ISSN 1343-2915

学術情報処理研究

No.15　　2011

JACN

学術情報処理研究編集委員会

学術情報処理研究

Journal for Academic Computing and Networking

No.15　2011

学術情報処理研究編集委員会

N0.15　2011 年

学術情報処理研究

第14回学術情報処理研究集会

センター紹介

報告

巻頭言

危機を乗り越える組織作り

奈良女子大学総合情報処理センター長
加古 富志雄

この度の東日本大震災により、多くの皆様が、これまで想像もしなかった危機に直面されたことと思います。被災された方々に心よりお見舞い申し上げます。いまだ危機が終息したのではなく、更なる災害の発生を防ぐための努力が現在も続けられている状態であります。また、東海から南海にかけてのトラフを震源とする大地震の発生も予測されており、これによる被害はさらに甚大な規模になると予想されています。

このような中にあって、情報系センターの皆様方に置かれましては、計算機やネットワークという教育や研究、さらには大学運営の基盤を支えているインフラの維持、管理といったこれまでの業務に加えて、災害発生時にどれだけの機能を維持するか、またどのように復旧させていくかについても考えていくことが求められています。

現在、多くのセンターでは、予算の削減や人的資源の不足といった問題を抱えながら、日々の業務に携わっておられると思います。組織の統合によって無駄をなくして、インフラを維持していくかに腐心されていることと存じますが、これは、別の見方をすると、非常時のための安全係数を限界まで小さくするということであり、非常時にそなえて予備を取っておくという方向とは逆の方向性である。今回の大震災では、想定される災害に対処するだけでは十分ではないということが明らかになり、今後は想定以上の災害が発生した場合の対処も考慮していくことが求められています。

このような、大災害に対処し、そこから発生する危機を乗り越えるための組織をどのように構築・維持していくかということがセンターとしての一つの大きな課題となります。これは、個々のセンターの努力だけでは対応することが非常に難しい問題です。大学の情報系センター間で連携を取り、共同で危機を乗り越えていくための組織ならびに人的体制の整備に取り組んでいくことが必要でしょう。

国立大学法人情報系センター関係者の研究発表と情報交換の場である学術情報処理研究集会も１５回目を数えるようになりました。本誌「学術情報処理研究」が、情報系センターに課せられた課題を解決する一助となり、その重要性を増していくことを期待します。

論文

災害時に備えた分散キャンパスによる情報基盤の整備

Construction of robust information infrastructures for disaster in decentralized campus

伊藤智博[†,†‡]，高野勝美[†,†‡]，田島靖久[‡,†‡]，吉田浩司[‡,†‡]
Tomohiro Ito[†,†‡], Katsumi Takano[†,†‡], Yasuhisa Tajima[‡,†‡], Hiroshi Yoshida[‡,†‡]
tomohiro_ito@ieee.org, ktakano@ieee.org, tajima@sci.kj.yamagata-u.ac.jp, yoshida@ncsc.yamagata-u.ac.jp

† 山形大学大学院理工学研究科
‡ 山形大学基盤教育院
† ‡ 山形大学情報ネットワークセンター
992-8510 米沢市城南 4-3-16

† Graduate School of Science and Engineering, Yamagata University,
‡ Institute of Arts and Sciences, Yamagata University
† ‡ Networking and Computing Service Center, Yamagata University
4-3-16 Johnan, Yonezawa 992-8510 Japan

概要

山形大学では，ネットワークを安定に運用するために様々な試みがなされてきた．2011 年 3 月 11 日に発生した東日本大震災以前には，比較的安価な商用 ISP によるバックアップ回線を準備し，ファイアウォールの複数 ISP 接続機能と DNS のラウンドロビン機能によるインバウンド通信の冗長化技術を構築していた．震災による停電によって，この冗長化構成が施されたサーバについては，学外から本学のサービスを利用することができた．一方，この冗長化技術だけでは，学内から学外への通信はできなかったため，震災後，アウトバウンド通信の冗長化技術を導入した．本稿では，震災前，震災時および震災後に実施した情報基盤を取り囲む様々な対応について報告する．

キーワード

ネットワーク，冗長化， WAN リンクロードバランシング，シボレス認証

1. はじめに

学内 LAN(Local Area Network)を始めとする情報基盤は，大学において日夜停止することなく運用されるネットワークであり，教育研究や業務などで広く利用されている．履修登録システムの Web 化や IC カードによる出席管理，キャンパス間の内線電話の VoIP 化などの様々な分野において，情報基盤が必要不可欠になってきている[1]．また，ブロードバンドネットワークの普及や公衆無線 LAN，WiMAX などの普及により，インターネットへの接続で

きる場所が広がりを見せており，ネットワークインフラが教育や生活の中で重要な位置づけになってきている．大規模災害時には，学生への情報発信や安否確認などでもインターネットが利用されるなど，情報基盤は教育や業務のみならず，大規模災害発生時の緊急用連絡手段としても必要不可欠な存在となっている[2],[3].

本学における学内 LAN システムである山形大学情報通信ネットワークシステムには，障害が発生したときのことを想定していくつかの試みがなされてきた. 一般に，障害に強いネットワーク構成するためには，Border Gateway Protocol (BGP)によるマルチホームを構成することが多い．本学では，表 1 に示すように，複数の冗長化方式を費用面および運用面から検討した．一般的な BGP によるマルチホーム接続は，インバウンド／アウトバウンド通信を相互に冗長化できるなど利点が大きい．しかし，高価な商用 ISP の回線が必要になることや経路障害を自力で解決できる人材の育成が必要になることから，BGP の導入には至らなかった．地理的負荷分散装置などによってもインバウンド／アウトバウンド通信を冗長化することが可能であるが，機器の導入費用が高額なことから，断念した．あくまで，一時的な障害発生時に，重要な通信（DNS サービスやメールの受信）のみを可能にすればよいと考えると，高額な回線費用や機器の導入，運用面での人的なコストの増大を行ってまで，BGP などによるインバウンド／アウトバウンドの通信の冗長化は不要であると判断した．そこで，緊急時の通信の確保のために比較的安価な商用 ISP によるバックアップ回線を準備し，ファイアウォールの複数 ISP 機能と DNS のラウンドロビン機能によるインバウンド通信の冗長化技術を取り入れた．特に，本学は，50km 以上離れた場所に複数のキャンパス（山形市，米沢市，鶴岡市）を有する分散キャンパスである．この分散キャンパスを活用して，複数のキャンパスに DNS サーバを配置したり，メールのトランスポートサーバを複数回線に接続したり，様々な手法で，緊急時のバックアップ機能について試みてきた.

2011 年 3 月 11 日に発生した東日本大震災においては，本学の情報基盤の要となっている小白川キャンパスが停電になり，インターネットと接続している主回線が停止した．震災以前には，長時間の障害を想定していなかったため，インバウンド通信における冗長化や負荷分散技術の運用が導入されていた．震災以降は，長時間の障害が発生することを想定して，アウトバウンドの通信における冗長化技術が試験的に導入された．さらに，大規模震災時の安否確認システムとして，学術認証フェデレーション（学認）[4]で採用されているシボレス認証を利用して構築した．本稿では，震災前，震災時および震災後に実施した情報基盤を取り囲む様々な対応について報告する.

以下，第 2 節では，震災前に試みられてきた情報基盤の障害対応および冗長化構成について述べ, 第 3 節では, 震災後に導入された情報通信基盤の冗長化構成について述べる.

表 1 冗長化方式の違いによる効果および費用面，運用面から導入検討事項

検討項目	冗長化方式		
	マルチホーム／BGP	地理的負荷分散	DNS ラウンドロビン
冗長回線費用 a)	数十万円～/月	数万円/月	数万円/月
機器導入費用	500 万円程度 b)	1000 万円以上 c)	0 円 d)
効果および利点	・インバウンド／アウトバウンドの通信が冗長化 ・インバウンド／アウトバウンドの通信が等価であるため IP 認証にも対応	・インバウンド通信が冗長化 ・回線が低価格 ・回線障害時に DNS の自動変更が可能 ・設計次第では，アウトバンドの冗長化も可能	・一部の回線に障害が発生したときに，ラウンドロビンによるインバウンド通信が可能 ・回線が低価格 ・短期間で導入可能
欠点・運用面の問題	・回線費用が高い ・導入機器が高価 ・経路障害は自力で解決することが前提のため，運用コストが増大および長期的な人材の育成が必要 ・機器の調達が必要なため導入までの期間が長い	・導入機器が高価 ・インバウンド／アウトバウンド通信時の IP アドレスが異なる場合があるため，IP 認証には対応不可能 ・機器の調達が必要なため導入までの期間が長い	・回線障害時に DNS の手動変更必要 ・アウトバウンド通信の冗長化が難しい ・インバウンド／アウトバウンド通信時の IP アドレスが異なる場合があるため，IP 認証には対応不可能

a) バックアップ回線のため，帯域は，10 Mbps 程度で算出. b) CISCO 社製 ASR 1002（フルルート対応，スループット数 Gbps）を導入したと仮定. c) F5 社製 BIG-IP Local Traffic Manager に Global Traffic Manager モジュールを導入したと仮定.
d) 本学で導入済みのファイアウォールは，導入時より，複数 ISP 機能に対応していたので，費用負担は発生しない.

2. 震災前の情報基盤

2011 年 3 月 11 日に発生した東日本大震災前に，障害発生時を想定して，複数回線の引き込みや DNS サーバの複数回線による冗長化などの様々な実証実験が試みられてきた．震災時および震災後の情報基盤の整備は，この実証実験の試みを基盤として，今後の大規模災害に備えるために拡張されたものであるので，本節では震災前までの情報基盤の概要と試みされてきた冗長化技術について述べる．

2.1. ネットワークの構成

2011 年 3 月 11 日の時点での本学におけるキャンパス内ネットワークは，図 1 に示すように，小白川キャンパスを中心としたスターネットワークによって，4 つのキャンパスを接続している．キャンパス間の通信は，1Gbps の 1 対 1 接続の専用線とイーサーネット網による 100Mbps のサービス回線の 2 つの回線に接続されている．平常時には，キャンパス間のデータ通信は前者の専用回線を利用し，後者は VoIP によるキャンパス間の内線電話などに利用されている．どちらか一方の回線が遮断されたときは，自動的にもう一方の回線に切り替わるように冗長化されている．通常のインターネットへのアクセスは，主回線である専用線を使用して，東北学術研究インターネットコミュニティ(TOPIC)に接続している．主回線に障害が発生したときを想定して，バックアップ用の回線として，米沢キャンパス内に商用 ISP，地域 IP 網経由の SINET の回線が引き込まれている．また，研究用の回線として，JGN2plus を経由して WIDE プロジェクトに接続している[5][6]．それぞれの回線の特徴を下記に示す．

[専用線による TOPIC への接続(回線 A)]
接続：小白川キャンパスから専用線にて TOPIC に接続
回線速度： 最大 約 100Mbps
備考：2011 年 3 月 30 日より SINET4-山形 DC に 10Gbps の専用線接続に変更．

[商用 ISP による接続（回線 B）]
接続：米沢キャンパスから商用 ISP に接続
回線速度： ベストエフォート 20Mbps
備考：DNS のバックアップ用および研究用回線

[JGN 経由による WIDE プロジェクト接続（回線 C）]
接続：小白川キャンパスから JGN2plus への接続
回線速度： 最大 約 1.0Gbps
備考：研究用回線，JGN2plus プロジェクトの終了および山形 AP の廃止に伴い 2011 年 3 月 9 日に停止

[地域 IP 網経由による SINET4 接続（回線 D）]
接続：米沢キャンパスから地域 IP 網に接続
回線速度： ベストエフォート 100Mbps
備考：主に研究利用のための回線

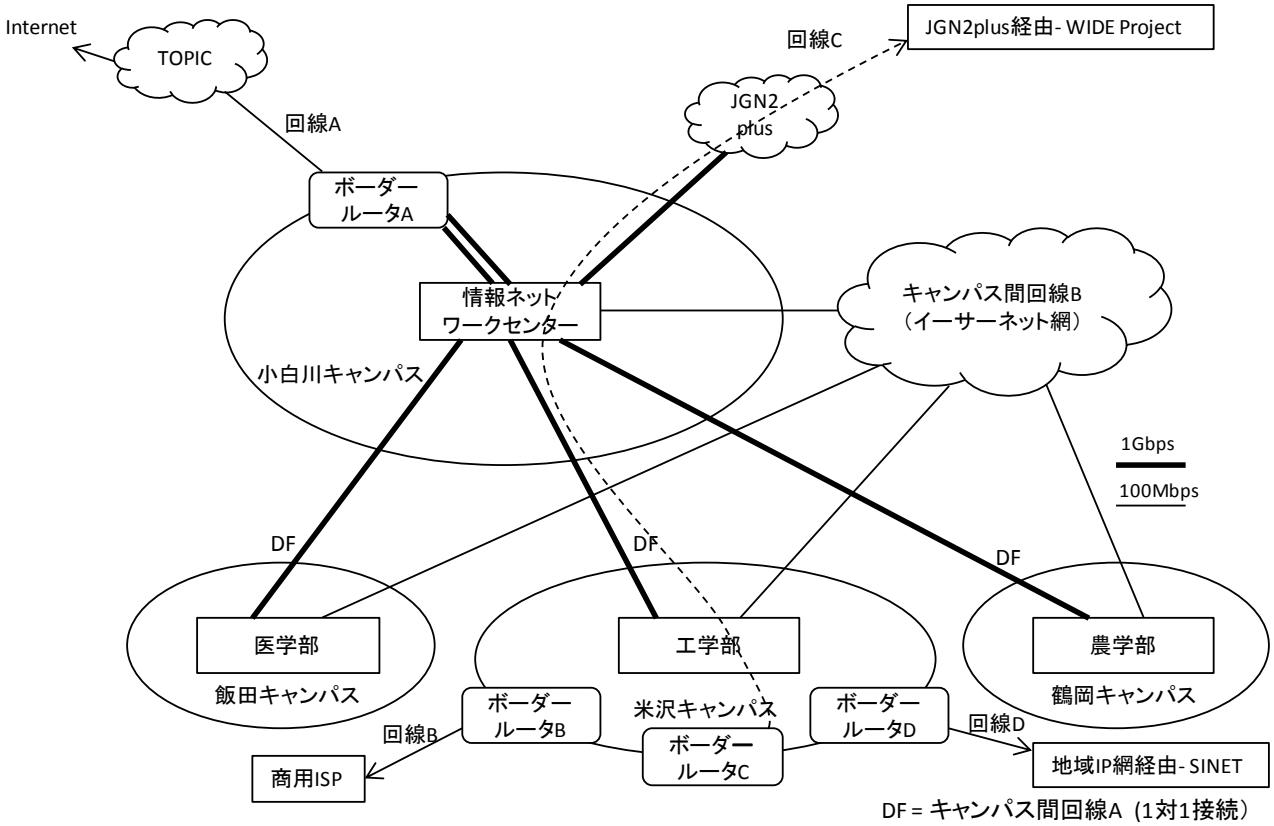


図 1 外部回線およびキャンパス間回線の構成

2.2. DNS サーバの分散配置

DNS サーバが停止または回線障害で通信不能になった場合，外部機関の利用者から本学のサーバの名前解決ができなくなり，本学の外部利用者のサービスが全て停止することになる．そこで，本学では，表 2 に示すように，DNS コンテンツサーバを 3 つのキャンパスに分散配置し，トップドメインの名前空間および PI アドレスの逆引きレコードの要求に応答できるようになっている．すなわち，主回線である回線 A に障害が発生しても，バックアップ回線である回線 B によって DNS コンテンツサーバに通信ができるため，外部利用者への DNS サービスを提供できるようになっている．また，複数キャンパスに配置したことによって，キャンパス間接続用のコアスイッチなどに障害が発生した場合でも DNS サービスを継続できるようになっている．

表 2 DNS サーバの配置構成

サーバ名	設置キャンパス	接続回線
dns0	小白川	回線 A
dns1	飯田	回線 A
dns2	米沢	回線 A
dns4	米沢	回線 B

2.3. バックアップ回線によるリモート接続

ブロードバンドネットワークの普及に伴い，これを経由した学外から学内 LAN への接続サービスの利用を求める要望が出てきた．この要望に対応するために，2005 年から本学の工学部を対象に，IPSec VPN によるリモート接続サービスが試験的に展開された．導入当初より，主回線の障害時に，リモートからの障害対応ができなくなる問題があったため，VPN 装置は，バックアップ回線（回線 B）を使用して，学外からのリモート接続サービスを提供することにした．すなわち，主回線や上位 ISP である TOPIC に障害が発生した場合でも，学内 LAN に接続し，リモートから障害対応およびインシデントなどへの初期対応が可能になっている．

2.4. 認証情報の分散配置

認証サービスは，計算機の利用やリモート接続，e-ラーニングなどのコンテンツ利用など様々なサービスを展開するために必要不可欠なもとのなっている．同一拠点に複数の認証サーバを配置して同期したとしても落雷や火災などによって，複数台のサーバが同時に故障し認証サービスの継続性が失われることが予想される．本学の学術研究用アカウントの認証システムは，Active Directory を採用し，ドメインコントローラーを複数キャンパスに分散配置することによって，認証サービスの継続性を保っている．

2.5. インバウンド通信の冗長化

複数回線を用いた冗長化方式としては，一般的な BGP によるマルチホーム接続が行われているが，本学では，運用面やコスト面の問題から導入されていない．そこで，1 つのホスト名のサーバに対して，A レコードや MX レコードに複数回線の IP アドレスを登録する DNS ラウンドロビンによる冗長化方式を採用し，図 2 に示すように構築した．具体的には，ファイアウォールに，回線 A，B，D の 3 つの外部回線を接続する．ファイアウォールの内部ネットワークは，プライベート IP が採用され，物理サーバが接続されている．外部機関からのインバウンド通信は，ファイアウォールの Network Address Translation (NAT)機能によって接続される．また，ファイアウォールのデフォルトゲートウェイのメトリックは，小さい方から回線 A，回線 B，回線 D の順番になるように設定された．アウトバウントの通信は，経路テーブルの回線コストの小さい方から選択されるため，回線 A のみによる通信となる．一方，インバウンドの通信は，ファイアウォールのセッション管理機能により，経路テーブルの回線コストに関わらずリクエストを受信した回線による通信となる．

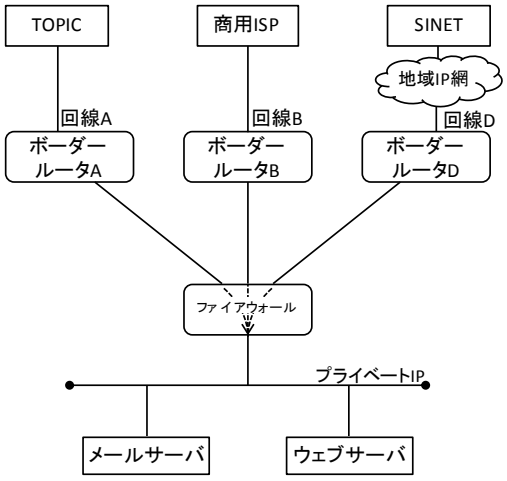


図 2　インバウンド通信の冗長化構成

実施したサービスとしては，工学部の教職員向けのメールサービスとバーチャルウェブホスティングサービスが， DNS ラウンドロビンによって冗長化されている．この手法の問題点としては，リンクの状態を監視して DNS サーバの登録情報を自動的に変更できないため，障害の発生している回線を選択した場合に，通信ができなくなる．この問題を解決する手段として，地理的負荷分散機能や WAN リンクロードバランシング機能があるが，

専用のネットワーク装置を必要とし，ハードウェア的にもライセンス的にも高価な装置であるため導入を断念した.

2.6. 重みつき DNS ラウンドロビン

DNS ラウンドロビンを用いることによって，冗長化および回線負荷の軽減は可能である．しかし，回線の容量に関わらず均等に回線が選択されるため，大容量の通信を行った場合，回線容量の低い回線は，回線帯域が飽和するなどの問題がある．この問題を解決する 1 つの手段として，重みつき DNS ラウンドロビンを採用した．具体的には，回線 A と回線 D を使用して，本学の Anonymous FTP サーバを利用して，重みつき負荷分散について試験的に運用した．一般に DNS サーバに利用されているアプリケーションとして，BIND，djbdns，Microsoft DNS Server などがあるが，重みつきの DNS レコードを取りあつかうことができない．また，地理的負荷分散装置に搭載されている Global Server Load Balancing (GSLB)や Global Traffic Manager (GTM)などの機能を利用することによって重みつき DNS ラウンドロビンは可能であるが, これらの機能を有するシステムは, 高価なライセンスや通信機器が必要であるため，予算的な理由により断念した．実験的であるため，図 3 に示すように，2 台の DNS サーバを立ち上げ，それぞれのサーバの A レコードに，回線 A と回線 D の A レコードを登録した．具体的には，DNS サーバ 1(DNS1)には，回線 A の IP アドレスを，DNS サーバ 2(DNS2)には，回線 D の IP アドレスを登録した．次に，負荷分散装置の DNS サービスに関する負荷分散先のリアルサーバの比が DNS1:DNS2 = 1:10 になるように設定した. このように設定することによって，回線帯域の異なるインバウンド通信の回線の帯域使用率の平滑化が可能になった.

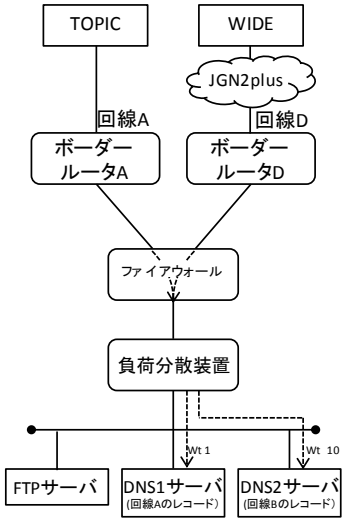


図 3　重みつき DNS ラウンドロビンの構成

3. 震災時および震災後の情報基盤

震災前の情報基盤の冗長化への試みは，前節で述べたとおりであるが，大規模災害を想定した冗長構成ではないため，様々な対応が必要となったので，本節では震災直後の状況やその後の対応について述べる.

3.1. 震災発生直後の状況

東日本大震災の発生直後に，東北地方では，停電が発生し，本学の主回線を収容している小白川キャンパスが停電となった．これに伴い，本学の外部接続用のボーダールータや DNS サーバ, コアスイッチなど停止により，主回線による外部接続が不可能になった．米沢キャンパスでは幸い停電が発生しなかったので，バックアップ回線は正常に利用でき，DNS サービス，リモート接続，インバウンド冗長化によって構成されていたメールサービスは，正常に動作していた．インバウンド冗長化によって構成されたウェブサービスについて，ラウンドロビンのため，エラーになることもあったが，ウェブの閲覧は可能であった. 一方, メールの送信サービスについては, 主回線のみによる送信を想定していたため，小白川キャンパスが復電した 3 月 14 日の朝までは, 全く送信できない状況であった．工学部のネットワークトポロジーの変更によりバックアップ回線によるメールの送信も可能であったが，主回線が回復したときの影響や想定外の障害の発生による全学のネットワーク機能の停止のリスクを考慮して，メールの送信機能の緊急復旧作業は実施しなかった.

3.2. 計画停電への対応

震災後, 東北電力管内でも 3 月 16 日より計画停電が予定された．実際には，計画停電は行われなかったが，初日の計画停電の対象エリアに，米沢キャンパスが含まれていたことや震災後の経過日数が少なく緊急時の情報発信サービスの必要性が高いことから，緊急対応として，外部サービスへの移行作業を実施した．具体的には，3 月 15 日の夕方より, アカマイサービスに工学部の緊急用ホームページのみを移行した．移行作業は，3 月 16 日の午前 1 時に完了した． 4 月 7 日に発生した最大震度 6 強の余震による停電では，山形市が停電になったため，主回線との通信が切断され，本学と学外との通信は不能になったが，工学部の緊急用ホームページはアカマイサイトに移行していたので，問題なく閲覧できた.

3.3. アウトバウンド通信の冗長化

本学の主回線に障害が発生した場合に，工学部のメールの受信は可能であるが, 送信ができない問題があった. この問題を解決するためには，アウトバウンド回線の冗長化が必要となる．アウトバンド通信を冗長化する方法としては, 複数キャンパスを活用して BGP によるマルチホーム化を行うことが，IP 認証によるサービスへの影響がないことや全学的なインバウンド通信を含めて冗長化できることなどから有効であろう. しかし, この手法は, 冗長化のための商用回線の調達が必要であるため，予算面や運用面を考慮すると早急に実施できるものではない. 一方，ICMP を用いて回線のリンク状態を監視し，障害発生時には，NAT 機能を用いて切り替える WAN リンクロードランシング方式がある．工学部には，WAN リンクモニタリング機能を有している UTM 装置（FortiGate; フォーティネットジャパン株式会社）が設置されている. この方式を採用する場合，新たな設備投資が発生しないことや構成変更によるネットワークの停止を伴わずに実施できること，比較的短い時間で実施できることから，WAN リンクロードランシング方式による冗長化を実施した.

具体的な構成は，図 4 に示すように，通常時のアウトバウンド通信は，小白川キャンパスに設置されたボーダールータ A を経由して，主回線からインターネットにアクセスする．もし，小白川キャンパスが停電などによって機能停止した場合，ICMP による死活監視機能が障害を検知し，工学部のアウトバウンド通信は，自動的にバックアップ回線に切り替わる．これによって，工学部の通信は，メールの送信のみならず，ウェブの閲覧なども障害発生時に継続的に利用できるようになっている.

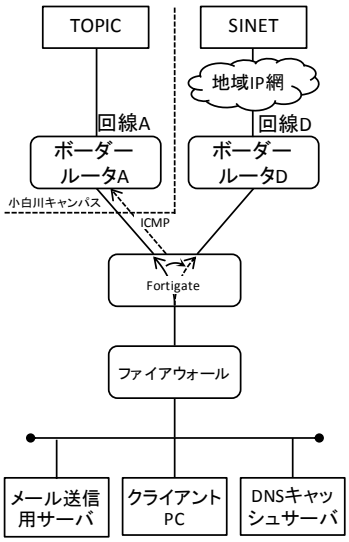


図 4 アウトバウンド通信の冗長化構成

3.4. 安否確認システムの構築

震災から数日経過し，電話回線などの通信網の規制が解除されるにつれて，学生などの安否確認の要請が高まり，インターネット経由による安否確認システムの構築が必要となった．重要なポイントは，短期間で安否確認システムを構築することであった．幸い震災による被害は少なく，認証システムやデータベースサービス，ウェブサービス，メールシステム，学認用 Shibboleth IdP サービスへの被害はなかったため，十分なリソースが利用できることが確認できた．認証サービスは，既に運用を開始している学認用 Shibboleth IdP サーバを利用することによって，開発期間の短縮を図った．さらにウェブサービスは，学認に提供しているサービスプロバイダー(SP)である科学技術の学術情報共有のための双方向コミュニケーションサービスのサイトを機能拡張することによって，新規のデジタル証明書の取得やシボレス SP の新規インストール作業などの時間を短縮した.

開発されたシステムは，図 5 に示すように，利用者はウェブサーバに接続し，認証要求のため，本学の IdP サーバにリダイレクトされる．認証が完了するとウェブサーバにリダイレクトされ，安否情報を送信する．送信された安否情報は，安否確認者にメールが送信されると同時に，データベース内に記録される．安否確認者は，メールの受信または Access などのデータベースソフトウェアを使用して, ODBC 経由でデータベースを参照して，安否情報を確認できる．学認の IdP システムおよび既存の SP を利用したことによって，安否確認システムの開発は，6 時間程度で完了した.

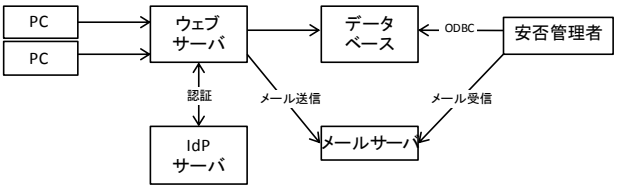


図 5 安否確認システムの概略図

4. まとめ

震災前に実施した様々な障害対応機能を基盤に，震災を踏まえて，災害時に備えた分散キャンパスによる情報基盤の整備を行った．震災前は，インバウンドの通信を中心に冗長化を試みており，それなりの効果があった. しかし，アウトバンドの通信については，全く対応していない冗長化システムであった．震災によって発生した 2 日以上の停電を考慮すると，大規模災害に備えたアウトバンド通信の冗長化システムの構築が必要不可欠であると判断した. 比較的安価な商用回線や地域 IP 網を利用

して，WAN リンクロードランシング方式によるアウトバウンド回線の冗長化システムを米沢キャンパス内に導入した．また，震災による情報基盤への障害や故障が小さかったことや学内でフラットに利用できるシボレス認証を既に採用していたことが幸いして，短時間で安否確認システムの構築することができた．長期的な運用を見つめると BGP によるマルチホーム接続が適切な選択であろうが，短期間で，震災に備える手段としては，安価な ISP 回線と WAN リンクロードランシング方式による冗長化構成も１つの解決策になるであろう．

今後の課題としては，現在，インバウンドおよびアウトバウンドの冗長化構成は，工学部のみであるため，全学規模の冗長化構成を進めることが必要であろう．

謝辞

IPv6 ネットワークを提供していただきました JGN2plus および WIDE プロジェクトの皆様に深く感謝申し上げます．計画停電の対応のために，「アカマイ」東日本大地震緊急配信無償提供プログラムを提供していただきましたアカマイ・テクノロジーズ合同会社様に深く感謝申しあげます．震災時の緊急対応を進めるにあたり，ご指導・ご協力を賜りました情報担当副学長，情報系センター，工学部執行部の皆様に深く感謝申しあげます．

参考文献

[1] 清水さや子，横田賢史，戸田勝善，吉田次郎：東京海洋大学における IC カード学生証の運用・評価および今後の展開，学術情報処理研究誌，No.13，pp. 64-73 (2009).

[2] 越後 博之，湯瀬 裕昭，千川 剛史，沢野 伸浩，高畑 一夫，柴田 義孝：大規模分散環境におけるロバストネスを考慮した広域災害情報共有システム，情報処理学会論文誌，Vol. 48，No. 7，pp. 2340-2350 (2007).

[3] 長谷川孝博，井上春樹，八巻直一：低コスト運用でユーザフレンドリな安否情報システムの開発，学術情報処理研究誌，No.13，pp. 91-98 (2009).

[4] 学術認証フェデレーション，https://www.gakunin.jp/

[5] 山本成一，金海好彦，中村一彦，三宅喬，長谷部克幸，太田善之，田中仁，美甘幸路，櫨山寛章，小林和真，下條真司 : JGN2plus における運用 安定性とチャレンジ,テストベッドネットワークに対する運用面からの試み, 電子情報通信学会技術研究報告, Vol. 108, No. 223，IA2008，pp.33-38 (2008).

[6]JGN2plus，https://www.jgn.nict.go.jp/jgn2plus_archive/

トレーサビリティネットワークの構築
Construction of traceability network

沖野浩二 †, 山田純一 †, 布村紀男 †, 柴田啓司 ‡

Koji Okino†,Junichi Yamada†,Norio Nunomura†,Keiji Shibata‡

{okino,j_yamada,nori2}@itc.u-toyama.ac.jp, shibata@eng.u-toyama.ac.jp

富山大学 総合情報基盤センター †
富山大学 大学院 理工学研究部 ‡
Information Technology Center,University of Toyama.†
Graduate School of Science and Engineering for Research, University of Toyama‡

概要

不特定多数が利用するネットワークでは、コンピュータ・ウィルスに感染したノードや不正なユーザによる利用が発生する場合がある。このような場合に対応するために認証を行い通信記録を取得する必要があるが、このようなトレーサビリティネットワークを構築するためには、メーカー独自の機構を利用したり専用装置を導入する必要があった。本論文では、既存ネットワークの構成を変更せずに導入可能な、トレーサビリティネットワークの構築手法を提案し、トレーサビリティネットワークを構築するに当たり、利用形態に基づいた階層とそれらの階層における要件の定義と提案手法の実装を行った。結果として、既存の無線 LAN AP やインテリジェントスイッチを用いて、ユーザ情報 (IP アドレス-MAC アドレス-利用者) の収集を行い、それぞれの階層において想定される不正利用を抑止することが可能になった。

キーワード

ネットワークセキュリティ, 情報コンセント, ユーザ認証

1 はじめに

昨今では、軽量なノート PC やスマートフォンの普及によって、各自の情報端末を持ち歩き、利用する機会が増えている。これに伴い、大学においても、旧来の固定 IP アドレスによる運用だけでなく、パブリックスペースでの情報コンセントや無線 LAN AP の整備が求められている。このような不特定多数が利用する環境では、IP アドレスではなく利用者単位で認証を行う仕組みが必要であり、不正利用が起きた場合には追跡調査できるような仕組みが不可欠である。

ネットワークにおける認証機構は、鈴木 [1] らや大谷 [2] らによるゲート認証方式と、石橋 [3] らや大江 [4] らによるエッジ側のコントロール機能を利用した方式に大別される。ゲート認証方式では、ゲートへの誘導やゲートの処理能力が課題になり、エッジコントロール方式では専用のネットワーク構成や無線 LAN に特化した方法など、エッジの種類に応じてそれぞれ対処することが必要になる。

実際に複数の異なるベンダーの機器が導入されている組織において、ゲート認証方式を導入する例が多いのは、エッジの種類ごとに対応することが難しいためだと考えられる。そこで本論文では、多くのメーカがサポートしている認証機構、無線 LAN での PEAP 認証機構および有線 LAN におけるエッジの MAC アドレス認証及び Web 認証を利用することにより、遠隔キャンパスも含めた組織内全域において適応可能なトレーサビリティネットワークを、エッジコントロール方式で実現する手法を提案する。

2　トレーサビリティネットワーク

2.1　要件

本論文におけるトレーサビリティネットワークとは、

1. いつ
2. どこで
3. だれが
4. 何をしたか

を、管理者が追跡することが可能なネットワークと定義する。

1. いつ　と　4. 何をしたかは、FW や組織内サーバ等に記録された通信記録の内容とする。2. どこでに関しては、一般にネットワークにおいて、FW 等のログに記録される IP アドレスしかわからない。IP アドレスから実際の利用者を特定するのは、組織によって採用されている IP アドレス等の管理方法に依存する。

本論文におけるトレーサビリティの確保とは

特定 正規の利用者がネットワークを利用した場合に、利用者（責任者）が特定できること

不正防止 他人へのなりすましや、身元を隠した状態でネットワークにパケットを送出できないこと

と定義する。

2.2　必要とされる要件と現実の問題

トレーサビリティを実現するには、FW 等に記録される IP アドレスとその IP アドレスの利用者とのひも付けを行うことが必要である。

組織内における IP アドレスの管理方法は、利用者の申請に基づいて固定的に割り当てる方法と自動的にネットワーク設定を取得する DHCP による運用の 2 種類に分けられる。申請制が適切に運用されている場合には、IP アドレスから利用者の特定は容易である。DHCP による運用では、IP アドレスから対応する MAC アドレスを調べ、MAC アドレスから利用者を特定する必要がある。

実際に、トレーサビリティネットワークを適切に運用するためには、管理者が

1. IP アドレス-利用者
2. MAC アドレス-利用者
3. MAC アドレス-IP アドレス

に関する正しい情報を収集し、これらの間のひも付けを保証する必要がある。

しかし、組織の規模が大きくなるにつれて、サブネットごとに別の責任者に管理業務が委任されるなど、階層的に管理されている場合も多く、組織全体における IP アドレス-利用者や MAC アドレス-利用者等に関する情報のひも付けを適切に行うことは難しいのが現状である。

本学においても、学部の研究室では固定 IP アドレスの申請制を採用し、教室や会議室などでは DHCP による運用を行っている。利用者が申請書を提出せずに勝手に利用する事例や PC を更新しても申請内容を訂正しないなどの事例が多発していた。そのため、IP アドレス-利用者等の情報に関して、適切にひも付けを行うことが難しく、障害対応の際の問題となっていた。

2.3　考えられる脅威

トレーサビリティを確実なものにするためには、

1. ユーザが正しく設定し、正しく情報提供していた場合
2. ユーザが誤った設定あるいは誤った情報提供をしていた場合
3. ユーザが意図的にトレースを回避し、不正利用を行った場合

の 3 つのパターンに対応する必要がある。1 パターンの場合は、申請書に記載された IP アドレスや MAC アドレスにより利用者は特定できる。しかし、実際には、悪意のない利用者においても 2 のパターンが発生する確率がかなりの程度ある。

なぜならば、現在仕様されている多くの PC には、有線用と無線用の 2 種類の MAC アドレスが割り当ててあり、この 2 つを区別して正しく申請できる利用者は多くないという現実がある。加えて、Windows では Tunnel adapter や IEEE1394 などが加わり、ユーザが実際に利用している IP アドレスや MAC アドレスを正しく認識することはより難しくなっている。そのため、申請制によるひも付け情報を利用したトレーサビリティの確保は、利用者の増大とともに難しくなることが考えられる。

3 のパターンのユーザが意図的にトレースを回避する場合に対応するためには、IP アドレスおよび MAC アドレス偽装について考慮する必要がある。

2.4　LAN の分類

組織内におけるネットワークは、利用形態に基づいて、次の 3 種類に分類することができる。

a. 管理された LAN 管理組織が確実に管理し、接続されている PC が固定化されている LAN。本学においては、情報センター端末室や事務室の PC を収容する LAN に相当する。

b. 委任された LAN 下位組織に管理が委任されている LAN。利用形態は多種多様であり、HUB を経由し、PC だけでなく、サーバやプリンタなどが接続される。上位の管理組織が実際の利用者を知ることはできない。本学においては研究室内 LAN に相当する。

c. 認証 LAN 構成員のうち誰が利用するかわからない LAN。認証によりユーザを特定する必要がある。アクセス方式により無線 LAN と有線 LAN に分けられる。本学においては、会議室や講義室などで提供される認証 LAN に相当する。

2.5 トレースレベル

上記の 3 つの LAN はそれぞれ求められるトレースレベルが異なっている。

管理された LAN では、組織的に管理された PC と IP アドレスが利用されるということが前提であり、MAC アドレス偽造や IP アドレス偽造は行われないものとする。実際の利用者を特定するには、PC 利用申請者の特定を行えばよい。

委任された LAN では、IP アドレスや MAC アドレスの積極的な偽造は行われないが、IP アドレスの設定間違いや MAC アドレス申請の際の間違い等は発生するものとする。利用者の特定を行うためには、接続されている情報コンセントの位置と管理者が誰であるかが判明すればよい。上位管理者は、下位組織管理者からの申請に基づき、IP アドレスと MAC アドレスの突き合わせを行い、適切に利用されているかを監視する必要がある。

認証 LAN では利用者の特定が必要である。また、認証の回避や IP アドレスおよび MAC アドレスの偽造が行われる可能性があることに注意する必要がある。LAN ごとに必要な確認範囲を表 1 に示す。

表- 1: LAN ごとの確認項目

	IP-MAC 確認	ユーザ認証
管理された LAN	任意	必要
委任された LAN	必要	委任側
認証 LAN	必要	必要

管理された LAN は、ログイン時認証など別の手段でトレースするものとし、委任された LAN 及び認証 LAN を対象として検討を行った。

3 求められる性能

組織全域で運用するトレーサビリティネットワークにおいて求められる要件としては、下記の 5 つがあげられる。

性能と拡張性 大規模なネットワークにも対応できる性能と拡張性を有すること

既存システムとの親和性 新規に導入する際、既存のネットワークを大きく変更する必要がないこと

メーカ非依存性 特定の製品でしか実現できないものでないこと

運用コスト システム運用のコストが大きく増大しないこと

追跡性の確保 トレーサビリティを確保できること。具体的には、IP アドレスと MAC アドレスと利用者の関係に関する情報が取得できること。

これらの要件を鑑み、本学のトレーサビリティネットワークを構築する際の、基本的要件を以下のように定義した。

1. 富山大学全域に対する広域サービス
   遠隔キャンパスにも対応でき、マシン台数 10,000 台に対応できること。OS は、Windows, Mac, Linux, Android, iOS に対応すること。
2. 性能低下の防止
   10,000 台のマシンが同時に利用しても著しい性能低下を起こさないこと。
3. メーカ依存の禁止
   本学では現在、CISCO 社製製品を主に利用しているが、今後の更新等に際して束縛とならないよう CISCO 社製以外の製品にも対応できること。
4. 導入コスト、運用コストの低減
   既存の機器を更新することなくそのまま利用できること。また、現在の運用手段が大きく変化しないこと。
5. 事前情報登録作業の削減
   MAC アドレスや IP アドレスの登録作業が必要でないこと。
6. 認証データの統合 (学内認証基盤との同一 ID)
   学内認証基盤の ID,Password を利用して認証を行えること。
7. IP-MAC アドレステーブルの監視
   IP-MAC アドレス対応表を監視でき、長期間利用していない IP アドレス等の把握ができること。

4　実現方式

4.1　製品比較

前記の基本要件を満たす製品を調査したところ、認証システムとして CISCO 社製 Cisco Secure Access Control System[5] を検討したが、3 及び 6 の仕様を満たすことができなかった。また、ネットワーク管理システムとしてダイキン工業社製 PNDDA[6] を検討したが、これは、仕様 6 を満たすことができなかった。ゲート認証方式も検討を行ったが、仕様 1 及び 4 を満たすことが難しいと判断した。

4.2　システム構成

そこで、3 節で定義したトレーサビリティネットワークに求められる性能の基本的要件を満たすため、エッジコントロール方式のトレーサビリティシステムを 3 つのシステムを組み合わせて構築した。構築したトレーサビリティシステムの構成を図 1 に示す。

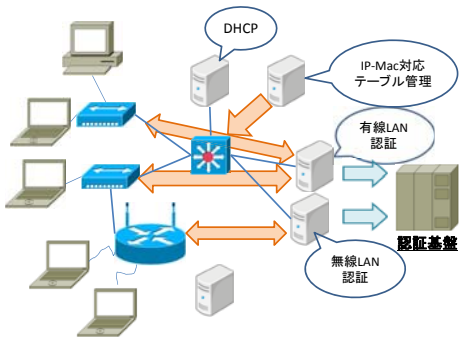


図- 1: システム構成図

システムは、MAC-IP 対応テーブル管理システム、無線 LAN 認証システム、有線 LAN 認証システムからなる。

4.3　MAC-IP 対応テーブル管理システム

MAC-IP 対応テーブル管理システムは、基幹スイッチ (L3) に接続して IP アドレスと MAC アドレスの対を取得して管理する。これは、次の項目で構成される。

- 基幹スイッチ IP リスト
- SNMP ポーリングプログラム
- MAC-IP アドレスリスト
- 差分抽出プログラム

一定時間ごとに、基幹スイッチに対して SNMP ポーリングを行い、MAC ー IP アドレスリストを作成する。これを一つ前のタイミングのリストと比較して、変更があった場合に、次のデータをメールで管理者に送付する。

- PC の新規接続 (New)
- 同一 IP アドレスに対する MAC アドレスの変化 (IP)
- 同一 MAC アドレスを複数の IP アドレスで利用 (Mac)

メールの具体例を次に示す。

```
New ---------------------------------
New  160.26.12.110  F8:0F:41:19:60:CC
Duplicate IP Address -----------------
IP   160.26.11.220  00:00:11:8F:77:88
        <- 00:12:23:45:AE:20
Duplicate MacAddress -----------------
Mac  00:00:CE:EE:D2:10 160.26.66.13
        <- 160.26.66.45 YAMAHA CORPORATION
Mac  00:00:CE:EE:D2:10 160.26.66.45
        <- 160.26.66.13 YAMAHA CORPORATION
```

加えて、週に一度、IP-MAC アドレスの対情報を管理者に送付する。

本学では、基幹スイッチ (Catalyst6500) の標準 ARP Table 保持時間が 4 時間であり、4 時間のうちに一度でも接続した場合には基幹スイッチ上に IP-MAC アドレスのテーブルが残ることから、ポーリングの頻度は、1 時間に 1 回としている。

4.4　無線 LAN 認証システム

無線 LAN については、EAP の一種である PEAP 認証を利用し、Radius サーバ経由で学内認証基盤のデータを用いて、ユーザ認証を行うことした。[7]

CISCO 社製 AP における設定例は次の通りである。

```
aaa new-model
!
aaa group server radius rad_eap
 server 160.26.ZZ.YY \\
   auth-port 1812 acct-port 1813
aaa authentication login \\
    eap_methods group rad_eap
!
dot11 ssid toyama
   authentication open eap eap_methods
   authentication network-eap eap_methods
   authentication key-management wpa
   guest-mode
interface Dot11Radio0
 encryption mode ciphers aes-ccm tkip
 ssid ITC
!
radius-server attribute 32 \\
```

```
    include-in-access-req format %h
radius-server host 160.26.ZZ.YY \\
    auth-port 1812 acct-port 1813 key ZZZZZZ
radius-server vsa send accounting
```

PEAP 認証におけるシーケンスは図 2 に示すとおりである。

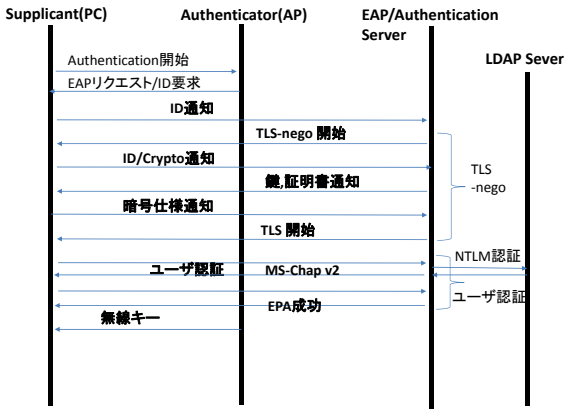


図- 2: PEAP 認証シーケンス図

IP アドレスから利用者を特定するのは、Radius サーバの記録

```
Sun Jun 26 12:28:58 2011 : Auth: Login OK:
[xxxx.ttt/<no User-Password attribute>]
(from client library2F_read2 port 11691
cli 0012.9d33.5b55)
```

DHCP サーバの記録

```
Jun 26 12:28:58 dhcpsvg dhcpd: DHCPREQUEST
for 160.26.YYY.204 from 00:12:9d:33:5b:55(ZZZ)
via 160.26.YYY.10
```

により可能となる。MAC アドレスの偽造は、認証時に記録されるため不可能であり、IP アドレスを手動で設定した場合には、認証時の MAC アドレスが Radius サーバに記録されており、Mac アドレスから MAC-IP 対応テーブル管理システムでその時に利用していた IP アドレスと MAC アドレスの対を確認することで可能である。PEAP 認証は、WPA/WPA2 において標準に組み込まれており、業務向けの Wi-Fi Alliance の承認機器で利用できる。

4.5 有線 LAN 認証における問題点

無線 LAN AP においては、認証手法が標準化されているため、メーカに依存しないシステムの構築が可能であった。しかし、有線 LAN 認証においては、下記に述べるのようないくつかの問題点がある。

1. メーカごとに認証部分の実装方法が異なる。
2. ネットワーク配下に HUB が接続される可能性がある。特に 802.1X 認証においてはポートあたり一台の機器が接続されると想定されており、HUB 経由で複数台が接続した場合の動作が不定である。
3. ファームウェアの更新によって、システムの動作が変更される場合がある。

4.6 有線 LAN 認証システム

有線 LAN 認証については、エッジスイッチで MAC アドレス認証と Web 認証を組み合わせて利用することとした。現在 MAC アドレス認証や Web 認証は多くのメーカで採用されている。MAC 認証はポートあたり複数の MAC アドレスの認証に対応し、Web 認証は IP アドレスごとに認証が行われるため、エッジスイッチの 1 つのポートに複数のユーザが同時に接続しても認証を行うことが可能である。

MAC アドレス認証や Web 認証を行うには、Radius サーバが必要となる。前述の問題点 1 と 3 を解決するために、有線 LAN 認証用の専用 Radius サーバを開発した。認証をすべて専用 Radius サーバで行い、Radius 側にメーカごとに対応した設定および attribute 属性を持たせることとした。これにより、メーカおよびファームウェアの違いによる動作の差異を吸収することができた。専用 Radius サーバは、機種や attribute が異なる認証スイッチからの認証を振り分ける機能、Mac アドレス認証機能、ユーザ認証からなる。MAC アドレス認証部分には三井情報社製の MKI SmartAuth Server を利用し、振り分け機能部分とユーザ認証の認証基盤への連携部分の開発を新たに行った。専用 Radius サーバの構成を図 3 に示す。

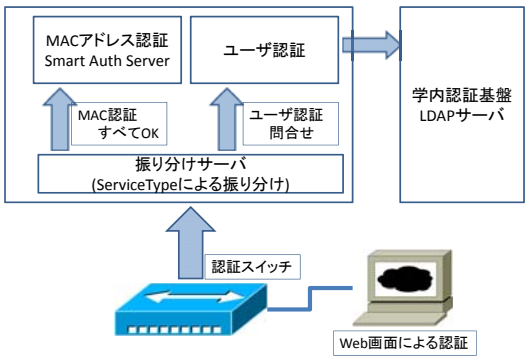


図- 3: 有線 LAN 認証用 Radius サーバ構成図

CISCO 社製 HUB における設定例は次の通りである。

```
aaa accounting auth-proxy default \\
   start-stop group radius
aaa accounting dot1x default \\
   start-stop group radius
aaa accounting network default \\
   start-stop group radius
!
ip device tracking
ip admission name rule1 proxy \\
   http inactivity-time 60
!
interface GigabitEthernet0/47
 switchport access vlan TTT
 switchport mode access
 ip access-group policy1 in
 authentication host-mode multi-auth
 authentication order mab webauth
 authentication port-control auto
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 1
 spanning-tree portfast
 ip admission rule1
!
radius-server attribute 8 \\
   include-in-access-req
radius-server host 160.26.X.Y \\
   auth-port 1812 acct-port 1813 key ZZZ
radius-server vsa send authentication
```

