キャンパスネットワークシステム案内

1. ネットワーク

1.1　ネットワーク設計方針の概要

第7期システムにおけるネットワークシステム設計方針の概要を，物理構成及び論理構成面から記す。

1.1.1　物理構成

物理構成としては，細部の配線経路改善や帯域増強を除くと，第6期システムの構成を継承している。詳細は図1を参照されたいが，主な物理的構成の特徴を以下に記す。

・3校舎を高速WANでトライアングル型に接続し，校舎間ネットワーク障害に備えている。

・インターネット接続は車道校舎のみとし，他校舎からの接続も車道を経由することで，運用管理負荷を軽減している。

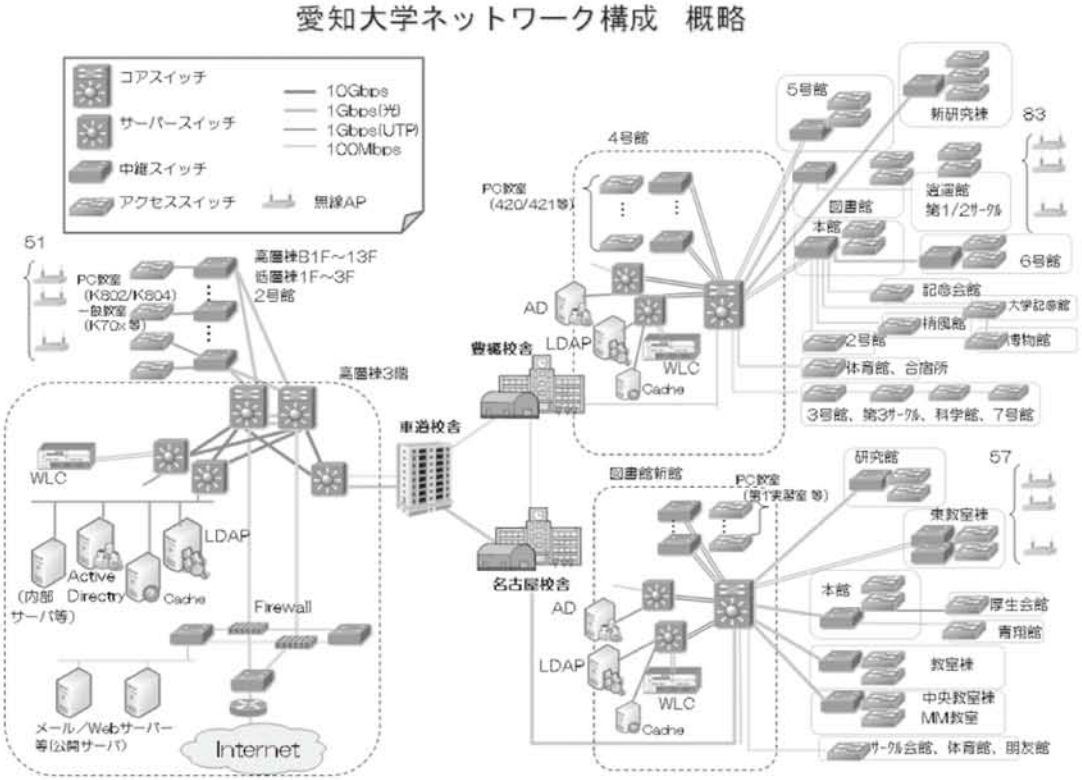

図1：ネットワーク構成概略

・各校舎内は，高速L3コアスイッチを中心としたスター型構成とし，原則としてコア層・ディストリビューション層・アクセス層の3層構成とする。
・各層には，必要十分な帯域と処理能力を持ったL3/L2スイッチを配置するが，アクセス層については後述する認証機能を備えた機器を選択した。
・車道校舎は，コアスイッチを冗長化し，コア・ディストリビューション層間の冗長化を行っている。

1.1.2　論理構成（VLAN設計）

論理構成としては，VLAN設計の見直しを行っている。以下の方針によるVLAN構成変更を行っている。
・場所及び目的別特性に応じて，学内ネットワークを論理的に分類し（図2），分類に沿ってVLAN分割を行っている。

なお，後述する認証ネットワークは，分類毎の特性に従って認証ポリシーを定めている。

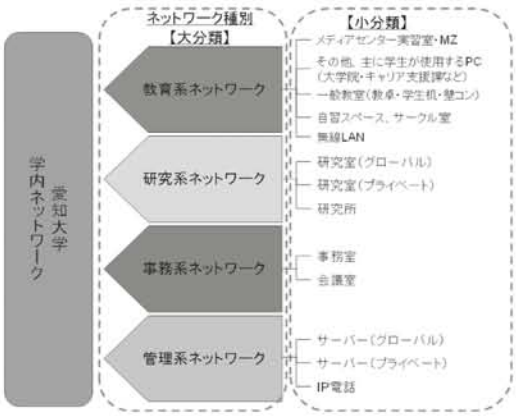

図2：学内ネットワークの論理的分類

・個人研究室でのグローバルIPアドレス利用によるリスク回避のため，個人研究室は原則としてプライベートVLANとする。ただし，サーバー設置等のために特別に必要な場合，情報メディアセンターへの申請・承認によりグローバルIPアドレスを取得することができる。

