山伸, 浅野善男, 辻斉, 藤井康雄, 中村順一: 既存の DHCP 端末で利用できる利用者にも管理者にも安全な情報コンセントシステムの構築, 情報処理学会研究報告 99-DSM-14, pp. 131--136 (1999).

[28] 渡辺義明, 渡辺健次, 江藤博文, 只木進一,"利用と管理が容易で適用範囲が広い利用者認証ゲートウェイシステムの開発,"情報処理学会論文誌, Vol.42, No.12, pp.2802-2809, 2001.

[29] 西村浩二, 秋成秀紀, 野村嘉洋, 相原玲二, 遠隔機器制御プロトコルを用いた有線/無線LAN用情報コンセントシステム, 情報処理学会論文誌 43(2), 662-670 (2002)

[30] Port-Base Network Access Control , IEEE-SA Standards Board, (2004)

[31] 久長穣, 北上悟史, 橘高浩二, 八木英俊, 渡邊孝博, 棚田嘉博, 井上裕二, 無線LANを利用した診療業務LANに接続する利用者端末の運用管理システム, 医療情報学, Vol. 22 (Suppl.), pp. 198-199 (2002)

[32] 久長穣, 八木英俊, 奥田昌之, 井上裕二, 山口における地域遠隔医療ネットワークの構築, 医療情報学, Vol. 20, No. 2, pp. 95-98 (2000)

[33] 奥田昌之, 久長穣, 小早川節, 國次一郎, 杉山真一, 石田博, 芳原達也, 井上裕二, 地域における医療・福祉情報共有システムの継続運用実現のための質的研究, 医療情報学, Vol. 24, No. 1, pp. 177-186 (2004)

[34] 久長穣, 北上悟史, 渡邊孝博, 棚田嘉博, 井上 裕二, 複数 VLAN の動的切り替えネットワークの構築について, 情報処理学会研究報告, DSM22-7, pp. 39-44 (2001)

[35] 久長穣, 渡邊孝博, 奥田昌之, 八木英俊, 石田博, 井上 裕二, セキュリティーポリシーの異なる複数ネットワークの統一的利用環境の構築, 医療情報学, Vol. 21 (Suppl.), pp. 719-720 (2001)

[36] 田島浩一, 西村浩二, 相原玲二,, VLAN 選択機能を持つ情報コンセントシステム, 学術情報処理研究 No.6, pp.5-12, (2002).

[37] Rigney,C.,Rubens,A.C.,Simpson,W.A. and Willens,S.: Remote Authentication Dial In User Service(RADIUS),RFC2138(1997).

[38] J.Postel,J.Reynolds: Telnet Protocol Specification,RFC854(1983).

[39] Case,J.D.,Fedor,M.,Schoffstall,M.L. and Davin,J.R.: Simple Network Management Protocol(SNMP),RFC1157(1990).

[40] IEEE: 802.1Q-1998 IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridge Local Area Networks,IEEE(1998).