有線 LAN 認証におけるシーケンスを図 4 に示す。

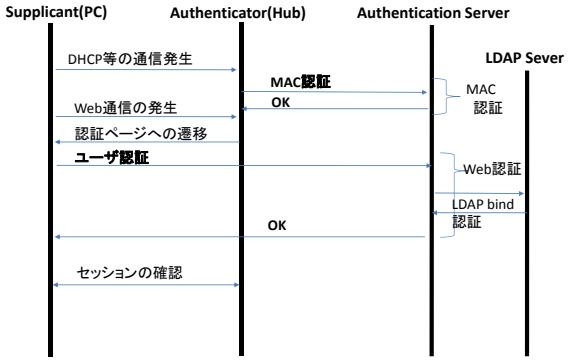


図- 4: 有線 LAN 認証シーケンス図

Radius サーバにおけるシーケンスを図 5 に示す。

利用記録は、Radius サーバ内にエッジの IP ごとのフォルダーに分けて格納される。利用記録の具体例を示す。MAC アドレス認証記録は、

```
Thu Jun 23 17:08:41 2011
    Acct-Session-Id = "0000033A"
    User-Name = "f0aabb086eee"
    Acct-Authentic = RADIUS
    Acct-Status-Type = Start
    NAS-Port-Type = Ethernet
    NAS-Port = 50047
    NAS-Port-Id = "GigabitEthernet0/47"
    Called-Station-Id = "00-12-CC-45-DD-FF"
    Calling-Station-Id = "F0-AA-BB-08-6E-EE"
    Service-Type = Framed-User
    NAS-IP-Address = 160.26.XX.101
    Acct-Delay-Time = 0
    Acct-Unique-Session-Id = "1c6bfff9ac26d8"
    Timestamp = 1308816521
```

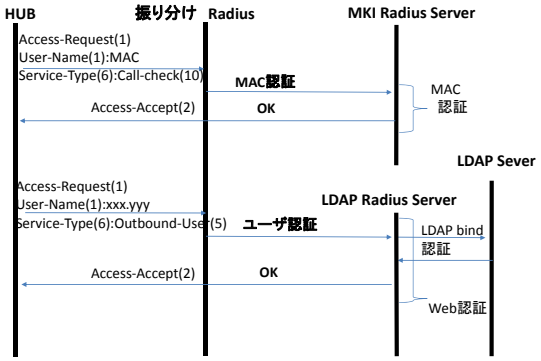


図- 5: サーバにおける Radius シーケンス図

```
    Request-Authenticator = Verified
```

と記録され、MAS-Port-ID から利用しているポートが、Calling-Station-ID から MAC アドレスを取得することができる。Web 認証の記録は、

```
Thu Jun 23 17:08:58 2011
    Acct-Session-Id = "0000033C"
    Calling-Station-Id = "160.26.24.178"
    NAS-Port = 50047
    NAS-Port-Id = "Gig"
    User-Name = "xxx.yyy"
    Acct-Authentic = RADIUS
    Acct-Status-Type = Start
    NAS-Port-Type = Ethernet
    NAS-Port = 50047
    NAS-Port-Id = "GigabitEthernet0/47"
    Service-Type = Outbound-User
    NAS-IP-Address = 160.26.XX.101
    Acct-Delay-Time = 0
    Acct-Unique-Session-Id = "074f11862693a4"
    Timestamp = 1308816538
    Request-Authenticator = Verified
```

と記録され、IP アドレスは、Calling-Station-Id 欄に記録され、ユーザ名は、User-Name に記録されることにより、IP アドレスからの利用者の特定が可能となる。

提案手法は、IP-MAC アドレスの対情報は MAC-IP 対応テーブル管理システムで確認しているため、ユーザを特定するためには、IP アドレス又は MAC アドレスのどちらか一方が特定されれば良い。

有線 LAN 認証システムでは、ユーザ確認の手段として学内認証基盤の統一 ID とパスワードを利用し Web 認証を行っている。本認証システムでの MAC アドレス認証の利用目的は、MAC アドレスがどの HUB のどのポートに接続されたかに関する情報を取得するためであり、認証の手段としては利用していない。そのため、Radius サーバは、すべての MAC アドレスに対して認証 OK を返答するように設計をしている。

MAC アドレスを認証のための手段として利用しない理由は、MAC アドレスは偽造が容易であるため、認証

用の個体識別番号として利用することは意味がないからである。

攻撃者が、調査のためにネットワークに接続した場合やMACアドレスを偽造した場合は、MACアドレス認証によって接続したエッジとそのポートが記録される。IPアドレスを手動で設定した場合には、Web認証によりIPアドレスが記録される。

加えて、有線LAN認証システムは、ポートごとに接続情報収集を目的とするMACアドレス認証と、ユーザ認証を目的とするMACアドレス認証かつWeb認証を管理者が選ぶことができる。具体的には、MACアドレス認証かつWeb認証の場合には、

```
authentication order mab webauth
```

と設定し、ポートに接続される機器のトレースが目的ならば

```
authentication order mab
no ip admission rule1
```

と設定すればよい。これにより一台のエッジスイッチで、委任されたLANと認証LANの機構を提供することができる。

5 システム評価

今回設計したシステムを、先述の7つの要件に基づいて評価する。

1. 富山大学全域に対する広域サービス
   PCごとの管理は、エッジによる認証で行われるため、エッジ機器のハードウェア性能による台数制限は存在するが、全体として利用数に対する制限はない。エッジとRadiusサーバとの間で通信が可能であれば、遠隔キャンパスであっても問題なく導入できる。三井情報社製Radiusの保証台数は、60,000台であり、本学での運用においては十分であると判断している。
   また、無線LAN認証はWindows, Mac, Android, iOS搭載機器については動作確認している。Linuxについては、ユーザから動作報告がある。有線LAN認証については、OSに依存しない実装となっている。

2. 性能低下の防止
   認証時には、認証サーバの負荷が問題となる可能性があるが、一度認証されると、すべての負荷はエッジの処理能力に依存する。認証機能を有しているエッジには専用ハードウェアが実装されており、性能限界に達することは少ないと考えられる。またエッジあたりの処理台数も、高々そのエッジに接続される台数である。本学の事例では、エッジあたりの収容数は、最高が90台で、平均は25台であった。認証サーバの負荷は、通信量とRadiusサーバの性能に依存する。一回の認証に必要な通信量は、無線LAN認証では、EAPメッセージで512Kbyte以下である。一方有線LAN認証では、Web認証とMAC認証の2回で8Kbyte以下である。そのため、ネットワークへの負荷はないと判断している。Radiusサーバによる認証はSmartAuth Server側が毎秒2,000台処理でき、認証基盤側は毎秒300回程度ならば問題なく認証できていることを確認している。

3. メーカ依存の禁止
   本認証システムでは、機種依存部分は有線LAN認証システムだけである。CISCO社以外のエッジに対応するためには、Radiusサーバの改良及びattribute追加にて対応することが可能である。

4. 導入コスト、運用コストの低減
   導入に際しては、既存のHUBのファームウェアをアップデートし、認証機能を追加することで対応した。導入から5年以上経過した認証に対応していないエッジに関しては更新が必要であったが、ユーザ数が少ない場合には上流のエッジで認証を行うことで対応できた。ネットワーク構成の変更の必要がなかったため、運用コストに関しては変化しなかった。認証システム側でユーザの追跡が可能となり、管理コストは低減できた。増加したコストとしては、認証用Radiusサーバの導入・保守コストがある。この費用については既存のRadiusサーバと統合により削減していく予定である。

5. 事前情報登録の削減
   MACアドレスやIPアドレスの登録作業は必要がない。頻繁に変更されるIPアドレスやMACアドレス等が発見された場合は、MAC-IP対応テーブル管理システムからの通知を受けて、管理者からユーザに問い合わせを行っている。IP-MACアドレスの対情報が正しいかの確認は別途行う必要がある。これについては毎年別途実施している実態調査により、突き合わせを行うことにより確認している。

6. 認証データの統合（学内認証基盤との同一ID）
   学内認証基盤のIDを利用し認証を行っている。このためID、パスワードを別途配布する必要がなく、導入をスムーズに行うことが可能となった。ユーザからの問い合わせも少なくなった。

7. IP-MACアドレステーブルの監視
   利用されていないIPアドレスはIP-MACアドレ

ステーブルの記録が存在しないことになる。これにより長期間利用していない IP アドレス等の把握ができる。

次に、LAN ごとのトレースレベルに対応しているかの評価であるが、委任された LAN において、情報コンセントごとに利用している IP アドレスと MAC アドレスの対情報を取得することは、エッジ側の設定を MAC アドレス認証モードで運用することにより可能である。また、認証 LAN においては無線 LAN、有線 LAN ともに利用者と IP アドレスと MAC アドレスの対情報を取得することが可能である。

最後に、脅威への対応であるが、認証 LAN においては認証情報を不正に利用されなければ、IP アドレス、MAC アドレスのどちらの偽造にも対応できる。委任された LAN において、IP-MAC アドレスの一方を実際に存在する機器と同一に設定すればトレースを回避することが可能であるが、このような場合には、正規の機器接続がされないことが必要である。もし同時に接続された場合には、MAC アドレス衝突はスイッチ側で MAC アドレスフラップとして検出され、IP アドレス衝突は正規の利用者側にエラーが発生する。このため、管理者が近くにいる委任された LAN では、このような攻撃の発生、または、その攻撃が成功する可能性は低いと判断している。

6　制限事項

現在、CISCO 社製 HUB の認証は、ポートあたり 8 台までという制限がある。そのため、多数の PC を接続している研究室において、そのままでは本システムによる認証が利用できないことが判明している。

このような 1 ポートに多数の接続を行う箇所については、今後、無線 LAN の利用の促進や情報コンセントの増設を検討している。

7　おわりに

既存ネットワークに導入可能なトレーサビリティネットワークを、MAC-IP 対応テーブル管理システム及び無線 LAN、有線 LAN 認証システムの構築により実装した。

これにより、不正利用の防止に寄与するだけでなく、ネットワークのレベルに応じた MAC-IP アドレスの対情報の保証、または、MAC-IP アドレス-利用者の対を取得することが可能となった。

現在、無線 LAN システムは全キャンパスで運用しており、有線 LAN 認証システムはキャンパスの一部にて運用を開始している。

今後は、このシステムを全学に広げるとともに、管理者が認証や利用状況のデータを Web から閲覧できるシステムの開発を検討している。

参考文献

[1] 鈴木 彦文，永井 一弥，浅川 圭史，今井 美香，不破 泰,”UTM を用いたユーザ認証ネットワーク「セキュアネット 2010」の構築”, 学術情報処理研究,No.14 p.21-30, 2010.

[2] 大谷 誠, 江藤 博文, 渡辺 健次, 只木 進一, 渡辺 義明,”シングルサインオンに対応したネットワーク利用者認証システムの開発”, 情報処理学会論文誌 Vol. 50 No. 3 1-9, 2010.

[3] 石橋 勇人, 山井 成良, 安倍 広多, 阪本 晃, 松浦 敏雄,”利用者ごとのアクセス制御を実現する情報コンセント不正利用防止方式”, 情報処理学会論文誌, Vol42 No1. p79-88, 2001.

[4] 大江　将史, 櫨山　寛章, 山本　成一, 白畑 真,”IEEE802.11 ワイヤレスネットワーク管理システムの構築と検証” , 電子情報通信学会論文誌. B, 通信 J87-B(10), p1607-1615, 2004

[5] CISCO Secure Access Control System

`http://www.cisco.com/web/JP/product/hs/security/acs/acs/index.html`

[6] ダイキン社製　PNDDA

`http://www.comtec.daikin.co.jp/IM/prd/pndda/`

[7] 沖野 浩二, 小林 大輔, 布村 紀男,”学外者向け認証無線 LAN の構築”, 富山大学総合情報基盤センター広報 ,Vol7 p.46-49, 2010.

[8] 沖野 浩二, 布村 紀男,”富山大学における認証基盤の整備による業務軽減評価”, 学術情報処理研究,No.14 p.31-38, 2010.

[9] Jonathan Hassell 著, アクセンス・テクノロジー訳, ”RADIUS ユーザ認証セキュリティプロトコル ”, オライリー・ジャパン,2003.

神戸大学教育研究用計算機システム導入における システム連携の取り組み

Integrated Intersystem Coordination for Kobe Academic Information System for Education and Research

佐々木博史*, 荻野哲男†
Hiroshi SASAKI, Tetsuo OGINO
神戸大学 情報基盤センター
Information Science and Technology Center, Kobe University
657-8501 兵庫県神戸市灘区六甲台町 1-1
1-1 Rokkodai-machi, Nada-ku, Kobe-shi, Hyogo-ken 657-8501, Japan

神戸大学では 2011 年 1 月に，学内の情報基盤を実現するシステムとして，神戸大学教育研究用計算機システム (KAISER: Kobe Academic Information System for Education and Research) を導入した．大学におけるメールや教育用端末の利用など，情報通信技術の重要性は増々重要になり，多くの要求があがっている一方，予算や人員についてはむしろ削減されているのが実情である．導入・運用コストの削減が叫ばれる中，サービスの向上をはかる上での神戸大学での取り組みについて紹介する．

キーワード：教育研究システム，電子メール，NetBoot

1 はじめに

神戸大学情報基盤センターでは，2006 年 1 月 (当時は学術情報基盤センター)，学内の計算機システムを全学的に管理・運用するため，神戸大学統合ユーザ管理システム (KUMA: Kobe University Integrated User Management System) を中核とする，教育・研究用計算機システムの導入を行った．そして，2011 年 1 月にシステム更新として，新・教育・研究用計算機システム KAISER (Kobe Academic Information System for Education and Research) を行った．本論文では KAISER の特徴と，その設計や導入について述べる．第 2 章では，KAISER の概要，第 3 章ではサブシステムとしての電子メールシステム，第 4 章では教育用端末システム，そして第 5 章で，本システムについてのまとめを述べる．

2 教育研究用計算機システム

大学における教育や研究を支える情報基盤システムには下記のような要求があり，その規模や範囲については，システムの更新を重ねるごとに広がりをみせている．

- 大学の学内共同利用システムとして，メールや Web，教育用端末や無線 LAN などの利用を提供すること
- 大学の全構成員が利用する大規模な情報技術の基盤として整備されること
- 将来の利用者のニーズや利用状況に柔軟に対応可能であり，かつ，サーバダウンの際の障害復旧が容易であること

* E-mail: sasaki@kobe-u.ac.jp
† E-mail: togino@port.kobe-u.ac.jp

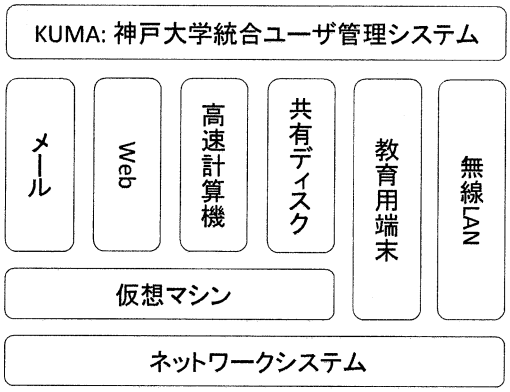


図1　KAISER の概要

一方，これらを実現するための予算は年々，効率化を求められることで削減されるというジレンマをかかえている．また，情報技術の分野における変化はめまぐるしく，安定的な運用を続けるには専門的な知識や経験をもつ人材が必要であるが，限られた大学のスタッフでそのような人材を確保し続けるのは容易ではない．

神戸大学では，このような相反する要求の中で，KAISER と呼んでいる教育研究用計算機システムを運用している．上にあげた問題を解決するため，KAISER では，提供するサービスの抽象化による運用インターフェースの統一を行っている．これにより，大学の構成員に数多くのサービスを提供する一方，サービスを正常かつ安定的に運用するための運用コストを抑えることが可能になっている．また，将来の利用者のニーズに対し，比較的低コストで新しいサービスを提供することも可能である．

このシステムの概要は，図1のようになっている．

KUMA　神戸大学統合ユーザ管理システム (KUMA: Kobe University Integrated User Management System) では，約 7,000 名の教職員及び約 18,000 名の学生を含め，全体で約 30,000 名のアカウントを，人事システムや教務システムとの自動連携により管理を行っている．また，認証に用いられる ID とパスワードを管理する LDAP サーバやメールアカウントおよびホーム領域を確保するファイルサーバと連携し，自動的に利用者が使用できるようにしている．

サブシステム　利用者に対しさまざまなサービスを提供するため，下記にあげるようなシステムを構築している．これらのシステムは，KUMA と連携しており，申請者からの申請により KUMA へサービス利用の登録を行うと，自動的に各サーバと通信を行いサービスの利用が可能になる．また，サービス利用の継続や停止・終了処理も KUMA から管理することができる．

仮想マシン　KAISER では，多くのサービスを提供するため，数多くのサーバが必要になっている．そこで，CPU やメモリなどのハードウェアを効率よく稼動させるために，仮想マシンを構築している．これにより，全体として必要なハードウェアリソースの削減を実現している．

神戸大学では，メールや Web などの基本的なサービスに加え，ホスティングサービスや認証サービスなど合わせて 30 種ほどのサービスを提供している．これらのサービスを個別に管理していたのでは，運用コストはサービスの数に比例し，将来の利用者のニーズに応えることも不可能になってしまう．

そこで，それぞれのサービスを統一して管理できるように下記のような設計を行っている．

サービスアカウント　サービスはその利用単位（メールサービスの場合はメールアドレス．DNS ホスティングサービスの場合は，ドメイン）でサービスアカウントを発行する．ただし，このサービスアカウントは利用者または申請者のユーザアカウントと関係付けを行い，サービス利用に係わる認証は LDAP に保存されたユーザアカウントで行う．利用者はどのサービスでも自身のユーザアカウントで認証し利用することができる．またユーザアカウントと関係付けを行うことで，退職により利用者がいなくなったサービスの出現を抑えるなどの適

切な管理が容易になっている．

サービス状態 すべてのサービスは，非停止・停止・完全停止の３状態を持ち，KUMA で管理された利用期限や申請者の操作により，状態の変更が行われる．非停止は通常の利用状態で，利用期限をすぎると停止状態になる．この状態では，一部機能（メールサービスの場合，転送機能）のみ利用で，場合によっては，非停止状態に移行することも可能である．これらの状態遷移は KUMA からサブシステムへの連携スクリプト呼び出しによって実現されている．

このように，サービスの ID であるサービスアカウントと，その状態遷移を KUMA で一元管理し，KUMA とサブシステム間の通信インターフェースを統一することで，利用者・運用者の双方にとって，サービスの統一した利用や管理が可能になっている．

3 メール

3.1 旧システムの問題点

今や電子メールシステムは，教育・研究活動における情報交換のみならず，日常生活においても必須の基幹システムである．しかしながら，神戸大学における電子メールの利用は，2005 年 12 月以前において，以下のような問題を孕んでいた．

- 電子メールの利用は申請・課金方式であり，高速計算機や電子メールを利用したい者が自らセンターへ申請書を提出・許可されない限り利用できない
- 一つの電子メールアカウントを複数人で流用するようなセキュリティ上好ましくないケースがあった
- 利便性の問題から，学部や研究室レベルで個別に立てられたメールサーバが乱立し，センターが十分に把握できない状況となっていた
- このため，セキュリティインシデントが生じた場合も，十分な対策を取るのが困難だった

3.2 新システムの設計

2006 年 1 月に整備された KUMA 及び教育・研究用計算機システム，並びに 2011 年 1 月に更新した新教育・研究用計算機システム（KAISER）においては，旧システムの問題点を考慮し，

- 1 ユーザ 1 アカウントを原則とし，神戸大学に所属する者全員にメールアカウントを配布することで，誰もが自由に無料でメール利用を可能とする
- 受付用のメールアドレス運用においては，複数人で電子メールアカウントを流用するのではなく，メーリングリストサービスを新たに立てて収容する
- 学部・研究室レベルで立てられたメールサーバの管理労力低減・セキュリティインシデントの削減を目指し，センターのセキュリティの保護の下，電子メールのホスティングサービスを行う
- 学部・研究室レベルで引き続き運用するメールサーバについては，対外公開サーバもしくはメール中継サーバとして登録をしてもらう
- センター職員の労力削減と設定ミスを無くすため，サーバに対するサービス登録作業を出来る限り自動化する

こととした．

現在，神戸大学におけるメールシステムの構成は図 2 のようになっており，大きくわけて次の四つのサービスを行っている．

1. メール中継登録
2. 個人メール（全学用メールシステム）
3. バーチャルメールサーバホスティングサービス
4. メーリングリストサービス

各サービスについて以下に詳述する．

3.2.1 メール中継登録

セキュリティ上の観点から，神戸大学においては現在，学外からの全 TCP/UDP ポートの受信ならびに，TCP25 番ポート他，セキュリティ上の問題あるポート等が Firewall により遮断されており，独自

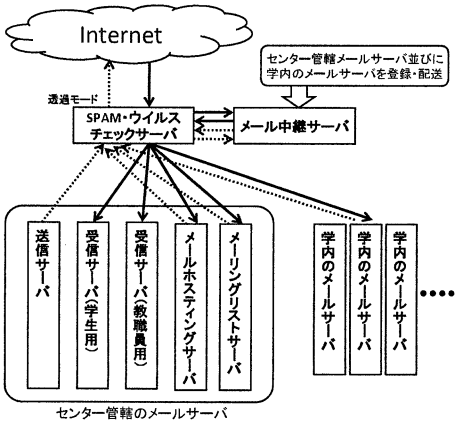


図2　メールシステムの構成

にメールサーバを立てたとしても学内のみでしか利用できないサーバとなるネットワーク設計となっている．学部や研究室レベルでメールサーバを立てたい場合，基本的には後述のセンターが運用するバーチャルメールサーバホスティングサービスを薦めることにしているが，過去の経緯や研究・管理上の必要から独自にメールサーバを立てる必要がある場合も生じている．またセキュリティ上の観点から，学外からのウィルス・SPAM メールの受信や学内からのウィルスメール発信を阻止する必要がある．

メール中継登録では，セキュリティに考慮しつつ安全なメール送受信の運用を実現するために，図2のメール中継サーバに，申請されたメールサーバを登録することによって，センターのウィルス・SPAM チェック機能を通しながら，各申請メールサーバのメールを処理できるようにしている．
これまでこのようなサービスを行うにあたっては，サーバ管理に熟達したセンター職員が，中継を受け付けるサーバ情報や，中継ドメインへの配送設定をメール中継サーバに直接定義する必要があり，労力と神経をすり減らすものであった．本サービスにおいては，操作は極めて簡単で，GUI を有する KUMA 上でメール中継サーバの IP，ドメインなど必要項目を入力し，メール中継登録としてサービスアカウント登録するだけで，自動的にサブシステムであるメール中継サーバに設定されるように構築した．このため，メールサーバの設定に熟知していないアルバイトの職員であっても，マニュアル通りに対応するだけで安全な登録が可能となった．

3.2.2　個人メール（全学用メールシステム）

先に述べた通り，2005 年 12 月以前においては，申請・課金方式をとっていたが，2006 年 1 月の KUMA の導入以降，上流システム（人事給与システム・教務システム）から一括して KUMA 上にユーザアカウントが登録され，同時にメール用アカウントも作成されるようになった．このため，神戸大学に所属する人なら誰でも，神戸大学に来たその日から電子メールを含む教育・研究用計算機システムが利用できる環境を整えている．

本システムはユーザ数 30,000 人規模のメールシステムになっており，神戸大学においては，KUMA 上にユーザアカウントを持つ者に対し，教職員ユーザにおいては，1 個のメインメールアドレスと最大 3 個のサブメールアドレスを，学生ユーザにおいては，1 個のメインメールアドレスと 1 個のメールエイリアスを持つことができ，KUMA 上からユーザが自由にアドレス名を変更することができるようにした．

- 教育・研究用計算機システム（2006 年 1 月～2009 年 12 月）での運用

2005 年 12 月までの旧システムにおいては，認証なしの SMTP による送信，並びに POP3 での受信を許可していたが，セキュリティを考慮して，原則，CRAM-MD5 もしくは DIGEST-MD5 を推奨とした認証付 SMTP 及び POP による送受信を必須とし，学外からのアクセスには SSL の使用を必須とした．学内からのアクセスについては，多数設置されている事務系端末を中心に，当時学内で標準としていたメールソフトが SSL に対応しておらず，一気に SSL の使用を必須とすることは大きな混乱が生じることから，学内からのアクセスについては，当面の間 SSL 推奨という形で運用を行った．

- 新教育・研究用計算機システム（2011 年 1 月～現在）での運用

従来以上にセキュリティに考慮し，メールの送受信においては，学内・学外からのアクセス共に SSL によるアクセスを必須とした．また，学外その他複数端末からの利用や，2009 年 10 月に整備された神戸大学キャンパスネットワークシステムにおける全キャンパスでの無線 LAN 利用開始とそれに合わせたモバイル端末の利用者急増への対応を考慮して，IMAP を用いたメール受信にも対応した．

メールスプール容量については，ユーザの利便性とトラブル対応へのコストを考えて，各ユーザ毎には容量制限を掛けないこととした．一方で，2011 年 5 月の時点において，教職員用のメールスプールが約 500GB，学生用のメールスプールが約 200GB にも達し，IMAP の運用によって今後一層，サーバ上にメールを残すユーザが増えることから，受信後 180 日を経過したメールは，”Archives フォルダ”へ移動したメールを除き，未読・既読を問わず自動削除するスクリプトを組み込むことで，メールスプールの超過に対処している．

SPAM・ウィルスメールへの対応には，一般的なアプライアンスを導入している他，怪しいドメインからのメール受信拒否や，センター管轄ドメインのメールについては，存在しないメールアカウントに対するメールを破棄するなどのフィルタ処置を施している．

3.2.3 メールサーバホスティングサービス

2005 年 12 月以前においては，学部・研究室レベル，その他でメールサーバが乱立している状況にあり，セキュリティ上の観点からも問題であった．2004 年 4 月の神戸大学情報セキュリティポリシー制定以降，各メールサーバにおいては対外公開サーバとしての登録義務が生じたが，セキュリティに対する運用水準は各管理者に委ねられておりバラバラの状態にあった．

本システムは，学部や研究室レベルで各々運用されていたメールサーバをセンターのセキュリティー保護の下収容することを目的に開始したサービスである．

- センターでの管理運用について

図 3　メールサーバホスティングサービスのユーザ管理画面

メールサーバホスティングサービスとして新しくメールサーバを立てる場合，センターでは，従来のようにサーバ管理に長けたセンター職員が面倒なサーバの設定を行う必要はない．サービスを開始するのに必要なドメイン情報などの必要項目を GUI を有する KUMA 上でサービスアカウント登録を行うだけで，自動的にサブシステムであるバーチャルメールホスティングサービスのサーバへ引き継がれ，サービスが開始できるよう構築している．

- メールサーバホスティングサービス利用者の管理・運用について

サーバの管理経験がほとんど無い者でも管理・運用できるよう，Web 上からアクセスできる GUI を有するユーザ管理システムを構築した（図 3）．

GUI 上では，管理者はメールアカウント登録及び承認書発行，変更，停止，再開，削除，及び，各メールユーザのステータスが閲覧できるようになっている．メールアカウントを登録し利用させたいユーザ

に承認書を渡すだけで，メールの利用が可能となっている．メールサーバ自体は，バーチャルサーバとしてセンターが一括して管理運用しており，システムのセキュリティを保っている．

3.2.4 メーリングリストサービス

2005 年 12 月以前においては，学部・研究室レベルで個別にメーリングリストを立てたり，メーリングリストの代わりに一つの電子メールアドレスを受付用に用いるなど，セキュリティ上問題となる運用があった．また，大学事務においては，様々な係の受付メールアドレスとして 200 件以上のアドレスを運用しており，本サービスはこれらをセンターで一本化し，セキュリティの向上とコスト削減を目指して開始したものである．

メーリングリストそのものは，一般的な fml を用いているが，センターでは申請のあったメーリングリストを GUI を有する KUMA 上で登録するだけで，特にサーバの設定を弄ることなく自動的にサブシステムであるメーリングリストサーバに登録されるよう構築している．

本サービスは，メーリングリストサービスと，メーリングリスト自動生成サービスの二つのサービスで構成されている．メーリングリストサービスは一般的なメーリングリストの利用と大きく異ならないため，本項では，本システムで特徴的なメーリングリスト自動生成サービスについて述べる．

- メーリングリスト自動生成サービスの特徴

大学事務においては，様々な係の受付用メールアドレスを有しており，現在，200 件以上のアドレスが運用されている．各係の人員は，人事異動により頻繁に変化するため，同じメールアドレスを流用して多人数で利用するか，人事異動の度にメーリングリストのメンバーを手動で更新する必要があり，その管理は非常に問題があった．本サービスでは，KUMA 上のユーザ登録情報を参照し，各メーリングリストに部局・係などの所属コードを登録しておくだけで，自動的に各部局・係に所属する人員を検索し，メーリングリストへ登録するメールアドレスを自動更新することを可能とした．所属コードなどの登録は，GUI を有する KUMA 上から簡単に登録・変更を行うことができる．また，センター管理下にないメールアドレスも，GUI を有するユーザ管理プログラムから個別に追加登録・削除を行えるシステムとなっており，非常に効率良くメーリングリストの運用を行うことが可能となった．

- メーリングリスト自動生成サービスの問題点

メーリングリスト自動生成サービスのシステムの問題ではないが，改組などにより部局・係そのものが無くなる場合は，所属コード上ではそのメーリングリストに登録されるメンバーが 0 人になる場合が生じる．従って，人事異動が起きる前に，メンバーが 0 人になるメーリングリストについては，新しい引き継ぎ先になる所属コードを追加登録するか，個別にメールアドレスを手動登録する必要がある．

4 教育用端末

高等教育における情報教育の実現や教育活動の情報化を支援するため，大学はこれを実現する教育用端末を整備する必要がある．しかしながら，教育用端末の導入にかけられる予算は年々削減され，少ないスタッフで運用しなくてはならない現実がある．また，大学での教育用端末の利用は，通常の計算機の利用や運用と比べ，以下のような特徴がある [1]．

- 講義での利用する際，ログインやアプリケーションの起動が一斉に行われる．
- 教員の指導のもとで利用する講義利用と，学生が自ら利用する自習利用がある．
- 学部の違い（特に理系と文系）で利用するアプリケーションや使い方が大きく異なることがある．

このような特徴をふまえ，多様な要求に答えつつ，低コストで安定した運用が行えないといけない．

神戸大学では 2011 年 1 月に教育用端末の更新を行うにあたり，旧システムの問題点を踏まえ，より快適かつ安定的に運用できるよう検討および設計を行った．この章では，教育用端末に関しての検討・設計・導入について述べる．

4.1 教育用端末の形態

多くの計算機を運用する場合，その方式として一般的に大きく分けて，1) スタンドアロン方式 2) シンクライアント方式の 2 種類が存在する [2]．スタンドアロン方式は，単独で起動し利用することが可能であり，CPU やメモリ，HDD などのリソースはローカルのものを利用するため，最近のハードウェアであれば十分な性能を活用することができる．一方，OS を含めたアプリケーションについては，それぞれの端末に分散するため，アップデートや新規インストールなどの作業が大変になることが多い．シンクライアント方式は，ソフトウェアの環境を一元管理することが可能であり，端末には高性能なハードウェアを必要としないが，その分サーバとネットワークに十分なリソースが要求される．

神戸大学では，端末が地理的に広範囲に広がっている上，全体の端末数も多い為，ソフトウェアの一元管理は必須である．ただし，近年の計算機は安価で十分な性能を備えている上，講義で一斉利用する際のネットワークへの負荷を考えると，端末側で出来ることは出来るだけ行う方がよいと考えた．

このような条件を踏まえ，教育用端末の形態としてはネットワークブート方式が最適であると判断し，具体的には Mac OS が提供する NetBoot[3] を採用した．NetBoot は電源投入後，ネットワーク経由でサーバ側にあるディスクイメージをファイルシステムとしてマウントして起動させるシステムである．その為，OS を含めたアプリケーションなどのソフトウェアの環境をサーバで管理することができる．また，端末に接続されたローカル HDD をシャドウイメージファイルの保存場所として利用できるため，一度サーバからダウンロードされたデータはローカル HDD にキャッシュされ，その後はサーバに負荷をかけず高速にアクセスできる．ファイルシステムへの書き込みもシャドウイメージに行われるため，サーバへの通信が発生せず高速である．

教育用端末の形態として，これまで述べたネットワークブートを実現するブートサーバと端末に加え，以下のシステムが必要である．

認証サーバ 利用者の認証は，学生や教職員などの神戸大学の構成員に対しアカウントを発行する神戸大学統合ユーザ管理システムと連携して行っている．

ファイルサーバ すべての端末において同じ環境で利用出来るように，利用者のホーム領域はファイルサーバに確保し，端末からオートマウントを行うことでアクセスを実現している．

4.2 旧システムの問題点

従来のシステムは 2006 年 1 月に導入し，その間の運用において，いくつかの問題点があった．

- ソフトウェアの更新に対しハードウェアの更新が出来ない為，相対的に性能が劣化する
- 長期利用者において，アプリケーションの起動に時間がかかるなどの性能低下が起こる

基本的に，NetBoot による教育用端末の運用は順調であり，大きな問題はみられなかった．ただ，細かい問題や不具合に対応するために，頻繁なソフトウェアの更新が必要となったが，イメージの更新に対する明確なポリシーがなかったため，端末を利用する教員や学生に対して多少の混乱を与えることがあった．

4.3 新システムの設計

従来の問題点を踏まえ，教育用端末をより快適かつ安定して運用することが重要であると考え，導入するアプリケーションの選択やイメージの更新方法を検討し，また，アプリケーションの利用に対し，十分な性能が発揮できるような構成と運用を目標とした．

全学で統一した環境の提供を目的として，15 部局等にまたがる 33 教室に，合わせて 1300 台規模の端末を導入することとなった（表 2）．NetBoot による同規模の事例として東京大学のシステムがあげられる [4]．

4.3.1 導入アプリケーション

教育用端末に導入するアプリケーションを検討する為に，各部局に対し，導入を希望するアプリケーションの調査を行った．調査の結果，有償アプリ

ケーション 20 種（表 1），無償アプリケーション 29 種が得られた．

表 1　導入希望の有償アプリケーション

種類	アプリケーション名
オフィス文書	Microsoft Office
	Microsoft Office 英語版
	iWork
マルチメディア	Adobe PhotoShop EL
	Adobe Premiere CS3
	iLife
	CLAYTOWN
CAD	Vector Workd
仮想化環境	VMware
科学技術計算	MATLAB
	MAPLE
統計計量分析	PASW
	STATA
	TSP
	AMOS
	Eviews
	Gauss
	LIMDEP
行列言語ソフト	OxMetrics
医用画像処理	OsiriX

選定の基本的な原則は以下の通りとした．

- 無償アプリケーションは，技術的問題がない限り基本的に導入する．
- 全学的な利用が見込めるアプリケーションは導入を検討する．
- 学部学科に利用が依存すると思われるアプリケーションは，部局で予算を確保する上で導入を検討する
- 利用が少数 (およそ 30 名以下) しか見込めないアプリケーションは，代替の無償アプリケーションを検討する

この原則に従って，それぞれのアプリケーションについて判断を行い，全学的な企画評価 WG での議論と承認を受けた後，各部局に回答を行った．

特に議論となったアプリケーションとして，有償の統計分析があげられる．経済学部や経営学部では，学部生の利用を考えた場合には同じような目的のアプリケーションでも，教員が普段利用するアプリケーションの導入を希望することが多く，同種類のアプリケーションが乱立する事になった．大学教育として統計分析におけるアプリケーションを絞るべきという意見も出たが，実際には非常に困難であり，最終的には部局の電子計算機運営委員会で調整して取りまとめて頂く事となった．

4.3.2　ファイルサーバ

教育用端末において利用者別のストレージは，ホームディレクトリとしてファイルサーバに用意されており，端末からマウントすることでアクセスできるようになっている．従来のシステムでは，マウントプロトコルとして NFS を採用していたが，いくつか問題点があった．

- Mac OS の Finder が適切にファイルシステムを扱えない場合がある
- 日本語ファイル名を適切に扱えない場合がある
- ファイルロックに過度な負荷がかかり，性能が低下することがある

これらの問題が，アプリケーションの動作に不具合を引き起こしたり，動作が遅くなるなどの性能低下の原因になっていたと考えられるので，新システムの安定運用には，ファイルサーバの見直しが重要であると判断し，これまでの NFS に加え AFP(Apple File system Protocol) の利用を検討に加えることにした．

機能面で NFS と AFP を比較したところ，表 3 のようになった．

日本語ファイル名　特に濁音や半濁音を含む日本語ファイル名は，Mac OS が Unicode の正規化の扱いに NFD を採用しているため，NFC を期待するアプリケーションが正常に動作するか．

ファイルクォータ　ディスク使用制限 quota が正

表 2　教育用端末の設置教室

部局等	講義室等	台数
情報基盤センター	分館 1 階 第 1 演習室	53
情報基盤センター	分館 1 階 第 1 演習室	53
	分館 2 階 第 2 演習室	53
	分館 3 階 第 3 演習室	51
	分館 1 階 自習室	46
	本館 1 階 計算機室 1 (管理用)	2
	本館 2 階 事務室 (管理用)	3
	分館 1 階 事務室 (管理用)	2
大学教育推進機構	講義棟 5 階 K-501 情報処理教育演習室	151
	講義棟 5 階 K-502 情報処理教育演習室	178
附属図書館	総合国際文化学図書館 3 階	37
	社会科学系図書館本館 1 階	15
	社会科学系図書館管理棟 2 階	3
	社会科学系図書館 1 階 (社会科学系フロンティア館)	10
	自然科学系図書館 2 階	27
	自然科学系図書館 3 階	5
	人文科学図書館 1 階 (人文学研究科 C 棟)	9
	人文科学図書館 2 階 開架閲覧室 (人文学研究科 C 棟)	4
	人文科学図書館 2 階 大型図書閲覧室 (人文学研究科 C 棟)	3
	人間科学図書館 2 階	13
	医学分館 1 階 (医学研究科管理棟)	14
	保健科学図書室 2 階	10
	海事科学分館 1 階	11
留学生センター	3 階 コンピュータ室	27
	3 階 メディア室	8
	2 階 情報資料室	10
六甲台	六甲台第三学舎 2 階 情報処理教室	79
(法・経済・経営・国協)	六甲台第三学舎 2 階 電算機室西側	41
	六甲台第三学舎 2 階 電算機室手前	27
	六甲台第三学舎 2 階 206 号室 情報処理演習室	41
	六甲台第三学舎 2 階 管理室 (管理用)	3
人文学研究科	人文学研究科 B 棟 3 階 322 情報処理演習室	49
国際文化学研究科	実験棟 5 階 F-501 情報処理室	51
人間発達環境学研究科	人間発達環境学研究科学舎 F158 情報教育設備室	61
国際協力研究科	六甲台第五学舎 411 情報処理演習室	53
保健学研究科	保健科学図書室 1 階 情報処理教室	61
農学研究科	農学研究科学舎 1 階 D103 情報処理教室	50
海事科学研究科	総合学術交流棟 2 階 情報処理演習室 (IPC)	30
合計		1291

常に動作するか.

ゴミ箱の動作　ファイル削除時，直接削除にならずゴミ箱として正常に動作するか.

Word **でのファイル保存**　上書き保存が正常に行えるか．Microsoft Office の実装に依存する問題だと思われる.

AFP に変更することで解決する項目もあるが，新しく発生した問題点もあり，それぞれに長所と短所があり一概に優劣がつけれなかったため，実際にファイルサーバでは両方をサポートできるようにした上で，高負荷における性能評価を実施した（表 4）.

実験の結果 AFP はファイルサーバにおいてユーザランドで実行されるため，カーネルで動作する

表 3　AFP と NFS の比較

項目	AFP	NFS
日本語ファイル名	o	x
ファイルクォータ	o	x
ゴミ箱の動作	x	o
Word でのファイル保存	x	o

記号例: o 問題なし x 問題あり

表 4　Word 初回起動時間の比較

	起動時間（分:秒）	
台数	AFP	NFS
30	1:16	2:28
60	1:28	3:28
100	1:33	4:46
150	13:57	6:58
180	17:30	7:56

表 5　iMac 性能表

	新端末	旧端末
CPU	Intel Core i3	PowerPC G5
クロック	3.06GHz	2.0GHz
メモリ	4GB	1GB
HDD	500GB	160GB
ディスプレイ	21.5 インチ LCD	17 インチ LCD
解像度	1920x1080	1440x900

NFS と比べ不利な上，アプリケーションの初回起動のような新規ファイルが大量に生成される時に CNID の生成に非常に時間がかかり，性能が極端に低下することがわかった．

この結果を踏まえ，ファイルシステムへのマウントプロトコルとしては NFS を採用することとした．

4.4　導入

教育用端末として導入した iMac のスペックを従来の端末と比較したものを表 5 にあげる．

導入中は，特にネットブートイメージの構築において，さまざまな問題が発生し，その都度対処する必要があったため，それらの問題を管理するために Redmine[5] を活用した（図 4）

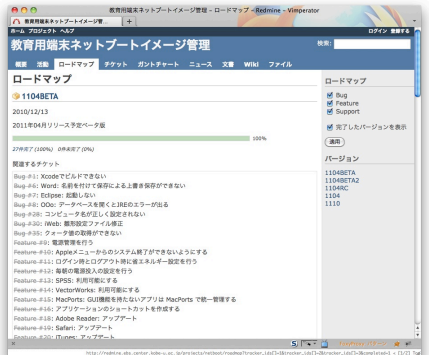


図 4　Redmine

Redmine とは，Web ベースのプロジェクト管理ソフトウェアで，主にソフトウェア開発中のタスク管理や進捗管理に用いられている．教育用端末の導入においては，ネットブートイメージの作成を，ソフトウェアリリースに見立て，以下のようなスケジュールで行った．

- 12/13 ベータ版(対処バグ 7 件, 新規機能 20 件)
- 01/07 ベータ版 2（対処バグ 5 件，新規機能 5 件)
- 02/01 RC 版（対処バグ 7 件，新規機能 10 件）
- 03/01 リリース版（対処バグ 6 件，新規機能 14 件）

旧システムで問題になったイメージ更新に関して，OS やアプリケーションなどのソフトウェア環境に対する問題や追加機能を可視化して情報共有することで，計画的に実施することが可能になった．

5　まとめ

神戸大学における教育研究用計算機システムに関して，アカウントなどを管理する統合ユーザ管理システム KUMA と，電子メールシステムや教育用端末システムについて述べた．これらを含むすべてのシステムは，統一的なインターフェースで連携されており，KUMA から管理することが可能になって

いる．このため，高度な専門的知識をもつ技術者でなくても，一般の事務系職員によって，マニュアルに沿った画一的な管理・運用が可能になっている．また，仮想マシンシステムを導入することで，必要なハードウェアリソースを削減している．このような設計により，大規模なシステムにも関わらず，必要なコストを減らしつつ，高度で安定したサービスが提供できるようになったと考えている．

参考文献

[1] 特集. 大規模分散ネットワーク環境における教育用計算機システム. 情報処理, Vol. 45, No. 3, 2003.

[2] 櫻田武嗣, 萩原洋一. シンクライアントと持ち込みノート pc による端末室デスクトップ環境の設計 (情報通信マネジメント). 電子情報通信学会技術研究報告, Vol. 111, No. 30, pp. 99–104, 2011-05-12.

[3] 竹林賢. Netboot for mac os x. 情報処理, Vol. 45, No. 3, 2004.

[4] アップルジャパン株式会社. 東京大学情報基盤センター - 3 万人が利用する情報教育システム. http://images.apple.com/jp/education/profiles/tkuv/pdfs/tkuv.story.pdf.

[5] 小川明彦, 阪井誠. Redmine によるタスクマネジメント実践技法. 翔泳社, 2010.