1.2　認証ネットワークシステム

不正な端末接続を防止するため，学内ネットワーク全域に認証システムを導入した。第6期システムではIEEE802.1x認証を採用し，無線LANや一部の有線LANで利用していたが，対応OSが限定的であることと，接続PC側での認証設定が複雑であることが障壁となり，学内ネットワーク全域への展開に踏み切ることができなかった。

今回，有線・無線を含めた学内ネットワーク全域に認証ネットワークを拡大するにあたり，多様なOSでの接続が考えられることと接続PCの設定変更をできるだけ簡易にすることが必要要件と考えられたため，認証方式としてユーザー認証（Webブラウザでのユーザー ID認証。図3及び図4参照）と端末認証（MACアドレス認証）を採用した。

ネットワーク分類によっては，両方式を組み合わせて利用している。

図3：有線LANのユーザー認証画面

図4：無線LANのユーザー認証画面

1.3　無線LANシステム

第6期システムで広範囲に無線LAN利用環境を構築したが，今回も広範囲での構築を行っている。主な方針・システムの特徴を記す。

1.3.1　無線LANシステムの概要

3校舎で190個を超えるアクセスポイント機器（以下，APとする）の設定及び運用管理負荷を軽減するため，集中管理型無線LANシステムを導入した。

AP側では出力電波やSSID・暗号化方式等の設定情報を一切持たず，各校舎に1式ずつ配備されたWLC（Wireless Lan Controller）にてそれら情報を一元管理することで，動的なチャネル割当てや干渉回避などの電波出力調整を自動で行い，接続クライアントの一元管理や通信ポート制御も実現している。

1.3.2　AP設置箇所・個数

第6期システムでの既設箇所に加え，教員の個人研究室でも利用できるように，との要望に応える必要があった。

個人研究室は3校舎で19フロア約290室あり，壁面が多く，さらに概して本棚に書籍類が敷き詰められていることから，電波の通りが非常に悪い。そのため多数のAPを増設する必要があり，コスト的な問題も生じたが，既設無線LANの利用実績をもとに一般教室等の設置個数を再調整し，全体的には既設数より少ないAP数を設置することで済ませることができた。

1.3.3　認証方式

前述したユーザー認証（Webブラウザでのユーザー-ID認証）と端末認証（MACアドレス認証）を組み合わせている。

なお，無線LANの場合，Webブラウザ起動時にユーザー認証画面へ自動遷移する。

2.セキュリティ

2.1　Firewallによるネットワーク保護

学内ネットワークとインターネットの

境界にはFirewallを設置し，インターネットから学内ネットワークへの攻撃や不正な接続を防いでいる。

また，学内ネットワークからインターネットへの通信についても，Web参照系やメール系などの一般的な通信または特別に必要性のある通信ポート以外を遮断することにより，万一学内ネットワークに不正PCが接続された場合等でもインターネットへの影響を少なくしている。

公開サーバー（メールサーバー／Webサーバー等）は，Firewallによって設けられたDMZ（非武装地帯）に集約し，必要ポートのみ学内外からのアクセスを許可することで，公開することによるリスクを低減している。

なお，Firewallは学外接続への要であることから冗長構成とし，さらにホットスタンバイとすることで信頼性を高めている。

2.2 IPSによるネットワーク保護

近年のインターネットにおける脅威は多様化しており，OSやP2Pソフトウェアなどの脆弱性を狙った攻撃や，スパイウェアやトロイの木馬型ウィルスなどの中には，通信ポートを制限するFirewallだけでは防ぎきることが困難なものがある。そのため，通信パターンやパケット検査を行って不正な接続を防止する「IPS(IntrusionProtectionSystem：侵入防止システム)」を導入した。

第6期システムでは独立したアプライアンス機器を設置していたが，今回はFirewall機能と統合された製品を選択し，運用管理負荷軽減及び通信検査処理効率の向上を図っている。

2.3 ホスト側のセキュリティ対策

今回のシステムで導入する全ての汎用サーバー（Windows／Linuxサーバー）及び全てのクライアントPCには，当然ながらウィルス対策ソフトを導入している。

特にWindowsに関しては，ウィルス対策の運用管理を一元的に行えるよう，各校舎にウィルス対策サーバーを配置した構成を取っている。

3. 全学認証

3.1 全学認証システム

これまで本学では，ユーザID/パスワードによるユーザ認証を必要とする情報システムが多数稼動していた。しかし，教員・学生用と職員用の認証システムが分かれている，PC実習室システムのWindowsドメイン環境へ認証が依存しているなどの問題が生じていた。問題を解決するため，第7期システムでは，全学の認証基盤を整備し，認証情報の一元化を実現するため，全学認証システムを構築した。

3.2　システム構成

全学認証システムの認証基盤構成を図5に示す。認証基盤は，認証サービスとしてのActiveDirectory，Sun Java System Directory Server，Radiusから構成される。