山口大学におけるネットワーク運用支援システム

The Network Administration Support System in Yamaguchi University

久長　穣†，杉井　学†，為末　隆弘†，金山　知余†，小河原　加久治†
Hisanaga Yutaka†, Sugii Manabu, Tamesue Takahiro, Kaneyama Chiyo†, Ogawara Kakuji‡

hisa@yamaguchi-u.ac.jp, manabu@yamaguchi-u.ac.jp, tamesue@yamaguchi-u.ac.jp,
kaneyama@yamaguchi-u.ac.jp, ogawara@yamaguchi-u.ac.jp

†山口大学メディア基盤センター

† Yamaguchi University Media and Information Technology Center

概要

ネットワーク利用者からのネットワークに関する問い合わせにはネットワーク障害に関するものあるが、その多くは利用者端末の設定ミスや接続不良によるものが多い。そのため、利用者端末の状況を的確に把握し、それに応じた対応が求められる。ネットワーク管理の経験者であれば、ネットワーク機器が記録している情報を取得し統合することで、ある程度利用者端末の状況を把握する事ができるが、経験の無い、または経験の浅い管理者には困難である。一般のネットワーク管理システムの活用も考えられるが、それらは、ネットワーク機器の管理及びトラフィック等の利用状況の分析が主であり、ネットワークの末端に接続される利用者端末の状況確認に利用するには困難である場合が多い。そこで、平成 13 年のギガビットネットワークの整備の際に、ネットワーク利用者研究室が個別に把握できる物理ネットワークの整備を行い、さらに平成 14 年からネットワーク機器の管理だけでなく利用者端末の状況を把握する事のできるネットワーク運用支援システムを提案し、随時構築してきた。また実際に運用を通してその有用性を確認した。本稿では、本ネットワーク運用支援システムについて述べるとともに、山口大学における運用状況について報告する。

キーワード

ネットワーク管理システム，ネットワーク利用者対応，　SNMP

1. はじめに

平成 5 年に整備した山口大学の全学ネットワークはイエローケーブルを用いて構成した。イエローネットワークは建物内に 1 本のイエローケーブルを配線し、それに利用者端末を接続して、ケーブルを共有して利用する形態をとるため､建物内でネットワーク障害が発生しても、発生場所、発生原因を特定するのが大変困難な状況であった。また、イエローケーブルのネットワークは支線と位置づけ、部局の管理であったため、そのすべてがメディア基盤センターで把握できていなかった。それでもネットワーク障害等が発生した場合に、利用者はメディア

基盤センターに問い合わせる場合が多かったが、対応が困難であった。

平成 13 年のギガビットネットワーク整備では、イエローケーブルを廃止し、各部屋まで UTP ケーブルを配線し情報コンセントとし、部屋までのネットワーク管理・運用がメディア基盤センターで一元的に可能な構成に変更した。これにより技術的には、障害の発生場所、障害状況等が把握できるようになった。さらに平成 20 年からは講義室及び会議室に全学無線 LAN 環境を整備した。ネットワーク利用形態が多様化し、ほぼ全域でのネットワーク利用が可能な環境へと発展した。

一方利用者からの問い合わせも増加し、多様化した。利用者からの問い合わせの多くは、利用者端末の設定や接続等によるものが多いことから、それらの問い合わせが窓口にあった場合は、一連の対処方法を案内し、利用者に利用者端末の設定等の見直しを行ってもらっていた。しかし、多くの利用者は「設定等何も変えてない」「間違っていなかった」等、問題解決に至らない場合が多くあった。その場合は、ネットワーク担当者がネットワーク機器に記録されている情報を調べて障害状況を把握し、個別に対応しなければならなかった。

山口大学は本部キャンパス、工学系キャンパス、医学系キャンパスの 3 キャンパスに分かれており、スタッフが少ないこと、ネットワーク担当者が工学系キャンパスにいたこと等から、概ね 1～2 名の窓口担当者でそのキャンパスのネットワークに関する問い合わせに対応しなければならない状況にあった。利用者の問い合わせに、ピンポイントで的確に対応するためには、窓口においても利用者端末の状況を把握し、その状況に応じた対処方法を回答することが望まれる。

通常、ネットワーク管理のためネットワーク管理システムが提案・導入されている[1-5]。ネットワーク管理システムは、ネットワーク機器の管理や利用状況の把握が主であり、利用者端末の状況を把握するためには、さらに、関連する複数のネットワーク機器を操作し、いくつかの情報を組み合わせて判断する作業と専門的知識が必要であるため、迅速な対応を求められる窓口での利用者対応に用いることは難しい状況にある。そこで、独自に平成 14 年よりネットワーク機器の管理だけではなく、窓口においても利用者端末の状況把握を容易に行えるネットワーク運用システムを提案し[1]、構築を進めてきた。構築に当たっては実際に窓口担当者に利用してもらい、表示してほしい情報や使い勝手等を相談しながら開発を進めた。

本稿では、開発を行ったネットワーク運用支援システムについて述べるとともに、山口大学での運用状況について報告する。

2. 山口大学ネットワークの概要

ネットワーク運用支援システムは、物理ネットワーク構成、論理ネットワーク構成及びネットワーク機器構成等を考慮して構成される。本章では、山口大学におけるネットワークの概要について述べる。

2.1. 物理ネットワーク構成

山口大学物理ネットワークは以下の構成としている。図 1 にキャンパス間・建物間物理ネットワーク、図 2 に建物内物理ネットワークを示す。ネットワーク設計・構築は以下のように構成している。

(1)建物に 1 か所、ネットワーク機器室を設ける。通常、建物内の EPS(Electric Pipe Shaft)を用いることが多い。

(2)その建物内の UTP ケーブルの配線は、上述のネットワーク機器室からすべての部屋に 2 本ずつスター型に配線し、情報コンセントを設置する。

(3)情報コンセントには、階毎に 1 から始まる連番で一意な番号を割当てラベリングを行う。これを情報コンセント番号という。情報コンセント番号は部屋名や部屋番号等とは独立したものを採用している。なぜなら部屋名や部屋番号は建物の管理部局によって変更される場合があり、コンセントの場所を一意に把握する事は困難だからである。建物改修後の利用開始直後に部屋番号が変更された例もある。

(4)ネットワーク機器室には、その建物に必要な台数のネットワーク機器を設置する。これらネットワーク機器のポートと全情報コンセントへの配線を接続する。どの機器のどのポートに、どの情報コンセントが接続したかの情報を、**キャンパス名、建物名、階数、情報コンセント番号、部屋名、ネットワーク機器名称、ネットワーク機器ポート番号**の組み合わせで管理データベースに記録する。また、部屋名について可能な範囲で記録する。全学に配置された情報コンセントは20,000個以上であり、ネットワーク機器は 1,500 台以上となっている。

ネットワーク機器を建物の 1 か所に集約することで、管理場所が限定され、ネットワーク管理・運用が容易になり、ネットワーク機器の空調・防塵等の環境対策を行う場所も限定される。また、情報コンセントに一連の番号を割り当てることで、学内における情報コンセントの場所の特定が容易になる。これらにより、ネットワーク利用者がトラブル対応の連絡をしてきた場合、窓口において建物名、階数及び情報コンセント番号を確認し、トラブルの発生した情報コンセントの位置を特定すること等ができる。

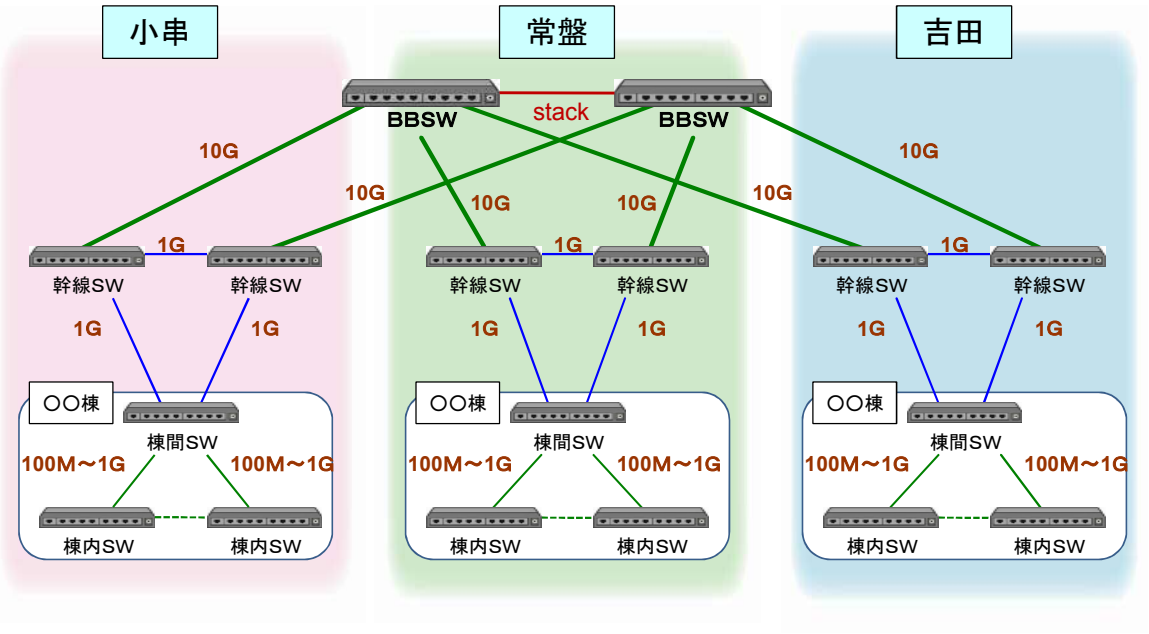


図１　ネットワーク構成

全学に１か所ネットワーク機器室を設け、そこから大学内の各部屋に光ファイバーでネットワークを構築する方法をとっている大学もある[6]。山口大学では、導入時期が早かったこと、キャンパスが分散していること、キャンパスのサイズが大きいこと、各部屋に配置するメディアコンバータに電源が必要なこと等から３階層構造で、各部屋の情報コンセントには電源を必要としないパッシブな構成をとっている。

さらに、講義室や会議室では部屋の中で各机に配線するなど、複数の情報コンセントに分岐する場合がある。これらの部屋内にラックを設置し、ラック内にネットワーク機器を収容、そこから各コンセントに UTP ケーブルを配線している。各情報コンセントには１から始まる一連の番号を割当て、ラベリングを行っている。また、研究室の学生実験室においても、同様な構成を推奨している。これらの部屋については、**建物名、部屋名または部屋の情報コンセント番号、各机の情報コンセント番号**によって情報コンセントの位置を特定している。

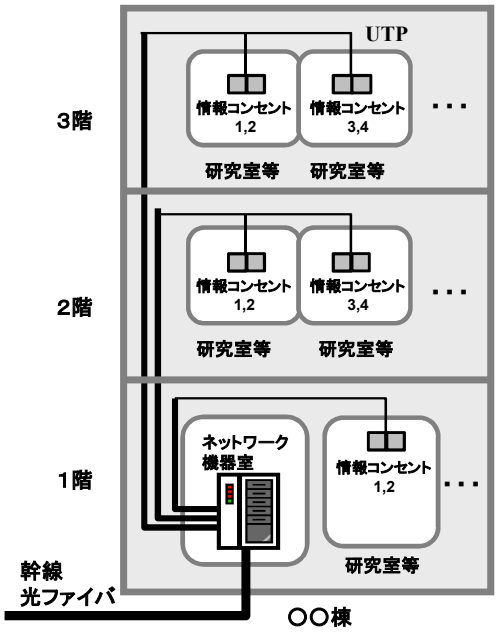


図２　建物内物理ネットワーク構成

2.2. 端末の接続申請

山口大学では、構成員が端末を学内ネットワークに接続する場合に、以下の二つの接続方法をとっている。教職員の接続申請に基づき固定(グローバルまたはプライベート) IP アドレスを発行する方法と、IP アドレス等を自動取得に設定した端末を情報コンセントに接続後、Web 認証により利用者の認証を行う方法とがある。後者については次節で述べる。

前者について、端末をネットワークに接続しようとする教職員は、**接続責任者、運用担当者、キャンパス名、建物名、階数、情報コンセント番号等**を記入して申請する。これらの情報を利用者データベースに記録する。この利用者データベースを参照することで、申請当初は IP アドレスの利用者、利用場所が特定できる。しかし、申請から数年経過すると利用者及び利用場所が変更される場合があり、その際、変更申請がなされないことが多く、利用者、利用場所等の特定ができないことがある。

2.3. 認証ネットワーク

講義室、会議室、図書館閲覧室等のオープンな部屋に

おいて、山口大学構成員がノートＰＣ等をネットワークに接続（有線・無線共に）して利用できるように、各机上に情報コンセント及び無線 LAN を整備している。このネットワークにおいて、利用者はネットワーク利用開始時に毎回利用者認証を行わなければならない。そのため、利用者は前節の利用者申請が不要である。

利用者がこのネットワークに端末を接続すると、DHCP により端末に IP アドレスが割り当てられ、さらにブラウザーのプロキシー設定が自動的に行われる。利用者が Web ページを開くと、認証ネットワークの認証サーバ（以下認証サーバ）に接続され、認証ページが表示される。利用者はこのページで利用者認証を行う事で、学内 LAN 及びインターネットが利用できる。認証の際に用いた情報（ユーザ名及び端末の IP アドレス）が認証サーバに認証時刻と共に記録される。また、認証済みの端末の通信が一定時間なくなった場合、当該端末の認証が解除される。平成 10 年にこの仕組みを提案[7]後、いくつかの改良を加えている。現在では利用者認証が設定されている情報コンセントは約 9,000 個となっている。

3. ネットワーク運用支援システム

ネットワーク運用支援システムは、ネットワーク障害通知機能、ネットワーク機器管理機能、トラフィック管理機能、ループ接続判定機能等のシステム管理者向けの管理機能を有している。さらに、窓口において、ネットワーク利用に関する利用者の問い合わせ対応のために必要な情報を表示する利用者端末管理機能を有している。本章では、特にこの利用者端末管理機能について述べる。

ネットワーク運用支援システムの構成を図３に示す。ネットワーク運用支援システムは、ネットワーク担当者及び窓口担当者のためのＷｅｂページを構成する主要サーバ、ネットワーク機器の FDB（Forwarding Database）を収集し、履歴を残す FDB 収集用サーバ、及びネットワーク機器の各ポートのトラフィックを収集し履歴を残すトラフィック収集用サーバの 3 台から構成される。それぞれのハードウェア構成及びソフトウェア構成を表１に示す。各サーバは既存機器を流用して構築したためスペックは高くない。

3.1. 利用者端末情報の収集

次の利用者端末にかかわる情報を取得し、これらの情報をもとに利用者端末情報を整理している。

(1)端末が接続するポートのインタフェース(リンク・トラフィック等）情報

(2)端末の MAC アドレスと接続ポート

表１　ネットワーク運用支援サーバの構成

サーバ	メイン	FDB 用	トラフィック用
CPU	Core2Quad 2.4GHz	Pentium4 2.4GHz	Pentium4 2.4GB
メモリ	8GB	1GB	1GB
HDD	1TB	250GB	250GB
Network	1Gbps	100Mbps	100Mbps
OS	FreeBSD6.4	FreeBSD5.5	FreeBSD5.5
開発言語	perl, PHP	perl, PHP	perl, PHP

(3)端末の IP アドレスと MAC アドレス

(4)端末が接続されるポートの VLAN 情報

(5)端末の認証情報

バッチ処理で情報を取得するプログラムは perl を用い、Web ページと連動して情報を取得するプログラムは PHP を用いて作成した。情報の取得方法について、以下に述べる。

(1)情報コンセントのリンク情報等の取得

各研究室等の情報コンセントに利用者のネットワーク機器を接続し、電源が投入されると、該当するネットワーク機器のポートとの間で通信速度等が調整され接続状態となる。情報コンセントに対応したネットワーク機器のポートがリンクアップ状態であることは、ネットワーク機器と利用者機器が物理的に正常に接続されていることを示している。

L2 スイッチ（以下 L2SW）はリンク情報として保持している。本システムでは、リンクアップ情報、通信速度、受信バイト数、送信バイト数、非ユニキャストパケット数等を SNMP の IF-MIB を用いて取得している。また、設置しているネットワーク機器ではリンクアップ及びリンクダウンと状態が変化した際には syslog に報告する機能を有しているので、リアルタイムにリンク情報を記録している。

(2)利用者端末の MAC アドレスの取得

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なすことができる。

通常、L2SW は MAC アドレスを用いて、宛先端末を特定している。L2SW 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、L2SW 内のメモリー上の FDB に MAC アドレスとポート及び VLAN を記録している。

ネットワーク管理システムでは FDB 情報を取得する

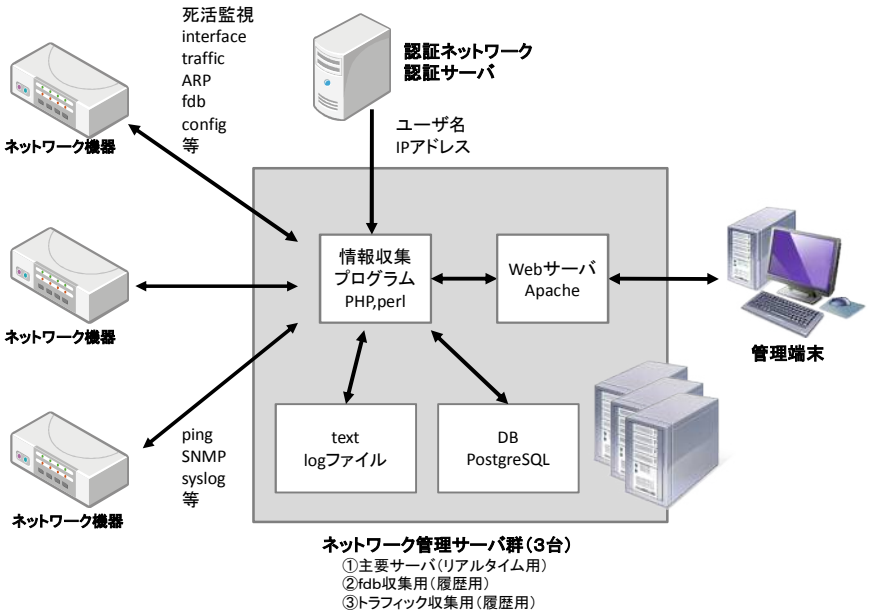


図３　ネットワーク管理システム

ために、対象ネットワーク機器が SNMP の BRIGE-MIB に対応している場合、定期的に SNMP マネジャーを用いて FDB の情報を収集し、取得時刻と共に記録している。一方、対象ネットワーク機器が SNMP の BRIGE-MIB に対応していない場合は、telnet によりログイン後、FDB を参照するコマンドを投入することで FDB を収集している。さらに、一部のネットワーク機器の場合、FDB が更新した際にその情報を syslog に報告する機能を有するものがある。このネットワーク機器の場合は syslog の情報から FDB の更新情報をリアルタイムに取得している。FDB 情報は 15 分毎に収集している。さらに、利用者端末管理機能を用いる際は、その都度該当する最新の FDB を取得している。

これにより**利用者端末 MAC アドレス、ネットワーク機器名、ネットワーク機器ポート番号**が管理データベースに記録される。

(3)利用者端末のＩＰアドレスの取得

一方、全学ネットワーク上の通信には IP アドレスが用いられ、各種サーバのアクセスログは端末に設定されている IP アドレスが記録される。端末の IP アドレスは 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 アドレスを用いるため、同一端末であっても利用場所・利用時刻等により異なる場合がある。例えば DHCP で割り当てられる IP アドレスは、割当毎に一定ではなく、利用場所・利用時刻により異なっている。管理者により割り当てられた IP アドレスも利用場所や利用者の変更、機器の交換等により異なった IP アドレスが設定される場合がある。中には、山口大学のルールでは禁止されているが、一つの IP アドレスを複数の端末で共有する場合もある。したがって IP アドレスは端末固有の情報とはみなせない。

通常、L3 スイッチ（以下 L3SW）は IP アドレスと MAC アドレスの変換テーブル（ARP テーブル）を検索し端末の MAC アドレスを把握している。本システムでは、FDB 情報の場合と同様に、SNMP の IP-MIB を用いて ARP テーブル情報を取得し、取得時刻と共に記録している。また、設置しているネットワーク機器の多くは ARP テーブルが更新した際に、その情報を syslog 機能を用いて syslog サーバに報告する機能を有しているので、syslog 機能を利用して ARP テーブルの更新情報をリアルタイムに取得している。SNMP による ARP テーブル情報は 5 分間隔で収集している。さらに、利用者端末管理機能を用いる際は、その都度該当するネットワーク機器の最新 ARP テーブルを取得している。

これにより**利用者端末 IP アドレス、MAC アドレス**が管理データベースに記録される。

(4)VLAN 設定情報取得

ネットワーク管理システムでは VLAN 情報を取得するために、対象ネットワーク機器が SNMP の BRIGE-MIB に対応している場合、定期的に SNMP マネジャーを用いて FDB の情報を収集し、取得時刻と共に記録している。一方、対象ネットワーク機器が SNMP の BRIGE-MIB に対応していない場合は、telnet によりログイン後、VLAN 設定を参照するコマンドを投入し、VLAN 情報を収集し

ている。VLAN 情報は 1 時間に 1 回収集している。さらに、利用者端末管理機能を用いる際は、その都度の該当する最新の VLAN 情報を取得している。なお、全学のネットワーク機器の VLAN 設定はネットワーク担当者のみが設定するので、設定の際に常に記録を残すことで対応可能ではあるが、記録ミスを避けるために、VLAN 情報をネットワーク機器から定期的に取得している。

これにより**VLAN 名、VLAN ID，ネットワーク機器名、ネットワーク機器ポート番号**が管理データベースに記録される。

(5)利用者認証情報の取得

認証ネットワークの認証サーバには、認証時の利用者のユーザ名と端末 IP アドレスが記録されている。ネットワーク運用支援システムは、利用者端末の IP アドレスに対応したユーザ名を次のように取得する。ネットワーク管理システムは認証サーバに対して SNMP の EXEC-COMMAND を用いて IP アドレスの問い合わせを行う。認証サーバは認証情報を検索し、該当するユーザ名を返信する。なお、認証サーバに SNMP サーバ機能（net-snmp）を組み込み、EXEC-COMMAND の問い合わせに対して IP アドレスからユーザ名を検索し、応答するプログラムを作成した。

これにより**利用者 IP アドレスと利用者ユーザ名**の組み合わせが取得される。

本ネットワーク運用支援システムに表示される内容は、ネットワークの現時点での利用状況を示していると考えられる。使い方によっては、プライバシー上の問題に発展する可能性は否定できない。そのため、このページの情報は山口大学情報セキュリティポリシーに基づき CIO が指定したネットワーク担当者、及びその監督のもと特定の担当者のみが必要な範囲で参照する。また、ネットワーク管理サーバに蓄積されたログ等の履歴情報は、山口大学情報セキュリティ緊急時対応基準に基づき、緊急事態担当者（上述ネットワーク担当者）が必要な範囲で参照する。

3.2. 利用者端末の状況表示

前章、前節の情報を統合し、一覧表示させることで、利用者端末にかかわる状況が把握できる。図４にネットワーク運用支援システムの利用者端末の状況を表示した Web ページの例を示した。管理者端末から Web ブラウザーを用いて、ネットワーク管理サーバに接続し、担当者のユーザ認証後、この Web ページを表示する事ができる。このページでは、以下の情報が表示されている。

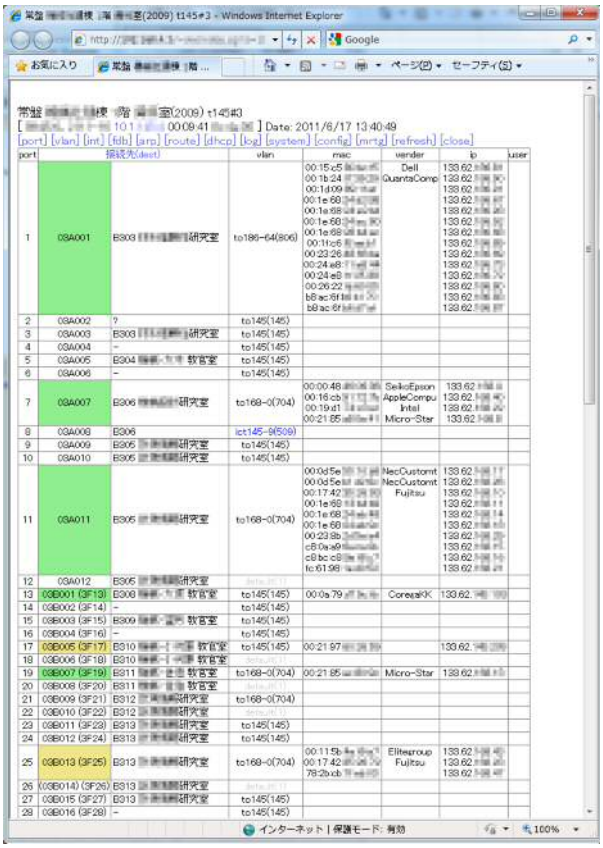


図４　ネットワーク運用支援システムの Web ページ例

(1)情報コンセント番号と部屋名

ネットワーク構築時に割り当てた情報コンセント番号と、その情報コンセントが設置されている部屋名が表示される。問い合わせの際これらの情報を利用者に確認し、該当する行を参照する。

(2)情報コンセントのリンクアップ状況

利用者端末やネットワーク機器が情報コンセントに正しく接続されている場合は、背景が色付きで表示される（黄色：10Mbps, 緑色: 100Mbps, 水色: 1Gbps, 紫色 10Gbps, 灰色 : disable）。色が表示されない場合は、リンクダウンしており、情報コンセントに LAN ケーブルの未接続や断線、あるいは、研究室内の HUB の故障や電源が落ちているなど可能性が指摘できる。とりわけ、HUB の故障である場合が多い。

(3)VLAN 情報の表示

各情報コンセントに割り当てられている VLAN が、表示される。利用者が使おうとしているネットワークが意図したサブネットや VLAN であるかどうか確認ができる。もし、意図したネットワークでなければ、情報コンセントに割り当てられているサブネットや VLAN の変更の手続きを案内する。また、ネットワーク機器の設定

ミスであれば、ネットワーク担当者に連絡し、設定変更を行う。なお、VLAN 名が青色で表示される場合は、認証ネットワークであることを示している。この情報コンセントを使っている場合には、利用者認証が必要であることを案内する。

(4)MAC アドレスとベンダーコードの表示

情報コンセントに現在接続されている、利用者端末の MAC アドレスとそれに対応したベンダーコード名が一覧で表示される。1 台分が表示される場合と複数台分が表示される場合がある。もし、この欄に全く MAC アドレスが表示されない場合は、研究室に設置している HUB が故障している可能性を指摘できる。また、MAC アドレスが複数表示されていて問い合わせ対象端末の MAC アドレスが表示されていない場合は、研究室に設置した HUB への接続不良等を指摘できる。なお、ベンダーコード名はネットワークインタフェースのメーカを表しているが、おおよその端末のメーカが想像できるので、利用者端末の特定のために表示している。

(5)IP アドレスの表示

情報コンセントに接続された利用者端末の IP アドレスが表示される。IP アドレスの上にマウスを合わせると、IP アドレスを把握した日時が表示される。情報コンセントが認証ネットワークの場合は、自動取得された IP アドレスが表示される。もし、MAC アドレスは表示されていて IP アドレスが表示されていない場合は、端末の IP アドレスの設定が間違っているか、設定されていない可能性を回答できる。現在の IP アドレスが表示できない場合は、利用者端末の MAC アドレスに対応した最も最近に把握された IP アドレスと把握時刻を表示する。もし、VLAN 情報と IP アドレスが異なっている場合は、利用者端末を移設した際に IP アドレスの変更設定がなされていないことを回答できる。

(6) 認証ユーザ名の表示

情報コンセントに接続されている利用者端末が利用者認証を行った際のユーザ名が表示される。この情報から端末の利用者が把握される。上述の(1)-(5)が正常であり、ユーザ名が表示されていない場合は、利用者認証を行っていないことが回答できる。

(7) ネットワーク管理に必要な情報

そのほか、各情報コンセントが接続されているネットワーク機器及びポートを表示される。ページ上段のメニューをクリックすることでネットワーク管理に必要な情報、例えば、各情報コンセントのトラフィックやネットワーク機器のコンフィグ、ルーティング情報等が表示される。ネットワーク機器が故障した場合は、最新のコンフィグが表示される。このコンフィグを新規機器に投入し、故障機器と交換することで、迅速に障害復旧が図れる。

これら Web ページの表示内容を利用することで、ネットワークの専門家でなくても、ネットワーク利用者からの問い合わせに対して、迅速かつ適切に対応することができる。

3.3. 利用者対応での表示例

(1) IP アドレスの競合対応

利用者端末の IP アドレスが競合する場合が時々ある。経験上その多くが同じ研究室内で誤って別の端末に同じ IP アドレスを設定してしまっている場合が多い。「先輩の端末の設定を真似して設定しました」という事例等がある。こういった場合では、IP アドレスが違う情報コンセントの行に表示されているので、IP アドレスが競合している端末の設置場所と、おおよその機器の特定する情報を回答できる。

ただし、同じ研究室ではない場合も同様に競合している IP アドレスを持つ端末を発見する場合がある。例えば、利用者端末の接続申請を行わず、不正に適当な IP アドレスを設定された端末がネットワークに接続されることで、IP アドレスの競合が発生する場合がある。この場合は、不正に IP アドレスを設定した利用者は、IP アドレスが競合していると分かると、また別の IP アドレスに変更することが多いので、同じ研究室内に競合している端末がない場合は、しばらく端末の電源を入れたままにしておくと解消すると思われることを回答できる。もちろん不正に IP アドレスを設定した利用者端末が接続されている情報コンセント及び部屋を特定することができるので、別途その部屋の管理者に連絡し対応を依頼する。

(2)ループ対応

時々、誤ってネットワークにループを作ることがある。原因の多くは、研究室内で複数の HUB を用いており、乱雑な配線となっている場合などである。このような場合、次のように表示される。

a. ネットワーク運用支援システムがトラフィックの異常を監視し、ループが発生したと推定できる場合は、その情報コンセントが障害リストに表示される。

b. トラフィックの異常やデフォルトルータの IP アドレスが、本来表示されるはずのない情報コンセントの IP アドレスの欄に表示される。

c. 利用者端末のMACアドレスが、本来接続されている情報コンセントではなく別の情報コンセントに表示される。
d. ネットワーク機器によってはループガードが機能し、当該ポートはディスエーブルになるので、リンク状態が灰色で表示される。
これらのことから、ループを作っている可能性を推測し回答できる。

(3) ネットワーク工事への対応

ネットワーク工事を行う場合には、情報コンセントの位置を確認、情報コンセント番号を割当、情報コンセントを接続するネットワーク機器とそのポートを割当、該当ポートのサブネットやVLAN設定等を行い、工事担当者、工事業者に指示する必要がある。これらの情報はネットワーク運用支援システムに表示されているので、この表示内容から指示書を迅速に作成し、新たに登録するができる。

4. 利用者への対応状況

山口大学において平成22年4月以降（ただし、医学系キャンパスにおいては平成22年7月以降)、記録に残っているネットワークに関する利用者からの問い合わせは以下のもの等があった。問い合わせ件数等を表2に示した。

(1) 利用者端末のIPアドレス等の設定ミス
情報コンセントに設定されているVLANやサブネットと利用者端末のIPアドレスの間違いを含む
耐震改修工事による研究室の移転や年度更新での利用者端末の利用者変更の際に多い
(2) ループ障害
乱雑配線、知識不足による不注意や無意識にループを作ってしまう場合が多い
(3) IPアドレスの競合
多くの場合、同じ研究室の他の利用者の場合が多い
(4) ネットワーク接続確認
(5) ケーブル抜け・ケーブルの断線
(6) 研究室等に設置しているHUBの障害

これら問い合わせの多くは、研究室内に原因があるものであった。これらの問い合わせは身近な人で対応できる場合を除いて、ほぼすべてがメディア基盤センターの窓口に寄せられる。研究室内に原因のある問い合わせであっても、原因がネットワークになるのか、または研究室内にあるのかの切り分けを行い、対応方法について、案内することができている。

問い合わせの多くは、学期の初め等に集中しているが、

表2　ネットワーク利用者からの問い合わせ状況

問い合わせ状況	件数
利用者端末のＩＰアドレス等の設定ミス（VLAN間違い含む）	74
ループ障害	24
IPアドレスの競合	19
ネットワーク接続確認	43
ケーブル抜け・ケーブルの断線	16
研究室等に設置しているHUBの障害	17
ネットワーク機器の故障（無線AP）含む	19
ウイルス感染	20
DHCP割り当てアドレス枯渇	6
無線LANでの接続アクセスポイントの確認	8
その他	10
計	256

各キャンパスともに窓口担当者（技術職員1名、及び技術補佐員1名、1キャンパスのみ技術補佐員1名）によって迅速に対応できている。窓口担当者で対応できない若干の問い合わせは、ネットワーク担当者が対応している。

利用者からのネットワークに関する問い合わせではないが、次のようなネットワークの障害対応及び調査等に本システムを用いる場合もある。
(1) 論理ネットワーク設定変更、ネットワーク機器の設定状況の確認と変更など（28件）
(2) ネットワーク工事の際の新規配線計画策定（14件）
(3) ネットワーク機器の障害対応
(4) ウイルス感染端末の利用場所の特定
(5) 不正アクセスや不正利用端末の調査

5. まとめ

ネットワーク管理及び、ネットワーク利用者支援のために運用しているネットワーク運用支援システムについて特にネットワーク利用者対応機能について述べた。本システムの導入以降、本システムを用いることで、ネットワーク利用者からの問い合わせの多くは、若干名の窓口担当者で迅速に対応できる状況にある。

さらに、ネットワーク障害時の対応についても、本システムが提供する情報（障害情報、最新コンフィグ等）を用いて、窓口担当者により迅速にネットワークの復旧が図れている。

山口大学ネットワークへ本ネットワーク運用支援システムを適応した場合について述べたが、ネットワーク情報の取得方法や表示情報の活用方法は一般的なものを用いており、他のネットワークへも柔軟に適応することが

できる。

最近では、学生や教職員の中でスマートフォン利用者や、その利用シーンが増加しており、より安定した無線LAN環境と利用者対応が求められている。そのため、ネットワーク利用者支援が今後重要になってくることが予測され、ネットワーク運用支援システムのサポートがより一層期待される。

しかし、稼働中の利用者端末が増加するとネットワーク運用支援システムのレスポンスが低下する事があり、電話対応の際、利用者を待たせる場合が生じる。また、バッチ処理のみで収集している情報について、最新の情報を必要とする場合があり、バッチ処理で取得した情報だけでは不十分な場合もある。そのため、サーバ構成の見直しや性能改善が必要である。

ネットワーク利用者にとってネットワークは、どのようにネットワークが構成されているかは関係なく、部屋に設置された情報コンセントがネットワークの出入り口としてあるのみである。実際、山口大学では各部屋以外のネットワーク機器は一元管理しており、ネットワーク利用者はどのように構成されているのか把握されていない状況にある。ネットワークを構成する全ネットワーク機器および全情報コンセントとそれらを接続する配線、つまりネットワーク全体を一つの仮想的なネットワーク装置に、情報コンセントをその入出力ポートに捉えることができる。本ネットワーク運用支援システムは、各ネットワーク機器の情報を集めてきて、利用者とのインタフェースである情報コンセントに関する情報に集約し直していることから、ネットワーク全体を一つの論理的なネットワーク装置に仮想化している。

ネットワークを一元的に運用するために必要なネットワーク管理機能の他、利用者対応機能等を有している本ネットワーク運用支援システムの運用を通じて、ネットワーク利用者からの問い合わせに対する対応という観点で本システムの有用性を示した。

謝辞

ネットワーク運用・窓口に関して日々対応いただいている、山口大学大学情報機構メディア基盤センターのスタッフの皆さんに感謝する。

参考文献

[1] 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)

[2] 森山京平, 飯田 隆義, 藤田俊輔 , 吉田和幸, イーサネットワーク構成情報管理のためのExcelファイル自動作成について, 情報処理学会研究報告インターネットと運用技術 (IOT) , 2010-IOT-8(4), 1-6 (2010)

[3] 川崎敏行, 和﨑克己, ネットワークサービスの可視化を主眼に置いた戦略的監視手法の提案, 研究報告インターネットと運用技術(IOT), 2010-IOT-8(15), 1-6 (2010)

[4] 佐々木正人, 斎藤卓也, 石黒克也, 豊永昌彦, 高知大学総合情報システムの監視と利用者動向, 学術情報処理研究 No.14, pp.64-71 (2010)

[5] 吉澤政洋, 沖田英樹, 上原敬太郎, 垂井俊明, 仮想ネットワークに関する文書作成を支援するネットワーク管理システムの実装および評価, 情報処理学会論文誌, 52(3), 1334-1347 (2011)

[6] 上田浩, 井田寿朗, 青木正文, 齋藤貴英, 酒井秀晃, 伊比正行, 高橋仁, 船田博, 矢島正勝, 久米原栄, キャンパス内光直収ネットワークの構築と運用, 学術情報処理研究 No.14, pp.56-63 (2010)

[7] 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)

無線AP配置の適正化による電波利用率の向上

Improved utilization of wireless lan by planning the placement of wireless access points

本村真一†, 木本雅也†, 大野賢一†

Shin-ichi Motomura†, Masaya Kimoto†, Ken-ichi Ohno†

motomura@tottori-u.ac.jp, kimoto@tottori-u.ac.jp, ohno@tottori-u.ac.jp

鳥取大学総合メディア基盤センター†
Information Media Center, Tottori University†

概要

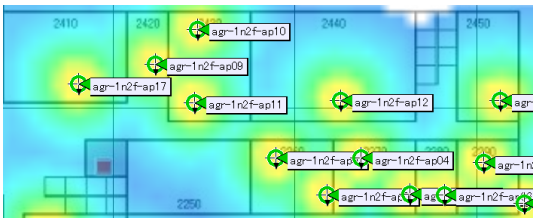
スマートフォンや iPad に代表されるタブレット型端末の登場で、鳥取大学においても無線 LAN の需要が増大している。この需要を満たすため、既存の無線 AP を再配置することで無線 LAN のカバレッジエリアの拡大を検討している。無線 AP の再配置には、配置前のシミュレーションの実行だけでなく、配置後にサイトサーベイを実施し、シミュレーション結果との比較を元に再設置箇所を検討する必要がある。本取り組みでは、シミュレーションの精度を向上させるため、配線工事を伴わない範囲で無線 AP の配置を見直した。再配置と同様に、本取り組みでもシミュレーションとサイトサーベイの結果を比較している。使用したシミュレーションソフトウェア、AirMagnet Planner は 2 次元平面を対象としおり、各階に設置した無線 AP だけを対象としたサイトサーベイの結果と比較すると、適切にシミュレーショ ンができることが分かった。しかしながら、実際には上下階に設置した無線 AP からの電波が大きく影響するため、作業者による予測にてこの問題に対処した。 本作業による知見はそのまま再配置作業に適用できるため、有益な結果が得ら れたと考えている。

キーワード

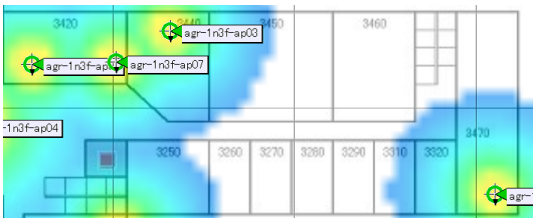
無線 LAN，電波サーベイ，無線 LAN プランニング

1 はじめに

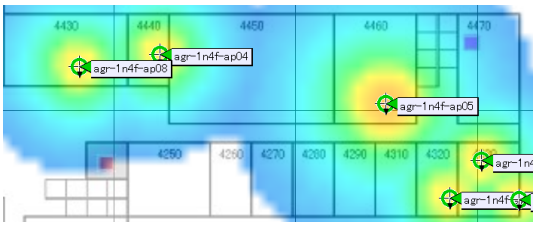
鳥取大学では、基本的に全ての学生にパーソナルコンピュータ（以下、「PC」という。）を講義時に持参するよう義務付けている。そのため、鳥取大学では教育用情報ネットワークと呼ぶ、有線 LAN と無線 LAN を全学的に整備している。講義室の多くは、講義において PC を活用できるように、卓上に有線 LAN の情報コンセントと電源タップを配置している。また、学生が PC を活用できるように、学部校舎や図書館のみならず学内の多くの箇所で無線 LAN の提供を行っている。鳥取大学では、学生数 6,500 名程度に対して 300 台程度の無線 LAN アクセスポイント（以下、「無線 AP」という。）を配置している。これは、一台の無線 AP で 20〜30 程度の無線 LAN 子機が利用できることを考えると、単純計算では全学生分の無線 LAN の同時接続がまかなえる台数である。しかしながら、実際には学生活動を広範囲に支えられるようには無線 LAN の提供ができていない。実のところ、これらのネットワークの整備は鳥取大学総合メディア基盤センター（以下、「センター」という。）ではなく、教育を担当する部署で 2002 年から整備されたものである。これが近年の大学運営の効率化に伴い、鳥取大学においてもネットワーク管理の一元化が行われることになり、2010 年度からこれらのネットワークもセンターに運用・管理、整備の役割が移譲された。センターにて教育用情報ネットワークの管理を行う



(a) 2F の設置状況



(b) 3F の設置状況



(c) 4F の設置状況

図- 1: 農学部 1 号館北東位置の無線 AP 設置状況

ことになった際、無線 LAN については次の点の調査を行った。

1. 無線 LAN の接続方法（セキュリティ管理）
2. 無線 AP 設置個所の適正性

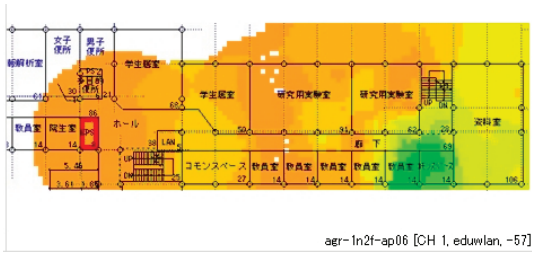
無線 LAN の接続方法については、それまで WEP-PSK を用いて無線 LAN を接続し、その後 VPN ソフトウェアを用いる方式であった。VPN 接続は IPSec トンネリングによる暗号化と、ユーザ名とパスワードの認証を行うため、WEP-PSK であっても十分なセキュリティを確保していたが、VPN ソフトウェアの配布管理に関する問題や、クライアント OS の多様性への対応が難しいという問題があった。そこでセンターでは、無線 LAN の接続方法を WPA2-PEAP に改めた。学内からは、接続方法がより簡易になるよう、WPA2-PSK と WEB 認証を組み合わせた方式の希望もあった。これは、WPA2-PSK により無線 LAN 子機の認証と暗号化を行い、その後 Web やメール等の IP サービスを利用する際には、ブラウザを用いてアカウントによる個人認証を行う Web 認証と組み合わせた方式である。しかしながら、PSK を用いた方式は PSK の更新管理の問題があることと、無線 LAN の暗号化に用いている一時鍵交換時の 4 ハンドシェイクを傍受することで、無線 LAN の盗聴や不正侵入が可能になることから、全学生を対象とした無線 LAN の接続方法には不向きであると判断した。

次に、無線 AP の設置個所の適正性を判断するために、無線 LAN のカバレッジエリア及び各無線 AP の同時接続数の調査を行った。本学の無線 AP は Cisco 社製 Aironet シリーズを使用し、Cisco 社製 Cisco Wiress Control System[1]（以下、「WCS」という。）を用いて管理しているため、本調査については WCS の機能を用いて行った。カバレッジエリアとしては、全校舎の 1/3 程度のカバー率であったが、無線 LAN の提供を希望する学部を優先的に整備を進めていたことから、学生から提供範囲についての不満は少なかった。無線 AP の同時接続数についても、 1 箇所を除き同時接続数 20 を上回る個所はなかった。

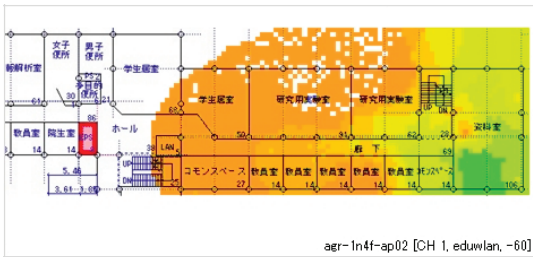
上記調査結果から、無線 AP の配置については一見問題ないように見えるが、本調査を通して実際にはいくつかの問題があることが分かった。図 1(a) は 2011 年 4 月の本学農学部 1 号館 2 階北東位置の無線 AP の設置状況を示している。この図の丸印及び吹き出しが無線 AP を示しているが、図の左上及び右下の方には無線 AP が多く設置されていることが分かる。図 1 の建物サイズが約横 38m ×縦 13m であることから、無線 AP が電波干渉を起こすほど密集していることが分かる。実際、無線 AP が近くにあるにも関わらず、無線 LAN の接続に支障がある旨報告を受けたこともあった。

IEEE 802.11b 及び IEEE 802.11g（以下、「IEEE 802.11b/g」という。）で使用する 2.4GHz 帯では最大 4 チャネルしか使用できない。さらにはチャネル 14 は日本でのみ利用できるため、多様な無線 LAN 子機に対応することを考えると、チャネル 14 を除いたチャネル 1 〜13 で運用するほうが望ましい。その場合、干渉を避けるためには、使用するチャネルの前後 2 チャネルの使用を避ける必要があるため、最大 3 チャネルで運用することとなる。本学の無線 AP は、IEEE802.11b/g だけでなく、5GHz 帯の電波を用いた IEEE 802.11a も提供しているが、学生が利用する PC に搭載されている無線 LAN 子機によっては、IEEE802.11b/g にのみ対応していることも多い。そのため、無線 LAN の設計としては IEEE 802.11b/g が利用できることを前提に考える必要がある。

また、本学の Aironet は Lightweight と呼ばれるモードで運用しているため、無線 AP 同士の電波が干渉しないように自動的に電波出力を下げる機能がある。そのため、無線 LAN のカバレッジエリアが小さくなり、無線 AP の個数に対して電波の提供効率が悪い状態であった。本無線 LAN システムを構築した他部署においても、無計画に導入したわけではないと考えられるが、



(a) 2F の無線 AP からの電波



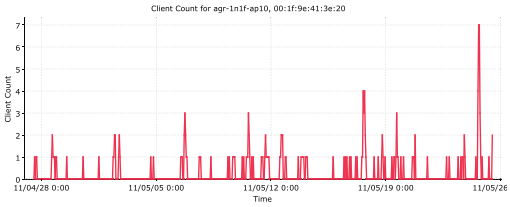
(b) 4F の無線 AP からの電波

図- 2: 農学部 1 号館 3 階における上下階の無線 AP の影響について

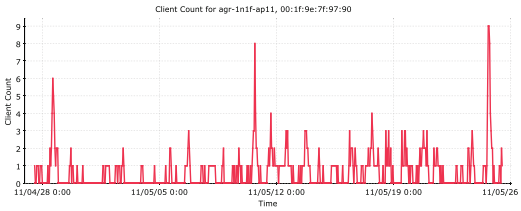
構築後の調査においてこのような不適切な状況が発見できるということは、それだけ無線 LAN の導入計画の立案が難しいことを示していると考えられる。

上述の理由から、無線 AP の配置を見直す必要性があることが分かったが、他にもその必要性が生じており、全学的に無線 LAN の利用が活発になっていることがあげられる。おそらく他大学も同様だと考えられるが、スマートフォンや iPad に代表されるタブレット端末の利用が活発になっていることが原因であると思われる。これは、情報端末や通信セキュリティに制限のある企業に比べて、研究や教育活動の多様化を支持する大学においては特に顕著だと思われる。これらの端末では無線 LAN が必須であり、そのため各研究室などで独自に無線 AP を設置する傾向にある。カバレッジエリアを考慮することなく無線 AP を設置することから、電波環境を悪化させるだけでなく、無線 LAN のセキュリティについても管理を難しくしている。そのため、これまでは学生向けに提供していた無線 LAN を教職員向けにも提供し、独自の無線 AP を不要とする対策が必要だと考えているが、無線 AP の数を単純に増やすことは経費の観点から難しい。そこで、無線 AP の電波出力を最大限大きくできるように再配置を行うことで、既存の無線 AP を使ってカバレッジエリアの拡大を図ることとした。

無線 AP の再配置は、どこに何台無線 AP を設置すれば良いかシミュレーションを行うことになる。無線 AP の配置にはカバレッジエリア以外にも、無線 LAN 子機の最大同時接続の問題もある。そのため、再配置については次のステップで検討を行うこととなる。



(a) agr-1n2f-ap10

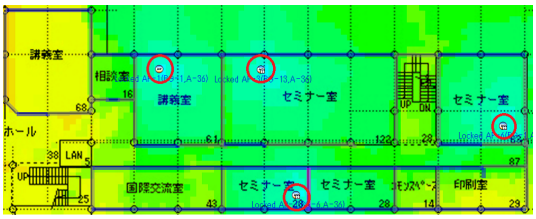


(b) agr-1n2f-ap11

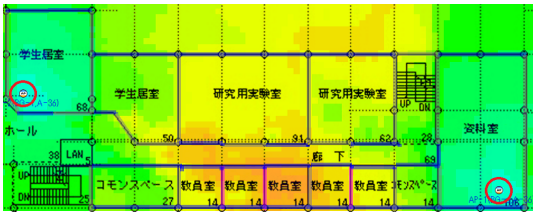
図- 3: 農学部 1 号館北東位置の無線 AP 毎の同時接続数

1. カバレッジエリアの各範囲における無線 LAN 子機の同時接続数を把握する
2. 無線 LAN のプランニングツールを用いて電波シミュレーションを行う

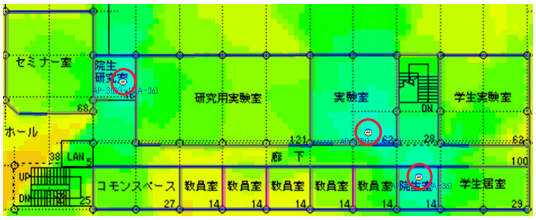
しかしながら、電波シミュレーションを正確に行うにはレイアウト図面の作成のみならず、壁や扉などによる電波減衰特性の正確な入力を必要とする。その他、各部屋に設置されている棚等の物体も実際の電波の伝搬に影響を与えるため、本来はシミュレーション時にデータとして与える必要がある。また、多くのシミュレーションソフトウェアは 2 次元空間を設計対象としているが、本学の建物においては上下 1 階分については高い電波の透過性があるため、2 次元のシミュレーションだけでは十分に対応できない。図 2(a)、2(b) は農学部 1 号館 3 階北東位置において、FLUKE networks 社製 AirMagnet Survey Pro[2] を用いて無線 LAN の電波を調査（以下、「サイトサーベイ」という。）した結果の抜粋である。ともに図の右下に位置する部屋において、2 階もしくは 4 階に設置された無線 AP から-60dB 前後の信号強度が検出されている。Cisco 社の資料 [3] によれば、-65〜-70dB で安定した無線 LAN 接続が保たれる旨記述があるが、実際の利用環境では-65dB 以上の信号強度が必要だと感じている。この違いは、無線 LAN 子機の性能の違いなどの理由が考えられるが、いずれにしろ十分に無線 LAN が利用できる信号強度であるとともに、電波干渉の点からも無視することはできない。無線 AP のアンテナを工夫することで、上下階に対して電波が透過しないよう対策を講ずる方法も考えられるが、



(a) 2F のシミュレーション結果 (無線 AP を 8 台削減)

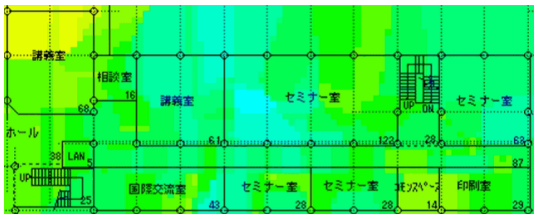


(b) 3F のシミュレーション結果 (無線 AP を 2 台削減)

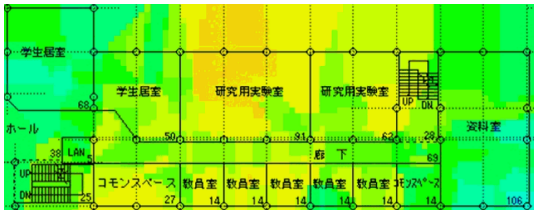


(c) 4F のシミュレーション結果 (無線 AP を 3 台削減)

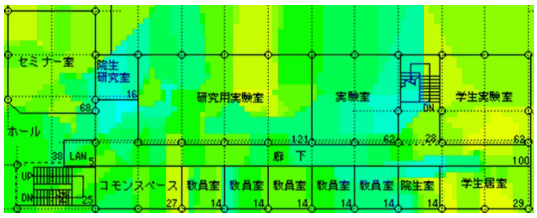
図- 4: 農学部 1 号館北東位置の無線 AP 配置シミュレーション結果



(a) 2F のサイトサーベイの結果



(b) 3F のサイトサーベイの結果



(c) 4F のサイトサーベイの結果

図- 5: 農学部 1 号館北東位置における各階の無線 AP だけを対象としたサイトサーベイの結果

ここでは無線 LAN のカバレッジエリアを広げることを目的としていることから、上下階への伝搬についても積極的に活用することとした。

上述のように、無線 AP の再配置はソフトウェアによるシミュレーションだけでは十分に対応できない。そこで、再配置前のサイトサーベイとシミュレーションの結果を比べることでその差異を学習し、再配置設計にフィードバックすることで対応することを検討している。

なお、配線工事が必要な無線 AP の再配置は 2011 年度中の実施を予定している。この度の取り組みでは、適切なシミュレーション結果が得られるように配線工事を伴わない作業、つまり無線 AP の間引き行う。本取り組みにおいても再配置と同様に下記の一連の作業を必要とすることから、その知見はそのまま再配置設計に生かせると考えている。

1. 無線 LAN 子機の同時接続数の把握
2. 作業前のサイトサーベイ
3. 作業後のサイトサーベイとシミュレーションの結果比較

2 無線 AP の配置の見直し

カバレッジエリアを拡大するために、無線 AP を再配置して無線 AP の電波効率を向上させることを目的とし、そのために既設の無線 AP におけるサイトサーベイとシミュレーションの結果を比較することとした。しかしながら、既設の無線 AP が隣接しすぎているため各無線 AP の電波出力が小さくなっている。この条件のシミュレーション結果と比較しても、適正な配置時の電波出力とは大きく異なっているため電波の到達範囲の予測が難しく、有益なフィードバックが得られない。そこで、本取り組みでは既設の無線 AP を適切に取り外し、シミュレーションの精度を向上させることを目的とする。

2.1 無線 AP 設置個所の判定

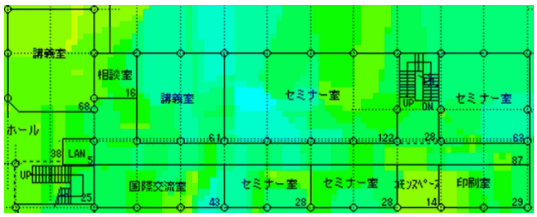
無線 AP の設置個所を検討する際、最初に行うのは無線 LAN を利用する環境で無線 LAN 子機の同時接続数を満たす無線 AP の台数を把握することである。当初は、各部屋の人数や講義時の受講者数をカウントす

ることで簡単に把握できると考えたが、実のところ講義室については様々な講義が行われるため、無線 LAN の利用者数を把握している部署はなかった。そのため、多くの場所では WCS の機能を用いて同時接続数のカウントを行った。図 1(a) の左上の講義室には 2 台の無線 AP、agr-1n2f-ap10 及び agr-1n2f-ap11 が設置されている。これらの無線 AP の 2011 年 4 月末から 5 月末にかけての同時接続数を図 3(a)、3(b) に示す。これらの図から、当該箇所の最大同時接続数は 16 であることが分かり、カバレッジエリアについて考慮しなければ、必要な無線 AP の台数は 1 台であることが分かる。最大同時接続数から各部屋に設置すべき無線 AP の台数を判断することになるが、本論文で対象としている農学部 1 号館北東位置、図 1(a)、1(b)、1(c) における最大同時接続数は前述の 16 であり、各部屋に 2 台以上無線 AP が必要な個所はなかった。

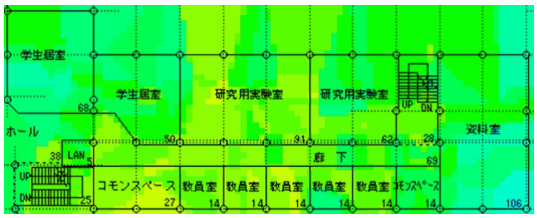
また、図 2(a)、2(b) にて示したように、事前に実施したサイトサーベイの結果から各無線 AP の電波到達範囲が把握できる。これらの情報を元に無線 AP を設置する箇所を判断しシミュレーションを行うわけだが、この度利用するシミュレーションソフトウェア、FLUKE networks 社製 AirManget Planner[4] は 2 次元にしか対応していない。そのため、上下階に設置された無線 AP の電波についてはシミュレーション結果に反映させることはできないが、先に示したように大きく影響を与える。この点については作業者の予測により対応することとする。例えば、先の図 1(a)、1(b)、1(c) においては、それぞれ階の右下の部屋に無線 AP が設置されていたが、3 階にだけ無線 AP を設置することで、2 階と 4 階の同一箇所においても無線 LAN が利用できることが予測できる。

2.2 サイトサーベイとシミュレーション結果の比較

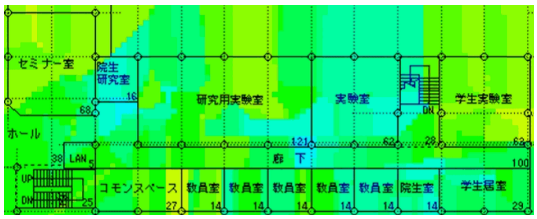
図 4(a)、4(b)、4(c) に農学部 1 号館北東位置の 2 階から 4 階のシミュレーション結果を示す。図中の丸印が無線 AP であり、2 階は 12 台の無線 AP を 4 台へ、3 階は 4 台を 2 台へ、4 階は 6 台を 3 台へ削減している。シミュレーションにおける壁や扉の減衰特性は、AirMagnet Planner の標準値を利用しており、コンクリート壁は 12dB、石膏ボード壁は 4dB、ガラス扉は 2dB としている。このシミュレーションの妥当性をサイトサーベイの結果により判断するため、図 5(a)、5(b)、5(c) に、無線 AP を取り外した後の農学部 1 号館北東位置における、各階の無線 AP だけを対象としたサイトサーベイの結果を示す。図 4 と図 5 を比較してみると、シミュレーションとサイトサーベイの結果は相似している。サイトサーベイの結果は、シミュレーション結果に比べて概ね強い



(a) 2F のサイトサーベイの結果



(b) 3F のサイトサーベイの結果



(c) 4F のサイトサーベイの結果

図- 6: 農学部 1 号館北東位置におけるサイトサーベイの結果

受信強度を示している。このことから、壁材等による電波減衰を増加させてシミュレーションを行う必要があることが分かる。

本シミュレーションでは、上下階に設置された無線 AP の電波については考慮されていないため、シミュレーション結果においていくつかのカバレッジホールが存在していた。これは、図 4(a) の右下の部屋や図 4(b) の中央下辺りの部屋が該当する。

検討した配置は、このようなカバレッジホールを生じないように予測したものである。全ての無線 AP の電波を受信したサイトサーベイの結果を図 6(a)、6(b)、6(c) に示す。これらの図から、懸念していたカバレッジホールが存在しないことが分かる。

3 おわりに

無線 AP の配置が適切でないため、電波干渉の発生や、電波干渉を避けるために電波出力を下げている無線 AP があった。増える無線 LAN の需要を満たすため、このような無線 AP の再配置を行うことでカバレッジエ

リアの拡大を計画した。無線 AP の再配置には、配置前のシミュレーションの実行だけでなく、配置後のサイトサーベイの結果と比較し、そのフィードバックを配置の検討に生かす必要があると考えている。本取り組みでは、シミュレーションを円滑に実行できるように、配線工事を伴わない範囲で無線 AP の配置を見直した。再配置と同様に、本取り組みでもシミュレーションとサイトサーベイの結果を比較している。本取り組みで使用したシミュレーションソフトウェア、AirMagnet Planner は 2 次元平面を対象としおり、各階に設置した無線 AP だけを対象としたサイトサーベイの結果と比較すると、適切にシミュレーションができることが分かった。しかしながら、実際には上下階に設置した無線 AP からの電波が大きく影響するため、作業者による予測にてこの問題に対処した。本作業による知見はそのまま再配置作業に適用できるため、有益な結果が得られたと考えている。

本取り組みにおいても、3 次元空間における電波状況の把握が重要であった。AirMagnet Planner は 2 次元空間を対象としたシミュレーションソフトウェアであったが、3 次元空間を対象としたシミュレーションソフトウェア [5] も存在している。また、3 次元空間を対象としたシミュレーションに関する研究 [6] も行われている。2 次元空間におけるシミュレーションに比べて、より多くの、またより正確なデータが必要となるが、利用を検討する価値があると思われる。また、無線 AP の更新が可能な環境においては、メルー・ネットワークス社の製品のように、単一チャネルで無線 LAN を構築できる製品の活用も有効な手段であると考えられる。

謝辞 本論文にて使用しているサーベイ及び図は、鳥取大学大学院農学研究科五藤由香理氏と中川卓也氏に測定、整形を協力いただきました。ここに感謝の意を表します。

参考文献

[1] Cisco wireless control system . http://www.cisco.com/web/JP/product/hs/wireless/wcs/index.html, 2011/07/24 11:05.

[2] Airmagnet survey . http://www.flukenetworks.com/enterprise-network/wireless-network/AirMagnet-Survey, 2011/07/24 11:05.

[3] Aironet ワイヤレス lan の安定接続要件 . http://www.cisco.com/JP/support/public/loc/tac/100/1006244/wiress.shtml, 2011/07/24 11:05.

[4] Airmagnet planner . http://www.flukenetworks.com/enterprise-network/wireless-network/AirMagnet-Planner, 2011/07/24 11:05.

[5] Radio area viewer qualitymeister3d. www.ntt-at.co.jp/product/quality/, 2011/07/24 11:05.

[6] 日比学, 菅澤祐子, 宇都宮隆介. 医療現場の無線 lan 構築における 3 次元伝搬シミュレーション. 日本生体医工学会専門別研究会　医療・福祉における電磁環境研究会　平成 22 年度第 3 回研究会資料, pp. 9–12, 2010.

教育用パソコンのネットワークブート起動時間に影響を与える要因の評価

An Evaluation of Factors Affecting the Boot-Up Time of PXE Boot Terminals for Education.

浜元 信州 †, 三河 賢治 †, 青山 茂義 †

Nobukuni HAMAMOTO†, Kenji MIKAWA†, Shigeyoshi AOYAMA†

hamamoto@cais.niigata-u.ac.jp

新潟大学 情報基盤センター †
Center for Academic Information Service, Niigata University †

概要

新潟大学では，平成 19 年 1 月に教育用コンピュータシステムを更改し，これまでのローカルブート形式の教育用パソコンから，ハードディスクを搭載しない，ネットワークブート形式の教育用パソコンに転換した．本システムの導入当初は教育用パソコンの起動時間が安定せず，これまでに様々な対策を講じてきた．このようなネットワークブート形式のシステムでは，教育用パソコンの起動時間に影響を与える要因を特定することが非常に難しく，ポイントのはずれた対策は莫大な時間とコストを浪費するだけである．新潟大学では，教育用パソコンの起動時間の短縮に効果的な要因を探るため，ネットワークブートサーバのハードディスク性能とネットワーク帯域を変更し，複数の組合せに対して教育用パソコンの起動時間を計測した．その結果，起動時間には，ネットワーク帯域の増強が大きく影響し，ハードディスク性能は大きく影響しないことが分かった．本論文で上記の実験結果を報告する．

キーワード

教育用コンピュータシステム，ネットワークブート，起動試験

Abstract

The educational computer system of Niigata university was replaced on January 2007 where diskless network boot terminals based on preboot excution environment (PXE) boot are introduced for the educational computers. However, the terminals boots much slower than the local boot termials which boot from local HDD. We tuned the network wiring and the settings of the network boot terminals and add new boot servers to boot the terminals faster. It is very diffecult to find suitble parameters affecting boot-up time of the network boot terminals because the parameters are differnet from that in the local boot terminals. To find the factors for faster boot of the terminals, we measured the boot-up time of the terminals by changing network bandwidthes, HDD drives of the boot servers and boot cache. We find the bandwidth of the network strongly affects the boot-up time. On the other hand, the boot-up time do not seriously changed by replacing the HDD and boot cache. In this paper, we describe the details of the result of our experiment.

Keywords

Computer system for university education, PXE boot system, experiment on boot-up terminals

1 はじめに

パソコンの起動方法には，内蔵ハードディスクから起動する一般的なローカルブート形式と，ディスクイメージを外部のサーバ上で管理して，パソコンの起動に合わせてディスクイメージを配信するネットワークブート形式がある．ネットワークブート形式では，パソコンに搭載するオペレーティングシステムやアプリケーションソフトウェアのハードディスクイメージをネットワークブートサーバ上で管理し，パソコンの起動に合わせて，ネットワークブートサーバからディスクイメージを配信し，パソコンが利用できるようになる．この形式では，ディスクイメージ全体を配信せず，必要なディスクイメージをパソコンのメモリ上に展開することができる．このため，パソコンにハードディスクを搭載しない運用とディスクイメージを一元的に管理する運用が可能となり，導入コストや管理コストの削減に対する意識の高まりと相まって，多くの企業，教育機関でハードディスクを搭載しないネットワークブート形式のパソコンの導入が相次いだ．[1, 3, 4]

新潟大学は，本州日本海側ではじめて政令指定都市となった新潟市に立地している．また，新潟大学は，市内にほとんど同規模の本部を含む文理系キャンパスと医歯学系キャンパスを有し，9 学部，7 大学院，2 研究所，1 総合病院から構成される総合大学であり，学生総数 12,676 人，教職員総数 2,265 人が在籍している．情報基盤センターは，新潟大学の教育用コンピュータシステム，基盤ネットワークシステムを管理，運用する責任部局であり，教育用コンピュータシステムについて，その導入から管理，運用を担当している．各キャンパスには，それぞれ 461 台，172 台の教育用パソコンが配置されており，毎日 1,000 人以上の学生，教職員が情報リテラシー教育や研究に利用している．

新潟大学では，平成 19 年 1 月に教育用コンピュータシステムを更改し，これまでのローカルブート形式の教育用パソコンから，ハードディスクを搭載しないネットワークブート形式の教育用パソコンに転換した．本学の教育用コンピュータシステムの構成は，各キャンパスの情報系サーバ室に，ユーザ認証用サーバ，ファイルサーバ（文理系キャンパスに集約），印刷サーバ，ネットワークブート用の管理サーバ，ブートサーバ等を配置し，附属図書館，学務部，その他の主要な部局等に対して，教育用パソコン実習室を 15 教室，合計 633 台の教育用パソコンを展開した．本システム導入後，教育用パソコンのオペレーティングシステムやアプリケーションソフトウェアのハードディスクのイメージを情報基盤センターで一元的に管理することが可能となった．また，教育用パソコンを運用するための基幹サーバを情報系サーバ室に集約したことにより，サーバ機器のメンテナンス性が向上し，現在も教育用システム管理者の負担軽減に大きく貢献している．

しかしながら，本システムの導入直後は，教育用パソコンの起動時間が安定せず，100 台以上の一斉起動に対して，全く起動できない端末，利用の途中で動作を停止してしまう端末，アプリケーションソフトウェアの動作が非常に重たい端末が少なからず見受けられた．この点に関して，情報基盤センターでは，

---

(1) すべての教育用パソコンに対して，512MB から 1GB にメモリを増設

(2) 一部の教育用パソコンに対して，内蔵ハードディスクを搭載

(3) ネットワークブートサーバを増設

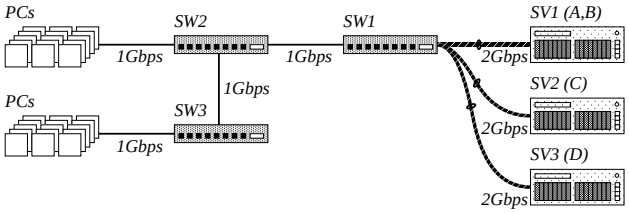
(4) ネットワークブートサーバに対して，教育用パソコンの割り付けを変更

等の対策を行い，現在では，安定して教育用パソコンを運用している．一方で，新潟大学と同様のネットワークブート形式の教育用パソコンを導入している他大学の教育用システムと比較して，本学の教育用パソコンの起動時間は多少なりとも時間を要しているようであった．教育用パソコン単体の性能の向上，ブートサーバの増設，教育用パソコンの割り付けの調整によって起動時間が短縮することは，上記の対策時に評価している．今回，ネットワークブートサーバを何種類か準備して，教育用端末の起動時間を計測する機会を得たので，ネットワークブートサーバのハードディスク構成とネットワークの帯域を変更し，これらの組合せが教育用パソコンの起動時間にどのような影響を与えるか実験を行った．

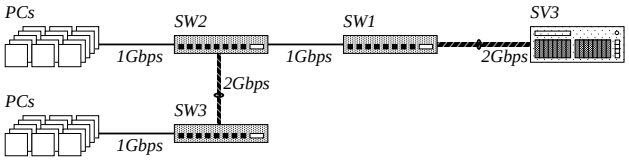
2 試験環境

教育用パソコンの起動試験に用いたネットワーク構成とサーバ機器等の配置の概要を図 1 に示す．これらの試験環境は，情報基盤センターのサーバ室で構築し，端末は情報基盤センターの実習室に設置してあるものを既存の配線を流用し接続している．図中の SV1，SV2，SV3 で示したネットワークブートサーバは，ヒューレットパッカード社製 Proliant DL160G6 を用いた．ネットワークブートサーバの構成を表 1 に示す．今回の起動試験では，SV1，SV2，SV3 ともに同一の CPU，同容量のメモリを搭載した．

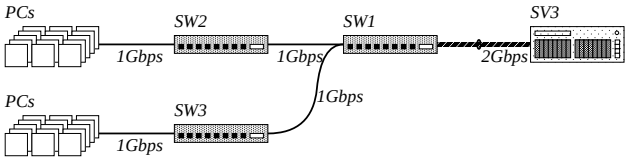
ブートサーバのハードディスク性能が端末の起動時間に与える影響について，文献 [2] で詳しい評価が行われた．文献では，SSD をブートサーバに搭載することに



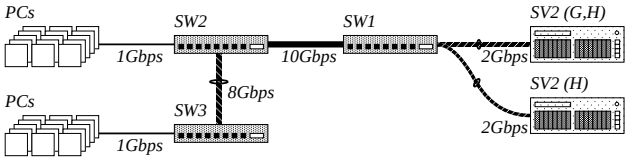
(a) 試験環境 A，B，C，D の場合



(b) 試験環境 E の場合



(c) 試験環境 F の場合



(d) 試験環境 G，H の場合

図 - 1: 端末起動試験の試験環境（ネットワーク構成とサーバ機器等の配置）.

よって，端末の起動時間が短縮される，との結論を得た．また，福岡大学では，ブートサーバに SSD を搭載した教育用システムが稼働している [1]．SSD は高価な製品であるため，残念ながら，今回の起動試験で SSD を用意することができず，SSD を用いた起動試験を見送ることとなった．また，ネットワークブート用ソフトウェアは，シトリクス社製 Provisioning Server（PVS）を用いた．また，パソコンは，複数台のデル社製 Optiplex GX620（スモールファクタ）を用いた（図中，PC）．起動試験に用いたパソコンの構成を表 2 に示す．

起動試験は，レイヤ 2 スイッチ間のネットワーク帯域，ネットワークブートサーバのハードディスク構成，ディスクキャッシュの有無，ネットワークブート用ソフトウェアの組合せを変更して行った．試験環境の詳細を表 3 に示す．表中，ネットワークブート用ソフトウェアのバージョンを変更して起動試験を行った環境があるが，これは，試験環境 G と H の環境を整備した時期に同じバージョンのネットワークブート用ソフトウェアを用意できなかったためである．したがって，試験環境 A から F と，試験環境 G，H では，起動試験を行った時期が異なっていることに注意されたい．表中のディスクキャッシュについて，本試験で用いた PVS は，ディスクイメージとの差分（ユーザがパソコンを利用することによって生成されたテンポラリ領域の一時ファイル等）をパソコン側もしくはブートサーバ側の内蔵ハードディスクに保存する機能を持つ（これをディスクキャッシュ機能とよぶ）．パソコン側でキャッシュする場合は，ネットワークブートサーバから配信されるディスクイメージとの差分をパソコンの内蔵ハードディスクにキャッシュし，サーバ側でキャッシュする場合は，ディスクイメージとの差分をブートサーバの内蔵ハードディスクにキャッシュする．

図 1 のネットワーク機器について，SW1 はアラクサラ社製 AX3630S-24T2X である．SW2 と SW3 は試験環境によって機種が異なり，試験環境 A から F まででは，SW2 はアラクサラ社製 AX2430S-48T，SW3 はアラクサラ社製 AX2430S-24T を用いた．試験環境 G，H では，SW2 は 10Gbps のインタフェースが接続可能な，AX2430S-24T2X，SW3 は，AX2430S-48T を用いた．どちらもワイヤスピードでレイヤ 2 スイッチングが可能なネットワーク機器である．

2.1 起動時間の測定

起動時間の測定は，各端末に自動ログインするよう設定し，ブートサーバから端末に対して電源投入を指示した時刻と，各端末がファイルサーバ上の領域をマウントした時刻を計測し，両者の差を端末の起動時間とした．ログイン画面が表示されるまでの時間ではないので注意されたい．

各端末は Wake on LAN 機能に対応し，PVS はマジックパケット送信機能を有している．そこで，ブートサーバから端末に電源投入を指示した時刻は，PVS のマジックパケットを一斉に送信する機能を利用し，ブートサーバからマジックパケットの送信を指示した時刻とした．端末に対してマジックパケットの送信を指示すると，ブートサーバは全端末に対してマジックパケットを送信するのであるが，全端末に同時に送信しているわけではないので，本試験では，マジックパケットの送信を指示した時刻を基準とした．

一回の端末の起動時間の測定方法は，起動時間の最も短い端末の起動時間と，起動時間の最も長い端末の起動

表 - 1: ネットワークブートサーバの構成一覧．全てのサーバについて，CPU 型番はインテル社製 Xeon E5504，メモリ容量は 4GB である．

サーバ	HDD I/F	回転数／分	RAID 構成
SV1	SAS 2.0	15,000	1
SV2	SATA 3G	7,200	1
SV3	SATA 3G	7,200	0

時間を除いた，残りの端末の起動時間の平均を求めた．また測定のばらつきを抑えるため，一斉起動を 3 回行い，3 回の平均を平均起動時間として表 4，5，6 に記載した．本試験の一斉起動は，PVS のマジックパケットを送信するタイミングに依存しているが，実運用において，端末が全くの同一時刻に一斉に起動することはあり得ないので，本測定は，実運用のための参考値として十分な意味をもつと考えている．

3 試験結果

はじめに，試験環境を A に固定して，基準となる起動試験を行った．試験環境 A のネットワーク環境は，表 3，および，図 1(a) に示したとおり，SW1 と SW2 との間の帯域を 1Gbps，SW2 と SW3 との間の帯域を 1Gbps，SW1 と SW3 との間を接続していない．また，試験環境 A のブートサーバ（SV1）は，SAS 2.0 インタフェース，15,000 回転／分のハードディスクで RAID1 を構成する．

起動試験は，1 台から 50 台の端末を一斉に起動して，その起動時間を計測した（表 4 参照）．試験環境 A は，SW2 に 30 台の端末を接続し，SW3 に 20 台の端末を接続している．表中，一斉起動の端末台数が 30 台以下の起動試験では，SW3 に接続された端末を起動しないように設定し，SW2 に接続された端末に対して，指定台数が起動するよう設定している．また，一斉起動の端末台数が 40 台の起動試験では，SW3 に接続された 10 台の端末を起動しないように設定している．

端末の台数が 1 台の場合，起動時間は 1 分 22 秒であった．試験環境 A では，一斉起動する端末の台数の増加にともない，端末の起動時間が増加する傾向にあり，端末の台数が 50 台の場合，1 台あたりの平均起動時間は 4 分 31 秒に達した．端末の台数が 30 台を超えると，台数の増加に対して，1 台あたりの平均起動時間の増加が少ない傾向にあるが，おおむね，台数に比例した起動時間の延長が認められる．

表 - 2: 教育用パソコンの構成一覧（デル社製 Optiplex GX620 スモールファクタ）．

構成部品	名称
CPU 型番	インテル社製 Pentium4 （2.8GHz）
メモリ容量	1GB（512MB × 2）
HDD	東芝社製 MK1655GSX （160GB，5,400 回転，SATA）
OS	マイクロソフト社製 Windows XP SP3

3.1 ブートサーバのハードディスク構成

次に，端末の台数を 40 台に固定して，試験環境の A から F について，一斉起動の実験を行った（表 5 参照）．ブートサーバのハードディスクの性能に注目すると，試験環境 A，C，D は，ネットワーク環境は同一で図 1(a) に示した構成であり，ブートサーバのハードディスクの性能だけが異なる環境である．そこで，試験環境 A，C，D の結果を比較していこう．表 1 に示したとおり，試験環境 A では，ブートサーバ（SV1）は，SAS 2.0 インタフェース，15,000 回転／分のハードディスク 2 台の RAID1 構成である．試験環境 C では，ブートサーバ（SV2）は，SATA 3G インタフェース，7,200 回転／分のハードディスク 2 台の RAID1 構成である．試験環境 D では，ブートサーバ（SV3）は，SATA 3G インタフェース，7,200 回転／分のハードディスク 2 台の RAID0 構成である．ハードディスクの構成から，ハードディスクのアクセス性能に関して，試験環境 A と D がほとんど同等であり，試験環境 C が劣る．

表 5 から，試験環境 A の平均起動時間が 4 分 8 秒で最も速く，試験環境 C の平均起動時間が 4 分 21 秒で最も遅い結果となった．また，試験環境 D の平均起動時間は 4 分 12 秒であった．ハードディスクの構成の違いが平均起動時間に忠実に反映された結果となったが，試験環境 A と C の平均起動時間の差は 13 秒であり，平均起動時間が 4 分を超える環境下でのこの差は，有意であるとは言い難い．

この結果から，ブートサーバに内蔵するハードディスクの性能を向上させても，端末の起動時間の短縮にはあまり貢献しないと言えそうである．この点に関して，ネットワークブートでは，端末の起動に必要なディスクイメージの容量は比較的小さく，各端末がブートサーバのハードディスクに直接アクセスしているというより，むしろブートサーバのメモリ上にキャッシュされたディスクイメージの内容にアクセスしていると考える方が自然であろう．

表 - 3: 端末起動試験の試験環境一覧（ネットワーク帯域，ブートサーバ構成，ディスクキャッシュ設定，ネットワークブート用ソフトウェアのバージョン）.

試験環境	帯域 SW1〜SW2	帯域 SW1〜SW3	帯域 SW2〜SW3	ブートサーバ（台数）	ディスクキャッシュ	ソフトウエアのバージョン
A	1Gbps	無	1Gbps	SV1（1 台）	パソコン	PVS 5.6
B	1Gbps	無	1Gbps	SV1（1 台）	サーバ	PVS 5.6
C	1Gbps	無	1Gbps	SV2（1 台）	パソコン	PVS 5.6
D	1Gbps	無	1Gbps	SV3（1 台）	パソコン	PVS 5.6
E	1Gbps	無	2Gbps	SV3（1 台）	パソコン	PVS 5.6
F	1Gbps	1Gbps	無	SV3（1 台）	パソコン	PVS 5.6
G	10Gbps	無	8Gbps	SV2（1 台）	パソコン	PVS 5.6(SP1)
H	10Gbps	無	8Gbps	SV2（2 台）	パソコン	PVS 5.6(SP1)

3.2 ディスクキャッシュ機能

本試験で用いたネットワークブート用ソフトウェアの PVS は，ディスクイメージとの差分（ユーザがパソコンを利用することによって生成されたテンポラリ領域の一時ファイル等）をパソコン側もしくはブートサーバ側の記憶装置に保存する機能をもつ．ブートサーバ側の記憶装置に保存する場合は，端末毎にディスクイメージとの差分を保存している．

前節の起動試験（表 5 参照）では，試験環境 A と B は，ネットワーク環境とブートサーバ性能が同一で，ディスクキャッシュ機能の設定内容だけが異なる環境である．そこで，試験環境 A と B の結果を比較していこう．試験環境 A は，ブートサーバ側のハードディスクにキャッシュを保存するよう設定を行った．内蔵ハードディスクは，SAS 2.0 インタフェース，15,000 回転／分のハードディスク 2 台の RAID1 構成である．一方，試験環境 B は，端末側のハードディスクにキャッシュを保存するよう設定を行った．表 2 から，内蔵ハードディスクは，SATA 3G インタフェース，5,400 回転／分のハードディスク 1 台の構成である．内蔵ハードディスクの性能を比較すると，ブートサーバに内蔵するハードディスクの方が端末に内蔵するハードディスクよりも高性能であるが，起動する全端末からネットワーク経由（帯域 1Gbps）でアクセスされることになる．

表 5 から，試験環境 A の平均起動時間は 4 分 8 秒で，試験環境 B の平均起動時間も 4 分 8 秒であった．この結果から，ディスクキャッシュ機能をブートサーバ側で有効にするか，端末側で有効にするか，の設定の違いが，端末の起動時間の短縮にはあまり貢献しないと言えそうである．実際，試験環境 A のブートサーバ上のディスクキャッシュの保存領域を確認したところ，端末毎の差分はほとんど保存されておらず，ディスクキャッシュ機能を利用した形跡は認められなかった．

表 - 4: ブートサーバ 1 台に対する端末 1 台あたりの平均起動時間.

試験環境	端末台数	平均起動時間
A	1	1:22
A	10	2:18
A	20	3:21
A	30	3:57
A	40	4:08
A	50	4:31

表 - 5: 端末 40 台の一斉起動に対する端末 1 台あたりの平均起動時間.

試験環境	端末台数	平均起動時間
A	40	4:08
B	40	4:08
C	40	4:21
D	40	4:12
E	40	3:57
F	40	3:16

3.3 ネットワーク環境

次に，ネットワーク構成の違いが端末の起動に影響を与えるかについて考察する．最大の帯域が 1Gbps であるネットワーク環境に限定すると，前節の起動試験（表 5）では，試験環境 D，E，F は，ブートサーバ性能が同一で，ネットワーク環境だけが異なる環境である．そこで，試験環境 D，E，F の結果を比較していこう．試験環境は，SW2 に 30 台の端末，SW3 に 10 台の端末を接続し，合計 40 台の端末を一斉起動している．

試験環境 D は，図 1(a) に示すとおり，SW2 と SW3 との間の帯域を 1Gbps，SW1 と SW3 との間を接続していない．試験環境 E は，図 1(b) に示すとおり，SW2 と SW3 との間の帯域を 2Gbps に増強し，SW1 と SW3 との間を接続していない．試験環境 F は，図 1(c) に示すとおり，SW2 と SW3 との間を接続せず，端末側の 2 台のスイッチを SW1 にそれぞれ帯域 1Gbps で直接接続している．試験環境 D，E と試験環境 F とのネットワーク構成上の大きな違いは，SW1 と SW2 との間の帯域がボトルネックにならないように構成されている点である．したがって，ネットワークの構成上，試験環境 F の平均起動時間が最速であることが期待される．

表 5 から，試験環境 D の平均起動時間は 4 分 12 秒，試験環境 E の平均起動時間は 3 分 57 秒，そして試験環境 F の平均起動時間は 3 分 16 秒であった．したがって，試験環境 D と E の平均起動時間の差は 15 秒，試験環境 D と F の平均起動時間の差は 56 秒である．ネットワークの構成に起因すると思われる有意な差が生じた．前節の実験結果からも，ネットワークブートに利用されるディスクイメージの大きさは小さいと思われるが，試験環境 D と E においても，平均起動時間に差が生じた．この結果から，ネットワーク帯域が 1Gbps 程度では，SW2 と SW3 との間もボトルネックになっていると考えられる．

この推論を検証するため，新規に試験環境 G，H を構築して，端末 50 台を一斉起動する実験を行った（表 6 参照）．ただし，表中，試験環境 A の平均起動時間は表 4 に示した結果から抜粋したものであり，平均起動時間の比較のために掲載している．試験環境 A は，図 1(a) に示すとおり，SW1 と SW2 との間の帯域を 1Gbps，SW2 と SW3 との間の帯域を 1Gbps で接続している．これに対して，試験環境 G は，図 1(d) に示すとおり，SW1 と SW2 との間の帯域を 10Gbps，SW2 と SW3 との間の帯域を 8Gbps（1Gbps × 8 でリンクアグリゲーション）にそれぞれ増強している．しかしながら，ブートサーバは同一の構成を用意することができなかったので，試験環境 A のハードディスク構成の方が高性能なものとなってしまった．試験環境 A と G，H の端末の接続形態は若干異なり，試験環境 A は，SW2 に 30 台の端末，SW3 に 20 台の端末を接続しているが，試験環境 G と H は，SW2 に 10 台の端末，SW3 に 40 台の端末を接続して，一斉起動を行った．

表 6 から，試験環境 A の平均起動時間は 4 分 31 秒，試験環境 G の平均起動時間は 3 分 24 秒であった．両環境の平均起動時間の差は 1 分 7 秒である．試験環境 A と試験環境 G では，ネットワークブート用ソフトウェアのバージョンも異なるため，端末起動のタイミングも異なっている．しかしながら，それを加味しても両者は 1 分以上の差が開いており，この実験結果から，平均起動時間に関して，有意な差が生じている．ブートサーバについて試験環境 A のハードディスク構成の方が高性能であることを考えると，ネットワーク環境を高速化することは，端末の一斉起動に対して，大きな影響を与えると言えそうである．

表 - 6: 端末 50 台の一斉起動に対する端末 1 台あたりの平均起動時間．

試験環境	端末台数	平均起動時間
A	50	4:31
G	50	3:24
H	50	2:50

3.4 ブートサーバの台数

最後に，ブートサーバの台数の違いによる起動時間への影響について考察する．試験環境 H は，試験環境 G のネットワーク環境と同一の構成で，さらに G で用いたブートサーバを 2 台用意して，端末 50 台を一斉起動させる．

表 6 から，試験環境 G の平均起動時間は 3 分 24 秒，試験環境 H の平均起動時間は 2 分 50 秒であった．両環境の平均起動時間の差は 34 秒である．ネットワーク環境の高速化との相乗効果もあり，端末 50 台の一斉起動に対して，非常に高速な結果を得た．この結果について，ブートサーバの台数が増加したことにより，各サーバの負荷が効果的に分散されたと言える．

3.5 試験環境と現行システムとの比較

試験環境は，現行の新潟大学教育用コンピュータシステムの一部を利用して構築した．端末，認証サーバ，ファイルサーバは，現行システムで実際に運用している機器を利用した．一方，ブートサーバは，サーバ機器，ソフトウェアともに本試験のために別に用意したものである．ネットワーク機器は，SW1，SW2，SW3 を本試験のために別に用意し，現行システムの配線のみを流用して，端末とブートサーバを接続した．認証サーバとファイルサーバは，実運用への影響が大きいため，現行システムの配置のまま利用し，SW1 は，認証サーバとファイルサーバへの通信を行うため，現行システムの L3 スイッチに接続した．

ブートサーバは，本試験のために別に用意したものであるが，現行システムのブートサーバの構成は，Xeon 3.2GHz × 1，メモリ 2GB，内蔵ハードディスク 80GB（15,000 回転／分，UltraSCSI320），ネットワークブー

ト用ソフトウェアは Ardence 3.5 である．本試験に利用したブートサーバの構成と比べ，性能が低い．

現行の教育用コンピュータシステムでは，端末を設置している各実習室の L2 スイッチと情報基盤センターに設置している L3 スイッチを帯域 1Gbps の光ケーブルで接続し，各実習室の端末台数に応じて L2 スイッチをカスケード接続している．試験環境 A のネットワーク構成は，本学の実習室のネットワーク構成とほとんど同等である．この試験環境 A の試験結果では，端末 50 台の平均起動時間は 4 分 31 秒であったが，これは，ブートサーバの性能差にも関わらず，現行システムの平均起動時間とほとんど同じであった．

本学では，平成 19 年 1 月の教育用コンピュータシステム更改以後に，何度かネットワークブートシステムを補強した．そのうちの一つとして，ブートサーバを追加し，起動時間の短縮を行っているが，その時の検証でも，起動時間の短縮には，ブートサーバの性能の向上は概して影響が少なく，むしろブートサーバ 1 台あたりに割り当てる端末数の分散による効果が高いことは確認していた．今回の起動試験でも，3.4 節で述べているように，同様の結論が導かれた．

また，導入当初はディスクキャッシュ機能をサーバ側に保存して運用していたが，導入後，パソコン側にディスクキャッシュを保存するよう変更を行った．3.2 節に示した通り，ディスクキャッシュをパソコン側，サーバ側のどちらに保存しても，起動時間には影響がないことが分かったが，起動後のソフトウエア利用時については，パソコン側にディスクキャッシュを保存した方が，端末の操作性の向上に貢献することが実際の運用で確認されている．

4 結論

本論文では，新潟大学の教育用コンピュータシステムの一部の環境を利用して，ネットワークブートによる端末の起動時間に影響を与える要因を実験的に評価した．端末の起動時間を短縮するため，端末に対して，大容量メモリを増設したり，ブートシステムの設計に対して，ブートサーバ 1 台あたりの端末の割り付けを変更したり等，システム導入以降，いくつかの対策を行ってきた．しかしながら，これまでの対策は（当然のことながらコスト的に）実現可能な範囲のものであって，抜本的な解決に至らなかった．

今回，帯域 10Gbps のネットワーク機器を用いて端末の起動実験を行い，限定的な実験の中で重要な知見が得られた．表 6 から，試験環境 G は，端末 50 台の一斉起動に対して，1 台あたりの平均起動時間およそ 3 分を達成している．ネットワークを 1Gbps から 10Gbps に増強することにより，起動時間の短縮に大きく貢献すると言える．一方で，ネットワークが 1Gbps の環境では，ハードディスクのアクセス性能を増強しても，起動時間の短縮に対しては，大きな効果がないことが分かった．ネットワークを増強した上でハードディスク性能を向上させた場合には，相乗効果が期待されるが，ネットワーク帯域が 1Gbps の場合には，ネットワークの増強がまずは優先であるといえる．

広帯域のネットワークの重要性は認識されていたが，今回の実験結果からより明確にコストの比較が可能となった．ネットワークシステムを含めた，今後の教育用コンピュータシステムの設計に寄与したい．

謝辞

本試験の実施にあたり，試験環境の構築にご協力を賜りました東日本電信電話株式会社に感謝の意を申し上げます．

参考文献

[1] 藤村丞，“ネットブート型 PC による大規模情報処理教育環境の構築”，情報教育研究集会講演論文集（CD-ROM 版），B1-3，京都，Dec. 2010.

[2] 宅間広大，桝田秀夫，“ネットワークブートシステムにおけるディスク性能の影響とその評価”，インターネットと運用技術シンポジウム 2009 論文集，No.15，pp.47-52，Dec. 2009.

[3] 鈴木徹，三村泰成，宝賀剛，“鶴岡高専の Vista ネットブート型教育用電算システム”，高等専門学校情報処理教育研究発表会論文集，No.28，pp.205-208，Aug. 2008.

[4] 佐々木芳弘，正木忠良，小林俊央，鷲谷貴洋，西田眞，中村雅英，“シンクライアントによる教育用端末環境の構築”，情報処理学会研究報告，Vol.2008-IOT-2，No.12，pp.61-66，July 2008.

大規模キャンパスネットワークにおける MAC アドレス認証端末の移動管理

Management of MAC Address Authenticated Host for Large-Scale Campus Networks

田島 浩一，近堂 徹，岸場 清悟，大東 俊博，岩田 則和，西村 浩二，相原 玲二
Koichi TASHIMA，Tohru KONDO，Seigo KISHIBA，Toshihiro OHIGASHI,
Norikazu IWATA，Kouji NISHIMURA，Reiji AIBARA

{ tashima, tkondo, kishiba, ohigashi, norita, kouji, ray } @ hiroshima-u.ac.jp

広島大学 情報メディア教育研究センター
Information Media Center, Hiroshima University

概要

イントラネットワークへのセキュリティ対策として，認証ネットワークと呼ばれるユーザ端末のネットワーク接続に認証を用いる事で，権限の確認や利用記録を行い，不正利用を防止する対策が現在では多くの組織で導入されている．認証操作では利用者へのユーザビリティの高い利用として，利用者が自身の ID を認証用の WEB ページへ入力して認証を行う WEB 認証や，ユーザ端末のネットワーク接続時に端末の MAC アドレスの登録の有無により認証を行う MAC アドレス認証等が利用されている．WEB 認証はこれまでにさまざまな研究や実装および製品化が行われ，実用的な方法が確立されているが，MAC アドレス認証は IP アドレスが不定な状態でも認証が行えるため，WEB 認証の手法をそのまま適用することができない．そこで本稿では，MAC アドレス認証の利用についてこの問題について整理するとともに，大規模キャンパスネットワークでの運用を前提とした MAC アドレス認証の運用方法として，MAC 認証したユーザ端末に不具合の生じる移動を管理する事による対策について述べ，構成事例と性能評価について報告する．

キーワード

MAC アドレス認証，キャンパスネットワーク，認証システム

1. はじめに

大学のキャンパスネットワークをはじめとする組織内のイントラネットワークにおけるセキュリティ対策として，認証ネットワークが現在では多くの組織で導入されている．認証ネットワークでの認証方法として利用者へのユーザビリティの高い WEB ブラウザを用いた認証（以下では WEB 認証と示す）が多く利用されているが，WEB 認証が困難な機器や WEB ブラウザを内蔵しない機器でも認証可能な MAC アドレス認証（以下では MAC 認証と示す）も利用される．

WEB 認証は，これまでにさまざまな研究や実装および製品化が行われており，認証操作を行う WEB アクセスによりユーザが認証して利用する端末（以下ではユーザ端末と示す）の IP アドレスを自動取得し，認証成功後の接続状態の確認等をこの IP アドレスで行なうといった実用的な方法が確立されている．しかしながら MAC 認証の場合にはユーザ端末が送信したパケットの送信元

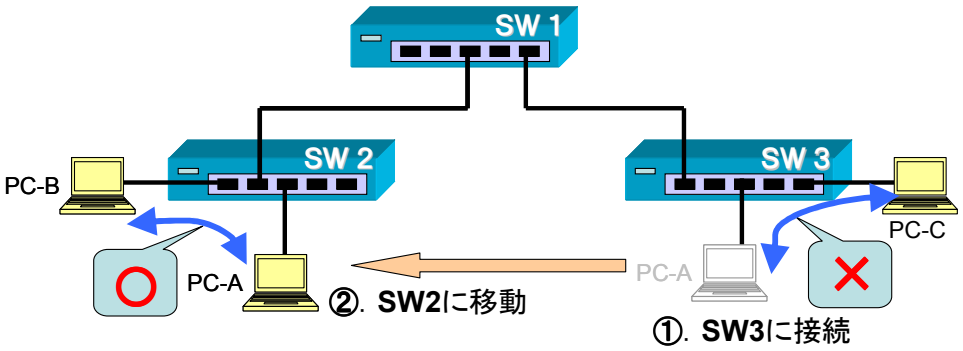


図 1　MAC 認証したユーザ端末の移動による通信障害の例

MAC アドレスによる認証のため，場合によってはネットワークに接続したユーザ端末が DHCP で IP アドレスを取得する際のリクエストパケットで認証が行われるなど，IP アドレスが不定の状態が当然ながら含まる．そのため，WEB 認証では可能であったユーザ端末の IP アドレスへ PING や ARP によっての接続状態を確認する方法をそのまま適用することができず，MAC 認証ではユーザ端末の接続終了を検出する事が困難である．

広島大学で運用されているキャンパスネットワーク HINET2007[1]では，ユーザ端末は原則として認証利用する事を必須としており，WEB 認証での利用を推奨とするものの，キャンパスネットワークの隅々全てで認証利用とするために約 460 台の認証スイッチで WEB 認証と MAC 認証を併用して提供しているが，MAC 認証したユーザ端末の接続終了の扱いについては 2 章に示す導入時には想定していない問題点が生じた．

そこで本稿では，大規模キャンパスネットワークでの運用を前提とした MAC 認証の運用方法について述べ，構成事例と性能評価について報告する．以下では，MAC 認証利用における運用上の問題点について 2 章で整理し，3 章でこの問題へ対処としてユーザ端末の移動管理を行う MAC 認証システムの構成について述べ，4 章で性能評価を行い，最後に 5 章でまとめについて述べる．

2. MAC 認証の運用上の問題点

本章では MAC 認証の運用上の問題点をまとめる．

2.1. MAC 認証したユーザ端末の移動による重複ログイン問題

認証スイッチでは，MAC 認証したユーザ端末が接続しているポートから離脱しても，前述のとおり存在の確認ができない事からユーザ端末の MAC アドレスが認証状態のまま接続していたポートに残り続ける．一部例外として，移動先が同一認証スイッチの別のポートであった場合に，認証スイッチによってはローミング機能を持ち，移動前のポートでの MAC 認証状態の解除と移動後のポートでの MAC 認証状態の開始が自動的に処理可能な場合がある．

他方，移動が異なる認証スイッチ間での場合は，図 1 に示す様な MAC 認証の状態が残る事による通信の障害が生じる．図 1 は，①の操作で一度 SW3 に接続した PC-A が，②の操作で SW2 へ移動して接続した状態を示している．ここで SW3 は，PC-A が移動した後も PC-A の離脱を検出できないため，SW3 は PC-A 宛のパケットを PC-A が接続していたポートに転送し続ける．そのため，PC-C と PC-A との間では通信が不可能な状態が生じる．この場合でも，移動先では PC-B と PC-A の通信など SW2 での折り返し通信や，PC-A が SW2 に移動したことを MAC アドレスの学習により検出可能な上位の SW1 側と PC-A との通信は正常に可能である．PC-A の利用者から見ると，移動先の他の端末との通信やアップリンクの通信に問題ないため気づきにくい障害である．

しかしながらこの様な不具合に気づいた利用者より，不具合が起きているという連絡が所属している情報センター窓口まで時々来ていたが，気づきにくい障害であるためキャンパス内では潜在的にもっと多くの箇所で同様の障害が起きていたと推測している．そのため MAC 認証したユーザ端末が認証スイッチ間を移動した場合には，MAC 認証の重複ログイン状態が継続しないように，移動の前に接続していたスイッチ側において接続終了の処理（以下ではログアウト処理と示す）が必要である．

2.2. MAC 認証利用時におけるユーザ端末の意図しないログアウト処理の影響

認証スイッチによっては，ARP キャッシュの保持時間程度の無通信状態が続くと強制的にログアウト処理が行える機能がある．しかし利用中であるにもかかわらず不必要に MAC 認証のログアウト処理を行うと，以下に示すユーザ端末が一時的に通信できない通信断が生じる事と，WEB 認証併用時のリダイレクトの問題が生じる．

・通信断による通信のロス　ログアウト処理で一時的に認証断が発生した際にも，MAC アドレスの登録が有効で再度の認証が可能であれば，認証断後の次のパケット送信時に MAC 認証が行われ通信可能な状態に戻る．本キャンパスネットワークで利用している認証スイッチで，ログアウト処理による通信断は，文献[2]の結果より最下位機種で，平均 62[msec] (最大 106[msec])程度の通信断が生じる．この間に認証スイッチでは，ログアウト処理（ブロックする様にフィルタを変更する処理）と MAC 認証処理（MAC アドレスの検出，外部 RADIUS サーバでの認証処理，認証成功後のフィルタ解除処理）の内容を考慮するとやむをえない時間程度であるが，スイッチのバッファでも回避できていないパケットロスが発生する．

・WEBリダイレクト発生の問題　WEB 認証では，ユーザへの利便性のために未認証時の WEB アクセスを認証ページへ誘導するリダイレクト機能がよく用いられるが，この機能を MAC 認証と同一ポートで併用利用すると次の問題が生じる．MAC 認証したユーザ端末で MAC 認証の認証断の時にユーザが WEB アクセスを行っていると，ユーザ端末が未認証状態のため，その直後の WEB アクセスにリダイレクトが発生し，表示するページが認証ページに置き変わってしまい，WEB のセッションが途切れる事や HTTP の POST により送信したデータが失われる場合がある．

以上2つの理由より ARP キャッシュの保持時間での自動切断などによる不必要なログアウト処理はユーザ端末への影響が大きく可能な限りさけるべきである．なお，WEB リダイレクトの問題は，問題が生じることを確認した時点では発生しても確率は極めて低いと考えていたが，学内で先行して認証利用を開始した一部の部局からセンター窓口に続けて苦情が寄せられたため，利用経過時間等でのログアウト処理や，利用者の少ない深夜にログアウト処理を一括で行っていた運用を中止し，それ以降は，夜間に全ての認証スイッチで MAC 認証の認証状態を確認して 2.1 節の重複ログインが見つかった場合のみログアウト処理を行う設定 [2] のみとした．

2.3. MAC アドレス詐称へのセキュリティ対策

MAC アドレスを用いた認証方法には，MAC アドレスの詐称による問題が懸念される．Linux やブロードバンドルータ等の機器では，ネットワークインタフェースにあらかじめ設定されている MAC アドレスとは異なる MAC アドレスとして動作させる事が可能であり，この機能により認証可能な MAC アドレスを詐称し，認証を回避してネットワークを利用する方法が可能である．この問題への対策として 2 つの方針で対策を講じている．

・MAC 認証が可能な場所の制限　学外からの訪問者や不特定多数の利用が想定される教室や会議室等の他，キャンパス内主要箇所で利用可能な全学予算で整備した大学公式の無線 LAN 等では，WEB 認証での利用のみ可能とし MAC 認証利用は不可とした．

・MAC 認証で利用するユーザ端末の利用範囲の制限　MAC アドレスの登録時に認証利用が可能な範囲を限定し，範囲内のみで利用可能となる方法を取っている．具体的には，単独の部屋や同じ研究室の部屋数箇所などを，1 つの管理者（研究室の場合は主にその研究室の教員）による管理範囲としてゾーンと呼び，このゾーン毎に別の VLANID を割り当てて独立させ，MAC 認証時には MAC アドレスとこの VLANID の組み合わせで認証する方法としている．そのため，異なる管理者の部屋からは VLANID が異なるため詐称による認証が不可能になる．

これらの対策により，MAC 認証の詐称による不正アクセスが発生した場合にも，発生場所の部屋がゾーンの範囲で限定され，また，利用者も特定のゾーン内の構成員に限定される事で，MAC 認証を利用する事におけるセキュリティ対策のコストと効果を考慮した結果，このような運用形態 [3] とした．

2.4. MAC 認証の運用上の問題点のまとめ

2.2 節より不必要な MAC 認証のログアウト処理は影響が大きく，また，2.1 節の重複ログイン問題も避けるべき問題であるため，MAC 認証のログアウト処理は障害が生じるユーザ端末の移動による重複ログイン状態が発生する時にのみ実行する方針とした．ここで， MAC 認証したユーザ端末がある認証スイッチから離脱する場合は，離脱と移動の 2 つに分けられ，離脱であった場合にログアウト処理を行わない事で認証スイッチに認証状態が残り続ける事の影響を検討したが，ARP キャッシュの保持時間程度無用なパケットの転送が続くのみで障害とはなら無いためである．

なお関連技術に，認証ネットワークにおけるユーザ端末の移動に関して無線 LAN でのローミング技術があり，無線 LAN スイッチとこれに対応した無線 LAN アクセスポイントを組み合わせ，アクセスポイント間のユーザ端末の移動を，無線 LAN スイッチ側で行いスムーズなローミングを提供する技術である．中でも標準化された 802. 11r では高速にローミングするために認証手続きを高速に行う方式等が定義されているが，対応しているアクセポイントのみで動作可能な事とユーザ端末側がこの方式に対応していなければならないという理由など，現在のキャンパスネットワークでは利用できる技術となっていない．

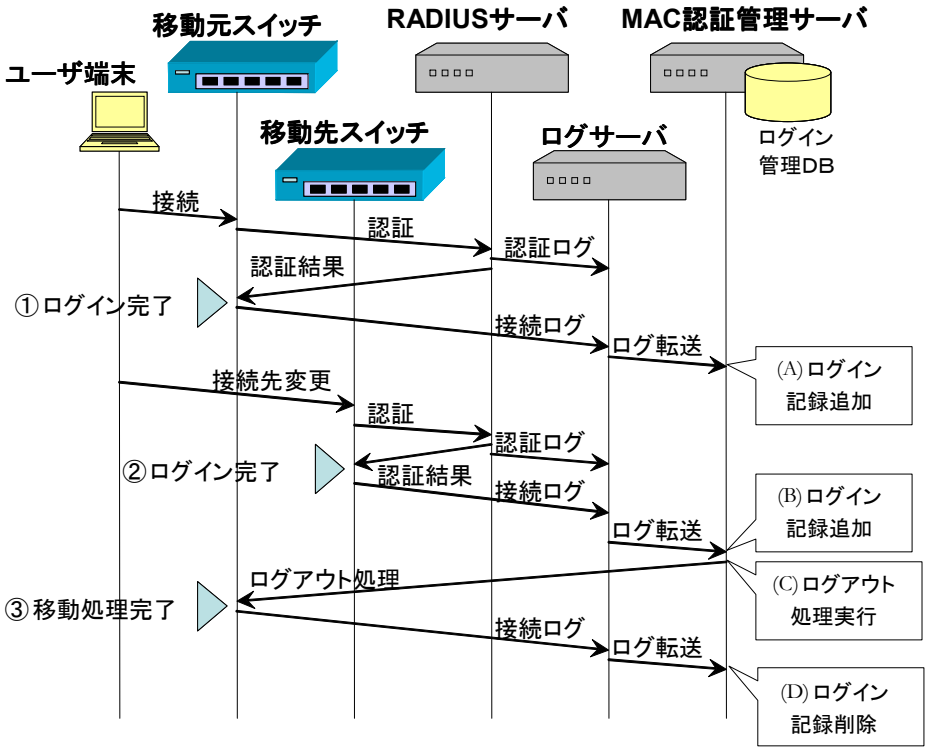


図 2　MAC 認証したユーザ端末の移動時における処理フロー

3. MAC 認証したユーザ端末の移動管理

本章では構築した MAC 認証管理サーバにより MAC 認証したユーザ端末の移動の管理と，移動検出時のログアウト処理について構成例およびその動作を示す．

3.1. MAC 認証システムの全体構成

MAC 認証システムには，MAC 認証で利用する MAC アドレスを登録する手段が必要であり，本学での構成例 [4] や 新潟大学での実装 [5] の報告の通り，ある程度の管理権限を持つ管理者に登録機能を提供する事で，ネットワークを管理する側の管理コストの低減とユーザ側の利便性の両方に配慮した構成が可能である．本稿での MAC 認証システムもそのような登録システムを併用する事を前提としている．

図 2 にユーザ端末が移動元スイッチに接続後に移動先スイッチへ移動した場合の MAC 認証システムを含めた全体の処理フローを示す．なお処理概要は以下のとおりである．

・ユーザ端末の移動元スイッチへの接続　ユーザ端末が移動元スイッチに接続し，RADIUS サーバで認証が行われ, 利用開始可能状態 である図 2 の①の時点まででユーザ端末側としては接続処理が完了する．MAC 認証管理サーバでは，①でログイン完了した接続ログをログサーバより取得し，ログイン状態を保持管理するための内部のログイン管理ＤＢへ登録する．

・ユーザ端末の移動先スイッチへの接続　ユーザ端末が移動先スイッチに移動して接続する場合も，ユーザ端末側からみると②のログイン完了までほぼ同様の接続処理がおこなわれ，MAC 認証管理サーバでは移動後の接続ログと以前のログイン記録より移動を検出する．移動の検出があると，移動元に残っている認証状態を MAC 認証管理サーバより直接スイッチを制御してログアウト処理を行う．その後で，このログアウト処理により生じる移動元スイッチからの接続ログ（ログアウトのログ）を受け取る事よって，MAC 認証管理サーバは該当するログイン記録の削除を行う．

3.2. MAC 認証管理サーバの構成

図 2 の MAC 認証システムの全体構成において，RADIUS サーバおよびログサーバは既設のサーバであり，ここに MAC 認証管理サーバを追加して MAC 認証システムとして動作する構成とした．

MAC 認証管理サーバでは，ログサーバからのログの取得に OpenSSL を用い，SSL により通信路の暗号化と 2048 ビット長のサーバ証明書によるサーバ確認を行う．認証スイッチへのログアウト処理は，スクリプト言語の expect を用い，スイッチのコンソールへ SSH (最下位機種では SSH 非対応のため telnet)を起動してログインし，管理コマンドをスイッチ上で直接実行する方法とした．

その他，ユーザ端末が意図せずに移動を繰り返す場面として，無線ＬＡＮの利用時に複数のアクセスポイント

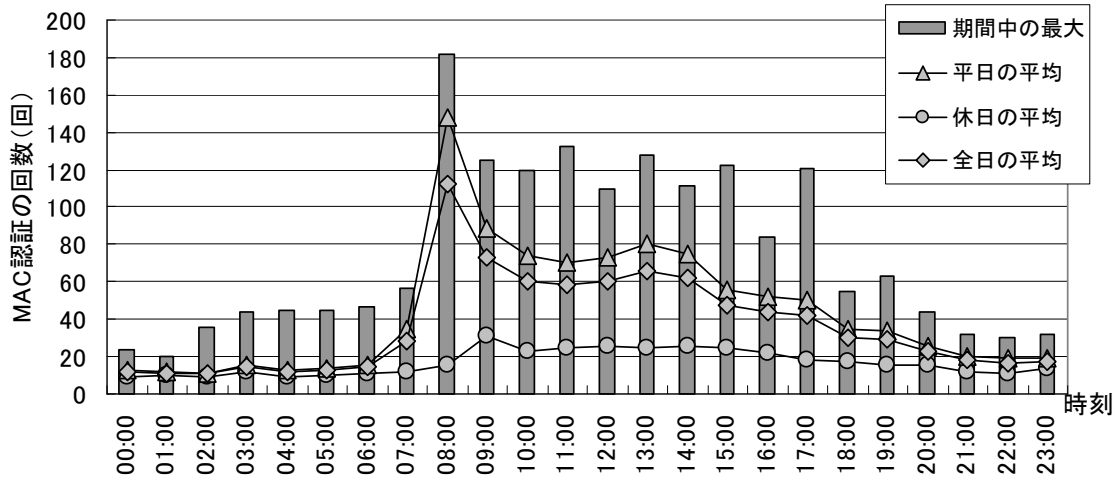


図 3　1 時間毎の平均 MAC 認証回数と最大認証回数 (2011 年 6 月)

間で移動を繰り返す事が予想されたため，同じ認証スイッチ間を行き来する移動で，移動して元の場所に戻るまでの時間が 30 秒以内の場合には，一定時間（初期設定では 60 分間）ログアウト処理は行わない制限を設けるなど，ログアウト処理の動作アルゴリズムを適宜見直す事を考慮して，接続ログの監視および認証スイッチへの管理操作の発行を行う管理プログラムはスクリプト言語の perl で実装した.