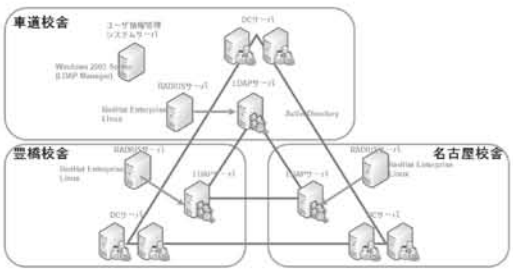

図5：全学認証システム構成概要

本学の場合，豊橋校舎・名古屋校舎・車道校舎の3校舎に分かれているため，認証サーバを各校舎に，ユーザ情報管理のサーバは車道校舎に配置している。電子メールシステム，有線・無線LAN利用，SSL-VPN, 印刷枚数管理システム, 愛知大学ポータルシステム（Universal Passport），グループウェア（サイボウズ ガルーン）などの諸システムは，全学認証システムに対しユーザ認証サービスを連携しており，認証情報の一元化を実現した。（図6）

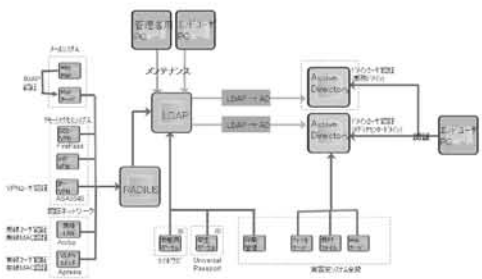

図6：全学認証システム連携概要

3.3　ユーザ情報管理システム

全学認証システムにおけるユーザ情報の運用管理ツールとして，LDAPManager（エクスジェン・ネットワークス）を導入した。LDAPManagerはLDAPサーバを一元管理用の中心に据え，ここに集約したユーザ情報をそれぞれのプラグインを介してActiveDirectoryへ自動反映する。（図7）

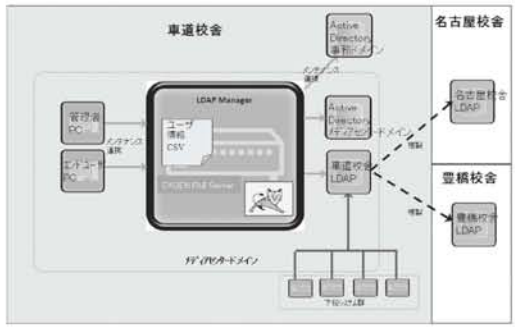

図7：LDAPManagerシステム概要

LDAPサーバに対しては，csvファイルからの一括メンテナンス処理や，専用のGUIツール（利用者用ツールおよび管理者用ツール）によるメンテナンスをおこなうことが可能である。（図8）

図8：専用のGUIツール（管理者用）

LDAPManagerは，メンテナンスの一連の処理により，各プラグインによりファイルサーバへのホームフォルダ作成や，メールフォルダ作成などを一括におこない，連携システムが利用可能となるよう連係情報を保持する。

この運用管理ツールの導入により，上述の通り利用者はパスワードをインターネットブラウザから変更できるようになり，利便性が向上した。(図9)

図9：専用のGUIツール（利用者用）

また，有線・無線LAN利用時の認証のため，LDAPManagerでのMACアドレスの管理も実現した。(図10)

図10：専用のGUIツール（MACアドレス）

4. メールシステム

4.1 メールシステムの構成

4.1.1 構成の概要

第6期システムでは，①豊橋校舎学生用 ②名古屋・車道校舎学生用 ③教職員用 ④法科大学院用⑤メーリングリスト用のメールサーバーをそれぞれ別ドメインにて運用していたが，今回は①②のメールサーバー及びドメインの統合を行った。

また，従来はウィルス対策サーバーによりウィルス・スパムメール対策を行っていたが，近年のスパムメール流量の増大は凄まじく，対策を強化する必要があった。そのため，スパムメール対策専用アプライアンス機を設置することにより，スパム検知の精度向上を図っている。

Webメールシステムとしては，従来利用していたActive!Mail 2003の後継であるActive!Mail 6を採用した。Webサーバーを車道校舎へ集約し，負荷分散サーバーを介することで，授業などによる一斉アクセスにも耐えられる構成となっている。