4. 性能評価

現在運用中のキャンパスネットワーク全体での利用を対象とするため，はじめにその様子について述べる.

MAC 認証用として用意している MAC 登録システムのデータベースには，登録済みの MAC アドレス数が 2011 年 6 月 30 日の時点で 9724 台が登録されている. また，本システムが処理すべきイベント数である MAC 認証の利用開始数（接続開始のログ数）について，2011 年 6 月の 1 ヵ月間の様子を図 3 に示す．グラフは時間帯毎のそれぞれ 1 時間の間に行われた MAC 認証の回数で，折れ線グラフに，「平日」，土日祝の「休日」と期間中全体の「全日」, について 1 時間毎の平均回数を示しており，時間帯毎の期間中最大値を棒グラフで図中に示している. グラフより 1 時間の間に処理すべき総数は図 3 より最大でも 200 程度，1 日の処理数は最大認証回数の累計でも 2000 件程である．データベースへの登録 MAC アドレス数に比べて認証回数が多くない理由は，多くの MAC 認証で利用しているユーザ端末がサーバの様に同一のポートで固定的に利用されるものが一定数あるため，移動等による MAC 認証によるログインが発生しにくい利用が多いと推測される．逆に，図 3 の認証数は多くは移動等で MAC 認証接続開始を行うユーザ端末であると考えられる．なお，WEB 認証の場合は，始業時刻の午前 8:30 前後に特に集中する傾向 [6] がみられたが MAC 認証は 8 時頃にそれ以降と比べて 1.5 倍程度の差はあるものの，始業から終業時刻の間は平均的に認証が行われており，ピーク値でも 10 分間に 30 台程度の認証数であった.

4. 1. 同時処理性能の測定

本システムの処理対象である MAC 認証したユーザ端末の移動の検出からログアウト処理が完了するまでの処理時間について，負荷テストとして同時に処理する台数を増やし，処理に要する時間の測定を行った.

測定方法は，図 2 の構成でユーザ端末として MAC 認証用クライアントを用意し，①の移動元の認証スイッチへの指定の台数分の MAC アドレスでパケット送信し MAC 認証でログインした状態から，②の移動先へ同じく指定の台数分の MAC アドレスでのパケット送信を行い移動した状態を再現し，③の移動処理を発生させその処理が完了までに要する時間についての測定を，運用中の認証ログ及び接続ログを収集するログサーバを用い，接続ログの時刻表記より求めた．測定で使用した機器の仕様は表 1 に示すとおりである.

これらの機器構成により 1 度に移動する MAC 認証のユーザ端末数が 5 台 ～ 30 台の場合について測定を行い，その結果を図 4 に示す．グラフは，横軸の各台数において 5 回の試行を繰り返して測定を行い，処理時間の平均値を折れ線グラフで，各台数での処理でその最大と最小の処理に要した時間をエラーバーで表示している. 同時処理台数の 5 ～ 30 台の様子では，同時に処理する台数の増加に応じて処理時間が増加する傾向は確認できるが，30 台の同時移動の際にも平均 8～12 秒程度，最も

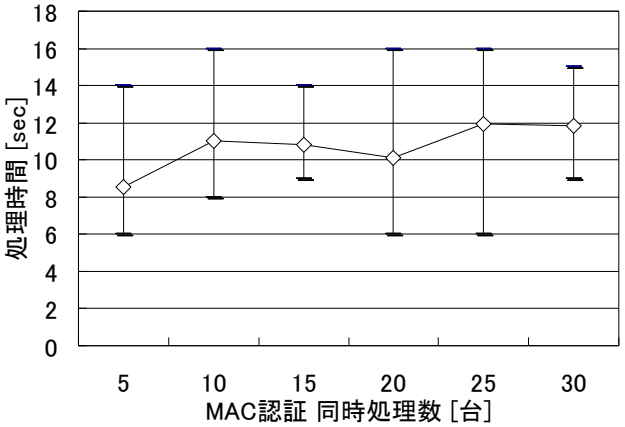


図 4　MAC 認証ユーザ端末の同時移動時の処理時間

表 1　測定に使用した機器の仕様

RADIUS サーバ（MAC 認証用 ）	
CPU	Inte Xeon X5355 @2.66GHz x2
Memory	4GB
OS	CentOS 5.0
Package	FreeRADIUS 1.1.7, OpenLDAP 2.3.41
ログサーバ（ 認証ログおよび接続ログ用 ）	
CPU	Intel　Xeon　X5355 @2.66GHz x2
Memory	4GB
OS	CentOS 5.0
Package	PostgreSQL 8.1.9
MAC 認証管理サーバ	
CPU	Intel Core2Duo E6550 @2.33GHz
Memory	3GB
OS	Fedora 8
Package	FreeRADIUS 2.0.5
MAC 認証用クライアント	
CPU	Intel Core i7 2600 @3.4GHz
Memory	8GB
OS	CentOS 5.6
認証スイッチ	
機種名	Alaxala 2430S
CPU	PowerPC 533MHz
Memory	256MB
ログサーバ（ 比較用 ）	
CPU	Pentium D 3.0 GHz
Memory	256MB
OS	CentOS 5.5

遅い場合でも 16 秒前後で処理が完了している． 事前の統計から予想される同時処理すべき台数は十分処理可能であると確認されたが，実際には使い始めに若干の時間

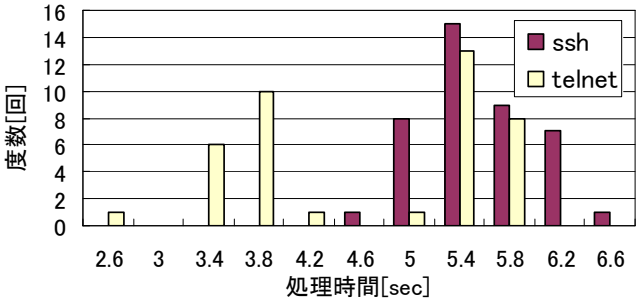


図 5　MAC 認証のログアウト処理に要する時間

の間，通信相手によっては不具合を感じる事がある程度の処理時間を要するため， MAC 認証したユーザ端末を移動させた場合は，使い始めに十数秒程度一部の通信に不具合が出る事があると案内しておく運用でカバーする事としている．なお，測定時における MAC 認証管理サーバで保持する MAC アドレスのログイン数は，すべての測定において 10000 台登録された状態から動作を開始しており，測定の間に MAC 認証ログインの失敗やログアウト処理の失敗等は発生しておらず，測定自体で問題は確認されなかった．しかしながら測定結果の図 4 の様子から同時処理台数に因らない，処理時間のばらつきや処理に要する最大の時間についての考察を行う．

4.2. MAC 認証のログアウト処理における処理要素毎の考察

移動の検出からログアウト処理完了までの処理時間を考察するため，その間に行われる処理を列挙し，それぞれサーバでの処理時間およびサーバ間でのログ等の転送時間等について考察を行う．

A. MAC 認証用クライアントの処理時間 MAC 認証用クライアントでは，1 台の LinuxPC で複数台 MAC 認証を行わせるため，ネットワークインタフェースの MAC アドレスを 1 回の認証毎に修正し，10 ～ 20 [msec] の間 PING コマンドで認証のためのパケット送信しこれを指定台数分繰り返し行っている．1 つの MAC 認証の処理あたり，20～30 [msec] 程度の処理時間を必要とするため，台数が少ない場合は測定結果への影響は小さいが，移動台数が 30 台の測定においては，最も遅い測定に 1 秒弱ほどの処理遅れを生じさせる．

B. RADIUS サーバでの認証時間　文献 [6] の結果より，既設の MAC 認証用 RADIUS サーバの構成では，1 秒間に 650 以上の同時認証処理が可能で，RADIUS 認証に要する時間は多重度が高い場合でもは数十 [msec] の処理時間で完了するため，全体の処理時間への影響はごく小さい．

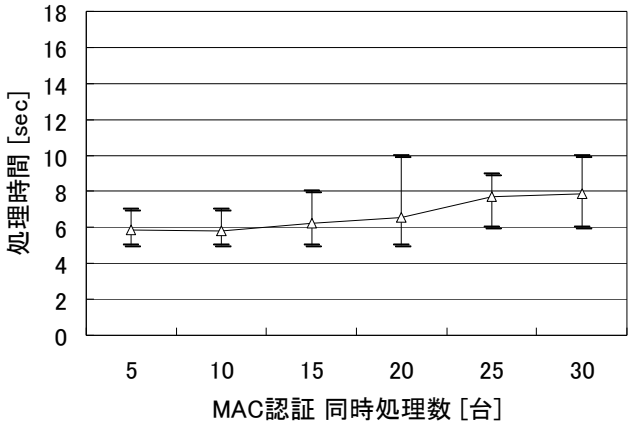


図 6　比較用ログサーバでの MAC 認証ユーザ端末の同時移動時の処理時間

C. MAC 認証管理サーバでの処理　ここでの処理は重複ログインの検出と検出後のログアウト処理である．まず重複の検出等ログイン管理 DB を用いる処理は，文献[4]の結果より，MAC 認証管理サーバに 10000 台がログイン中の状態で，ログイン記録からの参照とログイン／ログアウト記録の書き込みに要する時間は，それぞれ平均 3.4[msec]と平均 20[msec](最大 25[msec], 最小 19[msec])程度であり，全体の処理時間への影響はごく小さい．

認証スイッチへのログアウト処理のみを単体で動作させた場合の処理時間を図 5 に示す．図 5 の測定は，それぞれ SSH と telnet を用いて認証スイッチへ MAC 認証のログアウト操作を 50 回行った際の, 処理時間の区分毎の度数をグラフ化したものである．測定に用いている認証スイッチでは telnet および SSH での管理操作が可能であるが，グラフより telnet の場合には半分に近い時間で処理が完了する場合もあったが，可能な限りより安全な SSH を用いる．ここでの処理時間である 5〜6 秒程度は処理に要する時間の主要因の 1 つであった．

D. 接続ログの転送時間　接続ログの転送時間は，ログサーバでログを受け取りファイルへの書き出すまでの処理時間および出力されたログを MAC 認証管理サーバへ転送する処理時間が対象となる．

運用中のログサーバでは syslog 形式で認証スイッチから受け取ったログを，管理者向けの機能として用意しているログの検索や統計処理のために一度データベースに保管を行う事としており，あわせて運用中のある程度の負荷がかかった状態での測定であったため，図 4 の処理時間にはある程度遅延が予想されていた．運用中のサーバのためパケットダンプ等による測定が困難であったため, 比較用として syslog をファイルに書き出す動作のみを行うログサーバを別に用意し，認証スイッチからログサーバへ送信するログと同じログを比較用のログサーバに出力する構成で測定を行った．測定方法はログサーバが異なる点以外は 4.1 節と同じ条件で測定を行い，その結果を図 6 に示す．ログサーバを変えた際にも多少の処理時間の揺らぎは生じるが，図 4 の運用中のログサーバと比較すると処理時間のばらつきや遅延の程度が改善されているため，処理時間の短縮にはログサーバの見直しが必要であることが分かった．

ログサーバから MAC 認証管理サーバへのログ転送処理では，文献[2]の結果より今回の測定と同じ条件である 2048 ビット長のサーバ証明書を用いた SSL でのログの転送遅延は, 89[msec]±3[msec] であり全体の処理時間と比較すると処理時間への影響はごく小さい．

5. まとめ

本稿では，キャンパスネットワークでの MAC 認証の運用で問題として生じた，重複ログインの問題および不必要なログアウト処理を行わない方法として，MAC 認証したユーザ端末の移動を管理し，移動が検出された際にログアウト処理を実行する方法について実装ならびに評価を行った．特に，キャンパスネットワークでの実際の運用が本稿の目的であるため，MAC 認証利用者にとって不具合の少ない状態で利用できるようにすることに特に重点を置いて方針を決定した．

4.1 節の現行の運用環境での評価では, 処理に要する時間から利用開始時に十数秒程度，一部の通信に不具合が出る事があると案内して運用する事が必要であるという結果であったが，4.2 節の処理要素の考察より，B. の RADIUS サーバでの認証時間，C. の MAC 認証管理サーバでの重複ログインの検出処理, D. の接続ログの SSL での転送については十分短時間で処理可能であることが確認され，また，D のログサーバでの接続ログの処理について改善を行う事で図 6 の結果に近い処理時間が見込まれ，その場合には WEB アクセス等でユーザが通常待てる限界といわれる約 8 秒程度に改善が見込まれる．

その他，本稿で構築した MAC 認証におけるログアウト処理は, 本来は同様の機能が認証スイッチに実装され, 設定して利用できる環境が望ましいため，認証スイッチで実現する方法についても今後検討を行いたいと考えている．

謝辞

HINET2007 の構築および運用に尽力して頂いている広島大学総務室情報化推進グループおよび情報メディア教育研究センターの関係者に感謝致します．また，本研究の一部は日本学術振興会科学研究費補助金 課題番号

(2350008900) の支援を受けて実施しています. ここに記して謝意を表します.

文　献

[1]相原, 西村, 岸場, 田島, 近堂, “利用者認証機能を持つ大規模キャンパスネットワークの構築”, 2008 年電子情報通信学会総合大会 BS-8-7, pp.S-116 - S-117, 2008

[2]田島, 近堂, 岸場, 大東, 岩田, 西村, 相原, ”大規模キャンパスネットワークにおけるMACアドレス認証の管理手法”, 電子情報通信学会技術研究報告. IA, インターネットアーキテクチャ 108(460), pp.265 - 270, 2009

[3] 相原, 西村, 近堂, 岸場, 田島, “全教員に個別ファイアウォール機能を提供するキャンパスネットワークの構築”, 情報処理学会研究報告 2008-IOT-2, pp.29 - 34, 2008

[4]田島, 近堂, 岸場, 大東, 岩田, 西村, 相原, ”大規模キャンパスネットワークにおけるMACアドレス認証システム”, 情報処理学会 マルチメディア・分散・協調とモバイル(DICOMO)シンポジウム 2010 論文集, pp.1159 - 1165 ,2010.

[5] 浜元, 五十嵐, 青山, 三河, “ホスト登録システムを利用したネットワークアクセス認証システムの運用” , 情報処理学会研究報告 2010-IOT-9, pp. 1 - 6, 2010

[6]近堂, 田島, 岸場, 西村, 相原, ”PCクラスタによる認証スイッチの認証性能評価システム”, 情報処理学会研究報告 2007-DSM-47(5), pp.25 - 30, 2007

発達障害学生の修学支援を目的とした遠隔講義システムの開発

Development of Distance Learning Environment for Student with Developmental Disorders

伊藤　史人†，高見澤　秀幸†，丸田　伯子†，大内　佑子‡
筒井　泉雄†，山田　健司†，佐藤　郁哉†

Fumihito ITO†, Hideyuki TAKAMIZAWA†, Noriko MARUTA†, Yuko OUCHI‡
Izuo TSUTSUI†, Kenji YAMADA†, Ikuya SATO†

ito@poran.net, h.takamizawa@cio.hit-u.ac.jp, n.maruta@r.hit-u.ac.jp, yukoouchi-tky@umin.net
dir-rdche@dm.hit-u.ac.jp, yamada.kenji@dm.hit-u.ac.jp, ikuya.sato@cio.hit-u.ac.jp

†一橋大学
‡東京大学

†Hitotsubashi University
†Tokyo University

概要

本論文では，発達障害学生の修学支援として，ネットワークを用いた遠隔講義を実施した例を紹介する．近年，本学でも発達障害学生の存在が明らかになっており，その対策が急務となっている．支援の根拠としては「発達障害者支援法（平成 16 年法律第 167 号）」があり，大学は積極的に修学支援を実施していかなければならないとされている．これらの学生は，障害に起因したさまざまな問題により，通常の講義への出席が困難となり大学生活に問題を抱えていることが多い．一方で，特定の分野においては極めて高い能力を発揮することが知られている．本論文では，発達障害学生の修学支援を目的とした遠隔講義の実施について，その手法と効果について述べる．また，遠隔講義を行うに当たって生じた，機材の選定やネットワーク，現場での運用の問題についても述べる。

キーワード

発達障害，アスペルガー症候群，高機能自閉症，知的障害，遠隔講義，聴覚過敏，Web カメラ,ネットワークカメラ, Ustream

1. はじめに

発達障害に関わる法律として,「発達障害者支援法（平成 16 年法律第 167 号）」が発布されている．全国的に発達障害学生支援が行われつつあり，本学においても積極的に本障害学生を支援する義務がある[1]．しかし，これまでは十分な支援がなされていなかった。現在確認されている学生以外にも，潜在的にはより多くの障害学生が入学していると考えられており，本学も積極的に修学支援を行っていく必要がある．発達障害の症例は様々であり，修学支援も画一的な方法は適用できない[2] [3].

本論文では，発達障害による症状が原因となり，講義に出席するのが困難な学生の修学支援として遠隔講義を用いた例を報告する．今回の報告例では，発達障害のうち専門医の診察からアスペルガー症候群の診断を受けた学生を対象としている.

ところで，講義の遠隔配信の試みはすでに多くの教育機関で実施されており，決して新しい技術ではない．現状では，多くの大学で単位互換講義や一般公開講座，もしくはE ラーニングによる遠隔授業として広く利用されている.

ただし，遠隔講義配信システムは，比較的高額な機器を利用する必要があることから予算の確保が課題となる．そのため，学内外のプロジェクトとし補助金等で予算をねん出している例もある.

本学では，障害学生修学支援のための遠隔配信システム導入については，発達障害学生自体の認知が進んでいないことから優先的な予算配分による設備購入は不可能であった.

一方，今回の修学支援の例では，緊急支援として講義を遠隔配信で実施する必要があったことから，安価に簡単に実現できるシステムが必要であった.

運用にあたっては，講義毎に機材を各教室へ運搬して設置・設定・撮影・撤収を行う必要がある．そのため，簡便でより軽量なシステムを必要としていた．そこで，我々は安価な市販機材と学内無線 LAN（1284Wireless）を利用して配信システムを構成し，遠隔講義を配信することとした.

ここで，発達障害学生の講義における問題点を簡単にまとめる[3].

- 対人恐怖により講義室に入れない
- コミュニケーションが苦手であり，話しかけられるのではないかと講義中に不安を感じる
- 孤立してしまうのが怖い
- 周囲が気になり講義に集中できない

これらは一般の学生にも散見されることであるが，発達障害を持つ学生にとってはより大きな脅威に感じている．また，聴覚過敏の症状をあらわすことも多く，大勢の人の声の中で特定の人の声が聞き取れない症状や，講義室等の雑音や反響音の環境で講師の声に集中できないなどがある．この様な障害の場合，ICT（Information and Communication Technology : 情報通信技術）を活用することで解決できることも少なくない[4] [5].

本論文では，学生の修学支援として，安価に遠隔講義を実現し，発達障害学生の修学環境を構築して運用している．それにより，発達障害学生が安心して受講できた例を紹介する．さらに，運用する上で明らかになった各種問題へのアプローチについても報告する.

2. 発達障害とは

近年，高等教育の現場においても発達障害の存在が知られるようになってきたが，依然として周知されていないのが現状である.

発達障害は実に多様であり，個々人で症状が異なる場合が多く，複数の種別の症状を合わせ持つことも少なくない．以下に，発達障害者支援法において対象となる主な障害の特徴を示す[6].

2.1. 学習障害（LD）

文部科学省は「全般的な知的発達に遅れはないが，聞く・読む・話す・読む・書く・計算するまたは推論する能力のうち特定のものの習得と使用に著しい困難」と定義している[7][8]．大学生活の中では，板書を行う際に，他の学生と比較して，非常に時間を要する場合が考えられる.

2.2. 注意欠陥・多動性障害（AD / HD）

一般に,「注意力障害」と「多動性・衝動性」を特性とする．注意力障害とは，注意の持続困難や注意の配分の困難，あるいは注意の転換の困難などがある[7][8]．注意力障害がある学生は，時間管理の困難，物の管理の困難がある．大学生活の中では，レポートの期限を守れない・約束を忘れてしまうことや，整理整頓が苦手・借りた物をなくしてしまうことが考えられる.

2.3. アスペルガー症候群

言語による会話能力があるにもかかわらず，自閉症同様の「かかわり」「コミュニケーション」「こだわり」の

障害という 3 つの特徴を併せ持った発達障害である．知的障害域でないことが多く「知的障害がない自閉症」として扱われることが多い．対人関係の障害や，他者の気持ちの推測力などの障害が原因のひとつともいわれ，特定の分野への強いこだわりを示したり，運動機能の軽度な障害も見られたりする．

一方，早期からの療育によって，社会に妥当な範囲に行動や興味を統制していくことができる．そのユニークさが個性として認められる状況下にあっては，良好な人間関係を維持することができる[9].

3. 障害学生について

3.1. 発達障害学生の学生生活

発達障害学生は見た目としては健常者と変わりなく，個人の性格や努力不足として捉えられ誤解を受けることが多い．障害により，コミュニケーションや対人関係のトラブル，忘れ物や計画がきちんと立てられないなどの症状が出る．結果的に学業に集中できない状態に陥る場合が少なくない.

3.2. 対象とする障害学生

本論文で報告する遠隔講義システムは，障害学生（以下，当該学生）を対象とするものである.

当該学生は一般試験で入学し，入学時は発達障害の診断を受けていなかったが，学生生活を営む上で徐々に困難を感じるようになり，専門医によりアスペルガー症候群との診断を受けた.

現状の取得単位では卒業要件を満たすことができなくなる恐れがあり，そのため，今後受講する講義については単位を落とすことはできない状況であった.

それまでの講義では，IC レコーダーを用いて復習用に利用していたとのことだが，音声のみでは十分な学習ができず，次第に講義への出席が困難となっていったようである．また，障害の症状として健常者よりも疲労しやすいとの報告がある[6]．過度に集中するためとも考えられ，本例でも支援の必要性があると思われる.

3.3. 修学支援の内容

当該学生への修学支援については，講義への出席が困難なため，遠隔講義による受講が最も効果が高いものと考えられた．これは，本学精神科医と当該学生との結論であった.

遠隔講義による出席が正規の出席として認められるには，各担当教員との交渉が必要であったが，当該学生が所属する研究科長の協力で許可が下りた．ただし，当該学生への教育的配慮もあり，遠隔講義は学内から視聴することとなった．自宅からの視聴を許可してしまうと，通学する必要がなくなり他の学生との平等性が著しく損なわれることと，何よりも当該学生が大学に来るモチベーションを失わせてしまいかねないという配慮からである．その他，担当教員には講義室で配布する資料・レジュメを極力電子データで受け取れるよう配慮してもらった.

なお，現状では，遠隔講義による単位取得は正式なものではなく暫定的な対応となっている.

3.4. 倫理的配慮

本論文を公開するにあたり，学内の審査会において倫理面の配慮について検討し，問題ないとの結論に至った．また，当該学生には本論文の内容について確認をしてもらい同意書を取っている.

4. 遠隔講義配信システムによる修学支援

4.1. システムの要件

遠隔講義を実現するにあたり，保健センターをはじめ，大学教育研究開発センター・情報基盤センター・学生支援課からスタッフが招集された．数度の打ち合わせにより，遠隔講義配信システムの要件として表 1 の 5 つが挙げられた.

表 1　遠隔講義配信システムの要件

No.	内容
1	単位取得に必要なすべての講義の配信ができること（講義室がすべて異なるため）
2	別室で講義をリアルタイム視聴できること
3	誰でも容易に配信機器の運搬・設置・撤収が可能であること
4	ネットワークが切断された場合のバックアップとして HD ビデオカメラで撮影しておくこと
5	講義映像を録画できいつでも取り出せること

その他の重要な条件としては，安価に調達可能なことも含まれるが，PC を利用すれば実現可能と判断したため要件には含めなかった.

4.2. 支援体制

技術面においては，情報基盤センターが対応し必要な機材の購入については学生支援課が担当した．保健センターは当該学生から日々の要求を聞き取ることとなった．また，大学教育研究開発センターは，当該学生と各担当教員との橋渡しをして遠隔講義による出席でも不利益にならないよう配慮してもらうなどの交渉を行うポジションとした．

障害学生を積極的に支援している大学であれば，障害学生支援室などの組織が設置されているが，本学においては，それに代わる組織としては非定期に開催される障害学生支援委員会とそのワーキンググループのみである．実質的には能動的に修学支援活動を行う組織となっておらず，このような状態での支援体制となった．

4.3. Skype を利用した遠隔講義と問題点

表 1 の要件を満たすシステムとしては，まず，Skype[11] を利用したものが考えられた．

図 1 Skype による遠隔講義配信の構成（図中の番号は表 1 に対応している）

Skype は無料で使えるテレビ電話システムであり，リアルタイムの映像を送受信することが可能である．電話機のように，どちらかが「発信」をして「受話」することでコネクションが成立する．

以下，図中の番号に沿って説明する．

① において，講義室からノート PC と Web カメラを利用して Skype で映像と音声を転送する．インターネット回線は学内無線 LAN（1284Wireless [12] ）を活用する．幸いにもすべての講義室で電波状態が良好なためインターネット回線が利用できた．

② では学内の受講室から当該学生が Skype を利用して講義をリアルタイムで視聴する．その際，視聴用パソコンで Skype の画面を録画する．これは，Skype に録画機能がないためパソコン側で行う必要があるためである．

講義室では，映像の配信と同時にバックアップ用ビデオの撮影を行う（④）．これらの運搬から撤収は誰でも簡単に行えなければならない（③）．

さらに，⑤では HD ビデオで主に黒板を撮影し，撮影映像は圧縮作業の後，データ保管サーバーにアーカイブしておく．また，教員から提供されたレジュメ等があれば同時にアーカイブしておく．蓄積された講義映像のアーカイブは当該学生がいつでも視聴できるものとする．

以上により，当該学生はリアルタイムで講義遠隔視聴でき，かつ復習にも利用でいる状態が保証される．

しかしながら，Skype を試験的に運用したところ次の問題が発生し，当該学生に利用させることができなかった．主な問題点を表 2 にまとめた．

表 2 Skype 利用による問題点

No.	内容	原因
1	Skype の仕様として「発信が」必要であり，双方向通信環境では落ち着いて学習できない	障害由来と思われる
2	テレビ電話ソフトのため講義の遠隔配信用としてはしっくりこない	その他
3	教員側の作業が必要になる	技術的仕様
4	パソコン側で録画ができない	技術的仕様
5	ネットワークが一度切断されると再接続に手間がかかる	技術的仕様
6	ズームができないため黒板が十分に見えない	技術的仕様
7	カメラの向きを操作できない	技術的仕様

4.4. Ustream を利用した遠隔講義

Ustream [13] は，企業の会見やユーザーによるネットライブ放送ツールとして広く使われている．特別な設備がなくても Ustream のサーバーを利用して世界中にブロードキャストできる（図 2）．機材は Skype と全く同じものが流用できた．Skype では，講義の配信には不向きであったが，Ustream を利用することで表 2 の No. 1～ 5 を解消できた．

図 2　Ustream による配信と録画（パスワードで保護された“一橋大学遠隔講義 A 棟”にログインすることで講義の視聴ができる）

Ustream はもともと配信専用ツールであることから，ブロードキャストで視聴できる上，配信側（講義室側）としては配信開始後に特別な操作の必要はない．Skype のように「発信」に対する応答は不要である．

ネットワーク切断への対応は OS が担うため，パソコンと無線 LAN のコネクション次第となり，明示的な再接続は不要である．無線 LAN はまれに切断されることもあるが，再リンクされれば Ustream も自動的に再開される．

さらに，配信を行えば Ustream サーバー上に録画が自動的に作成されアーカイブされるため，別途パソコン上での録画作業は必要ない．作業としては録画の公開範囲を決定し，タイトル・タグ等を入力すればよい．

一方，標準の配信アプリケーション（Ustream Broadcaster）では画質が大きく制限され，HD 画質対応の Web カメラを利用しても標準画質でしか配信できない．

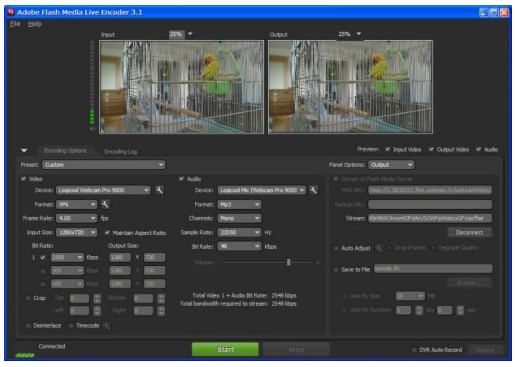


図 3　Abobe 社製 Flash Media Encoder による配信（FME を利用することで大幅に画質が改善される）

そこで，外部ツールである Adobe 社製の Flash Media Encoder [15]（図 3）を利用することにより HD 画質（1280 px × 720 px）の映像配信が可能になった．ただし，無線 LAN の帯域を考慮すると，高フレームレートでの運用は難しい．今回の講義配信では，安定性を優先して 1 フレーム / 秒 での運用に留めた．通常の講義においては，主に見たい部分は黒板であり，音声さえ途切れなければ高フレームレートはそもそも必要ない．黒板を映した画像が HD 画質になったことにより，これまで見えなかった板書が判読できるようになった．

ところで，講義における機材の設置および撤収であるが，おおむね誰でも簡単に行えるものとなっている．カメラの接続とパソコン上の数回のクリックで配信が開始されるようにセットアップされている．参考のため，図 4 に保健センターの看護師が設定している写真を示す．

以上により，Skype では難しかった遠隔講義の配信が運用できるようになった．当該学生からの反応も良好であった．

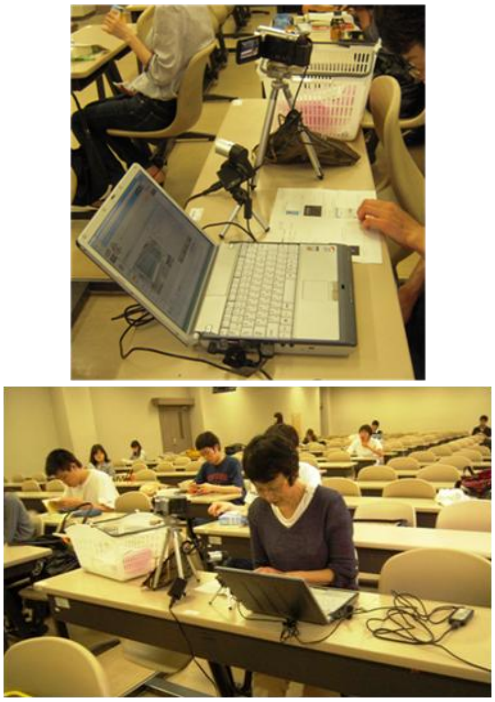


図 4　Ustream による配信現場（講義室の座席に PC・カメラ 2 台を設置し無線 LAN への接続を行う）

4.5. Ustream を利用した遠隔講義の問題点

HD 画質での配信を行っても，なおも表 2 の No.6 および 7 は未解決のままである．当初，HD 画質にすることですべての黒板の文字が判読できるようになり，これらの問題は解決するかと思われた．

しかし，非常に幅広の講義室においては，黒板も横長になることからフレームに入りきらない場合や，癖のある字・薄い板書の場合は判読がたいへん困難である．それらの例を図 5 および図 6 に示す．いずれも HD 画質の配信であるが，十分に判読できない文字が多数存在する．

特に，当該学生にとっては，聴覚情報よりも視覚情報

がより重要であるとの報告があった．仮に板書が不鮮明な部分が多いと，やや混乱して集中が保てないとの意見があった．健常学生であれば，聴覚情報からでも多くの情報を得ることができる[16]が，当該学生の場合は聞くことにはかなりのストレスを感じるとのことである．

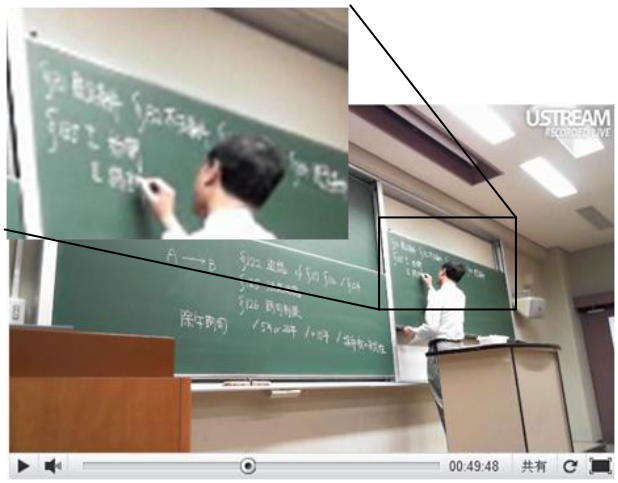


図 5　FME を利用した HD (1280×720) 配信 ①（左上の写真は一部を拡大したもの）

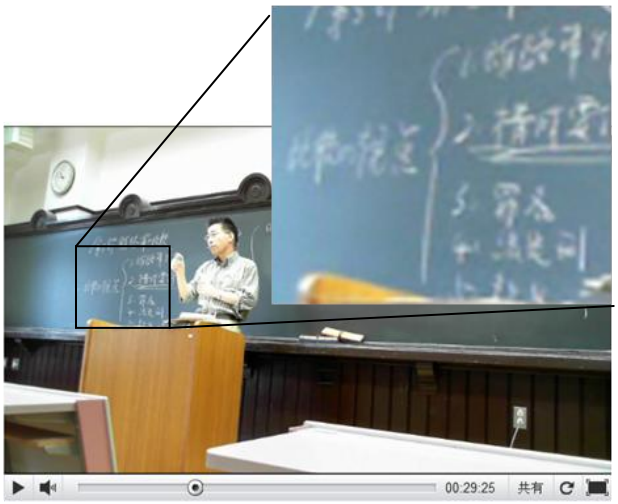


図 6　FME を利用した HD (1280×720) 配信 ②（左上の写真は一部を拡大したもの）

Ustream 利用による問題点を表 3 に示す．これらの根本的な解決策としては，オンデマンドでカメラのズーム・パン・チルトができるシステムが必要なことは明らかである．

業務用の高価なシステムを導入すれば可能であるが，現状では当該学生のみの利用者となれば購入は不可能である．

表 3　Ustream 利用による問題点

No.	内容	原因
1	ズームができないため黒板が十分に見えない	技術的仕様
2	カメラの向きを操作できない	技術的仕様

また，今回の機器構成では，マイクは Web カメラのものであるため高音質とは言えない．教員が使うマイクからラインとして取ればノイズ等は解消できるが，設置の手間が増えてしまうことから現在は対応していない．

4.6. 遠隔操作カメラを利用した遠隔講義

Ustream を利用することで，たいていの講義を安心して受講することができた．当該学生にとって，講義を傍観できることは集中できることにつながる．

そして，2 か月ほど Ustream を利用しているうちに不満な点が増幅されてきたようであり，板書が不鮮明であることの対応を求められた．これについては我々も懸念していたため，新しい機材により解決を図った．

用意した機材は主に防犯用に使われるネットワークカメラ[17] である（図 7）．これは Web カメラとは異なり，このカメラ自体にブラウザ経由でログインすることで映像を視聴できる．機能としては，ズームをはじめパンとチルトも可能であり，板書の見やすさは飛躍的に向上することが期待された．

しかし，使用にあたっては大きな問題があった．配信側のインターネット回線は学内無線 LAN 環境しか使えないのであるが，取得できる IP アドレスはプライベートであり，NAT 越しの通信は不可能であった．つまり，当該学生が利用するパソコンからはアクセスできないのは明らかであった．

図 7　ネットワークカメラ　BB-HCM581

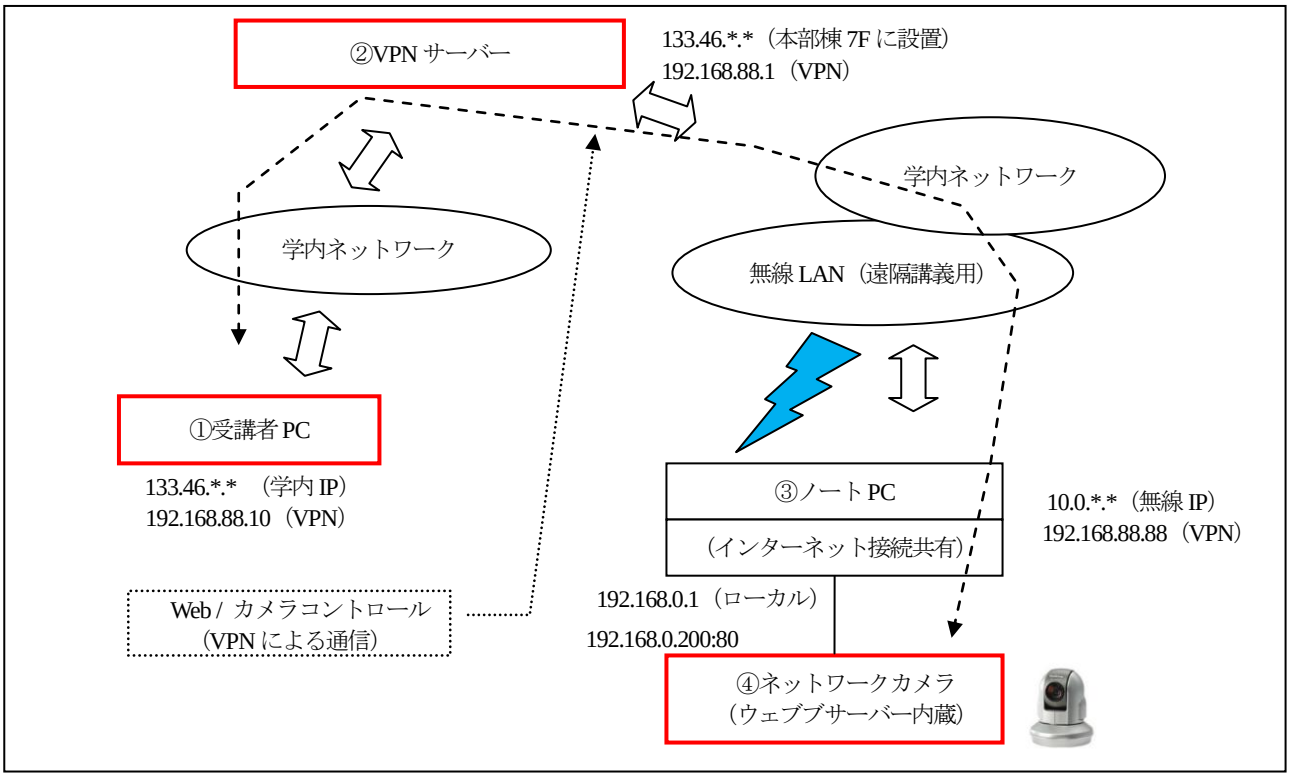


図 8　遠隔操作カメラを利用するための VPN 構成図

表 4　ネットワークカメラの主な仕様

項目	値
品番	BB-HCM581
製品形態	ウェブサーバー機能内蔵タイプネットワークカメラ
画像圧縮方式	JPEG または MPEG-4
解像度	640×480 ドット、320×240 ドット、192×144 ドット
セキュリティ	ID・パスワード
同時アクセス数	最大 30 アクセス
ズーム	21 倍光学ズーム
パン・チルト	あり

http://panasonic.biz/netsys/netwkcam/lineup/hcm581.html

そこで，学内ネットワーク環境に専用の VPN 網を準備して，受講用パソコンからカメラへの通信を確保することとした．ネットワークの概要図を図 8 に示す．

図中 ① は受講用パソコンであり，通常は DHCP よりグローバルアドレスが振られている．VPN サーバー (②) は学内のグローバル IP アドレスセグメントに設置し，受講用パソコンとカメラから参照できるようにした．

なお，カメラは無線 LAN 機能を搭載していないので，Windows パソコンを無線ルーターとして利用した．カメラとパソコンは有線接続し，パソコンには Windows 標準のインターネット接続共有（ICS）を設定し，このパソコン（192.168.88.88）への 80 番ポートでのアクセスはすべてカメラ（192.168.0.200）へ向かうようにした．

VPN のセッションを張る場合は，双方から VPN サーバーへの接続認証を通す．接続認証が通れば，受講用パソコンとカメラ（カメラに接続されたパソコン）間の仮想プライベートネットワークが生成される．これにより，受講用パソコンからカメラへの通信が確保される．

VPN での通信は通常の通信よりもコストのかかるアクセスとなる．講義映像が滞りなく転送できるのか懸念していたが，結果的には特に問題なく動作した．今回の遠隔操作カメラ用の VPN 接続は，学内ネットワーク上に展開していることもあり，スループットの低下はほとんど感じられなかった．

ここで，遠隔操作カメラでの講義映像の例として，図 9 と図 10 にキャプチャ画面を示す。それぞれ，プロジェクター画面と黒板文字のズームの例である．図で表した通り，光学ズームの利点が生かされており，本来は不鮮明になる条件でもズームすることで鮮明に映すことが可能になっている．本カメラによる画質できれば板書に困ることはないと思われる．

当該学生に感想を求めたころ，画質についてはたいへん満足してもらったが，音声が聞き取りにくくなったという指摘を受けた．今回の構成では，カメラのマイク端子に外付けの安価な市販マイクを接続している．健常者が聞き取る場合は特に問題は無いようであるが，マイクを通した音質では障害由来による聞き取り難さを感じているようであった．

図 9 プロジェクター画面の拡大（投影文字のピクセルが見えるほどにズーム可能）

図 10 黒板文字の拡大（判読しにくい色でも十分別可能）

遠隔操作カメラは同時 20 アクセスまで対応しており，学生が複数となっても本システムを利用できる．カメラ操作は同時 1 アクセスとなるため，頻繁なカメラ操作は行いにくい．ただし，通常の講義においては板書を映すことになるため，カメラ操作による問題は起きにくいと考えられる．

機材構成としては Web カメラから今回の遠隔操作カメラに替えたことから，Ustream の配信が行えなくなった．厳密には，遠隔操作カメラからの外部出力をエンコードしてパソコンに入力すれば可能であるが，現場での負担が増えるため採用していない．代替として本体に記録されている映像をアーカイブして閲覧できるようにしている．

4.7. 遠隔講義による修学支援活動のまとめ

本論文での遠隔講義の手法としては以上の 3 パターンでの取り組みについて報告した．いずれも一長一短はあり，障害から由来する視覚聴覚の特性を考慮して調整し変遷していったものである．

現在の遠隔操作カメラを中心とした構成機材にも，前述のように音声の問題があるが，順次ハードウェア・ソフトウェア面で対応していきたい．

障害者の支援は，多くの場面で ICT を利用することで改善することができる．例えば，携帯電話は聴覚障害者にとって無くてはならない道具である．音声機能は利用できなくてもメール機能が彼らのコミュニケーションを大きく変えた．同様に，パソコンの読み上げソフトウェアは視覚障害者の情報環境を一変させている．

今後本学においても ICT を上手に活用した修学支援が重要になってくるのは間違いないだろう．

5. オフラインの修学支援

本章では，地元のシルバー人材を活用した修学支援の取り組みを紹介する．

5.1. ノートテイクとカメラ設置

遠隔講義の配信を行うには，授業毎に機材を運搬して設置する必要がある．運用開始間もない時期は，我々が直接設置しに行っていた．遠隔講義の対象となるコマ数は週 10 回になり，対応する教職員の負担が増大していた．また，どうしてもカメラでは撮りきれない情報はノートテイクで対応する以外になかった．ノートテイク自体専門的な作業であるが[18][19][20]，今回は板書を見た目通り書きとってもらうことから始めてもらっている．

そこで，地元のシルバー人材に依頼してノートテイクとカメラの設置作業のお手伝いをしてもらうこととなった. 現在は週 10 回の講義を 5 名ほどのシルバー人材でカバーしている.

6. まとめ

講義の遠隔配信手法はありふれた技術であるが，障害学生支援を目的として行うと，障害由来による課題が多く発生し，ICT のみでは解決できない難しい問題を含んでいることがわかった．我々が実用上問題ないと判断しても，実際に使ってもらうと使えない場面も多かった．現状においても，なお未解決課題も残っており順次できる限り対応していきたい.

今回の報告では，主に映像配信に関して重点的に行なったが，一方，音声の改善については十分行われなかった．アスペルガー症候群においては，聴覚能力に問題を抱えている場合も多く，当該学生でも映像音声の聞き取りが困難になる場合が散見された．困難になる原因として，可聴範囲の周波数特性によるものと，脳の音声処理に関わるものがある．後者の場合は特に詳細な調査が必要である．映像配信において音声は重要な情報源であるため, 今後は重点課題として取り組んでいく予定である.

我々の障害学生への修学支援のモチベーションとしては，何よりも学生の将来への期待である．発達障害者の中には、極めて高度な知能を有する者もおり，歴史上，障害を乗り越えて偉業を成し遂げた人物は枚挙に暇がない．特に，アスペルガー症候群は，特定の分野において極めて高い能力を発揮したケースも複数知られており，環境次第ではその能力を大きく開花させることも可能である．我々はその芽を摘んでしまわないように大切にかつ力強く生きていけるように支援していきたいと考えている.

参考文献

[1]. 飯田由美, “大学において見られる精神疾患とその対応,” 東京大学保健センター, 2011

[2]. 市川奈緒子, “高等教育機関における発達障害を持つ学生の支援の現状と課題,” 白梅学園大学･短期大学紀要 47, 65-78, 2011-03-14

[3]. 石川裕紀, 城田謙司, 浦崎源次 ,久田信行, 霜田浩, “信特別支援教育サポートセンターにおける発達障害児指導・支援の変遷 —5 年間の活動を振り返って,” 佛教大学教育学部学会紀要 10, 163-174, 2011-03-14

[4]. 宮本信也, “心身医療における発達障害,” 心身医学 51(3), 211, 2011-03-01

[5]. 桶谷文哲, 水野薫, 吉永崇史, 西村優紀美, 斎藤清二, “発達障害学生の大学移行支援,” 学園の臨床研究 10, 39-49, 2011-03

[6]. 井澤信三, 山本真也, 半田健, “高機能広汎性発達障害青年における社会的コミュニケーション行動支援に関する文献的検討,” 兵庫教育大学研究紀要 : 学校教育・幼年教育・教育臨床・障害児教育・言語系教育・社会系教育・自然系教育・芸術系教育・生活・健康系教育・総合学習系教育 38, 63-70, 2011-02

[7]. 鳥山由子, 竹田一則, “障害学生支援入門—誰もが輝くキャンパスを,” ジアース教育新社, 2011

[8]. 福岡教育大学附属特別支援教育センター, “第 6 回特別支援教育公開セミナー--テーマ 発達障害学生の支援と課題,” 福岡教育大学附属特別支援教育センター研究紀要 (3), 124-152, 2011-03

[9]. Ｗｈａｔ’ｓ？アスペルガー症候群－「アスペルガー症候群」に関する私的研究ページー, http://www2u.biglobe.ne.jp/~pengin-c/autism-as.htm

[10]. 井上博之, 日山雅之, 近堂徹, 前田香織, “利用制限のあるネットワーク下でプレゼンテーション同期をするための遠隔講義支援ツールの開発,” 情報処理学会論文誌 51(3), 1008-1018, 2010-03-15

[11]. スカイプ公式サイト, http://www.skype.com/intl/ja/home/, スカイプ

[12]. 1284Wireless & Wired, http://cc.hit-u.ac.jp/, 一橋大学

[13]. Ustream, http://www.ustream.tv/

[14]. 萩原洋一, 櫻田武嗣, 川島幸之助, “全国 18 国立大学高精細遠隔講義システムの設計構築と課題,” 学術情報処理研究 (13), 40-48, 2009

[15]. Flash Media Live Encoder 3.2, http://www.adobe.com/products/flashmediaserver/flashmediaencoder/

[16]. 内藤一郎, 加藤伸子, 河野純大, 村上裕史, 若月大輔, “聴覚障害者のためのリカレント教育の検討,” 筑波技術大学テクノレポート 15, 57-61, 2008-03

[17]. ネットワークカメラ BB-HCM581, http://panasonic.biz/netsys/netwkcam/lineup/hcm581.html

[18]. 勝丸徳浩, 秋田祐哉, 森信介, 河原達也, “大学講義のノートテイク支援のための音声認識用言語モデルの適応,” 情報処理学会研究報告. SLP, 音声言語情報処理 2008(68), 25-30, 2008-07-11

[19]. 岡本香, 林信治, “障害学生の学習支援に関する一考察 : ノートテイクに関するアンケート調査より,” 東海学院大学紀要 1, 95-98, 2007

[20]. 古賀文子, “高等教育における情報保障の問題点--奈良女子大学のノートテイク実践を例に,” 人間文化研究科年報 (22), 奈良女子大学, 245-255, 2006

大学間遠隔講義システム及び遠隔講義収録・配信システムの自動制御と制御デバイスの拡張

Development of Intelligent Intercollegiate Distance Learning Systems and an Extension of System Control Device

森下　孟†，茅野　基‡，鈴木　彦文*，永井　一弥*，新村　正明**，矢部　正之***
Takeshi MORISHITA †, Kizuku CHINO ‡, Hikofumi SUZUKI*,
Kazuya NAGAI*, Masaaki NIIMURA**, Masayuki YABE***

morisita@shinshu-u.ac.jp, chintan@shinshu-u.ac.jp, h-suzuki@shinshu-u.ac.jp,
kznagai@shinshu-u.ac.jp, niimura@shinshu-u.ac.jp, yabe@shinshu-u.ac.jp

†信州大学大学院総合工学系研究科
‡高等教育コンソーシアム信州
*信州大学総合情報センター
**信州大学 e-Learning センター
***信州大学高等教育研究センター

† Interdisciplinary Graduate School of Science and Technology, Shinshu University
‡ The Consortium of Higher Education in Shinshu
* Shinshu University Integrated Intelligence Center
** Shinshu University e-Learning Center
*** Shinshu University Research Center for Higher Education

概要

本研究では，既設の大学間遠隔講義システム及び遠隔講義収録・配信システムの問題点を解決するため，「遠隔講義接続・切断の自動化」「講義コンテンツ配信の自動化」「カメラの遠隔制御」「コントロールプログラムの iPad 対応」の 4 要件を満たすシステム及び機能を構築・実装し，より効果的・効率的に通常の対面講義でのネットワーク配信を可能にすることを目的とした．本研究の結果，既設システムの問題点をそれぞれ解決・改善することができたが，講義コンテンツの自動配信では「プロキシサーバ環境下で視聴できない」，カメラの遠隔操作では「操作の煩雑さや柱の陰にいる受講生を捉えることができない」といったシステム面・運用面での新たな問題点が明らかになった．

キーワード

遠隔講義，講義コンテンツ，自動制御，遠隔制御，大学コンソーシアム

1. はじめに

文部科学省の戦略的大学連携支援事業[1]をはじめとし，地域大学間の積極的な連携が様々な方法で進められている．その 1 つとして，テレビ会議システム等の ICT（Information and Communication Technology）機器を活用した複数大学間での遠隔講義が挙げられる．例えば，大学コンソーシアム佐賀では, Adobe Connect Pro を利用し，ネットワークや音声・映像の遅延・切断等の大きなトラブルを発生させることなく，加盟 5 大学間での同期型遠隔講義を年間 6 科目配信している[2]．また，e-Knowledge コンソーシアム四国では，H.323 プロトコルで映像・音声等の相互配信が可能な Polycom，TANDBERG，SONY 各社製のテレビ会議システムを利用し，加盟 8 大学間での同期型遠隔講義を，2009 年度には 13 科目，2010 年度には 3 科目配信している[3]．

上述のような大学間連携組織では同期型遠隔講義を年間数科目程度配信しており，その際，システム管理者あるいは講義支援者がテレビ会議システムの接続・切断を毎回マニュアル操作していた．また，配受信大学間における時間割の違いが問題点として指摘されており，その解決策としては加盟大学間の時間割を統一した組織や，通常の対面講義は配信せず特別講義や集中講義等の比較的短期間かつ不定期な講義をテレビ会議システムによって配受信することとした組織もある．

一方，信州大学が加盟する「高等教育コンソーシアム信州」（以下，本コンソーシアム）においては，講義の共同利用を通した長野県内高等教育の個性化と魅力ある人材育成を目指すため，通常の対面講義を積極的にネットワーク配信する必要がある．その背景には，通常の対面講義を前提とした従来の大学間単位互換制度の踏襲と大学間における物理的・地理的な障害があった．

そこで本研究では，前述の問題を解決し，通常の対面講義でのネットワーク配信を実現するため，テレビ会議システムを活用した大学間遠隔講義システムを構築した[4]．そのシステム制御には，簡便な操作性を実現するためにタッチパネルを利用し，各遠隔講義室内にあるテレビ会議システムの接続・切断やカメラの操作，プロジェクタ用スクリーン等への PC・映像出力の切り替えをタッチ操作で行えるようにした．なお，本研究の大学間遠隔講義システムとは，各大学の遠隔講義室や遠隔会議室に講義や会議を配受信するためのシステムのことを示す．

2. 通常講義を遠隔配信する場合の問題点

信州大学においては，通常の対面講義を，ネットワークを用いて遠隔配信することを目標としている．しかしながら，先行研究[2][3]での指摘の通り，配受信大学間の時間割や学年歴の違いに起因した学生の受講に対する時間的制約が, 本コンソーシアムにおいても問題となった．そこで前研究では，先の大学間遠隔講義システムの構築に続いて，同期型遠隔講義を収録・コンテンツ化し，時間割や学年歴の違いによってリアルタイムで受講できない学生が，収録された講義コンテンツを視聴して補講できるための仕組み（以下，遠隔講義収録・配信システム）を設計・構築した[5]．

2010 年度前期（4 月～8 月），本コンソーシアムでは 11 科目の同期型遠隔講義が配信された．この期間，テレビ会議システムの接続・切断は各配受信大学のシステム管理者あるいは講義支援者が毎回マニュアル操作で実施した．また，遠隔講義収録・配信システムでの収録開始・停止，及び講義コンテンツの公開作業は信州大学のシステム管理者が毎回マニュアル操作で実施した．これらの遠隔講義配受信の結果，①遠隔講義収録・配信システムの利用によりリアルタイムで受講できなかった学生へのフォローアップ，②リアルタイムで受講した学生の自発的学習につながる可能性を示唆することができた[6]．しかし，この期間の遠隔講義配受信を通して新たに次のような 5 つの問題点が明らかになった．

問題点 1．システム操作者の拘束

テレビ会議システムの接続・切断はマニュアル操作であるため，各配受信会場のシステム管理者あるいは講義支援者は，毎日 2～3 回開講される各遠隔講義の開始・終了時刻前後に遠隔講義室に行かなければならない．そのため，遠隔講義がある度，彼らは時間的に拘束されてしまい，会議への参加や休み時間中の学生指導等の他の業務に支障を来すことがあった．また，彼らが学外出張等で不在の場合には，講義担当教員あるいは受講生がテレビ会議システムの操作を実施したが，操作に慣れていないため講義準備に手間取る等の問題が発生し，遠隔講義を円滑に配受信することが困難となる問題が発生した．

問題点 2．接続遅延に伴う講義時間の短縮

テレビ会議システムではコンピュータ画像を送信することが可能であるが，すべての配受信会場が接続されてから送信開始しなければ正常に送信できない問題が多々生じた．そのため，すべての配受信会場が接続されるまで講義担当教員はコンピュータ画像の送信及び講義開始を待つことになり，1 会場でも接続が遅れるとその分講

義時間が短くなってしまう問題が度々生じた.

問題点 3. 講義コンテンツ公開作業の煩雑さ

すべての遠隔講義は収録・コンテンツ化され，LMS（Learning Management System）上で公開される．しかし，収録から公開までに係る作業は信州大学のシステム管理者がすべてマニュアルにて操作しており，その作業内容は煩雑なものであった．そのため，学生が講義コンテンツを視聴できるまでには講義終了後 1 日程度の時間を要する問題が発生した．また，講義コンテンツの公開を忘れてしまうといった人為的なミスがあり，1 週間程度講義コンテンツの公開が遅れる問題も発生した.

問題点 4. 受信会場の学生把握の困難さ

受信会場にあるカメラのズーム機能によって画角が広くなっており，受講生がカメラから遠く離れた場所に座っていた場合，講義担当者からは受講生が小さく見えるため，講義担当者が受信会場にいる受講生の様子や表情を覗うことは困難であった．また，接続時のカメラの画角から外れている受講生は講義担当者から見ることができないため，受講生の把握が困難であった.

問題点 5. システム操作用タッチパネル数の不足

各遠隔講義室にはテレビ会議システム操作用のタッチパネルが 1 台しか設置されていない．そのため，特に TA（Teaching Assistant）等を配置している講義（2010 年度前期では 11 科目中 4 科目）や講義以外の遠隔配信イベントにおいては，タッチパネルが講義担当教員や演者に専有されてしまうと，システム管理者や TA を含む講義支援者による遠隔配信中のカメラ操作支援が困難であった．また，講義担当教員と講義支援者との間で講義中にタッチパネルを授受する状況が生じ，その度に講義進行の妨げとなった.

そこで各テレビ会議システムに対するタッチパネルの増設を検討したが，ハードウェア自体が大変高価なものであり，予算面から容易に増設することができなかった.

3. 研究目的

本研究の目的は前章で示した 5 つの問題点を解決し，より効果的・効率的に通常の対面講義でのネットワーク配信を可能にすることである．これらの問題点はシステム操作の大部分がマニュアル操作であることに起因しており，すべての操作を自動化することによって大幅に改善できるものと考えられる．そこで本研究では，次の要件を満たすシステム・機能の構築・実装によってこれらの問題点を解決することを提案する（隅付括弧内は各要件に対応する前章中の問題点を示す）.

(1) 遠隔講義接続・切断の自動化【問題点 1，2】

遠隔講義の予約・スケジューリング機能を構築し，講義開始・終了時刻にテレビ会議システムが自動的に接続・切断するシステムを開発する．これにより，接続・切断のために各配受信大学のシステム管理者あるいは講義支援者が毎回遠隔講義室に行かなくとも，予約された時間と配受信会場で遠隔講義が開始・終了できるようになる．また，時間通りに接続されるため，接続遅延に伴う講義時間の短縮も同時に防止することができる.

(2) 講義コンテンツ配信の自動化【問題点 3】

遠隔講義収録システムで収録された講義コンテンツを配信サーバに自動転送するシステムを開発する．さらに本システムでは，受講生が LMS 上の各遠隔講義コースにアクセスすると，配信サーバ上にある講義コンテンツの一覧が見られるように構築する．これにより，受講生は遠隔講義終了後すぐに LMS 上から毎回の講義コンテンツを視聴できるようになる.

(3) カメラの遠隔制御【問題点 4】

これまで各受信会場の操作は各受信会場に設置されているタッチパネルでのみ操作が可能であったが，これを配信会場のタッチパネルから各受信会場のカメラを遠隔操作できるようにシステムの実装を変更する．これにより，配信会場にいる講義担当教員は受信会場のカメラの向きを自由に操作し，ズーム機能を利用して各受信会場にいる受講生たちの様子や表情を覗うことができるようになる.

(4) コントロールプログラムの iPad 対応【問題点 5】

Apple 社製 iPad はマルチタッチ操作に対応したタブレット型コンピュータであり，比較的安価に導入することが可能である．そこで，既設タッチパネルに導入されているテレビ会議システム用コントロールプログラムを iPad 上で実行する．さらに操作対象となる遠隔講義室を特定せず，コントロールプログラムが導入された iPad をどの講義室に持ち込んでも，その講義室のテレビ会議システムが操作できるようプログラムを開発する．これにより，iPad に対応したコントロールプログラムを複数の iPad に導入・複製するだけで，容易かつ安価にタッチパネルを増設することができるようになる.

本稿では，上述の要件を満たした「遠隔講義予約システム」「カメラ遠隔制御システム」「講義コンテンツ自動配信機能」「iPad 対応コントロールプログラム」の構築・実装について述べる.

4. 既設システムの概要

第 1 章及び第 2 章で述べた通り，これまでに，通常の

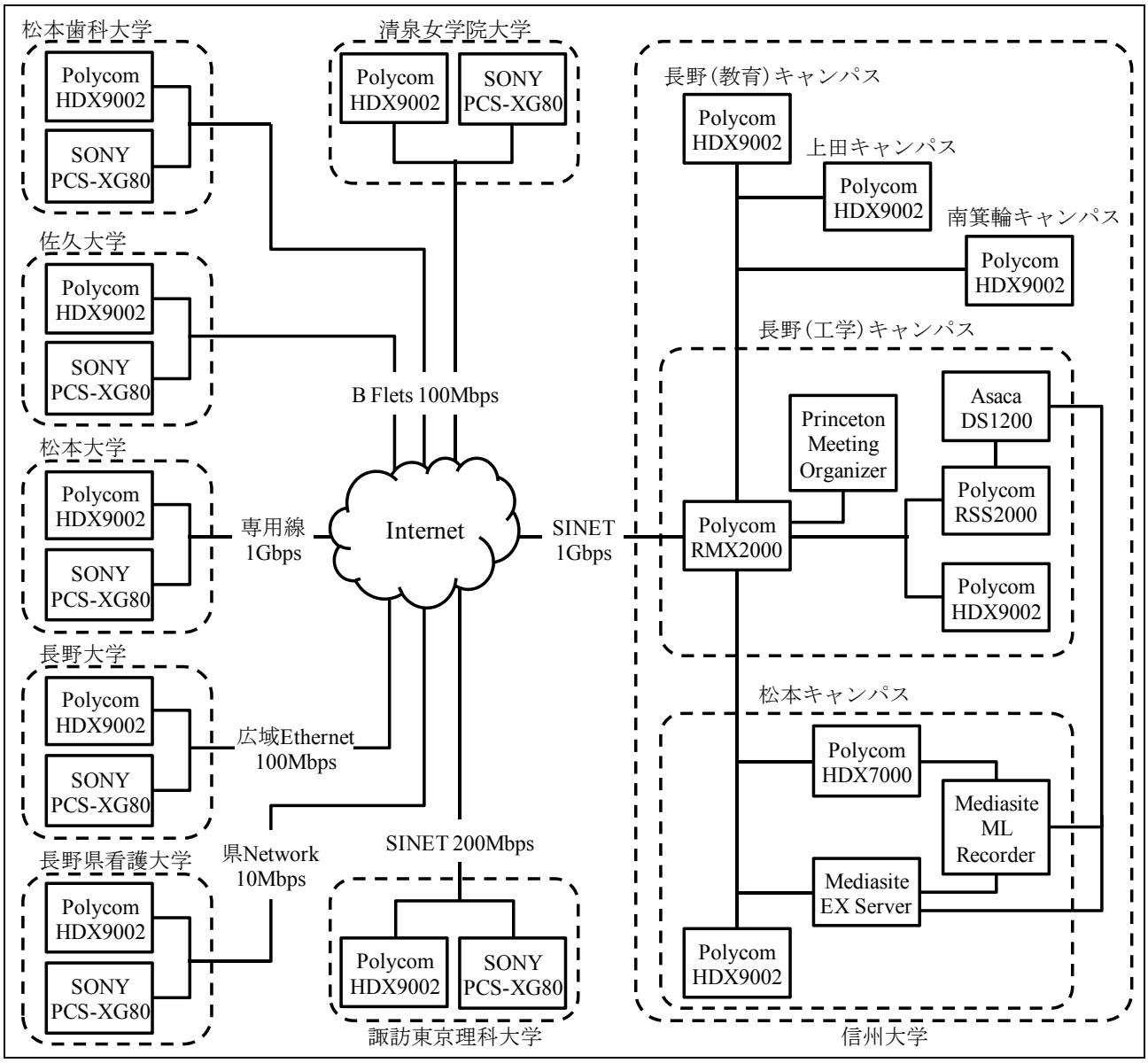


図 1　大学間遠隔講義システムの概要（2010 年度末時点）

対面講義をネットワーク配信するための「大学間遠隔講義システム」と，同期型遠隔講義を収録・配信するための「遠隔講義収録･配信システム」を構築してきた[4][5].

4.1. 大学間遠隔講義システム

各大学には，HD（High Definition）画質の映像・音声及びコンピュータ画像が一般のインターネット光回線等を利用して配受信可能なテレビ会議システムを設置した. テレビ会議システムは各大学 2 台ずつあり，遠隔講義室には Polycom 社製 HDX9002 を，遠隔会議室には SONY 社製 PCS-XG80 を設置した（図 1）.

各遠隔講義室には，講義担当教員等が比較的容易に遠隔講義を実施できるようにするため，タッチパネルが 1 台設置されており，専用無線 LAN アクセスポイントを経由してテレビ会議システムを操作できるようにした[4]. ただし，このタッチパネルに導入されたコントロールプログラムは Polycom 社製テレビ会議システムに対応したものであるため, 遠隔会議室には設置されていない.

また，複数の遠隔講義室あるいは遠隔会議室が同時に講義あるいは会議に参加できるようにするため，信州大学内既設の多地点接続装置（Multi-point Control Unit ; 以下，MCU）: Polycom 社製 RMX2000 を利用した.

4.2. 遠隔講義収録・配信システム

すべての遠隔講義では，信州大学内に設置された Polycom 社製 HDX7000 を通じ，遠隔講義収録システム：Mediasite 社製 ML Recorder（以下，Mediasite Recorder）にてコンテンツ化できるようにした. また，収録された

講義コンテンツは配信サーバ：Mediasite 社製 EX Server（以下，Mediasite EX Server）にアップロードされ，LMS を介して当該遠隔講義の受講生のみに公開されるようにした[5]. なお, Mediasite Recorder 及び Mediasite EX Server 内の HDD（Hard Disk Drive）空き容量を確保するため, 経年化した講義コンテンツをコンテンツ蓄積サーバ：Asaca 社製 DS1200 に定期的に転送し, その後両システム上から削除することにした.

一方， Mediasite Recorder にて遠隔講義が収録できなかった場合に備え，既設テレビ会議レコーダ：Polycom 社製 RSS2000 を利用し，すべての遠隔講義を録画した. このテレビ会議レコーダについても, HDD 空き容量を確保するため，経年化した録画コンテンツをコンテンツ蓄積サーバに定期的に転送し，その後テレビ会議レコーダ上から削除することにした.

4.3. 2010 年度前期遠隔講義の実施方法と問題点

2010 年度前期は信州大学を含む 6 大学から 11 科目の遠隔講義が毎週配信され，全 8 大学 100 名の受講生（うち，45 名は聴講・市民受講生）が遠隔地の会場から参加した. 遠隔講義の配信曜日及び時限は表 1 の通りであり，毎日 2～3 科目が配信された（表中の“✓”は遠隔講義配信があったことを示す）.

各遠隔講義実施における大学間遠隔講義システム及び遠隔講義収録・配信システムの運用方法は表 2 の通りであった. 表 2 のような運用を行った結果，すべての配受信会場が接続完了するまでに最大 5 分程度の時間を要してしまい，時間通りに講義を開始できないことが平均 1 割（週 1 回）程度あった. また，すべてのシステム操作をマニュアルで行ったため，MCU の接続先 IP アドレスや会議室番号を間違えて入力してしまったり，テレビ会議レコーダや Mediasite Recorder での収録開始をし忘れたりといったミスオペレーションが平均 1 割（週 1 回）程度あり，遠隔講義実施や講義コンテンツ提供に大きな支障を来していた.

表 1　2010 年度前期遠隔講義配信スケジュール

	月曜	火曜	水曜	木曜	金曜
1 限	✓			✓	
2 限		✓	✓	✓	✓
3 限		✓			
4 限					
5 限	✓		✓	✓	✓

5. 遠隔講義接続とコンテンツ配信の自動制御

4.3.の遠隔講義実施から明らかになった問題点を解消するため，第 3 章で述べた要件（1），（2）を満たす「遠隔講義予約システム」を構築し，テレビ会議システムの

表 2　2010 年度前期遠隔講義の実施方法

時間	各大学講義支援者	信州大学システム管理者
5 分前	● テレビ会議システムの起動	● Polycom HDX7000 の起動 ● 遠隔講義収録システムの起動 ● テレビ会議レコーダの Web コントローラーにアクセス
2 分前	● あらかじめ指定された MCU の会議室番号に接続	● あらかじめ指定された MCU の会議室番号に Polycom HDX7000 を接続
講義開始時刻		● テレビ会議レコーダによる収録を開始 ● 遠隔講義収録システムによる収録を開始
講義実施		
講義終了時刻	● テレビ会議システムの切断 ● テレビ会議システムの終了	● 遠隔講義収録システムによる収録を停止 ● テレビ会議レコーダによる収録を停止 ● Polycom HDX7000 の切断
講義終了後		● 講義コンテンツの配信サーバへの転送 ● 講義コンテンツ配信サーバ内の各講義コンテンツへのリンクを LMS 内の各講義コースに貼り付け

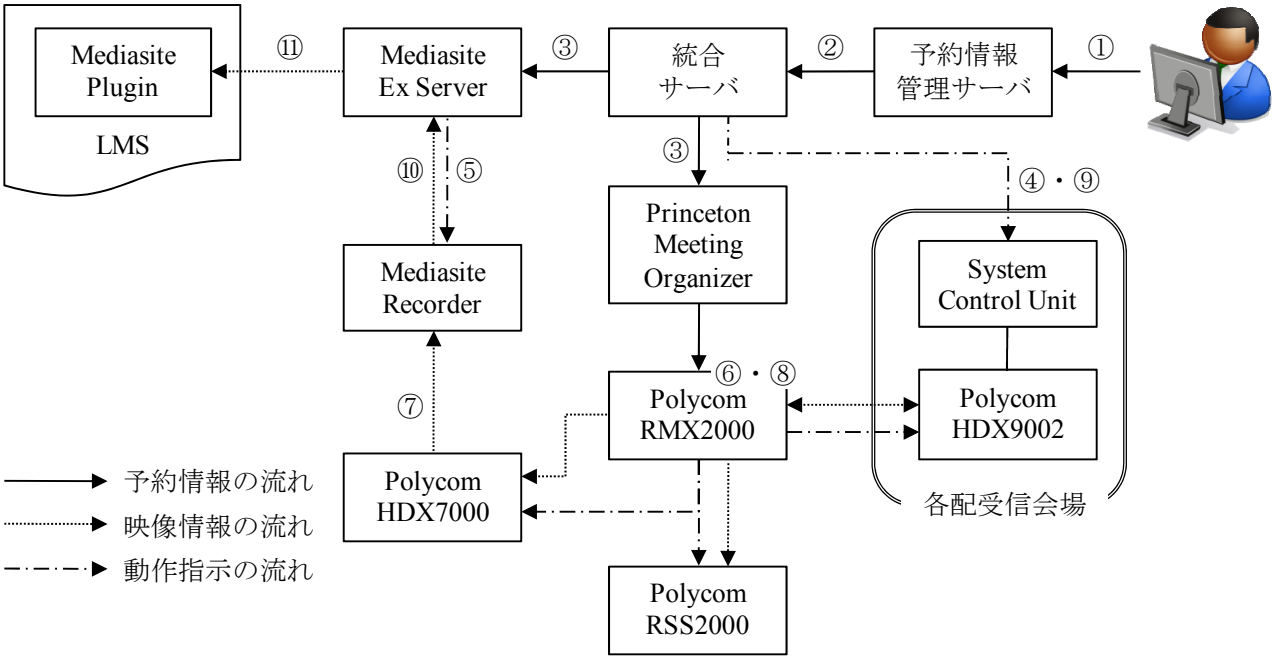


図 2　遠隔講義予約システムの概要

起動・終了及び接続・切断と講義コンテンツの収録・配信に係るすべての作業を自動化することにした.

5.1. 遠隔講義予約システム

遠隔講義予約システムは第 3 章で述べた要件 (1), (2) を満たし，テレビ会議システムの起動・終了及び接続・切断と遠隔講義収録・配信システムの収録開始・終了を予約・スケジュール管理，自動制御するための仕組みである．このシステムの主な構成は次の通りである.

予約情報管理サーバ : 本コンソーシアム事務局員が入力した遠隔講義開始・終了時刻や講義コード，配受信会場等をもとに予約情報を生成・管理する.

統合サーバ : テレビ会議システム接続に関する情報を会議マネージメント&スケジューリングシステムである Princeton 社製 Meeting Organizer（以下，Princeton Meeting Organizer）に，講義コンテンツの収録に関する情報を Mediasite EX Server に，機器の起動・終了情報を各配受信会場にある System Control Unit にそれぞれ送信する.

Princeton Meeting Organizer : 各配受信会場にあるテレビ会議システムとの接続・切断を，予約情報に従って MCU に指示する.

遠隔講義予約システムにおける動作の流れは次の通りである（図 2）．なお，図 2 中の実線矢印は予約情報の流れ，点線矢印は映像や音声，コンピュータ画像情報の流れ，長鎖線矢印は起動・終了や接続・切断，あるいは収録開始・終了等の機器動作に関する指示の流れを表している．さらに，図中の丸付数字は本文に対応している.

① 当該遠隔講義の前日までに，当該講義の開始・終了時刻，配受信会場等の情報を予約情報管理システムに入力する．なお，予約日時は定期（毎週・毎月）指定することができるため，前・後期の始めに当該講義のすべての日時を予約しておくことで毎回の入力の手間を省くことができる.

② 予約開始時刻 15 分前に，予約情報管理システムから統合サーバに予約情報が送られる.

③ 統合サーバから Mediasite EX Server 及び Princeton Meeting Organizer にそれぞれ予約情報が送られる.

④ 予約開始時刻 3 分前に，統合サーバから各配受信会場の System Control Unit を経由してテレビ会議システムに起動指示が送られる.

⑤ Mediasite EX Server から Mediasite Recorder に対して，予約情報及びアップロード先となる Mediasite EX Server 上の講義フォルダ情報とともに，予約開始時刻に収録を開始するよう指示が送られる.

⑥ 予約開始時刻になると，Princeton Meeting Organizer から MCU に配受信会場の情報が送られる．その情報に基づき，MCU は各配受信会場のテレビ会議システム及びテレビ会議レコーダを呼び出し，MCU に接続させる．また，テレビ会議レコーダは，MCU への接続が完了すると自動的に録画を開始する．万が一，ある配受信会場のテレビ会議システムが接続できなかった場合は，そのシステムに対して自動的に再接続を試みる.

⑦ MCU から送られた映像・音声及びコンピュータ

画像は Polycom 社製 HDX7000 を経由して Mediasite Recorder に送られ，オンタイムでコンテンツ化される．

⑧ 予約終了時刻 1 分前に，MCU は各配受信会場との接続を切断する．切断前であれば，コントロールプログラム上に用意された[予約延長]キーから予約終了時刻を 10 分単位で延長することができる．ただし，[予約延長]キーを操作しても Mediasite Recorder の収録時間は延長されない．

⑨ 予約終了時刻になると，統合サーバから各配受信会場の System Control Unit にシステム終了指示が送られ，各テレビ会議システムはスタンバイモードに移行する．

⑩ Mediasite Recorder は⑤の講義フォルダ情報に基づき，収録した講義コンテンツを Mediasite EX Server 上の講義フォルダにアップロードする．

⑪ 受講生は LMS にインストールされた Mediasite Plugin を通して，Mediasite EX Server 上の講義コンテンツを視聴する．

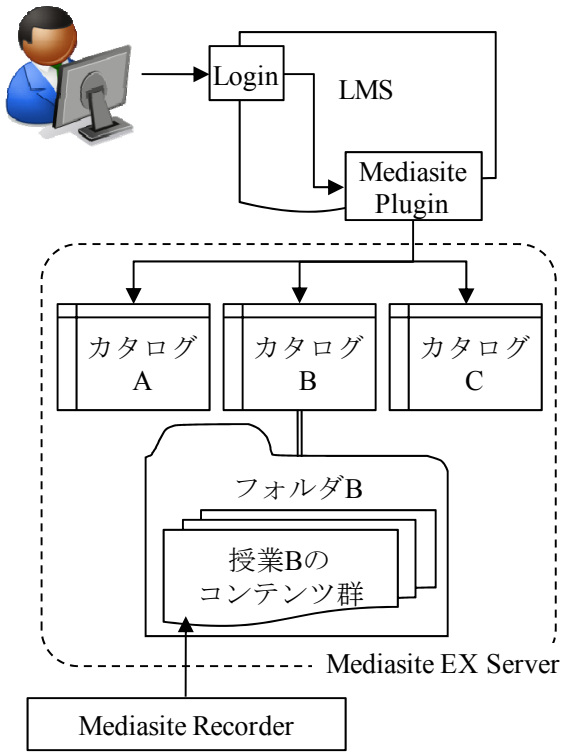


図 3　講義コンテンツ自動配信機能の概要

5.2. 講義コンテンツ自動配信機能

遠隔講義予約システムの利用により Mediasite Recorder で収録された講義コンテンツは，自動的に Mediasite EX Server 上の講義フォルダにアップロードされる．この講義フォルダにアップロードされた講義コンテンツ群を公開する場合には，講義フォルダごとに「カタログ」と呼ばれるオンラインコレクションを作成する．カタログでは任意の講義フォルダから選ばれた複数の講義コンテンツをグループ化し，講義の詳細とリンクを一覧表示させることができる．また，講義コンテンツの検索・ソート機能を有しており，講義コンテンツを検索し，結果を絞り込んだり，並び替えたりすることもできる．

一方，Sonic Foundry, Inc.では，Blackboard や Moodle, Sakai 等の LMS から Mediasite EX Server 上にある講義コンテンツあるいはカタログの参照を可能とする Mediasite Plugin を無料配布している[7]．Mediasite Plugin を利用することにより，LMS にログインしている講義担当教員及び受講生は，新たなログイン認証操作をせずに，Mediasite EX Server 上にある特定の講義コンテンツあるいはカタログを参照できるようになる．そこで，本研究では要件（2）を満たすべく Mediasite Plugin を LMS に導入し，講義コンテンツ自動配信機能を構築した（図 3）．

5.2.1. 機能運用に係る準備

講義コンテンツ自動配信機能の運用には各遠隔講義の初回講義時に準備が必要であり，その手順は次の通りである．なお，本研究の LMS には Moodle を使用した．また，LMS には Mediasite EX Server の管理者アカウントと同一のユーザ ID 及びパスワードを持つアカウント（以下，接続用アカウント）を予め作成する必要があった．

(1) 各遠隔講義の初回講義終了後，Mediasite EX Server 上に当該講義用のカタログを作成し，当該講義フォルダを参照するように設定する．

(2) 接続用アカウントで LMS にログインする．

(3) LMS 上の当該講義コースに「Mediasite コンテンツ」を追加する．Mediasite コンテンツは LMS に Mediasite Plugin をインストールすることによって LMS 上に追加されるコンテンツである．

(4) Mediasite コンテンツのタイトル名とリソース ID を設定する（図 4）．リソース ID とは，Mediasite EX Server 上の各講義コンテンツが持つ固有 ID である．なお，リソース ID は図中の [Mediasite コンテンツを検索]から検索・指定することができる．

以上の準備が完了すると，Mediasite Recorder で収録された講義コンテンツは図 2⑩のフローにより Mediasite EX Server 上の講義フォルダに自動的にアップロードされ，⑪のフローにより LMS 上の当該講義コースにある Mediasite コンテンツを通して公開されるようになる．これにより，受講生は講義終了直後から LMS 上の Mediasite コンテンツから講義当日の講義コンテンツを視聴することができるようになった．

図 4　Mediasite コンテンツの追加画面例

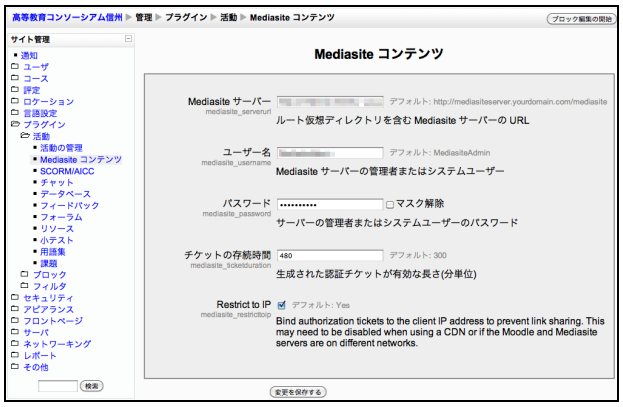


図 5　Mediasite コンテンツのプラグイン設定画面

5.2.2. LMS-Mediasite EX Server 間の認証

受講生は自身が履修している科目の講義コンテンツを利用できなければならないが，講義コンテンツを管理する Mediasite EX Server にはアクセス権を設定する機能がない．そのため，受講生が LMS にログインする操作のみで Mediasite EX Server に適切にアクセスすることができるようシステムを構成した．図 3 で示すように受講生は LMS にログインし，履修している科目の講義コンテンツにアクセスする．そして，講義コンテンツにアクセスする場合，LMS 内の Mediasite Plugin を通じて Mediasite EX Server 上の適切な講義コンテンツにアクセスする．これによりアクセス権を設定できない Mediasite EX Server にて適切なアクセス制御が可能となる．

Mediasite Plugin では，LMS 上のプラグイン設定フィールドにおいて，接続先となる Mediasite EX Server の URL と Mediasite EX Server の管理者アカウントを設定している（図 5）．受講生が LMS 上の Mediasite コンテンツにアクセスすると，これらの設定に基づき LMS-Mediasite EX Server 間の接続認証がなされる．LMS-Mediasite EX Server 間の認証が完了すると，Mediasite EX Server はユーザに対して認証チケットを発行する．認証チケットには LMS ログイン時の「ユーザ名」「IP アドレス」，Mediasite コンテンツの「リソース ID」「接続開始時刻」「接続用アカウント」情報が格納される．従って，認証チケットの有効時間（本研究では 480 分に設定）内であり，かつ認証チケットの格納情報が一致している限りにおいては，再認証を必要とせずに LMS 上の Mediasite コンテンツから Mediasite EX Server にアクセスすることができる．

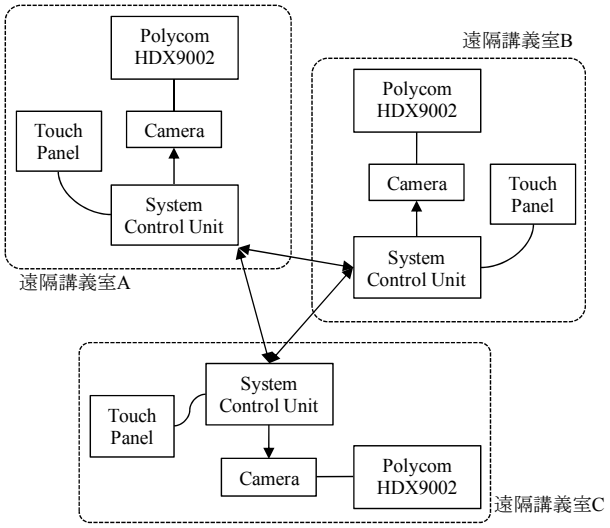


図 6　カメラ遠隔制御システムの概要

6. 制御デバイスの拡張

6.1. カメラ遠隔制御システム

第 3 章で述べた要件（3）を満たし，配信会場にいる講義担当教員が各受信会場の受講生の様子や表情を自由に把握できるようにするため，カメラ遠隔制御システムを構築した．このシステムでは，各配受信会場に設置された System Control Unit 間のカメラ制御信号の送受信によって，配信会場から受信会場のカメラ向きの上下左右移動，ズーム操作，受信会場内前後に設置されたカメラの送出切替ができるようにしている（図 6）．なお，図 6 中の実線矢印はカメラ制御信号の向きを示している．

System Control Unit の制御は，配信会場の講義担当教員等がタッチパネルを使用して行う．図 7 は実際のタッチパネル画面例であるが，画面左下にある[カメラ制御] ボタンをタッチし，操作する対象（自局カメラか遠隔カメラか）を選択する仕組みになっている．ここで[遠隔カメラ]を選択すると，図 8 のようなカメラの遠隔制御画面が表示される．

カメラの遠隔制御をするには，まず“拠点選択”一覧から操作したい受信会場を選択する．続いて“カメラ制御”から受信会場の前後どちらのカメラを操作するかを選択する．その後，MCU から送られてくる受信会場の

図 7　タッチパネル画面例（“カメラ制御”選択時）

図 8　カメラの遠隔制御画面例

映像を見ながら画面中央の上下左右ボタン及び[ZOOM]ボタンをタッチしてカメラを遠隔操作する．なお，映像送出するカメラを切り替えたい場合は，画面右側にある“カメラ切替”にて映像送出したいカメラを選択する．

6.2. コントロールプログラムの iPad 対応

iPad は Apple 社から販売されているマルチタッチ操作可能なタブレット型コンピュータである．ディスプレイサイズは 9.7 インチであり，既設タッチパネルの大きさと大きく変わらない．そのため，従来の操作性を損ねない上，薄く軽量な iPad であれば会場内の様々な場所で利用が可能であり利便性が向上する．また，既設タッチパネルでは専用無線 LAN アクセスポイントを経由してテレビ会議システムを操作しているが，iPad にも Wi-Fi 機能が搭載されており，既設タッチパネルと同様に無線 LAN 通信でテレビ会議システムを操作できると考えられた．そこで第 3 章で述べた要件 (4) を満たし各講義室のタッチパネルをより安価に増設するため，既存コントロールプログラムを iPad 上でも実行できるようにした．

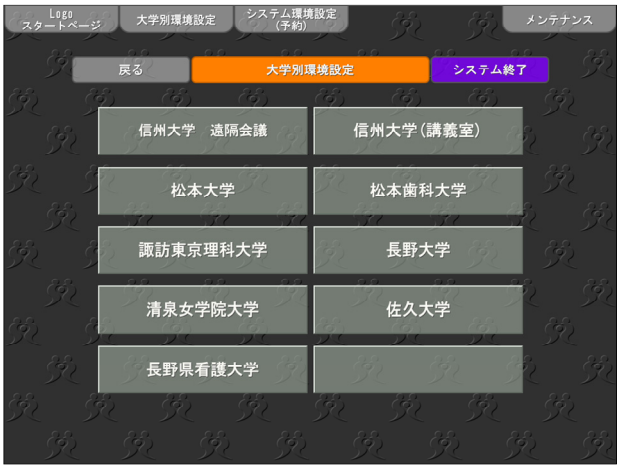


図 9　コントロールプログラム切替画面

6.2.1. iPad 専用デバイスアプリケーションの導入

既設タッチパネルは AMX 社製のものを使用しており，既存コントロールプログラムは AMX 社製タッチパネル専用のデバイスアプリケーション上で動作していた．そのため，既存コントロールプログラムを iPad 上で実行するためには，iPad 専用のデバイスアプリケーションを導入する必要があった．

そこで，本研究では AMX 社製アップルデバイスアプリケーション「TPControl」（TPC-IPA）を iPad に導入することにした[8]．既設タッチパネルと同じメーカーから提供されているデバイスアプリケーションであったため，iPad に AMX 社製 TPControl を導入し，TPControl 上で既存コントロールプログラムを実行させることは比較的スムーズに実現できた．

6.2.2. コントロールプログラムの切り替え機能

遠隔講義室の機器環境は加盟大学ごとに大きく異なっている．また，既設タッチパネルは遠隔講義室間の持ち運びを想定していなかったため，各講義室の機器環境のみに対応した専用コントロールプログラムを導入していた．しかし本研究では，第 3 章で述べた要件 (4) の通り，同一の iPad 対応コントロールプログラムを複数の iPad に複製するだけで加盟大学のどの遠隔講義室のテレビ会議システムでも操作できるようにすることを要件としており，各講義室のコントロールプログラムを 1 つに集約し，対象の講義室にあわせてコントロールプログラムを切り替えられる仕組みが必要であった．

そこで，コントロールプログラムの iPad 対応にあたってはコントロールプログラム切替機能を実装し，対象の遠隔講義室の機器環境に応じてコントロールプログラムをユーザが選べるようにした（図 9）．ただし，コントロ

ールプログラムを切り替え，対象のテレビ会議システムを操作するためには，①TPControl 上で対象のテレビ会議システムの IP アドレスを設定する，②対象のテレビ会議システムのタッチパネル操作専用無線 LAN アクセスポイントにネットワーク接続する必要があった．

7. 運用と評価

第 3 章で述べた 4 つの要件を満たしたシステム及び機能を構築・実装し，2010 年度後期（9 月～2 月）から実運用を開始した．2010 年度後期は 3 大学 12 科目の遠隔講義が配信され，全 8 大学 59 名の受講生（うち，聴講・市民受講生は 9 名）が遠隔地の会場から参加した．遠隔講義の配信曜日及び時限は表 3 の通りで，2010 年度前期同様に毎日 2～3 科目が配信された（表中の“✓”は遠隔講義配信があったことを示す）．

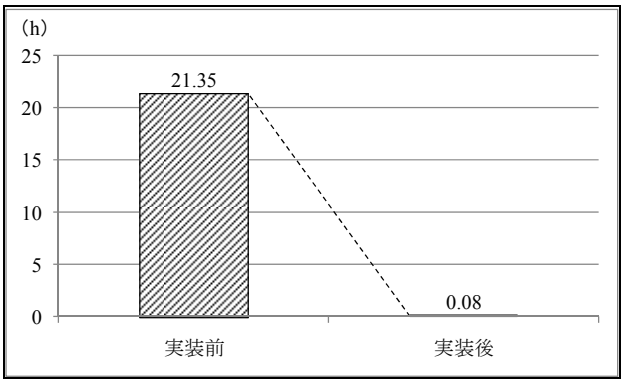
表 3　2010 年度後期遠隔講義配信スケジュール

	月曜	火曜	水曜	木曜	金曜
1 限		✓	✓	✓	
2 限	✓		✓		✓
3 限		✓	✓	✓	
4 限					
5 限	✓				✓

7.1. 遠隔講義予約システム

遠隔講義予約システムは第 3 章で述べた要件（1）を満たし，テレビ会議システムの起動・終了及び接続・切断に係る操作をすべて自動化させることができた．これにより，表 2 のようなマニュアル操作はすべて不要となり，配受信会場のシステム管理者あるいは講義支援者が毎回の講義開始・終了時刻に遠隔講義室に行く必要がなくなった．そして，講義担当教員や受講生のみで遠隔講義の開始・終了が時間通りに行えるようになった．また，すべての配受信会場のテレビ会議システムが時間通りに MCU に接続できるようになり，講義開始時刻が遅れることもなくなった．そのため，平均 1 割（週 1 回）程度生じていたテレビ会議システムの接続遅延に起因した講義時間の短縮は，遠隔講義予約システムの構築後には全く起こらなくなった．

以上のことから，遠隔講義予約システムの構築によって，第 2 章で述べた「問題点 1．システム操作者の拘束」「問題点 2．接続遅延に伴う講義時間の短縮」は解決されたといえる．



※ 実装前の値は 2010 年度前期中の各講義コンテンツを公開するまでに要した平均時間（単位：時間）を示す．ただし，2010 年 4 月は履修登録期間中につき LMS へのアクセス制限をせず講義コンテンツを公開していなかったため，2010 年 5 月から 8 月までに公開されたコンテンツを算出の対象とした（N=108，SD=25.24）．

※ 実装後（2010 年度後期）の値は，公開時刻を記録することができなかったため，ある 1 週間中の各講義コンテンツを公開するまでに要した時間を実測し，そのうちの最大時間（単位：時間）とした．

図 10　授業コンテンツ公開までに要した時間

しかし運用を続けるなかで，講義担当教員らから「講義終了時刻ちょうどにテレビ会議システムが切断されてしまうと，講義終了後に教員と受講生との質疑応答ができない」「チャイムと同時に切断されてしまうと講義終了のタイミングがわからず，中途半端に終わってしまう」といった意見が寄せられ，テレビ会議システムの切断タイミングに関して新たな問題点が明らかになった．システム上では予約終了時刻 5 分前になると終了時刻間際であることを伝えるアナウンスが入るが，話をしていると聞き取りにくく，常に時計を確認していない限り講義終了時刻が近付いていることを把握することは難しかった．

そこで，遠隔講義予約システムの運用方法を一部変更し，予約終了時刻を講義終了時刻の 5 分後に設定することにした（例えば，講義終了時刻が 10 時 30 分の場合は予約終了時刻を 10 時 35 分とした）．これにより，通常の対面講義と同様にチャイムを聞いて講義を終了することができるようになり，さらに講義終了後でも配信会場にいる講義担当教員と受信会場にいる受講生との同期的な質疑応答ができるようになった．

7.2. 講義コンテンツ自動配信機能

LMS 上に実装された講義コンテンツ自動配信機能は第 3 章で述べた要件（2）を満たし，Mediasite Recorder で収録された講義コンテンツが，LMS 上の講義コースから Mediasite EX Server を通して自動的に公開されるようにした．本機能の実装前における講義コンテンツの収録・公開作業はすべてマニュアル操作であり，そのため

公開までに1日程度の時間を要していたが，本機能の実装によりすべての作業は自動化され，受講生は講義終了直後から講義コンテンツを視聴できるようになった（図10）．従って，第2章で述べた「問題点3．講義コンテンツ公開作業の煩雑さ」は解決されたといえる．

しかし実際の運用を通じて，プロキシサーバを経由するネットワーク環境下では講義コンテンツを視聴できないことが明らかになった．その原因は，プロキシサーバを経由する際に IP アドレスが変わってしまうことにあり，発行された認証チケットの格納情報と一致しなくなってしまうことにあった．本研究の運用では，プロキシサーバを経由するネットワーク環境を持った加盟大学が1校あったが，現在はMediasite EX Serverに接続する場合に限り当該プロキシサーバを経由しないように設定を変更している．

7.3. カメラ遠隔制御システム

カメラ遠隔制御システムは第3章で述べた要件（3）を満たし，配信会場にいる講義担当教員によって各受信会場のカメラを遠隔操作できるようにした．これにより，配信会場から受信会場のカメラ向きの上下左右移動，ズームアップができるようになり，カメラから離れたところに座っている受講生の様子や表情等を把握することができるようになった．

しかし，受信会場数が比較的多い遠隔講義の場合では，講義担当教員が各受信会場のカメラを遠隔操作して受講生を捉えるにはかなりの時間を要していた．また，時間割の都合等で遅刻してきた受講生にあわせ講義中に受信会場のカメラを再度遠隔操作することは，講義を一時中断させる必要があるため非常に困難であった．このため，一部の遠隔講義では講義支援者が講義開始時に受信会場のカメラを遠隔操作していた様子が見られた．その結果，「問題点 1．システム操作者の拘束」を解決した遠隔講義予約システムの意義に齟齬を来してしまった．この点については，講義担当教員や講義支援者らから「カメラの自動追尾システムを導入して欲しい」という要望があり，システム改善の余地が認められた．

一方，毎回の遠隔講義において「受信会場内の柱の陰に隠れて受講している受講生がおり，カメラに映らない」といった意見があった．各受信会場のカメラは固定されているため画角は限られてしまい，柱の陰等にいる受講生を捉えることは物理的に困難である．従って，カメラの遠隔操作のみではなく，受講生がカメラの画角内に座るよう指導することが必要であると考えられた．

以上のことから，カメラ遠隔制御システムの構築によって，受信会場数が少なくカメラの画角内に受講生が集まっている場合に限り，第2章で述べた「問題点4．受信会場の学生把握の困難さ」は解決できたといえる．しかし，それ以外の場合にはカメラの操作性やカメラが捉えられる画角の限界からシステム面，運用面で改善の余地があるものと考えられる．

7.4. コントロールプログラムの iPad 対応

AMX社製TPControl及びコントロールプログラム切替機能は第 3 章で述べた要件（4）を満たし，iPad を用いた各遠隔講義室のテレビ会議システムの操作と iPad 対応したコントロールプログラムの複製によるタッチパネルの増設を可能にした．これにより，AMX 社製タッチパネルを導入するよりも比較的安価に，そして容易にタッチパネルを増設することができるようになった．さらに，各遠隔講義室でタッチパネルを特定させる必要がなくなり，1 台の iPad を持ち運ぶことでどの遠隔講義室のテレビ会議システムでも操作できるようになった．

以上のことから，コントロールプログラムの iPad 対応によって，第 2 章で述べた「問題点 5．システム操作用タッチパネルの不足」は，従来に比べて比較的容易かつ安価に解決できるようになったといえる．

なお，遠隔講義時の iPad 利用に際しては，複数のタッチパネル操作により講義進行時の操作がバッティングを起こしてしまうことが懸念されていた．しかし，実際には講義支援者が講義担当者の様子を見ながら操作したため，バッティングしてしまうことはなく，スムーズな操作が行われた．

8. まとめ

本研究では，2010 年度前期遠隔講義を通して明らかになった 5 つの問題点を解決するため，「遠隔講義接続・切断の自動化」「講義コンテンツ配信の自動化」「カメラの遠隔制御」「コントロールプログラムの iPad 対応」の 4 つの要件を満たすシステム及び機能を構築・実装し，より効果的・効率的に通常の対面講義でのネットワーク配信を可能にすることを目的とした．

それぞれの要件を満たす「遠隔講義予約システム」「講義コンテンツ自動配信機能」「カメラ遠隔制御システム」「iPad 対応コントロールプログラム」を構築・実装した結果，遠隔講義の自動接続・切断が可能となり，「問題点 1．システム操作者の拘束」「問題点 2．接続遅延に伴う講義時間の短縮」を解決することができた．また，コントロールプログラムの iPad への導入及び iPad を用いたテレビ会議システムの操作が可能になり，「問題点 5．シ

ステム操作用タッチパネルの不足」に対しては比較的容易かつ安価にタッチパネルの増設ができるようになった．さらにコントロールプログラム切替機能の付与により，タッチパネル（iPad）を各遠隔講義室間で持ち運び，各講義室のテレビ会議システムを操作することができるようになった．

「問題点 3．講義コンテンツ公開作業の煩雑さ」については，講義コンテンツ配信の自動化を通して受講生が講義終了直後すぐに講義コンテンツを視聴できるようになり，大きく改善することができた．しかしプロキシサーバを経由したネットワーク環境下では LMS-Mediasite EX Server 間の認証時にエラーが発生し，講義コンテンツが視聴できないという問題が明らかになった．また「問題点 4．受信会場の学生把握の困難さ」については，配信会場から受信会場のカメラを遠隔操作することを通して，受信会場数が少なくカメラの画角内に受講生が集まっている場合に限り解決することができた．しかし，カメラの遠隔操作の煩雑さや柱の陰にいる受講生を捉えることができないといった新たな問題から，操作性やカメラの画角といったシステム面，着席位置に関する受講生への指導といった運用面から改善の余地が認められた．

本研究における今後の課題は，2010 年度後期の運用を通して明らかになった新たな問題点の解決を図り，遠隔講義における利便性をより向上させることである．

謝辞

本研究は平成 20 年度戦略的大学連携支援事業「大学間地域ネットワーク構築による高等教育の質保証と人材育成の実質化」により実施しました．また，本研究にご協力いただきました株式会社映像センター様，メディアサイト株式会社様，株式会社ディライトテクノロジー様，NEC ネッツエスアイ株式会社様，そして「高等教育コンソーシアム信州」関係各位に心より感謝申し上げます．

参考文献

[1] 文部科学省，“大学教育充実のための戦略的大学連携支援プログラム”，http://www.mext.go.jp/a_menu/koutou/kaikaku/senryaku2.htm，2008

[2] 米満潔，古賀崇朗，藤井俊子，永渓晃二，梅崎卓哉，大谷誠，高崎光浩，岡崎泰久，角和博，中村隆敏，穂屋下茂，近藤弘樹，“多大学間での同期型遠隔授業の実践～大学コンソーシアム佐賀での取り組み～”，大学教育年報，6，pp.66-79，2010

[3] 鈴木正信，林敏浩，“e-Learning による四国の大学連携”，教育システム情報学会研究報告，25，3，pp.39-42，2010

[4] 森下孟，茅野基，鈴木彦文，永井一弥，新村正明，矢部正之，“高等教育コンソーシアム信州における大学間遠隔講義システムを活用した遠隔講義「K^3 茶論」の実践”，学術情報処理研究，14，pp.105-116，2010

[5] 茅野基，森下孟，鈴木彦文，永井一弥，新村正明，矢部正之，“長野県内 8 大学を結ぶ遠隔講義システムを用いたコンテンツ配信の設計”，電子情報通信学会技術研究報告，109，453，pp.53-58，2010

[6] 森下孟，新村正明，茅野基，鈴木彦文，永井一弥，矢部正之，“大学間遠隔講義を支援するための講義ビデオの活用”，日本教育工学会第 26 回全国大会講演論文集，pp.937-938，2010

[7] Sonic Foundry, Inc.，“Work with your current systems? Absolutely”，http://www.sonicfoundry.com/mediasite/integration/，2009

[8] Electori Co., LTD.，“スマートフォンから AMX システムをコントロールするアイデア”，http://amxjp.net/amxpro/comparing_apples.html，2010

学内無線LANアクセスポイントを利用した位置推定における歩行者の影響について

Effects of Walking People on Position Estimation Employing Accese Point in the Campus WLAN system

久保田真一郎† 副島 慶人† 川村 諒† 杉谷 賢一† 武藏 泰雄†
永井 孝幸† 入口 紀男† 右田 雅裕† 喜多 敏博† 松葉 龍一†
辻 一隆† 島本 勝† 木田 健† 宇佐川 毅† 中野 裕司†

Shin–Ichiro KUBOTA†, Yoshito SOEJIMA†, Ryo KAWAMURA†, Kenichi SUGITANI†, Yasuo MUSASHI†, Takayuki NAGAI†, Norio IRIGUCHI†, Masahiro MIGITA†, Toshihiro KITA†, Ryuichi MATSUBA†, Kazutaka TSUJI†, Masaru SHIMAMOTO†, Takeshi KIDA†, Tsuyoshi USAGAWA†, Hiroshi NAKANO†

†kubota@cc.kumamoto-u.ac.jp

† 熊本大学 総合情報基盤センター
† Center for Multimedia and Information Technologies, Kumamoto Univ.