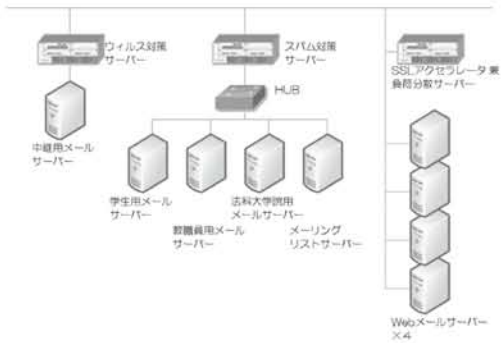

図11：メールシステム構成

4.1.2　送受信の流れ（pop3/smtp）

学生用，教職員用及び法科大学院用メールサーバーは，それぞれpop3/smtp及びpop3s/smtpsによるメール送受信通信に対応している。

学内メールサーバーのメール受信は，以下の流れで行われる。（図12参照）

①学内メールドメイン宛のメールは，全て中継用メールサーバーへ配送される。

②中継用メールサーバーの前の透過型ウィルス対策サーバーにてウィルスチェックを行う。

③中継用メールサーバーから，該当ドメインサーバーへ向けて配送される。

④該当ドメインサーバーの前の透過型スパム対策サーバーにてスパムチェックを行う。

⑤スパム対策サーバーから該当ドメインサーバーへ向けて配送される。

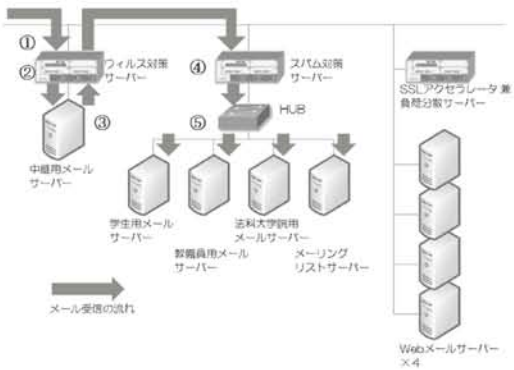

図12：pop3によるメール受信の流れ

smtpによるメール送信は，以下の流れで通信が行われる。（図13参照）

通常は中継用メールサーバーをsmtpサーバーとして利用することを推奨しているため，その場合の流れを記す。

（学内宛メール送信）

①中継用メールサーバーから，該当ドメインサーバーへ向けて配送される。

②ウィルス対策サーバーにてウィルスチェックを行う。

③該当ドメインサーバーの前の透過型スパム対策サーバーにてスパムチェックを行う。

④スパム対策サーバーから該当ドメインサーバーへ向けて配送される。

（学外宛メール送信）

①’中継用メールサーバーから，該当ドメインサーバーへ向けて配送される。

②’ウィルス対策サーバーにてウィルスチェックを行い，学外へ配送される。

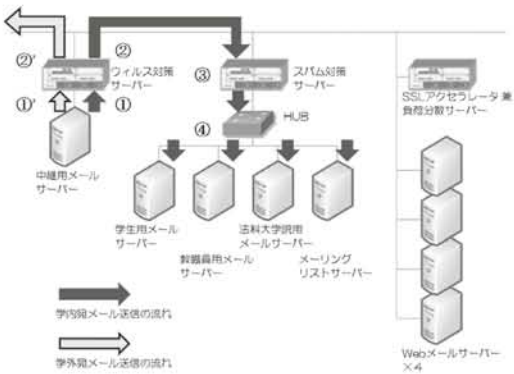

図13：smtpによるメール送信の流れ

4.1.3　送受信の流れ（imap）

imapとは，メールをクライアントPCにダウンロードせず，サーバーに置いたままメールの読み書きができる通信プロトコルである。今回導入したWebメールシステム（Active!Mail6）は，imapを活用

して実現している。

Active!Mail6を利用した際のhttp通信の流れ及びimap通信の流れを，図14に示す。

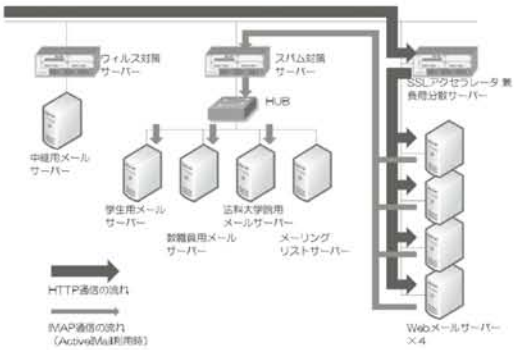

図14：http通信及びimap通信の流れ

4.2 Webメールシステム

4.2.1 従来との違い

今回のWebメールシステムにおける大きな変更点は，(1)ソフトウェアのバージョンアップ(2)SSL通信実装によるセキュリティ向上(3)負荷分散によるレスポンス向上の3点である。

(1)に関しては次項で概要を述べる。

(2)に関しては，パスワード及びWebメールの暗号化保護対策としてSSLを実装した。通信の暗号化・復号化処理は，レスポンスを考慮してSSLアクセラレータにて実施している。なお，SSLアクセラレータは，負荷分散サーバーにて処理を兼用している。

(3)に関しては，従来授業などでのWebメール一斉アクセスの際に処理遅延が問題視されたことと，Active!Mailのソフトウェア仕様変更に伴うレスポンス遅延への不安，及び(2)に関連するSSL処理に伴うレスポンスへの影響を考慮した結果，負荷分散サーバーを設置することとした。

4.2.2 Active!Mail6の諸機能

Active!Mail2003からActive!Mail6へのバージョンアップにより，ユーザーインターフェイスや詳細な機能において，大きな変更が生じた。主な変更点や特徴的な機能を以下に紹介する。

・ログイン画面

従来は学生用，教員用でログイン画面URLが異なっていたが，今回は負荷分散サーバーを導入したこともあり，ログイン画面は仮想的に一元化されている。利用者がログイン画面にてメールドメインを選択することにより，imapアクセス先メールサーバーを判断している。

図15：Active!Mailログイン画面

・メールホームタブ

管理者からのお知らせ，新着メール情報，メールボックス使用量などを確認で

き，メールポータルとして構成されている。なお，ツールにて，ログイン後のページをメールホームでなくメール受信に変更することも可能である。

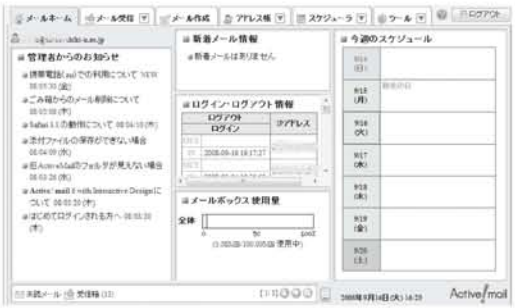

図16：メールホームタブ

・メール受信タブ

Webシステムの操作性を格段に向上するAjaxという新技術を採用することにより，メールのドラッグ＆ドロップ操作やダブルクリック操作を実現している。メールフォルダの作成やメール本文の別窓表示も可能である。