概要
無線 LAN を用いた位置推定の研究は多く行われており，2.4GHz 帯を用いた位置推定については，無線 LAN に限らず，IEEE802.15.4 規格の無線センサネットワーク機器においても広く研究されている．IEEE802.15.4 規格の無線センサネットワーク機器を用いた研究において，歩行者がある場合に位置推定精度が向上するという研究結果が発表されており，同様の周波数帯で通信を行う無線 LAN で構築された情報インフラ環境であっても同様の結果が起こるか検証を行った．その結果，先行研究を支持する結果とはならず，不可視 AP を位置推定に利用する影響に比べると歩行者の往来が誤差に及ぼす影響は小さいことが確認された．本研究結果は，先行研究を否定するものではなく，学内の無線 LAN インフラを用いた場合の位置推定誤差について知見を与えるものである．

キーワード 無線 LAN，位置推定，歩行者

1. はじめに

GPS 端末を利用した位置情報の取得はよく知られているが，端末から GPS 用の衛星への見通しが重要であり，GPS 用衛星への見通しのない屋内において GPS 端末を用いて位置情報を取得することはできない．このような背景のもと，屋内での位置情報を取得する方法として RFID や無線 LAN などの屋内での電波通信を利用したものや超音波を利用したなど様々な研究が行われ，実用化されている．その中でも機器配備などが安価であり，目的は異なるがすでに情報インフラとして配備されているため，無線 LAN による位置情報の取得技術が注目されている [1]〜[3].

位置推定を行うために配備されたアクセスポイント（AP）から受信する受信電波強度（RSSI）の値を利用し，最尤推定手法を用い位置推定を行う Arias らの研究 [4] は十分精度の良い結果を与えている．

情報インフラとして AP が配備される場合は，混信による通信容量の減少を防ぐために，AP からの電波ができるだけ重ならないように配備される．例えば，情報インフラを目的に無線 LAN が整備された大学などの教室では，接続数や各教室のレイアウトにより，見通しの効く位置に AP が少なくとも 1 つ存在するが，不必要に AP が設置されることはない．しかし，隣接する教室に設置された AP の電波や廊下に設置された AP の電波も間接的に受信される．見通しの効く AP（可視 AP）1 台からの受信電波強度のみでは，位置推定の精度は良くないが，見通しの効かない AP（不可視 AP）からの RSSI を利用し，できるだけ精度良く位置推定を行うことが可能である [5], [6]．情報インフラとしての AP を利用した位置推定は，不可視 AP を利用し位置推定を行うため，その精度が悪くなるが，その誤差の大きさを知った上で，その誤差をもつ位置情報を利用することは可能である．

位置推定の研究は，同じ 2.4GHz 帯を利用する IEEE802.15.4 規格の無線センサネットワーク機器においても広く研究されている [7]〜[9]．IEEE802.15.4 規格の無線センサネットワーク機器を用いた研究において，歩行者が存在する場合に位置推定精度が向上するという研究結果 [8] が発表されている．同様の周波数帯で通信を行う無線 LAN で構築された情報インフラ環境であっても同様の結果が起こると予想されるが，一般に，通常の距離による減衰に加えて，歩行者の存在により無線 LAN の電波強度が弱くなると想像され，位置推定精度が下がると予想される．そこで，本研究では情報インフラとして設置される無線 LAN 環境を使い，歩行者が存在する環境と歩行者が存在しない環境とで位置推定を行い，その誤差について考察を行った．

2. 先 行 研 究

Zemek らの研究 [8] では，IEEE802.15.4 規格の 2.4GHz 帯を利用する機器を用い，各ノードは 1.79 メートルから 6.1 メートル離し，各部屋を四角形で区切るようにアンカーノードを設置し，実験を行っている．各アンカーノードの位置は分かっており，この位置をもとに位置の分からないノードの位置が推定される．なお，実験では廊下，待合室，研究室の 3ヶ所で行われており，それぞれにおいて歩行者が存在する環境と歩行者が存在しない環境で実験を行っている．また，位置推定は最尤推定手法を用いて行われ，その位置推定には，RSSI の距離による減衰特性を表すパラメータが必要となるため，それぞれの場所で歩行者が存在する環境と存在しない環境に分けてパラメータを導出し，位置推定を行っている．Zemek らは，各環境において位置の分からないノードの RSSI を測定し，各 RSSI により推定される位置を求めた．いろいろな位置で推定された結果と本来の位置との誤差を各位置で 2 乗平均誤差（RMSE）として求め，それらの平均の変化についてグラフに示している．その中で，廊下と待合室の場合には，RSSI 測定値を 1 つないし 2 つ用いて得られる推定結果に対して，歩行者の存在は推定精度を悪化させ，RSSI 測定値を 3 つ以上用いて得られる推定結果に対しては，歩行者の存在は推定精度を良くする効果があると主張している．また，研究室の場合には，RSSI の測定値の数によらず，歩行者の存在は推定精度を良くする効果があると主張している．このようなことが起こっている原因として，歩行者の存在により測定される RSSI が確率的に独立であると述べている．

Zemek らの論文では，RMSE の平均の推移を示しており，その変化により，前述の主張となっている．この平均の差が確かなものかについて統計的に検証は行っていないため，これ以上のことは不明であるが，歩行者の存在が測定値をよりランダムな値とさせることが，確率的な独立事象性を強め，確率論的な推定にポジティブな効果をもたらすという点は非常に関心がある．そこで，われわれは歩行者の存在

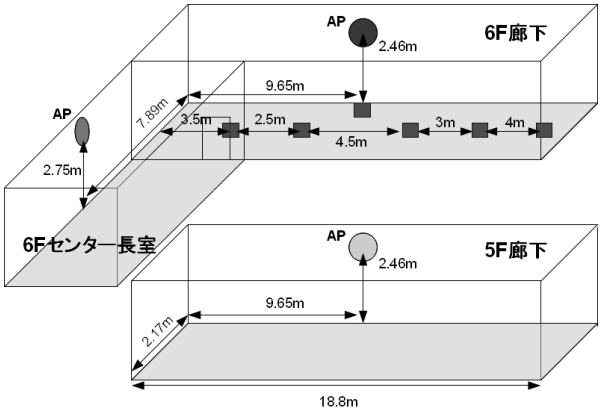


図 1　実験フィールド

図 2 「歩行者あり」の実験の様子

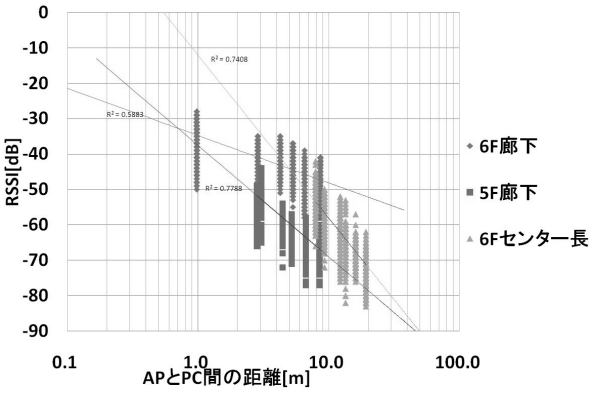


図 3 「歩行者あり」における RSSI と距離の関係

が無線 LAN 推定に与える影響について次節以降で検証を行う.

3.　歩行者の存在が与える影響を調べる実験

インフラのために整備された無線 LAN 環境を用い

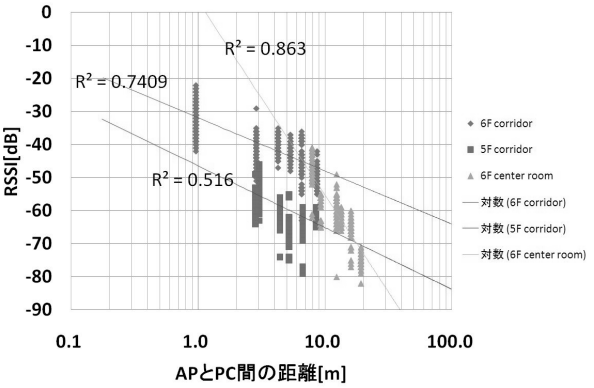


図 4 「歩行者なし」における RSSI と距離の関係

て，歩行者が存在する場合（「歩行者あり」）と歩行者が存在しない場合（「歩行者なし」）とで，位置推定を行い，その RMSE を比較することで歩行者の効果を検証する．今回，実験フィールドには，図 1 のように，6 階の廊下，6 階のセンター長室，5 階の廊下に設置された AP3 台を用いて位置推定を行う．図 1 に示すように，6 階廊下の 6 箇所（壁から 3.5 メートル，6 メートル，9.65 メートル，11.5 メートル，14.5 メートル，18 メートルの位置）を測定ポイントに定め，各測定ポイントにおいて RSSI を測定する．PC の高さは 0.5 メートルに固定し，1 秒ごとに 45 分間 RSSI を測定した．また,「歩行者あり」も「歩行者なし」も人のいない深夜に実験を行い,「歩行者あり」では 4 人の人が廊下をランダムに歩き回る状態とした．図 2 に「歩行者あり」の実験の様子を示す．実験に用いた AP は学内無線 LAN 環境のために配備されている Cisco 社製 AIR-AP1252G-P-K9 を用い，2.4GHz 帯の通信により測定を行った．

先行研究で行われている最尤推定法を用いるためには，事前に推定を行う環境での減衰特性を求めておく必要がある．無線通信において受信電力は距離のベキ指数で減衰し，自由空間であれば距離の-2 乗で減衰することが知られている．マルチパスフェージングなどの他の環境因子による減衰のため，実環境においてはベキ指数の値はさらに小さな値をとる．受信電力を $\Lambda(r)$，AP と測定 PC の距離を r とし，そのベキ指数を α として，実環境での減衰を式に表すと

表 1　減衰特性を表すパラメータ α と C

	「歩行者あり」		「歩行者なし」	
	α	C	α	C
6 階廊下	-1.332	0.000335	-1.504	0.000649
5 階廊下	-3.159	0.000175	-2.166	0.000053
6 階センター長室	-4.604	0.062373	-5.658	1.083927

$$\Lambda(r) = Cr^{\alpha} \tag{1}$$

となる．C は比例定数である．われわれは実環境での距離と RSSI の測定結果をもとに，その実環境における α および C を決定し，そのパラメータをもとに最尤推定法を用いて位置推定を行う．RSSI の確率密度関数が正規分布にしたがうと仮定すると，位置 r で受信信号強度 P_r を受信する確率密度 p は

$$p(P_r|r) = \frac{1}{\sqrt{2\pi\delta^2}}\exp\left(-\frac{(P_r - A(r))^2}{2\delta^2}\right) \tag{2}$$

と表される．ただし，δ^2 は分散を表し，$A(r)$ は $10\log_{10}\Lambda(r)$ で定義される．測定されたデータをもとにパラメータ α および C が決まり，式 (1) を使うと RSSI 測定値から r の期待値が得られる．しかし，それが尤もらしい値かどうかは判別できないため，尤もらしい期待値を導出するために式 (2) を r の関数として考え，測定される RSSI をもとに各 AP に対応する確率密度の積をとり，その積が最大となるような r を求める．この方法が最尤推定法である．

今回の測定による RSSI と距離の関係について「歩行者あり」を図 3 に,「歩行者なし」を図 4 に示す．それぞれ 3 台の AP からの RSSI と距離 r との関係がプロットされている．これより式 (1) にある α および C がそれぞれの AP に対して決定する．表 1 にその結果を示す．次節では，これらのパラメータを用いた位置推定の結果を示し，歩行者の影響について考察する．

4. 考察：不可視 AP を含む環境下における歩行者の影響

実験で行った各測定ポイントでの RSSI をもとに位置推定を行うには，各 AP について式 (2) の積をとり，次式 (3) で定義される尤度関数

$$l(r) = \prod_{i=1}^{n} \frac{1}{\sqrt{2\pi\delta_i^2}}\exp\left(-\frac{(P_{ri} - A_i(r_i))^2}{2\delta_i^2}\right) \tag{3}$$

が最大となる $r(x, y, z)$ を求めればよい．すなわち，x, y, z についての極値を求めることで，推定位置が求まる．このとき，r_i は i 台目の AP と PC との距離を表す．PC の位置を (x, y, z)，i 台の AP の位置を $(x_i, y_i, z_i)[i = 1, 2, \cdots, n]$ と表すと，$r_i = \sqrt{(x - x_i)^2 + (y - y_i)^2 + (z - z_i)^2}$ と表される．推定によって得られる結果と実際の位置との誤差は RMSE を用いて表す．実際の位置を (x_0, y_0, z_0) とし，推定される位置を (x_e, y_e, z_e) とすると RMSE は

$$\sqrt{(x_0 - x_e)^2 + (y_0 - y_e)^2 + (z_0 - z_e)^2} \tag{4}$$

で与えられる．ただし，今回の研究では 6 階フロアのみで測定を行っており，その値をもとに位置推定を行うため，高さ方向の推定は行っていない．

測定した全データにより得られる RMSE の平均は,「歩行者あり」で 2.92 であり,「歩行者なし」で 2.29 となった．これは「歩行者あり」では本来の位置から平均して 2.92 メートルの誤差で位置が推定されることを示し,「歩行者なし」では平均して 2.29 メートルの誤差で位置が推定されることを示している．このことから「歩行者なし」における位置推定精度がよいといえる．また,「歩行者あり」の RMSE の平均と「歩行者なし」の RMSE の平均との差について t 検定を行った結果，その差 0.63 は $P < 0.01$ で有意な差であることが確かめられた．この結果は先行研究とは異なる結果となっており，先行研究で用いられる 2.4GHz 帯のセンサネットワーク機器と学内無線 LAN 機器との相違，および，先行研究のアンカーノード（われわれの研究の AP に相当）がすべて測定位置から可視できるノードによる位置推定であることと本研究のように不可視 AP を利用した位置推定であることとの相違が考えられる．

次に各測定ポイントにおいて「歩行者あり」と「歩行者なし」とで，RMSE の平均を比較した．その結果を表 2 に示す．表 2 を見ると，壁から 3.5 メートルの測定ポイント以外の測定ポイントにおいて,「歩行者あり」の RMSE が大きく,「歩行者あり」の誤差が

大きいことを示している．今回，壁から 3.5 メートルの測定ポイントにおいてのみ「歩行者あり」の誤差が小さいことを示しており，先行研究を支持する結果となった．

この結果は先行研究を一部支持するが，その多くは異なる結果となっており，位置推定に利用するノードを可視できる環境と可視できない環境との違いによる影響が考えられる．そこで，不可視 AP を含む環境の影響と歩行者の影響を区別するために，次節において可視 AP 環境における歩行者の影響について考察を行う．

5. 考察：可視 AP 環境下における歩行者の影響

本節では，前節の不可視 AP を含む環境下における歩行者の効果を理解するために，可視 AP 環境下での推定精度に対する歩行者の効果について考察する．具体的には，歩行者環境が同一の条件となるよう前節の実験データをそのまま用い，各測定ポイントから可視 AP の位置にある 6 階廊下に設置された AP のデータのみを利用し，「歩行者あり」のときの RMSE と「歩行者なし」のときの RMSE について考察する．しかし，測定ポイントに対して可視 AP は，6 階廊下にある AP1 台であり，可視 AP を用いた PC の位置推定は不可能である．そこで，ここでは位置推定の対象を AP とする．つまり，測定ポイント 3ヶ所における RSSI のデータとその 3ヶ所の位置情報をもとに AP の位置を推定する．本来の推定対象である PC とは異なるが，位置推定に利用される技術は同一であり，位置推定誤差の検証は可能である．

表 2 「歩行者あり」と「歩行者なし」における RMSE の平均

壁から PC までの距離	RMSE		RMSE の差
	「歩行者あり」 A[m]	「歩行者なし」 B[m]	$A-B$[m]
3.50	2.26	2.79	-0.53†
6.00	2.28	1.22	1.06†
9.65	1.11	0.61	0.50†
11.50	2.35	1.16	1.19†
14.50	4.53	4.14	0.39†
18.00	4.98	4.02	0.96†

†$P < 0.01$

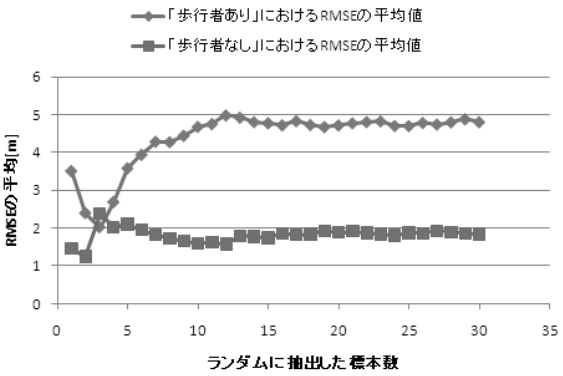


図 5 可視 AP 環境下における「歩行者あり」と「歩行者なし」の RMSE 平均の推移

可視 AP 環境下の減衰特性を表すパラメータ C と α は，前節の表 1 に示される「6 階廊下」における「歩行者あり」と「歩行者なし」のパラメータとなる．いま推定の基点となるのは各測定ポイントであり，測定ポイントの位置情報が既知であるとして，6 階廊下にある AP から受信される RSSI をもとに AP の位置推定を行う．

壁から 11.5 メートル，14.5 メートルと 18 メートルの測定ポイントの位置情報を既知とし，「歩行者あり」と「歩行者なし」のそれぞれの環境での RSSI データをランダムに 30 個抽出し，抽出したデータをもとに位置推定を行い，RMSE の平均をプロットしたグラフを図 5 に示す．その結果，RMSE の平均は，「歩行者あり」で 4.81 であり，「歩行者なし」で 1.84 となり，この平均の差について t 検定を行った結果，その差は $P < 0.01$ で有意な差であることが確かめられた．すなわち，可視 AP 環境下においても，「歩行者あり」の誤差が大きいことが示され，この結果は先行研究とは異なる結果となっている．

表 2 のように不可視 AP を含む環境と比べて，可視 AP 環境下における「歩行者なし」と「歩行者あり」の RMSE の差は大きく，顕著に違いが現れている．これは不可視 AP の場合，その RSSI の値はすでに壁や床の影響を受けた後であり，歩行者の往来による影響と比較すると壁や床の影響による変化が大

きいためであると考えられる．つまり，可視 AP から直接受信される RSSI は歩行者の往来による変化が大きいが，不可視 AP からの RSSI はすでに壁や床の影響を受けており，歩行者の往来による変化は小さいと考えられる．

6. 考察：歩行者の影響と不可視 AP の影響

この節では，これまでの実験結果より位置推定結果の RMSE に着目し，歩行者による影響と不可視 AP による影響の 2 点について考察を述べる．

今回実験を行ったすべての測定ポイントにおいて，6 階センター長室に設置される AP と 5 階廊下に設置される AP を可視することはできない．特に，壁から 14.5 メートルと 18 メートルの測定ポイントでは，他の測定ポイントと比較して明らかに RMSE が大きく，これらの測定ポイントが 6 階センター長室の AP と 5 階廊下の AP と遠ざかっていることからも，不可視の AP の影響により RMSE が大きくなっていると考えられる．このことは前節の考察からも理解できる．前節では，壁から 11.5 メートル，14.5 メートルと 18 メートルの測定ポイントを基点として可視 AP のみを用いた環境下での RMSE を考察した．その結果は,「歩行者なし」で RMSE が 1.84 と，不可視 AP を利用した場合よりも明らかに小さく，不可視 AP を利用すると推定誤差が明らかに大きくなることを示している．

歩行者の影響について，各測定ポイントでその差を確認すると壁から 3.5 メートルの測定ポイントにおいて,「歩行者あり」の場合に精度が向上していた．一方で，それ以外の測定ポイントでは,「歩行者あり」の場合に精度が下がっていた．壁から 3.5 メートルの測定ポイントの結果をさらに詳しく検討するために，壁から 3.5 メートルの測定ポイントで測定した RSSI のデータに対して,「歩行者あり」と「歩行者なし」とでランダムに 30 個抽出し，抽出したデータをもとに位置推定を行い，RMSE の平均をプロットしたグラフを図 6 に示す．その結果，7 個目の推定結果の差までは「歩行者あり」の RMSE の平均が小さく，その後は「歩行者なし」の RMSE の平均が小さくなっている．これらについて t 検定を行ったが，有意な差は見られなかった．このことから標本数の少ない状態では明確にその違いを確認することはできず，歩行者により精度が向上する現象を確認するためには，相応の標本が必要であると考えられる．

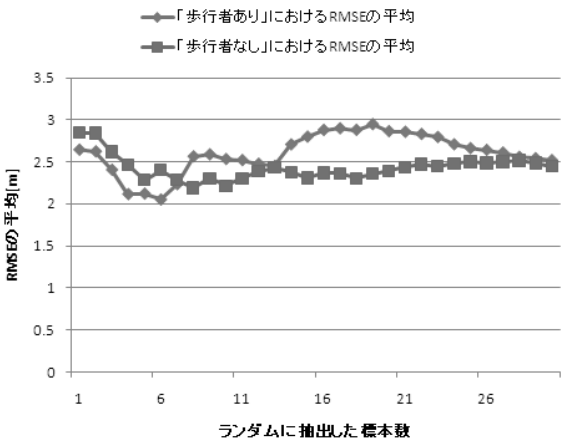


図 6 「歩行者あり」と「歩行者なし」における RMSE の平均の変化（壁から 3.5 メートルの測定ポイント）

その他の測定ポイントにおいて同様の検討を行ったが,「歩行者あり」と「歩行者なし」における RMSE の平均の大小が入れ代わる変化を見せる結果は得られなかった．検証結果のひとつを図 7 に示す．これは，壁から 6 メートルの位置の測定ポイントにおいて測定した RSSI のデータに対して,「歩行者あり」と「歩行者なし」とでランダムに 30 個抽出し，抽出したデータをもとに位置推定を行い，RMSE の平均をプロットしたグラフである.「歩行者あり」と「歩行者なし」における RMSE の平均の大小が入れ代わる変化は見られない．

7. ま と め

45 分間の実験で測定されたデータすべてを用いて位置推定を行い，その RMSE を求め，平均を比較した結果,「歩行者あり」において RMSE の平均が大きくなり，歩行者の往来による影響と不可視 AP の影響を比較すると不可視 AP の影響が大きく，不可視 AP の環境下では歩行者の影響による誤差の変化は小

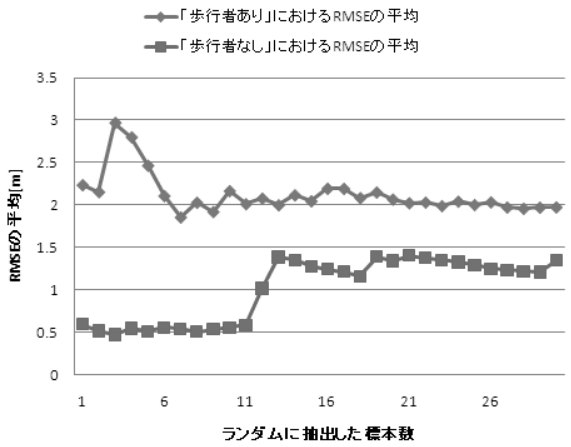


図 7 「歩行者あり」と「歩行者なし」における RMSE の平均の変化（壁から 6 メートルの測定ポイント）

さいことがわかった．また，各測定ポイントに着目し，RMSE の平均を比較した結果，不可視 AP との位置関係による影響があり，われわれが行った情報インフラのための AP を用いた位置推定を行う場合には，不可視 AP を利用する影響が大きく，歩行者の往来の影響は顕著には現れないことが示唆された．Zemek らの先行研究では，歩行者の存在は確率的独立性を向上させ，結果的に推定誤差を小さくするという効果が見込まれたが，インフラとして整備される AP を用いる場合には，直接的にその恩恵を受けることはなかった．

インフラとして整備された AP を利用した位置推定の研究において，これまで歩行者の存在による影響について知見を与える研究はなかった．今回の研究により，不可視 AP を利用した位置推定において，歩行者の往来による推定精度の誤差は，不可視 AP を利用している影響による誤差に比べて小さく，不可視 AP による影響が歩行者の往来の影響を吸収してしまうことがわかった．あらためて言うまでもないが，可視 AP による位置推定が優れており，不可視 AP を含む環境での位置推定は相応の誤差を理解したうえでの利用が必要である．

今回，IEEE802.15.4 規格の無線センサネットワーク機器による先行研究において，歩行者が存在する場合に位置推定精度が向上するという研究結果をもとに，同様の周波数帯で通信を行う無線 LAN で構築された情報インフラ環境であっても同様の結果が得られるか検証を行った．その結果，先行研究を支持する結果とはならず，歩行者の往来による影響と不可視 AP の影響を比較すると不可視 AP の影響が大きく，不可視 AP の環境下では歩行者の影響による誤差の変化は小さいことがわかった．われわれの結果は先行研究を否定するものではなく，学内の無線 LAN インフラを用いた場合において先行研究の示す結果とならず，歩行者による誤差と不可視 AP の影響による誤差について知見を与えるものである．そして，これらの結果は，歩行者の影響を考え，既設の AP を利用した位置推定による位置情報を利用するユーザにとって有用であると考えている．

文　献

[1] 北須賀 輝明, 中西 恒夫, 福田 晃, “無線 LAN を用いた屋内ユーザ向け位置測定方式 WiPS の実装”, 情報処理学会マルチメディア, 分散, 協調とモバイル (DICOMO 2004) シンポジウム論文集, pp.349–352, 2004.

[2] N.Patwri, J.N. Ash, S. Kyperountas, A.O. Hero, III,R.L. Moses, N.s. Correal, “Locating the nodes”, IEEE Signal Process, Vol.22, No.4, pp.54–69, 2005.

[3] 伊藤誠悟, 河口信夫, “アクセスポイントの選択を考慮したベイズ推定による無線 LAN ハイブリット位置推定手法とその応用”, 情報処理学会研究報告, Vol.38, pp.13–18 2006.

[4] J.Arias, A.Zuloaga, J.Lazaro, A.Astarloa, “An RSSI based ad hoc location algorithm”, Microprocessors and Microsystems, Vol.28, pp.403–409, 2004.

[5] 副島慶人, 川村諒, 古川誠一, 杉谷賢一, 久保田真一郎, “学内無線 LAN 環境における電波強度測定による位置推定技術の検討”, 電気関係学会九州支部連合大会講演論文集, Vol.62, 03-1A-10, 2009.

[6] 川村諒, 久保田真一郎, 副島慶人, 古川誠一, 杉谷賢一, “既設アクセスポイントを利用した屋内位置情報取得システムのための位置推定精度による分析”, 情報処理学会論文誌ジャーナル, Vol.52, pp.1357–1364, 2011.

[7] 趙大鵬, 高島雅弘, 柳原健太郎, 武次潤平, 福井潔, 福永茂, 原晋介, 北山研一, “センサネットワークにおける受信信号電力を用いた最尤位置推定法”, IEICE technical report, 104(690), pp.409–414, 2005.

[8] R. Zemek, M.Takashima, D. Zhao, S. Hara, K. Yanagihara, K. Fukui, S. Fukunaga, and K. kitayama, “Effect of walking people on target location estimation performance in an IEEE 802.15.4 wireless sensor network”, IEICE Trans. Commun., Vol.E90–B, No.10, pp.2809–2816, 2007.

[9] S. Hara, D. Zhao, K. Yanagihara, J. Taketsugu, K. Fukui, S. Fukunaga and K. Kitayama, “Propagation Characteristics of IEEE 802.15.4 Radio Signal and Their Application for Location Estimation”, Vehicular Technology Conference,2005. VTC 2005-Spring. 2005 IEEE 61st, Vol.1, pp.97-101, 30 May-1 June 2005.

センターサービス利用登録システムの再構築
Reconstruction of the Registration system of Center Services

岩沢和男 [1], 宮原俊行 [2], 中川 敦 [3],
岩田則和 [4], 西村浩二 [5], 吉冨健一 [6]

IWASAWA Kazuo[1], MIYAHARA Toshiyuki[2], NAKAGAWA Tsutomu[3],
IWATA Norikazu[4], NISHIMURA Kouji[5], YOSHIDOMI Ken-ichi[6]

{iwasawa[1],tmiyahar[2],nakagawattm[3],norita[4],kouji[5],domi[6]}@hiroshima-u.ac.jp

広島大学情報メディア教育研究センター
〒 739-8526 東広島市鏡山 1-4-2
Tel:082-424-6252, Fax:082-422-7043
Information Media Center, Hiroshima Univ.,
Kagamiyama 1-4-2, Higashi-Hiroshima,Hiroshima 739-8526,JAPAN

概要

広島大学情報メディア教育研究センターでは、2010 年 9 月にシステム更新を完了した。新システムで再構築したセンター・サービスの利用登録システムにおいては、「誰がどの機能を使用できるか」を一元管理するため、サービスの機能単位とユーザーグループで構成するサービス管理表を導入した。これにより、サービス利用条件を可視化でき、且つ、利用条件の変更も容易になった。

事務方とのデータ連携においては、教職員、学生および学外者の ID について、LDAP で連携している。何回か起きた大規模な ID 消失等のトラブルに対して、実害を極力抑制できる仕掛けを構築した。

キーワード

サービス管理, ユーザー管理, トラブル回避

1 はじめに

広島大学情報メディア教育研究センター (以下、センター) では、2010 年 9 月にシステム更新を完了した。2000 年度、2005 年度および 2010 年度という都合三回 (約 11 年間) の全システム更新を経て、センターのサービスは多様化し、提供形態も複雑化してきた。その間、システムトラブルや誤操作等による一括削除等が、何度も発生した。センターのとるべき防御的措置について、その都度、貴重な経験を積んで来た事になる。

今回、再構築したセンター・サービスの利用登録システムにおいては、複雑化し多様化するサービスに関して、「誰がどの機能を使用できるか」を一元的に管理するため、サービスの機能単位とユーザーグループで構成する「サービス管理表」を導入した。これにより、サービス利用条件を可視化でき、且つ、利用条件の変更も容易になった。

また、事務方とのデータ連携に際しては、これまでの大規模な ID 消失等のトラブルを教訓に、トラブルが発生した際の実害を (皆無ではないまでも) 極力抑制する仕掛けを構築した。

本センターの実践とその教訓が、多様で複雑なサービスを提供されている他大学情報センターの参考になれば幸いである。この論文では、第 2 章でセンターを取り巻く情報環境の変遷を概観し、利用登録システム再編への必然性を示す。第 3 章でセンターサービスの概要と、

表- 1: 現在のアカウント体系

種別	期限	用途
個人	ID*	各人がメール等のサービスを利用
グループ	ID*	グループでのホームページ公開等
クラス	あり	講習会の講師、受講生等が利用
ゲスト	あり	来学者が情報コンセントを利用

ID*:期限はないが ID が離籍になると無効化

利用登録システムに実装したサービス管理機能について説明する。第 4 章では、センターと事務方とのデータ連携、防御的措置、及びトラブル再発防止に向けた対応の例を説明し、第 5 章で今後の課題を整理する。

尚、セキュリティ等に配慮し、データ連携やトラブルの詳細、事務担当名称等の記述は、必要最小限に留めさせていただく。

2 センター情報環境の変遷

2.1 アカウントおよび ID 管理の変遷

2000 年度のシステム更新時には、それまで各システム個別に発行していたアカウント群に対して、「情報システム利用には、個人の責任を明確化させる」という基本方針で、新しいアカウント体系を導入した [1, 2]。その後、ネットワーク認証用のゲストアカウントを追加して、現在のアカウント体系としている (表-1 参照)。これまでの運用で、アカウント種別については、現状の体系で十分であると判断している。尚、2000 年当時、センターは非構成員情報を独自に管理していた。即ち、学外者へのアカウント発行は、その ID 作成も含めて、センターで勝手に実施していた。

2005 年度に導入したシステムから、センターがサービス対象とする個人の情報は、全学で統一的に ID 管理する事務方の LDAP サーバーから、利用登録システムに日々取り込むようになっている。その際、教職員・学生はもちろん、学外者の登録および ID 管理も、全学レベルで事務方が担当することとなった。そのため、センターで独自に ID を発行する必要はなくなった。

2007 年度には、アカウントに年度更新制を導入するため、センター利用登録システムに対してのみ、改修を行った。これについては、2.3.1 節に記す。

2010 年度のセンターシステム更新においては、サービスの利用主体を、アカウントから ID に変更することとなった。実際、2005 年度のシステムは、LDAP 連携してはいても、サービスの中心は、個人アカウントであった。即ち「個人アカウントを持つ常勤職員は○○ができる」というのが、サービスを提供する際の考え方であった。しかしながら、全学レベルで LDAP 連携してきたことで、様々な個人の属性情報が LDAP 上に登録されてきた結果、「個人アカウントもセンターが提供するサービスの一つに過ぎず、過度な依存はやめるべき」という考え方が生まれてきた。そこで、サービスを「アカウントに紐付くもの」から「ID に紐付くもの」に方針を転換した。「常勤職員の ID では○○ができる」「○○の管理者はこの ID である」等が、その場合の例になる。

2.2 職種・職名等のコード体系

センターでは「常勤職員がサービス利用の責任を担うべき」と考えている。単純に言えば「常勤職員には提供するが、そうでない者には提供しない」というサービスが、多々ある。つまり「常勤職員」に相当する方がどんな職種・職名で存在するのか、正しく把握しておかなければ、サービスを適切に運用できないことになる。

2.2.1 フルタイム、パートタイム

大学運営業務の実務を担う方々には、非常勤職員の方も数多い。表-2 に、広島大学における職種・職名と常勤・非常勤の区分の例を挙げる。非常勤職員の中には、ほぼフルタイムで働く「パートタイム契約職員」という職種の方がおられる。表-2 に示した、特任教授や特任准教授、契約一般職員の方々がそれにあたる。仮に、この方々の権限を低く設定すると、実務担当者がセンター・サービスを利用できず、非常に多くの問題を引き起こす。例えば、他の常勤職員の ID やパスワードを借用して、センターサービスの利用手続きを行わざるを得ない等。

一方、ティーチングアシスタント (TA)、リサーチアシスタント (RA) は、アルバイトの位置づけであり、権限も責任も非常に小さいものと考えなければならない。

それ故、常勤・非常勤などの名称のみで判断すると、実務上の重要性を見誤ることになる。

今回のシステム更新で、これらの区分の扱いを、センター側で自由に制御できるようにした。

2.2.2 職種・職名の更新頻度

加えて、広島大学においては、非常勤職員の職種・職名等は、かなり頻繁に (ほぼ毎月) 更新される。2005 年度に開発・運用した前利用登録システムにおいては、職名等の人事系コードの更新時には、随時、利用登録システムのマスターを更新する必要があった。取り込みが遅れると、該当するユーザーの情報がエラーで読み込めず、「その人が存在しない」扱いになっていた。つま

表- 2: 職種・職名の例

職種の例	職名の例	区分
大学教員	教授, 准教授	常勤
一般職員	主査, 主任	常勤
パートタイム契約職員	特任教授・准教授	非常勤
パートタイム契約職員	契約一般職員	非常勤
パート職員	TA,RA	非常勤

表- 3: ユーザーが選択するサービス

利用サービス選択の対象
メール, ホームページ, Login サービス, センター端末, HPC, VPN 接続, フレッツ接続

り、前の利用登録システムは、上流工程の異動に追随してメンテナンスする必要があった。

今回のシステム更新で、この点にも対策を施した。

ID についてデータ連携を充実させて置きながら、メンテナンスは手動という中途半端なシステムであったのは、センターがコード体系と実務の関係を充分に理解していなかったためと、今ならば言える。

2.3 セキュリティ対策

2.3.1 遊休アカウント排除等

利便性向上のため、2005 年度に、学内の認証統合 (ID 用パスワード＝個人アカウント用パスワード) が実施された。その後、セキュリティー向上のために、遊休アカウントをロックするべく、2007 年度末から、全アカウントに年度更新制を導入することとなった [3]。その際、「不要サービスは『利用しない』を各ユーザーが選択」できる様に、利用登録システムを改修した (表-3 参照)。

2010 年度からは、更に、セキュリティホール等が放置されやすい学内各部局のサーバー群の巻き取りを意図して、新たにホスティング・サービスを開始することとなった。また、前システムまで別サーバーで運用していたメーリングリストの管理も、今期から利用登録システムに統合された。

こうして、サービスを統合するたびに、利用登録システムの管理機能が追加され、徐々に複雑化していくこととなる。

2.3.2 ID の大量消失事故

一方、大規模なトラブルも度々起きる。

大学においては、学生の卒業・入学、教職員の退職・新規採用等により、大量の離籍・登録が、定期的に起きる。各学生の卒業予定日は不確実であり、教職員の任期制は部分的であり再任もされる。それ故、在籍期限という情報は、あまり一般的ではない。むしろ、学籍データや認証システムとの関係から、「離籍した者の ID は不要」という考え方が、本学の事務方にはある。その結果、「ID の一括削除」という処理が、正常な処理として、センター上流の ID 管理システム上で、定期的に実施される。

従って、センターは、大量の ID が削除されたデータに対しても「正常の状態」として、サービスの利用停止やアカウント削除猶予の通知等、離籍に関連する一連の処理を、実施しなければならない。

その際、上流工程で操作ミスやシステムトラブル等が起きていると (実際に頻発していたが)、まるで天災の如く、被害がセンターユーザー側に発生する。ユーザーからしてみれば、「自分は大学に在籍し続けるのに、なぜ離籍の扱いを受けねばならないのか」と、大量の質問・クレームがメールや電話で、センターに、届く。

実際、数千人規模の教職員 ID の誤削除が、3 年の間隔を経て発生したこともある。「常勤職員が全員離籍、職員は非常勤のみ在籍」という事故もあった。恐らく、人事異動により、それまで特定個人が対応していた危険な処理を、不慣れな新人が作業して発生させたものと、センターでは推測している。

離籍処理を削除ではなく「離籍した日付を記入する処理にしてほしい」と、センターから事務方に要望したが、他システムとの関係もあり、その方法は未だ採用されていない。

暫定措置として、利用登録システム側に「削除された人数が特定の値以上であれば、異常と見なす」という予防的措置を施した場合もあったが、微妙にその数値に届かないケースも起きた。「件数で保険」をかけても無駄である。

今回のシステム更新後の 2011 年 5 月にも、数百件の教職員 ID が離籍になるトラブルが起きた。ただし、今回は、システム更新時に導入した防御的措置のため、復旧に若干の作業は要したが、実害はなく、対処できた。防御的措置については、4.3 節に記す。

3 利用登録システムのサービス管理

3.1 利用登録システムの概要

センターは、広島大学の構成員約 2 万人のユーザーに対して、アカウント、メール、メーリングリスト、ホスティング、HPC 等、数多くのサービスを提供している [4]。そのサービスを管理する利用登録システムは、Web

表- 4: 常勤教職員が利用できる機能

機能
利用サービス選択 (表-3)
使用領域確認
アカウント自主ロック・ロック解除
ML 登録・管理
クラス/ゲスト/グループアカウント登録
ホスティング管理
DB 管理
メール振分・転送設定
メールアドレス変更
メールアドレス引継ぎ
WWW 公開認定試験

ベースの一般利用者機能、センタースタッフが使用する管理者機能、システム管理者機能、および、バッチによる自動処理で、稼働している。

既に 2 章で述べたように、基本となる構成員情報は、事務方が管理する「広島大学統一 ID 管理システム」から、入手している。統一 ID 管理システムでは、教職員、学生、学外者の ID 情報および、所属・職種・職名コードなどの各種データが、統合的に管理されている。

センターで提供するサービスは、システム更新の度に、徐々に増加し続けている。各サービスの利用条件も、複雑化しており、運用を続けるにつれ、その条件の見直しが必要となることもある。

3.2 利用登録システムの基本機能

利用登録システムは、一般のユーザーがログインした場合、アカウントの有無、身分および属性により、表示する情報を選択し、どの機能ボタンを提供するかを管理している。

例えば、常勤職員が個人アカウントでログインした場合、表-4 の機能が使用できる。

学生であれば、グループアカウント、クラスアカウント、ゲストアカウントは作成できない。学外者であれば、ICE 端末を使用できない等、各種の機能制限を、実施している。これは、利便性とセキュリティのバランスを考慮した選択である。

3.3 誰にどのサービスを提供するか

さて「誰にどのサービスを提供するか」は、どのようにして制御するべきか。

例えば名誉教授は、学外者であり、来学されることは少ないが、ネットワーク経由でセンターシステム等を利用されることが多い。留学直前の「日本語研修生」もまた学外者ではあるが、既に来学して日本語を研修中であり、センター端末の必要性は高いと思われる。従って「学外者」という「身分」の情報のみでは、センターがサービス提供を判断するには不十分である。ユーザー毎にサービスの必要性を考慮し、且つ、不要なサービスは提供しないために、「誰にどのサービスを提供するか」を、柔軟に管理できる工夫が必要である。

「誰に」に相当する部分を指定するにあたって、これまでのセンターサービスの利用条件を整理したところ、身分 (職員、学生、学外者) と職種で分類できることがわかった。表-2 に示したような職名 (職種の下の階層) までは不要であった。学外者に対しても「職種」に相当するコードが作成され、管理されている。従って、すべての身分に対して「職種コード」を判断の基準に使用できる。

ところで、運用方針が変更を求められることもある。実際、ML を登録できる者について、前システムでは「個人アカウントを持つ常勤教職員または大学院生」であったが、現システムでは「個人アカウントを持つ常勤教職員」のみと変更することとなった。

前回までのシステムでは、これらの「条件」をプログラムのチェック機能として実装していた。判定に「個人アカウントを持つ常勤職員」等のロジックが入り、同様なチェックが、システム内に多数ばらまかれていた。この方法では、「誰に」の判定部分は、柔軟性に欠け、メンテナンスも難しい。つまり、前システムの方法は、単純な場合では問題なくても、「誰にどんなサービスを提供するか」の詳細度を上げようとすると、いずれ破たんする実装方法であったと言える。

3.4 サービス管理表

上記の問題意識の基づいた対策として、今回の利用登録システムに導入した「サービス管理表」を図-1 に示す。一般利用者が何をできるかを定義したもので、行が機能群を表し、列がユーザーグループを表している。

利用登録システムは、ログインしたユーザーが、どのユーザーグループに属しているかを判定し、どの機能が利用可能かを調べて、対応する「ボタン」をユーザーの Web ページに表示する。

利用可能なサービスには、デフォルトが ON と OFF の区分を用意した。セキュリティリスクの高いものはデフォルト OFF であり、利用開始にはユーザー自身で「利用する」の選択が必要である。

一方、利用開始時に、簡単な試験に合格する必要のあるサービスを設けた。Web ページを作成して学外に開示したい者は、センターが「WWW 公開認定試験」と呼ぶ簡単な試験に、合格しなければならない。

ユーザーグループ / 機能群	個人アカウントなし							個人アカウントあり								その他		
	職員		学生		学外者			職員		学生				学外者				
	常勤等*	パート	正規生*	非正規生	端末利用可*	端末利用不可	無効*	常勤等*	パート	学部生*	大学院生*	専攻科生*	非正規生	端末利用可*	端末利用不可	グループ	クラス	ゲスト
個人アカウント登録申請					○	○												
個人アカウント登録	○	○			○	○												
個人アカウント引継ぎ	○	○			○	○												
アカウント年度更新								○	○	○	○	○	○	○	○	○		
アカウント自主ロック・解除								○	○	○	○	○	○	○	○	○	○	○
グループアカウント管理								○										
クラス・ゲストアカウント管理								○										
メール								○	○	○	○	○	○	○	○	○	○	
メール引継ぎ								○	○	○	○	○	○	○	○	○		
センターメール利用								△	△	△	△	△	△	△	△	△	△	
www公開利用								△	△	△	△	△	△	△	△	△	△	
loginサーバ利用								▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	
ICE(教育用端末)利用								○	○	○	○	○	○	○			○	
HPC利用								▲	▲	▲	▲	▲	▲	▲	▲		▲	
DB利用サービス								○	○	○	○	○	○			○	○	
メーリングリスト登録								○										
メーリングリスト運用								○	○	○	○	○	○	○	○			
セキュリティ試験										○	○	○	○					

○：Default ON(利用する)
▲：Default OFF(利用しない)
△：認定試験合格後、認可属性を与える
空白：利用不可等

図- 1: サービス管理表 (抜粋)。「*」は対応するユーザーグループ定義画面へのリンクを表す。

運用ルールを変更する場合は、利用登録システムのシステム管理者 Web ページで、サービス管理表の情報を更新できる。一般利用者画面は、その更新結果に応じて、自動的にサービス提供内容を変更する。更新されたサービス管理表は、スタッフ用管理者 Web ページで表示でき、センターのスタッフは常に現状を確認できる。

3.5 詳細機能のグループ化

サービスをユーザーに提供するにあたっては、詳細機能レベルで、ユーザーグループ毎に定義することも、一応は可能であろう。だが、例えば、ML を作成する者は、ML を更新・削除できるべきである。つまり「作成・更新・削除」は、詳細機能としては 3 つでも、一組で考えるのが妥当である。これらは一般に「ロール」と呼ばれている。利用登録システムの Web ページにおいて「○○の管理」としてボタンで表示している機能が、これに相当する。

一群の機能を、選択的に特定グループに提供できると、センター管理者にとって便利であり、運用ルールも説明しやすい。「ログインしてみて、ボタンが表示されていれば、その機能は使えます。」というのが最も簡単な説明である。

表- 5: 現在のユーザーグループの分類

身分	グループ		位置づけ
職員	常勤等 パート		デフォルト
学生	正規生	学部生 大学院生 専攻科生	
	非正規生		デフォルト
学外者	端末利用可 端末利用不可 無効		デフォルト

3.6 ユーザーのグループ化

身分に対応するユーザーグループを、表-5 に示す。

3.6.1 個人アカウントを持たないユーザ

個人アカウントを持たないユーザは、基本的に、アカウント登録ができるだけである。学生の個人アカウントは、センター管理者が一括生成させるため、学生の機能としては、使用不能にしている。また、学外者は、アカ