図17：メール受信タブ

・メール作成タブ

アドレス帳及び送信履歴からのアドレス入力が可能であるが，さらにアドレス入力補完機能もあり，メールアドレス入力機能に関してはかなり強化されている。

図18：メール作成画面

・モバイル機能

携帯電話などのモバイル端末からもアクセス可能である。アクセス先URLはQRコード表示が可能であるため，携帯電話からのアクセスを容易にしている。

図19：モバイル設定画面

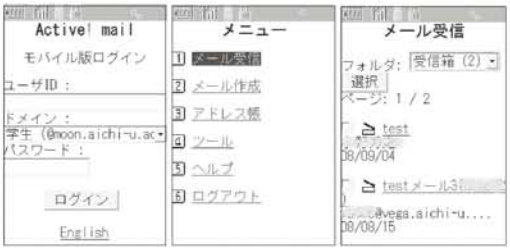

図20：携帯電話でのアクセスの様子

・その他

ツールタブから，様々な機能の設定が可能である。

フォルダ管理では，mbox形式のメール

データをインポート／エクスポートでき，メールデータのバックアップに有用である。POPアカウント管理では，外部プロバイダ等のメールをPOP受信する設定が可能である。フィルタリングでは，メール振り分け設定を行うことができる。転送では他アドレスへのメール転送が設定できるが，件名や差出人などの条件による転送設定も可能である。迷惑メールフィルタでは，学習型迷惑メールフィルタ機能を利用者ごとに設定できる。

図21：ツールタブでの設定項目一覧

以上がActive!Mail6の特徴的な機能であり，機能強化されて便利になった点も多いが，導入バージョンでは幾つかの動作不具合や利用上の不都合も生じている。マイナーバージョンアップで修正される部分も多く，随時対応していく予定である。

4.3 迷惑メール対策

4.3.1 ウィルスメール対策

4.1で述べたように，メール送受信時にウィルスチェックを行うよう，透過型ウィルス対策サーバー（専用アプライアンス機）を中継サーバーの前に配置している。

ウィルス対策サーバーは，ウィルス定義体を毎時更新しており，通過するメールを定義体と照合してウィルス検知した際に，ウィルスを削除してレポートメールを受信者に送信している。

また，不正なsmtpセッションを判断して切断する機能も活用している。

さらに，ウィルス対策サーバーにおいて第1段階のスパムチェック処理も行っており，毎時更新される定義体と照合するなどしてスパムスコア（諸条件からスパムと判断される度合を点数化）を算出し，スパムスコアが一定以上の場合はメール配送をブロックする処理を行っている。

4.3.2 スパムメール対策

ウィルス対策サーバーの後に，第2段階のスパムチェックを行うよう，スパム対策サーバー（専用アプライアンス機）を配置している。

スパム対策サーバーは，定時に更新される定義体・データベースとの照合や，学習型フィルタなどで複合的にスパムスコアを算出し，スパムスコアが一定以上の場合は配送メールの件名に[Spam]を付与して受信者に配送している。

スパム配送側の傾向は随時変わるため，スパム検知も困難であり，すり抜けや誤検知は発生せざるを得ないが，明示的に

ブラックリストやホワイトリストとしてフィルタ設定することも可能なので，必要に応じて人為的に対処している。

4.3.3 迷惑メールの状況

ウィルス対策サーバーで検出できているウィルスは，日によりばらつきがあるが，250件～1300件/日 程度で推移している。また，ウィルス対策サーバーとスパム対策サーバーで検出されるスパムメールを合計すると，全体のメール流量の4割程度がスパムメールで占められているのが実状である。さらに，スパムメールと判断された中の3割程度が件名に[Spam]付与され受信者に配送され，その他は配送がブロックされている。

検出状況を見ると，専用アプライアンス機の効果が発揮されているようにも見えるが，すり抜けや誤検知は数字に現れにくく，精度の面では効果判定が難しい。迷惑メール配送側の技術は，ここ数年においては数ヶ月単位で変化していく傾向があるため，継続して対策を検討していく必要がある。

また，利用者の情報セキュリティ意識が低い場合，ウィルス感染や不正アクセスなどを足がかりとして，無意識のうちに利用PCが迷惑メール配送端末となる可能性も考えられる。本学のネットワーク及びメール利用者が迷惑メールの加害者にならないよう，利用者側での情報セキュリティ意識向上も必要である。

4.4 メーリングリストシステム

本学では，メーリングリストシステム（以下,MLとする）として,メールサーバーのエイリアス配送機能を活用したエイリアス型MLと，会員制ML管理ソフトであるMailmanを利用している（前者は一般的にはMLと区別されることが多いが，本学ではMLとして取り扱っている)。7期システムでも同様のサービスを提供するため，ハードウェア更新とソフトウェア移行及び更新を行った。

利用者が用途により，エイリアス型MLかMailmanかを選択して利用できるような運用を行っている。

4.4.1 エイリアス型ML

メールエイリアスに複数メールアドレスを記載して配送するだけの単純な仕組みであるが，メンバーリストを利用者にて容易に管理できるようにWebツールが稼動している（図22参照)。

図22：エイリアス型ML管理ツール

投稿管理はできないので，迷惑メール受信が増えてしまう一般公開用としては

不向きであるが，メンバー間の連絡用として利用するには手軽なシステムである。

4.4.2 Mailman

Mailmanは，投稿管理が可能な会員制ML管理ソフトである。多彩な機能を持ち，メンバー管理や投稿管理などを柔軟に行うことができる。

管理画面での設定箇所が少し分かりにくく，初心者には取っつきにくい印象を持たれることが多いが，メンバー外からの投稿は管理者承認を必要とさせるなどの設定も可能で，迷惑メール対策に効果を発揮するため，一般公開用MLを利用する際には推奨している。

図23：Mailman管理ツール（上：会員リスト管理画面　下：投稿管理画面）

5. 実習室システム

5.1 システム概要

本学の実習室システムは，ドメインコントローラー，クライアントパソコン，ストレージおよび印刷管理システムから構成される。実習室システムのクライアント環境は，LDAPサーバ(3. 全学認証参照)と連携したAcrive Directory(Windowsサーバで実装されたディレクトリサービス)によるユーザ認証とした。また3校舎全ての実習室PCやメディアゾーンなどの開放スペースのPC，および車道校舎のシンクライアントPCで，3校舎どのPCを利用しても同じユーザごとの個人環境を実現した。クライアント環境のOSは，Microsoft Windows Vista Businessを採用し，ドメインは3校舎で1つのドメインで構成している。

5.2 システム構成

実習室システムのシステム規模としては，教職員および3校舎の学生を合わせ15,000ユーザ程度であり，全てのユーザは3校舎いずれの実習室・開放スペースのPCへログオンでき，同じデスクトップ環境を利用することが可能である。それぞれの校舎には認証サーバとしてDCサーバが2台ずつ，ホームディレクトリの保存領域としてストレージ（NAS）が1式ず

つ，教材用保存領域として教材用ファイルサーバが1台ずつ，印刷管理システムとして印刷管理サーバが1台ずつ，ウィルス対策のためSymantecEndPointProtectionの親サーバが1台ずつ配置されている。（図24）

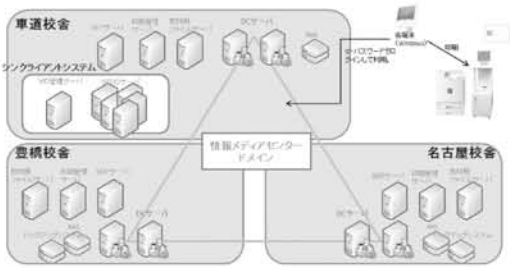

図24：システム構成

また，各校舎の実習室および開放スペースにクライアントPC（Windows Vista Business）およびカラープリンタを設置している。

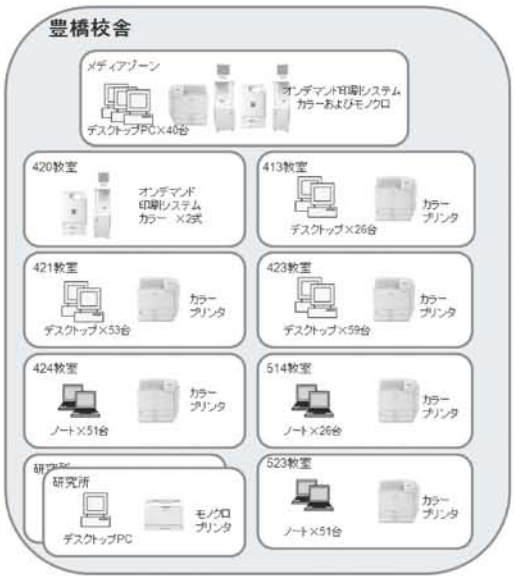

図25：クライアント構成（豊橋校舎）

図26：クライアント構成（名古屋校舎）

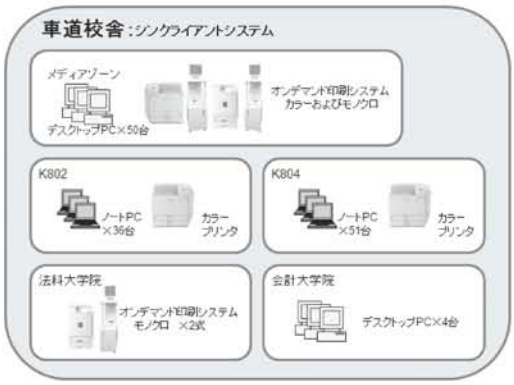

図27：クライアント構成（車道校舎）

5.3 実習室クライアントサーバシステム

実習室システムとしてのアカウント情報は，全学認証システムのユーザ情報管理ツールより，LDAPサーバ上の情報からActiveDirectory上へ自動連携されている。ユーザは実習室クライアントPCで自分のユーザID/パスワードを入力し，情報メディアセンターのドメイン環境へログ

インすることができる。また，DC（ドメインコントローラー）では，各校舎教員，学生，スタッフごとにOU（Organization Unit）が構成されており，それぞれ適切なグループポリシーをかけている。

クライアント環境では，ブラウザやMS-Officeなどで，日本語だけでなく英語，中国語，韓国語，タイ語，ロシア語，独語，仏語などの多言語入力が可能である。また，多く設置されているノートPCについては，セキュリティワイヤーでの盗難防止策を施し，デスクトップPCは地震対策を実施している。

5.4　シンクライアントシステム

車道校舎のクライアントPCは，Ardenceを基としたネットワークブート型シンクライアントシステムを導入した。これは，ネットワーク上のサーバで管理されるWindowsのディスクイメージからクライアントPCを起動する方式であり，クライアントPCのCPUとメモリを利用しOSやアプリケーションが処理されるものである。今回車道校舎で導入したシンクライアントシステムは，VID（Virtual Image Distribute）システムと呼ばれる製品である。（図28）

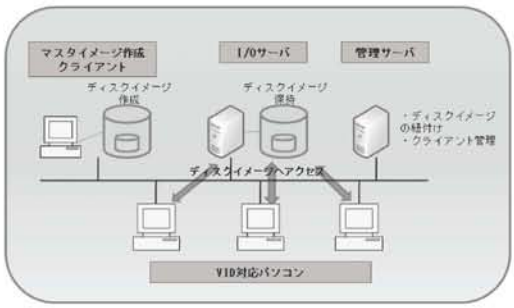

図28：VIDシステムイメージ

VIDシステムの管理用GUIツール（図29）により，ディスクイメージの運用管理やクライアントを起動・再起動・シャットダウンするなどのクライアント制御などが容易に管理できている。

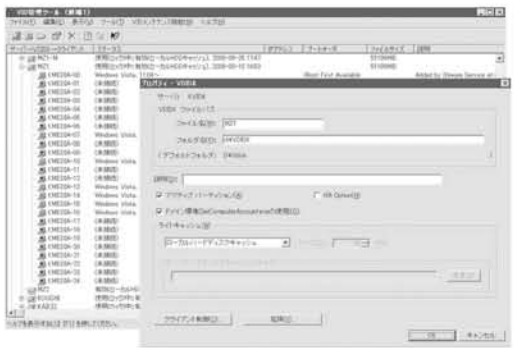

図29：VID管理ツール

図30：VID管理ツール（クライアント制御）

5.5　ファイルサーバ

実習室システムでは，ファイルサーバとして①個人用マイドキュメントとしてのストレージ（NAS）…Zドライブ（容量:100MB），②実習用データドライブとして教材用ファイルサーバ…Oドライブを用意した。

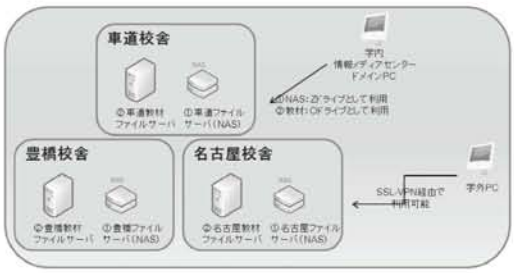

図31：ファイルサーバ構成

図32：利用者環境（コンピュータ）

5.5.1　ストレージ（NAS）

利用者数を3校舎合わせて15,000，ホームディレクトリとして1利用者あたり100MBとしてNASを用意した。また個人用マイドキュメントのバックアップは，通常のバックアップに加え，スナップショットも取得している。利用者は，実習室や開放スペースのPCでZドライブとしてホームディレクトリを利用可能である。（図33）ただし容量利用制限が存在するため，制限を越えた場合，個人環境としてリダイレクトしているデスクトップやドキュメント，ダウンロードフォルダなどで，リダイレクトの失敗が発生するという問題がある。このため，利用者のログイン時にログインスクリプトにて空き容量のチェックを実施している。

図33：Zドライブ（ホームディレクトリ）

5.5.2　教材用ファイルサーバ

3校舎それぞれ規模に応じた保存領域の教材用ファイルサーバを用意した。共有保存領域が必要な講義については，担当

図34：0ドライブ（教材用ファイルサーバ）

教員の申請により講義用フォルダを準備する。これを利用者は，Oドライブとして利用可能である。

5.6　プリンターシステム

第6期システムに引き続き，情報メディアセンターでは印刷管理システムを導入し，新たに印刷ミスや印刷物の取り間違い防止のためオンデマンド印刷機能を各校舎の開放スペースに導入した。

5.6.1　プリンター

5.6.2で述べる印刷管理システムに対応したプリンターを設置した。（カラープリンター：IPSio SP C810，モノクロプリンター：IPSio SP6220/IPSio SP6210）なお設置プリンターは，登録外のクライアントからの印刷をIPアドレスで制限している。

5.6.2　印刷管理システム

本学の教員および学生の印刷管理として，印刷管理システム（RidocIOGate）を導入した。印刷管理システム内の印刷は，全学認証システムと認証を連携しており，5.6.3のオンデマンド端末からの印刷時には学生証・教職員証でのICカード認証も可能である。

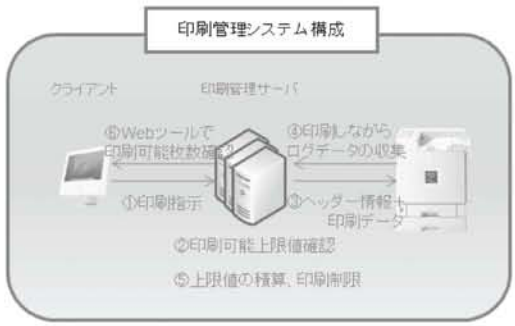

図35：印刷管理システム構成

また本学では，印刷制限を年間ポイント制とし，ポイントをカラーおよびモノクロの印刷で利用することができる。ポイントの有効期限は年度末であり，ポイント制限に達した利用者は有料で追加申請が可能である。なお，印刷ジョブ途中にポイント制限に達した場合，印刷は中止される。

印刷枚数は決まっているのですか？

★ 2008年度より、ポイント制となりました。
★ ポイントはモノクロ・カラー共通でご利用いただけます。
★ ポイントの有効期限は年度末までです。
★ 配布印刷ポイント数・消費ポイント数は、下記の表をご覧ください。
★ 制限を越えた場合、300円で100ポイント分を追加申請できます。

配布印刷ポイント数		
区分		印刷ポイント
学部生（一般）		800 ポイント
学部生（卒業年次）		900 ポイント
大学院生・専門職大学院生		1000 ポイント
教職員（非常勤含む）		1000 ポイント
科目等履修生		350 ポイント
その他（オープンカレッジ生）		700 ポイント
消費ポイント数		
モノクロ	A3 未満	1 ポイント
	A3 以上	2 ポイント
カラー	A3 未満	10 ポイント
	A3 以上	20 ポイント

図36：印刷枚数のポイント制

印刷ポイントは，専用のWebページで確認することができる。
https://kpri.joho.aichi-u.ac.jp/rgate/（図37）

図37：印刷状況確認ログイン画面

ログイン画面で自分のユーザID/パスワードを入力し，印刷状況確認Webページにログインし，印刷状況の確認が可能である。

図38：印刷状況確認画面

5.6.3 オンデマンド印刷

5.6.2で述べたとおり，印刷管理システムでは開放スペースでの印刷として，オンデマンド印刷という仕組みを取り入れた。

オンデマンド印刷は，クライアントPCで印刷を実行し，学生証・教職員証を印刷指示専用端末にかざすことで認証した後，印刷専用端末のタッチパネルで出力したいジョブを選択し，プリンターから出力される仕組みである。(図39)

オンデマンド印刷の導入により，印刷物の取り違えや置き忘れによる情報漏洩を防ぎ，無駄な印刷や放置された印刷物を減らす効果を期待している。

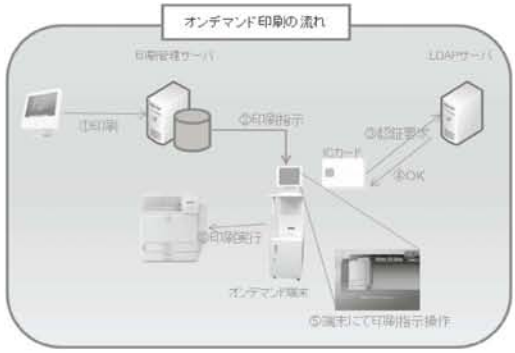

図39：オンデマンド印刷の流れ

5.6.4 持ち込みPC対応

教員および学生が学内に持ち込むPCから，第7期システムのプリンターへ印刷ができ，なおかつ印刷管理システムによる管理を可能としている。持ち込みPCで印刷サービスを利用するためには，専用のプリンタドライバをインストールする必要がある。

6. その他サービス

6.1 VPNシステム

第7期システムでは，第6期システムと同様にリモートアクセスシステムとして「SSL-VPNシステム」と「IPsecVPNシステム」を構築した。それぞれの概要を以下に記す。

6.1.1 SSL-VPNシステム

利用者は，WebブラウザからSSL-VPNシステムにログオンすることにより，学

外からの学内専用Webページへのアクセスと，学外からのファイルサーバーアクセスが可能である。

特に利用者PCにソフトウェアをインストールする必要はない。また，SSL通信で暗号化されており，セキュアな通信を実現している。

ファイルサーバーアクセスについては，JOHOドメインの個人フォルダと教材用共有フォルダをネットワークドライブへマウントすることができる。

ただし，Windowsの場合はActiveXコントロールを使用してネットワークドライブへの自動割当てが可能であるが，それ以外のOSでは挙動が異なるので注意が必要である。

図40：SSL-VPNシステムのログオン画面とログオン後の画面（教職員向け）

図41：ネットワークドライブ接続の様子（左）と，割当てられたネットワークドライブ（右）

6.1.2 IPsecVPNシステム

利用者は，PCにインストールされた専用ソフトウェアからログオンすることで，学外から学内LANにIPsec通信で暗号化された状態でアクセスすることができる。

先に紹介したSSL-VPNでは，SSLに対応したアプリケーションでないと利用の保障がされないという弱点があるが，IPsecVPNはネットワーク層で暗号化される技術のため，アプリケーションによる動作の違いは無く，学内LAN接続とほぼ同じ状態を実現することができる。

大変便利なシステムである一方，接続PCはセキュリティ管理がされている必要がある。

図42：IPsecVPNソフトウェア