ウント登録の前に、アカウント登録申請が必要であり、許可を得たものがアカウント登録を実施できる。一部の者を除き、一般に学外者には、センター端末を利用させない設定としている。

「無効」と呼ぶユーザーグループは、個人アカウントを持たず、利用登録システム上は、何もできないユーザーである。このグループには、「臨時カード」と呼ぶ認証のみに使用する IC カード用のダミー ID や、「入退室管理が必要だがアカウントは不要な出入り業者」などが、登録してある。様々な ID が登録される様になった結果、全ての ID をサービス対象とする訳には行かなくなっているのも事実である。

3.6.2 ユーザーグループのデフォルト設定

センターに個人アカウントを持つ常勤職員が、利用できるサービスの種類が多い。もっともサービスを利用できないのは、先に述べた「臨時カード用 ID」である。

図-1 および表-5 に示したユーザーグループの名称は、センターが作った勝手な呼称である。2.2 節で述べたように、大学が管理する構成員の種別・名称が、センター業務に直接使用しにくい。例えば、職員を分類するユーザーグループとして「常勤等」とそれ以外にあたる「パート」の 2 種類を作成した。

「常勤等」のユーザーグループに属する者は、「身分が職員」で且つ「職種を明示的に定義」してある。先の述べたように「パートタイム契約職員」という職種は、非常勤ではあるが「常勤等」に登録している。それ以外の職種をもつ「職員」は、デフォルトグループである「パート」として分類する。新規の職種が追加された場合には、例え大学運営上常勤であってもセンターシステムは「パート」として扱う。これは、必要に応じて手動で対応することを意味するが、頻度的に、非常に少ないことが予想される。

これまでの職種・職名コードの改定から、通常でいう常勤職員および正規生は、改定されたことはほとんどない。従って、常勤職員相当のグループあるいは、正規生のグループを明示的に指定しておけば、職員のデフォルト、また、学生のデフォルトは「それ以外」で済ませられる。身分毎にデフォルトのユーザーグループを定義することで、職種・職名コードのメンテナンスの手間を大幅に削減できた。

学外者についても、同様の考え方を適用した。即ち、変化しないものを明示的に指定し、それ以外をデフォルトとする。学外者にはセンター端末（ICE 端末）を利用させない、がデフォルトである。端末利用可とするグループと、何もさせないグループを、例外として明示的に指定した。

尚、今年 3 月までは、学生では大学院生のみに ML の管理権限を与えていたため、学生を 4 つのユーザーグループに分けていた。ルール変更で、大学院生を特別扱いする必要がなくなったので、学生のユーザーグループは、正規生、非正規性の 2 つでも十分ではある。

システム管理者機能により、サービス管理表でのユーザーグループは、適宜、分類を追加できる。

3.7 サービス管理機能の弱点

現システム稼働後の運用から、サービス管理表がルール変更および現状把握にきわめて有効であることは、確認できた。だが、以下の状況では、管理上の問題が発生し易いことも分った。

アカウント引継ぎ 身分等が変わってアカウント所有者の ID が変更された場合に、これまでのアカウント資産を引き継ぐこと。システム的には、アカウント所有者の ID を書き換えることで実現する。

職員から学外者、学生から職員等、身分変更を伴う場合が多いため、利用可能なサービスが異なり、その結果、使えるべき機能が使えなくなる、使えない筈が使えてしまう等の問題が顕在化した。

サービス条件変更 運用ルール変更により、これまで提供していたサービスを使用不能にする、またはその逆。

その結果、管理表では使えない筈の機能を、利用可能な ID・アカウントが発生する。

つまり「サービス管理表」に従えば、利用できない筈のサービスを、アカウントあるいは ID が使用するケースが、発生しえる。その場合、チェック機能不足 (バグ) の場合もあり得るが、ルール変更による「置き去り」の場合もある。尚、管理者機能として、必要な機能が不足する場合、対応に時間を要することになる。

システムの自動的な監視機能 (夜間バッチ等でのチェック) として、サービス管理表からのずれを監視し、管理者に通知する機能は実装済みである。見つかった異常には、個別に対処する必要がある。

4 ID 消失事故への予防的措置

上流工程での ID 管理にトラブルが起きると、センターの利用登録システムには、誤った構成員情報 (ID の大量消失等) が届けられる。受け取ったデータが正常・異常のいずれにしろ、センターの利用登録システムは、消失した ID に対して離籍の処理を行う。

4.1 通常の離籍処理

離籍になったIDがセンターサービスを利用していた場合、離籍処理が走る。即ち、各アカウント所有者宛に「アカウント削除猶予」のメールを発送する。センターでは、IDが離籍になっても、例えば、個人アカウントは90日間削除を猶予する運用を行っている (表-6の「変更前」を参照)。かつて、医学部で卒業後3か月程度してから改めて在籍する研修生が多数いたため、この削除猶予期間を設けた運用としている。

卒業後あるいは離籍後に再度、在籍になった場合を「再在籍」と呼ぶ。この場合「削除猶予解除」のメールを当該アカウント宛てに送信する。

再在籍にならず削除猶予を過ぎたアカウントは、一定期間ロック (利用停止) したのち、削除する。

IDに期限はあっても、個人アカウントおよびグループアカウントには、元々、有効期限はない (表-1の注参照)。所有者のIDが離籍になると個人アカウントに「有効期限＝当日、削除猶予期限＝90日後、利用停止期限＝120日後」を指定し、削除猶予メールを送付する。所有者のIDが再在籍になると、個人アカウントが存在する間であれば、再在籍処理が走り、各期限を無効にして、アカウントを再度有効にしている。

従って、アカウント削除事故と復旧措置が上流で起きた場合、削除猶予および削除猶予解除メールが飛びはするが、個人アカウントおよびグループアカウントは、ファイルを一つも失うことなく、自動的に復旧できる。ここまでは度重なるトラブルを経て、前システムで既に実現していた。

一方、クラスアカウントおよびゲストアカウントは、予め、有効期限を指定したアカウントであり、期日が来たら直ちに削除していた。IDの削除事故が起きた場合、これら期限付きアカウントの扱いが、センターにとっての問題となっていた。

4.2 期限付きアカウントの削除猶予

クラス・ゲストアカウントは期限付きアカウントである。その所有者がアカウントの期限前に離籍した場合、当該アカウントは無効とするのがセンターの方針である。

前システムでは、事故である可能性を考慮して、削除猶予ののち (ロックはせずに) 削除してていた。問題は、ID削除事故からの復旧措置で発生していた。

センターの利用登録システムでは、現システムも前システムも、アカウントの有効期限について日付情報は1つしか用意していない。個人・グループでは、通常、NULLであり、クラス・ゲストでは、申請時に指定した有効期限がセットされている。

表- 6: 離籍時のアカウント運用方針の変更

誤ったID削除を想定し、期限付きアカウントの運用方針を「削除猶予」から「利用停止」に変更した。

種別	変更前		変更後	
	猶予日数	停止日数	猶予日数	停止日数
個人	90	30	90	30
グループ	30	30	30	30
クラス	10	0	0	10
ゲスト	10	0	0	10

前システムでは、「所有者が離籍した日をアカウントの有効期限」としていたため、復旧措置による再在籍処理では、個人・グループは、NULLに戻すだけだが、クラス・ゲストは、元に戻すべき日付が残っていないことになる。

従って、IDの削除事故が起きて、クラス・ゲストアカウントの所有者が巻き込まれた場合、クラス・ゲストアカウントを正常に復帰させるために、センター管理者は以下の手順を実施していた。

- センター管理者が各アカウントの登録申請記録から、該当日付を手動で検索する。
- センター管理者が、手動で、各アカウントに有効期限を設定する。

つまりセンターは、前システムにおいては、「期限付きアカウントの有効期限」という管理情報を、自ら消失させていたことになる。

4.3 期限付きアカウントのロック

今回のシステム改修の際、クラス・ゲストアカウントの有効期限前に所有者が離籍となった場合、当該アカウントは直ちに「利用停止 (ロック)」とすることとした。以下の理由による。

- ID削除事故であった場合の復旧措置は、ロックを解除するだけ済む。
- 「期限付きアカウントの有効期限」を失わずに、アカウントを無効化できる。

表-6に変更内容の日数部分を示す。これ以外にも、前システムで実施していた有効期限を書き換える措置も廃止した。

この場合、アカウント所有者が再在籍処理で復活すると、ロック解除で回復でき、本来の有効期限も失われない。この措置により、これまでの様な、センター管理

者が各アカウントの登録申請をかき集めて手動で再設定する必要がなくなり、復旧措置が自動化できたことになる。

ユーザーから見れば削除猶予メールが届くのは変わらず、「なんで私が離籍なの」というクレーム対応するスタッフの苦労も変わらないが、事故からの復旧が自動化できたことは、センター管理者にとっては、非常に大きなメリットである。ただ、復旧措置が済むまで講習会等での利用に影響が出ることは、覚悟しておかなければならない。

上流工程で事故があっても、「情報を失わない」仕掛けを用意しておけば、ユーザーおよびセンターにとっての実害は最小限に抑えられる、という当然の結論ではある。一般のユーザーにしてみれば、ばたばたした印象を与えているであろうが、実害は極力抑えることができる様になった。

4.4 システムの妥当な振る舞い

因みに、前システムにおいて「削除猶予猶予」を設定したことがある。度々ID の誤削除が起きたことに対応ため、「ID が消えても間違いかもしれので、削除猶予メールの発送を数日間遅らせる」という運用を取ったことがある。その結果は、逆に、正常時に「離籍した ID が所有するアカウントが、直ちに削除猶予にならないのはシステムの異常か？」という疑問を、抱かせることとなった。つまり、削除猶予猶予は忘れられ易く、防衛線として機能するより「自作のトラップ」という位置づけに近くなる。

複雑なシステムには「もぐりの定数」を組み込むべきではない。システムが担う論理に照らして妥当な挙動を維持させることが、当然のことながら、極めて重要である。

4.5 誤操作手順の原因究明と対策の提案

何度も起きる ID の誤削除について、非難することなく、原因を調査した。場合ごとに、トリガーとなる行為が異なっており、優れた教訓を得るのは容易ではない。

その中で、「非常勤職員の ID とパスワードを保存し、書き戻す際に、追加ではなく上書きしてしまい、既存構成員の ID を消去した」というケースがあった。

その行為の理由は、広島大学と一部の非常勤職員との契約で、年度の切り替わり時に数日間契約が切れる場合がある。その結果、ID 管理システム上から ID とパスワードが削除されてしまう。後日、契約完了した場合に、各人は同じ ID で再度登録されるが、パスワード情報がクリアされている。そこで「それらの ID とパスワードを保全し、パスワードの再登録作業を不要とする」ための行為であることが分かった。

この善意に基づく行為は、システム化されておらず、従って、手動で実施する作業として、事務方の現場対応として、行われていた。

センターによる聞き取り調査の結果、統一 ID 管理システムの改修時期でもあり、問題となる作業を、統一 ID 管理システムでのパスワードバックアップ・リストア機能として、実現することを提案し、実装された。これにより、「現場の隠れた作業」をシステムの機能として実現することで、云わば「善意のテロ行為」を排除することができた。

もちろんこれは、単なる例に過ぎず、一般化できるものではない。本来のセンター業務からも踏み出している。だが、上流工程のワークフローに無関心なままでは、結局、センターは事故の被害を垂れ流すしかない。

センターは、ID および各種コードを事務方から受け取り、センターのユーザーにサービスを提供する。既に、身分・職種・職名等のコード体系を適切に理解するには、大学内での現場を把握する必要があることを学んだ。同様に、上流工程での ID 管理等のワークフローについても、ある程度までは把握するべきであり、助言していくべきである、と考えている。

5 まとめと今後の課題

5.1 現システムで実現したこと

センターシステムを更新し、利用登録システムを抜本的に改修した。どのユーザーグループがどのサービスを利用できるかを管理する「サービス管理表」で、利用登録システムが提供する機能 (ボタン群の表示) を、直接、制御している。これにより、誰がどのサービスを利用できるかの把握が容易になり、同時に、ルール変更に伴う条件の変更が、容易になった。

尚、サービス条件を変更した場合、期間を区切った移行措置を実施する必要がある。運用ルール変更が、時に、システムの機能不足 (おもに管理者側) を露呈させる場合もあるので、注意が必要である。

また、度々発生した ID の大量削除というトラブルに対しては、アカウントの猶予期間、利用停止期間を活用して、管理情報を含めて、データの消失を防ぎ、実害が出ないように配慮している。削除猶予メールおよび削除猶予解除メールが大量に飛び、センターに苦情・質問が来る事態に変わりはないが、正常な状態に復帰させるのは、以前よりはるかに容易になった。

5.2 今後の検討課題

かつて、センターの個人アカウントには「サービスを利用する権利」に相当する位置づけがあった。だが、IDで個人を管理する体制が大学として整い、センターがIDに基づきサービスを提供する状況においては、「IDが主たる個人情報」であり、「アカウントはセンターのサービスの一部」に過ぎない。

現状は、センターにとって利用者の権利等の関連付けが、まだアカウント主体のものがあるかもしれない。今後は「サービス利用者の連絡先」程度に扱う必要があるだろう。

ところで、「IDは離籍により失効する」「IDに引き継ぎはない」とするのは、事務方のポリシーである。一方、「アカウントの削除には猶予を設ける」「アカウントは引き継げる」とするのはセンターのポリシーである。これまで、ID失効後も猶予のある(つまり認証可能な)アカウントに各種サービスを紐づけていた。従って、そのアカウントを引き継いでしまえば、すべてのサービスを一括して引き継げていた。IDにサービスを紐づける場合、その「一括引継ぎ機能が消失」しつつある可能性がある。各種サービス停止までの猶予も失われる。今後、この点について、考え方を整理する必要があるだろう。

参考文献

[1] 岩沢和男, 津久間秀彦, 新畑道江, 岸場清悟, 入江治行, 稲垣知宏, 隅谷孝洋, 秋元志美, 勇木義則「大学情報サービス基盤としてのアカウント体系」, 学術情報処理研究 No 4, pp.63-72, 2000.

[2] 岩沢和男, 津久間秀彦, 岸場清悟, 隅谷孝洋,「アカウント体系再編の評価」、学術情報処理研究 No 5, pp.43-48, 2001.

[3] 岩沢和男, 吉冨健一, 宮原俊行,「セキュリティ強化のためのアカウントへの制限」, 平成 20 年度 情報教育研究集会、基盤システム,p491-494,2008.

[4] 広島大学情報メディア教育研究センター Web ページ, http://www.media.hiroshima-u.ac.jp/services

学内サーバー室の環境温度の考察

A Study of Temperature of Server Room in Hitotsubashi University

伊藤　史人†，高見澤　秀幸†，佐藤　郁哉†
Fumihito ITO†, Hideyuki TAKAMIZAWA†, Ikuya SATO†

ito@poran.net, h.takamizawa@cio.hit-u.ac.jp, ikuya.sato@cio.hit-u.ac.jp

†一橋大学情報基盤センター

†Center of Information and Communication Technology, Hitotsubashi University

概要

電力不足に起因する節電対策については，本学においても喫緊の課題となっており，講義室の空調をはじめ屋内照明等についても積極的に節電対策を実施している．我々が管理する学内情報機器の節電に当たっては，PC への対策は当然ながらサーバー機器への対策も考えなくてはならない．サーバー機器はサーバー室に集中配置していることから，排気によるサーバー室温上昇を防ぐため空調による適切な冷却が必要である．しかしながら，サーバーの安定動作を求めるあまり，空調の設定温度を必要以上に下げてしまう傾向がある．その結果，無駄な電力を消費することとなり，Power Usage Effectiveness（PUE：電力使用効率）を悪化させる要因となる．本論文では，サーバー環境温度の調査結果について報告し，サーバー機器の吸気・排気・CPU 温度および外気温に関連して考察した．今回の調査では，マイクロソフト社の提唱する 27℃設定は妥当性のあるものであることが確かめられた．なお，本研究を実施するにあたり，偶然に空調機器故障が発生し，サーバー室の温度上昇によるシステムダウンが発生するまでの実測結果を得た．これらの実測値を利用し，サーバー室の環境温度を考察した．

キーワード

節電対策，空調温度，サーバー，消費電力, PUE，吸気温度，排気温度，温度環境

1. はじめに

平成 23 年 3 月 11 日に発生した東日本大震災により原子力発電所が大きく損傷し，主に東京電力管内の電力需要がひっ迫しているのは周知の事実である．特に，夏場における電力不足は深刻であり，7 月 1 日からは 37 年ぶりの電気事業法第 27 条による電力使用制限令が発動した[1]．電力使用制限令の対象としては，東京電力及び東北電力並びにその供給区域内で供給している特定規模電気事業者と直接，需給契約を締結している大口需要家（契約電力 500kW 以上）であり，制限内容としては「昨年の上記期間・時間帯における使用最大電力の値（1 時間単位）」の 15%削減した値を使用電力の上限とするものと定められている．大学においても，例年以上の節電が

必要であり，あらゆる方面での使用電力削減に努めなくてはならない.

ところで，本学は文科系大学であるため，大規模な実験設備等は設置されておらず，他の総合大学と比べると電力を大規模に消費する設備は少ない．また，学生数は全学で約 4,400 名であり，設備にかかる消費電力は他大学と比べると少ない.

そこで，本学における節電対策としては，主な対象として照明・空調・パソコン等の情報機器としている．照明や空調については，利用者に節電を徹底させて効果を挙げており，パソコンについては，Microsoft 社による自動節電プログラム[2]の利用および Windows ドメインのグループポリシーによる節電設定を実施することで，およそ 25%程度の節電効果を見込んでいる．小型電力測定機[3]によるパソコン単体の調査では，自動節電プログラムとグループポリシーによる対策で25～30%程度の節電効果が確認されている.

その他，情報機器設備の節電対策においては，学内に設置しているサーバー機器類が対象となる．グループウェアやメールサービスは常時稼働させていることから積算では比較的大きな電力を消費していると思われる．また，サーバーを稼働させる電力と同時に，サーバー室の空調も大きな電力を消費していると考えられる．サーバーを安定稼働させるには適切な冷却が必要であることは当然であるが，必要以上の冷却は電力の無駄となる.

そこで，本論文ではサーバー室の空調の適切な温度設定を評価することにより，サーバーの環境温度を調査した．その結果は学内の節電対策の一環で活用し，今後のサーバー室運用の基礎資料とする.

一般に，サーバー室の環境は様々であり，環境温度を一般化することは極めて困難である．サーバー室の大きさ・空調の性能・サーバーの数や密度さらに設置位置等の条件が多様なためである．一方，サーバーを安定稼働させるための条件は客観条件として規定されていると考えられる．例えば，サーバー機器の適切な吸気温度や CPU 温度等は，安定動作できる温度条件がベンダーにより公表されている.

本論文の温度の調査結果においては，サーバー室の環境を考慮してサーバーの環境温度を考察した. そのため，安定稼働のための参考資料としては有用であると考える. なお，調査中において，偶然にもサーバー室の空調故障が発生し, 多くのサーバーがダウンする障害が発生した. それにより，図らずもサーバー室の温度上昇が限界に達するまでの記録を取得することができ，サーバーの環境温度を考察する上で極めて有用な情報となった．幸いにも，高温を原因とするシステムダウンによる，深刻な物理的･論理的障害は残らなかったことを付け加えておく.

2. 調査対象としたサーバー室の環境

本学にはサーバー室は２つあるが，調査対象としたサーバー室は，事務関連システムを中心に全学で利用するシステムを設置している.

2.1. サーバー室の概要

サーバー室は，7.5 m × 5 m の間取りで，気密が保たれた部屋であり，北向きの窓が一つ付いている．図 1 にサーバー室の見取り図を，図 2 に空調の冷気吹き出し口を示す.

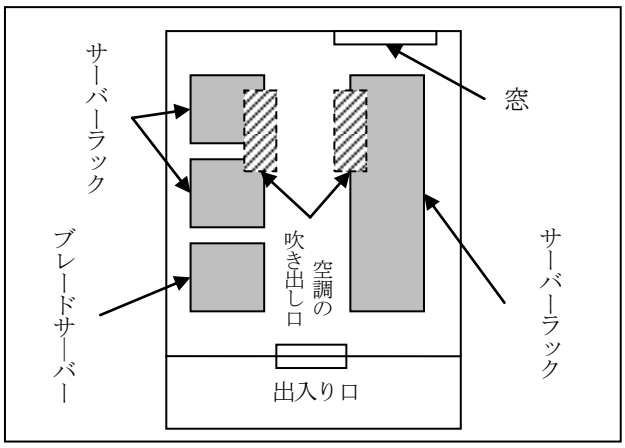


図 1　サーバー室のラック配置図（灰色部：サーバーラック，網掛け：天井の空調吹き出し口位置）

図 2　空調の冷気吹き出し口（出入口付近から天井方向を撮影）

サーバー室に設置しているシステムの内訳としては，表 1 の通りである. すべてのブレードサーバーは一つのエンクロージャーに収容されており，その他ラックマウントサーバーは各ラックにシステム毎に収容されている. 各システムには通常は USP が装備されている. おおむね,

各ラックの収容密度には余裕を持たせており，また，背面のスペースを十分に取って過度に排熱が阻害されることはないように設置されている．空調の冷気はラックの吸気面側(ラック前面)に流れるようになっているため，冷気が効率よく吸入される状態となっている．

表 1　サーバー室のシステム一覧

サーバー	形態	台数
ドメインコントローラ	ブレード *1	2
その他システム	ブレード *1	6
グループウェア	ラックマウント	2
その他	ラックマウント	12
学内規則集管理システム	PC サーバー	1
その他	PC サーバー	2
事務用統合ストレージ	その他 *2	
スイッチおよびファイアウォールアプライアンス	ラックマウント	4

*1 HP BladeSystem c7000 エンクロージャー内に収容
*2 EMC Celerra NS-120 ユニファイド・ストレージ

2.2. 空調温度設定による節電対策

サーバー室に設定している空調機器の仕様は表 2 の通りである．インバーター式ではないため，現状としては省電力対策を実施するには不向きな機器である．今回の調査ではサーバーの環境温度の考察を行うため空調の電力計測は行わなかった．

調査開始前の空調設定は，設定上最低温度の 20℃としており，実質的には最大冷房での運用となっていた．仕様により，定格消費電力はおよそ 4.7 kW であることから，最大冷房時の電力はおよそこの値だと推測される．

表 2　空調機器の仕様

項目	値
メーカー	三菱重工
形式	空冷ヒートポンプ式
型式	FDCP1601H
電源	三相 200V
コンプレッサー	4.5 kW
消費電力（冷房定格）	4.73 kW
重量	124 kg

図 3　空調機器本体　（屋外に設置されている）

2.3. PUE による評価法

PUE（Power Usage Effectiveness：電力使用効率） は，サーバー室やデータセンターのエネルギー効率を表す指標であり[4][5]，2007 年に米国のデータセンターの省電力化を推進する業界団体 The Green Grid（グリーングリッド） が発表したものである．PUE は，(1) 式より算出でき，数値が大きいほど効率の悪い設備ということになる[6] [7].

$$\mathrm{PUE} = \frac{\text{サーバー室全体の消費電力量}}{\text{情報機器の消費電力量}} \qquad (1)$$

つまり，情報機器の消費電力とその他に使う電力が同じ場合は 2.0 となり，情報機器の消費電力のみであれば 1.0 となる．一般的には 2.0 ～ 3.0 であるが，高効率の設備では 1.21 を発表した Google のデータセンターの例[8] もある．この指標が生まれた背景には，IT 設備自体の省電力化が求められていることが挙げられる．

また，同様の考え方に DCiE（Data Center infrastructure Efficiency） がある．これは PUE の逆数であり，数値が大きいほど効率の良い設備となる．DCiE を(2) 式に示す.

$$\mathrm{DCiE} = \frac{1}{\mathrm{PUE}} = \frac{\text{情報機器の消費電力量}}{\text{サーバー室全体の消費電力量}} \qquad (2)$$

なお，本論文においては，前述のようにサーバーの温度環境の考察を目的としているため，PUE / DCiE は算出していない．しかし，PUE は情報機器の節電対策を考える上で極めて重要な要素であるためここに挙げた．今後省電力化を進めるにあたって，電力の実測は不可欠であり，学内の計測機器等が整い次第調査を行い PUE の算出をする予定である．

3. サーバー機器の環境温度の測定

サーバー機器の環境温度としては，サーバーの吸気温度温・排気温度・CPU 温度・外気温度および空調の設定温度が挙げられる．ただし，空調の設定温度はあくまでも目安であり，実測による温度情報が重要である．

3.1. 測定機器

温度変化の実測にあたっては，温度ロガーの佐藤商事社販売 4 チャンネル温度 SD カード記録計 47SD [10] を利用した（図 4）．これは，4 か所分の温度データを SD カードに蓄積できるものである．温度センサーとして，K 型熱電対を利用した．主な仕様を表 3 に示す．

図 4　4 チャンネル温度 SD カード記録計 47SD（左図：装置の外観，　右図：ブレードサーバー上に設置した状態）

表 3　温度ロガーの主な仕様

項目	値
製品名	4 チャンネル温度 SD カード記録計 47SD
タイプ	K 型熱電対
測定範囲	-100 ～ 1,300 ℃
分解能	0.1 ℃ （-100 ～ 999 ℃）
測定精度	± 0.4 % + 0.5 ℃
測定間隔	1 ～ 3,600 秒
重量・サイズ	489 g・177×68×45 mm

CPU 温度については，CPU 温度計測ソフトウェアの Core Temp[11] を利用した．これは，CPU の温度センサーから温度情報となる DTS（DigitalThermalSensor）を読み取るものであり，精度は CPU の温度センサーに依存し，Xeon E5520 の場合 ±0.2 ℃ であるが[13]，出力のオーダーは 1 である．前述の温度ロガー同様に，計測情報を蓄積できるため，サーバーの環境温度の推移を調査することが可能である．なお，使用時の最新バージョンは 0.99.8 である．今回の調査では，2 台のブレードサーバーと 2 台のラックマウントサーバーに Core Temp を導入して温度情報を収集した．

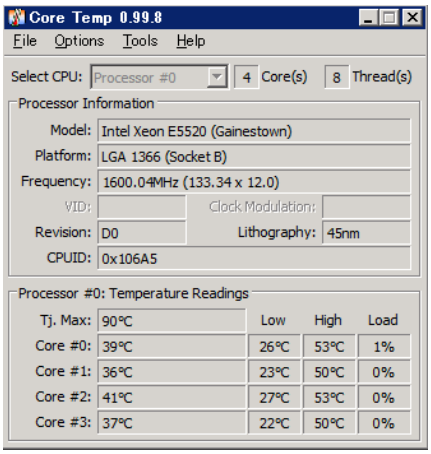


図 5　Core Temp のメイン画面（Intel Xeon E5520 の場合）

メイン画面中に CPU 動作の最大許容温度である Tj. Max の項目がある．画面では 90 ℃ となっているが，Intel 社製 Xeon E5220 のスペックシート[13] では TCASE（最大動作温度）として 72 ℃と公表されている．表示上の違いがあるので注意を要する．本論文では，スペックシート上の TCASE を優先して考察する．

3.2. 安定運用のための環境温度

サーバーの安定動作が保証される温度については日本マイクロソフト社により詳細に検証されている[9]．最も設置密度が高く，温度上昇の影響が大きいと想定されるブレードサーバーのエンクロージャー（HP BladeSystem c7000）における動作保証温度は 10 ～ 35 ℃ であり，その他，サーバー室内の各ラックマウントサーバーの仕様においても，動作保証温度は 15 ～ 35 ℃ としている機器が多い．また，ネットワークストレージ（EMC Celerra NS-120）は，10 ～ 40 ℃ である．

日本マイクロソフト社の示した吸気温度 27 ℃は，高負荷運用による筐体温度の上昇を考慮しても十分余裕のある温度としている．

以上のことから，本論文では，この結果を参考にしてサーバー吸気温度が 27 ℃で十分に安定動作するものとして仮定する．

3.3. サーバーの吸気・排気・CPU 温度および外気温度の実測

サーバーの吸気や排気を実測するため，図 6 のように温度ロガーから延長したセンサー（熱電対）を取り付けた．今回の調査では，ブレードサーバーのみとしているが，他のラックマウントサーバーにおいても，吸気の上部と下部をスポット検温したところ，ほぼ同様の温度となっていた．本論文においては，吸気については他のサーバーと共用できるデータであるが，排気温度と CPU 温度については別途行う必要がある．なお，前述の通り，CPU 温度については，他の 2 台について温度を収集した．

3.4. サーバー機器と外気温度との相関

空調は空冷ヒートポンプを利用してサーバー室内の温度を調整していることから，排熱個所の温度が影響すると考えられる．そこで，数日間連続でサーバーの環境温度を調査し，外気温との相関を考察した．外気温とサーバー室の温度の差が大きいタイミングに調査するのが適当である．つまり，熱は高い方から低い方へ移動するため，外気温とサーバー室の温度（吸気温度）の差が大きい場合に，空調によるサーバー室の温度変化の傾向が確かめられる[14].

温度調査の結果を図 7 に示す．図から分かるように，外気温度の変動が大きくてもサーバー室の温度を示す吸気温度に顕著な変動は確認できない．排気温度についても吸気温度によってのみ変動しているのが明らかである．

このことから，サーバー室の温度変化は，外気温に顕著な影響は見られず，恒温状態を保つことが確認された．

しかしながら，この恒温性は空調の性能にも大きく左右されることが想定される．なぜなら，空冷ヒートポンプは外気温が高いほど性能が落ちる特性があるからである．仮に，空調に十分な排熱性能がない場合，サーバーから排出される熱を十分に除去できずサーバー室の温度が上昇する．

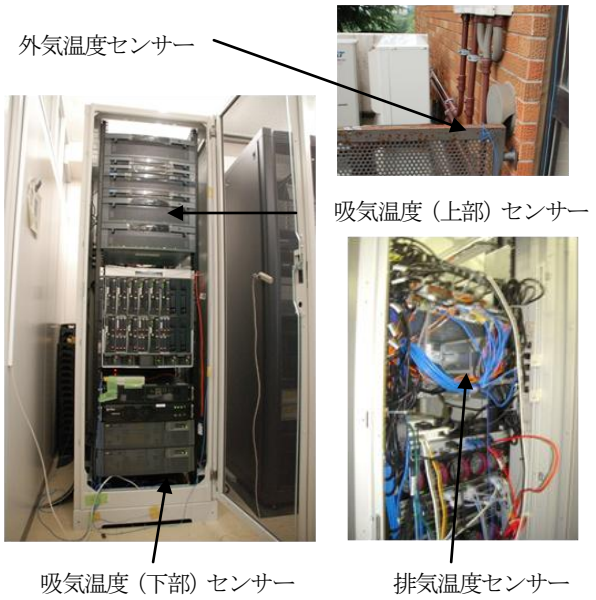


図 6　ブレードサーバーの各センサー設置位置（左図：ブレードサーバー正面，右上図：屋外，右下：ブレードサーバー裏面）

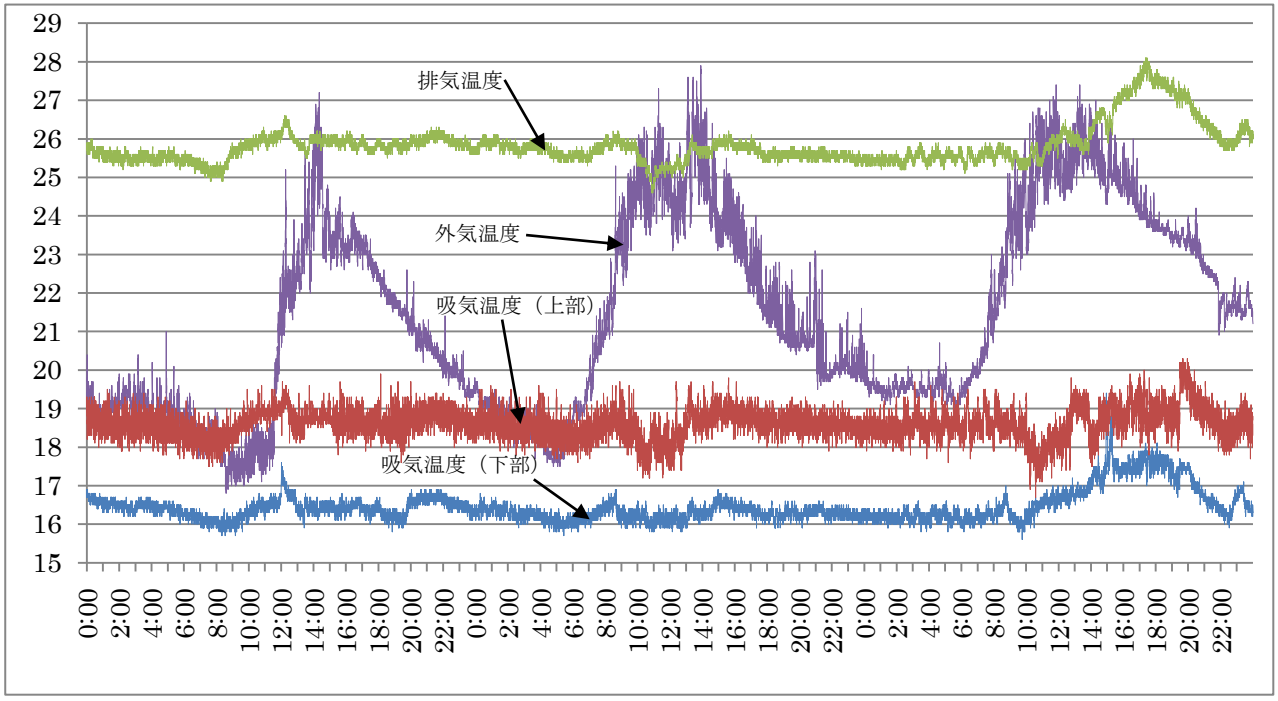


図 7　サーバーの温度環境の相関　（空調設定 20 ℃ の場合）

ところで，図の右側 10:00 頃から排気温度が急激に上昇しているのが確認できる．これは意図的に室温設定を上昇させて温度推移の確認を行ったためである．その結果，吸気温度（上部および下部）の変動が発生した．通常よりも温度の高い空気が流入したことでサーバー室内の空気の循環が乱れたと推測できる．

3.5. サーモグラフィによる温度の可視化

サーモグラフィによるサーバーの筐体温度の可視化の例を示す．撮影時，空調の温度設定は 20 ℃ であり，十分に冷却された状態である．

図 8 はブレードサーバーを収容するラックの写真である．最も高温な部分でも 22 ℃ 程度となっており，十分に冷却していることが分かる．元来，ブレードサーバーは高密度での運用が想定されているため冷却性能が高いためと考えられる．

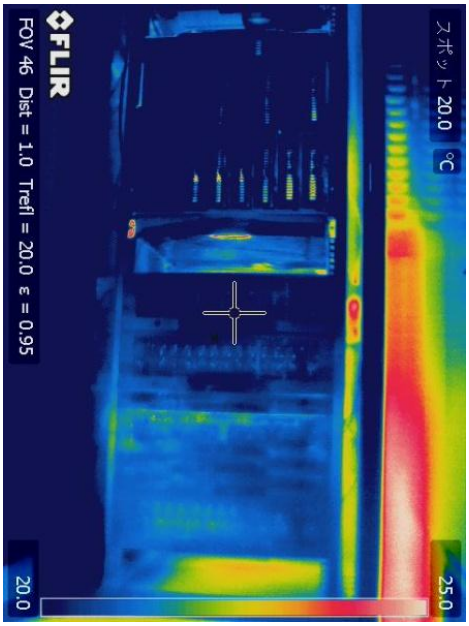


図 8　ブレードサーバーの例　（図中上部はネットワークストレージの筐体であり，中央部がエンクロージャーの筐体，下部は UPS 装置である）

図 9 は各ラックマウントサーバーの例である．ラック間隔は余裕を持たせてあるが，動作中のサーバーは周辺部と比べて高温となっているのが分かる．図の例では，温度レンジが 20.0 ～ 25.0 ℃ となっているため，安定動作に影響するほどの高温は検出できないが，各ラックの上部に高温部が集中しているのが確認できる．これは，サーバー筐体が温めた空気が，ラック内で上昇したためと考えられる．ラックは密封されているわけではないので，暖気がたまり続けることはないが，適切な空気循環の対策を行うことは重要であろう．空調温度をマイクロソフト社が提唱する温度にした場合，安定動作のための温度の余裕がなくなっているので，現状の設置状態における十分な空気循環を措置できていない場合，予測できない高温部分が発生し，システムに悪影響を及ぼす可能性がある．

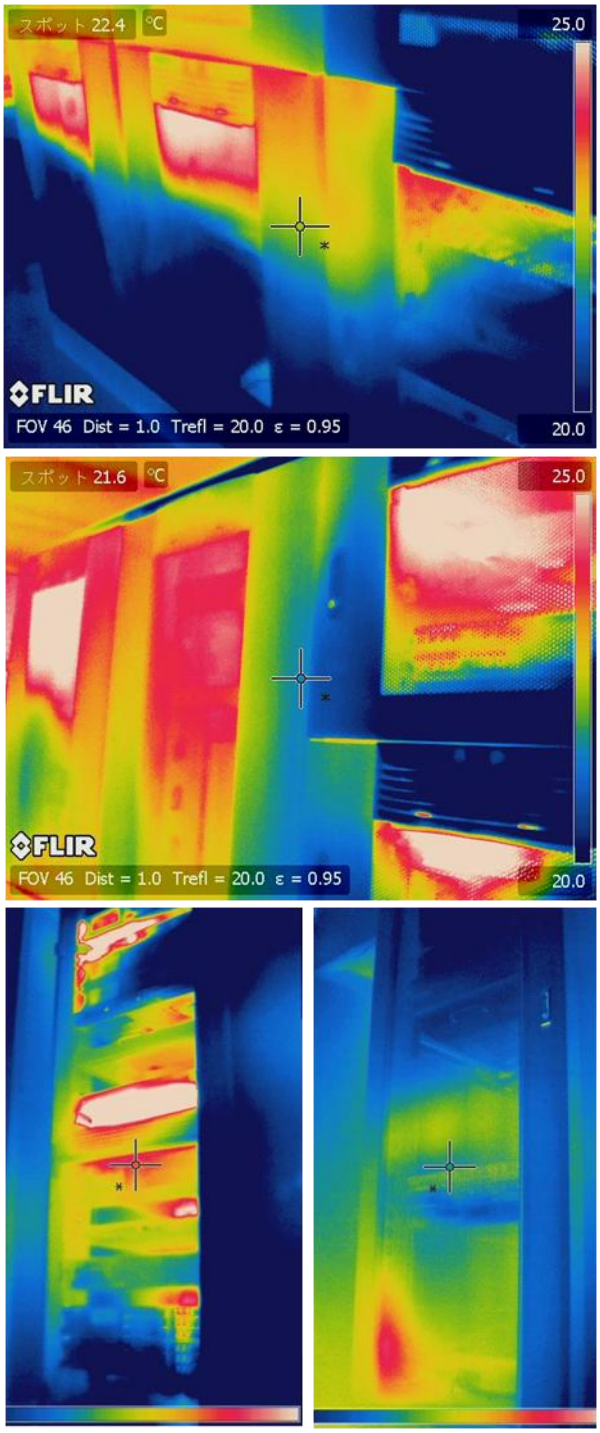


図 9　ラックマウントサーバーの例　（上段図：IC カード管理システム 等，中段図：手前は FW アプライアンス 等，下段左図：グループウェア 等，下段右図：財務会計システム 等 であり，淡色部分ほど温度が高い）

4. 空調故障によるシステムダウン

4.1. システムダウンの概要

2011 年 6 月 6 日月曜日の始業直後，教職員が利用するグループウェアおよび事務職員が利用するメールサービスにアクセスできない旨の連絡が本学情報推進課に相次いだ．職員がサーバー室に入室すると，これまでにない熱気が襲ってきた．この異常な熱気から，サーバー室の温度が上がり過ぎたことによるサーバー停止は明らかだった．その後，関係者を招集し，しばらくはサーバー室のドアや窓を開放し室温度の低下に努めた．午前中だったこともあり外気温は 22 ℃ 程度のため，扇風機等で外気を導入しつつサーバー群を順次起動してサービスを再開した．幸いにもすべてのサーバーで物理的・論理的な破壊は無かった．この理由としては，各サーバーは温度上昇により CPU もしくは周辺機器が異常停止（熱暴走）したのではなく，システムがあらかじめ余裕のある温度で緊急停止（非常停止）したためと思われる．

なお，当日の午後には代替の空調を設置し，翌日には故障した空調の修理を完了した．

4.2. 温度上昇の原因

サーバー室の空調設備は，室外機のファンがリレースイッチにより Low / High モードに切り替わる仕組みになっている．修理時の報告によると，Low モードから High モードになるべきところ切り替えに失敗して熱交換が行えなくなったことが分かった．当該機器は，およそ 3 年間最大冷却状態で連続稼働していたため，部品劣化により動作が不安定になっていたと推察される．

ところで，推測の域は出ないが，空調設備停止時間帯にはゲリラ豪雨による落雷があったことが確認されており，電気系統に不具合が生じた可能性もある．何らかの故障の原因になった可能性は否定できない．

空調設備は多重化していなかったことからサーバー室の温度を維持することが不可能となり，また，サーバー室には温度変化を通知する警報装置等は備えていなかった．

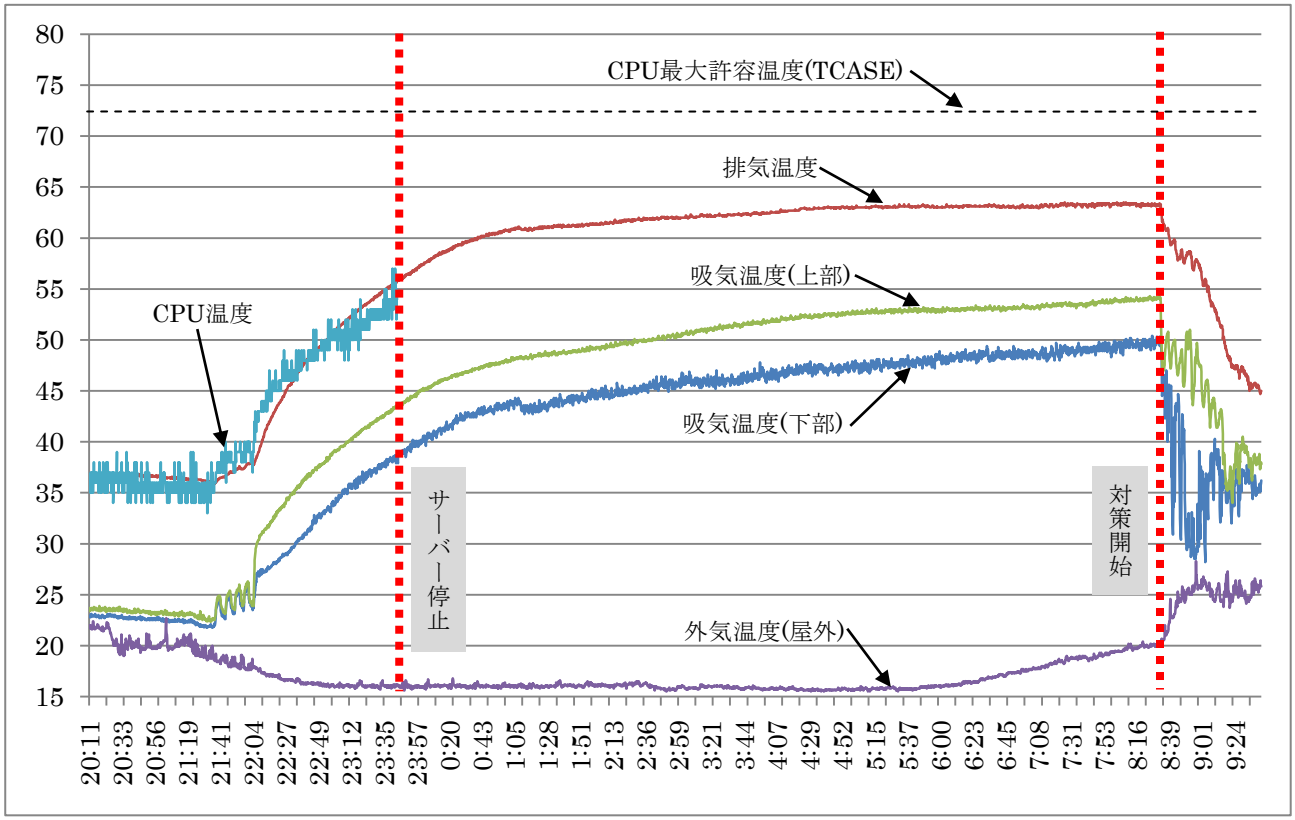


図 10　空調故障によるシステムダウンにおけるサーバーの温度環境　（空調の不調から対策開始まで）

4.3. 温度推移の考察

図 10 に空調故障が発生したと思われる時間から，翌朝に外気導入するなどの対策を開始した時間までのサーバー環境温度推移を示す. 図中の排気温度・吸気温度（上部）・吸気温度・外気温度は温度ロガーで，CPU 温度は Core Temp による計測である．計測機器の違いにより若干の温度誤差が生じている可能性はあるものの，温度推移を考察するには問題はないと考えられる.

なお，CPU 温度（Intel Xeon E5520）は Windows 2008 Server R2 を搭載したブレードサーバー（ドメインコントローラー）のものである.

21:20 頃, 外気温を含めすべての温度に変化が現れた. 外気温の変化が激しいことから気象の変化があったと思われる. その後，吸気温度が 20 分程度の間で 4 回の温度変動を起こしている．この時，空調に不調が発生していたと推測される．変動終了直後から外気温を除くすべての温度で極めて急な温度上昇が発生している．完全に空調が停止しサーバーの排熱を排出できなくなった.

ここで，図の温度推移から興味深い現象として以下の 4 点が確認できる.

1. 空調停止直後のみ，吸気温度（上部）の上昇率が高く，他の温度同様の上昇率となる
2. 排気温度・吸気温度（上部）・吸気温度（下部）・CPU 温度がほぼ同じ温度上昇率である
3. 吸気温度（上部）と吸気温度（下部）は 5 ℃の差を維持している
4. CPU 温度と排気温度は，温度と温度上昇率ともにほぼ一致している

これらの現象を踏まえて，次章にてサーバー室の環境温度について論じる.

5. 空調設定温度の検討

前章のシステムダウンにおけるサーバー温度環境の推移から，サーバー機器と周辺温度がどの様に推移するか考察する．定常運用しているサーバー室では，空調の温度を大きく上昇させることはできないが，前章で収集したデータを分析することでサーバー室の耐温度特性等を考察する.

また，日本マイクロソフト社が提唱するサーバー室温度 27 ℃ が妥当な設定であるか, 本学のサーバー機器の例を挙げて考察する.

5.1. サーバーの環境温度上昇の特徴

前章 3 項の 1 に挙げたように，空調停止後の数分間は吸気温度（上部）の上昇は極めて急速である（図 11）. 空調不調時の上下変動時は吸気温度の上部と下部は同じ温度を示していたにも関わらず，数分で約 5 ℃ の温度差が生じている．それに比べると他の温度上昇は比較的緩やかである.

この現象の原因としては，サーバー機器からの排気熱がラック前面に回り込んだ影響が大きいと考えられる. 数分で平衡状態になったのは，サーバー室内の排気と吸気の循環が固定化したことによる可能性が高い．なぜなら，約 5 ℃ の差はセンサー位置の高さの差でしかなく，これ以降安定して温度が上昇しているということは空気の乱れがほぼ生じていないと考えらえるからである.

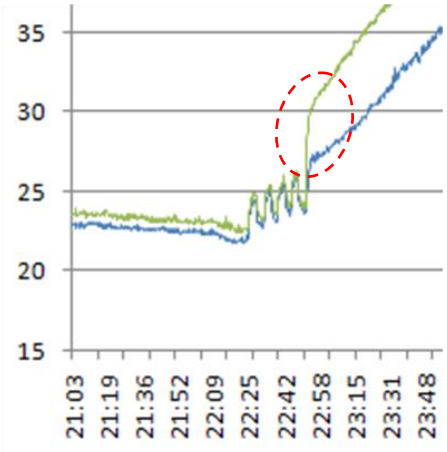


図 11　吸気温度（上部）のみが急激な温度上昇（点線円に該当部分を示す）

5.2. 各温度の上昇率の傾向

空調故障後，各温度は安定した温度上昇を続けるが，実際にはどの程度の類似性があるか定量的に評価する. 解析対象とした温度データは，排気の回り込みが落ち着いた 22:00 頃から，システム（ドメインコントローラ）が停止した 23:30 頃までとした．その理由としては，システムが停止することでサーバー室内の排気量が異なり温度変化に影響が出ると考えられるからである.

評価手法としては，最小自乗法による線形近似および回帰分析による重決定 R^2 を用いた．線形近似としたのは，安定した温度上昇部分かつ狭い時間間隔においてはおおむね線形変化していると想定したからである.

結果を図 12 に示す．図において縦軸は温度，横軸は秒としている.

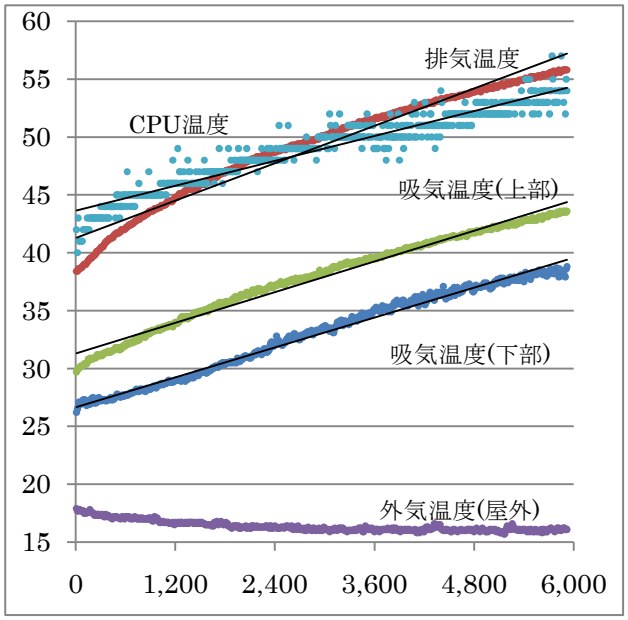


図 12　線形近似による温度上昇の分析（温度上昇時の 22:00 頃 からシステム停止の 23:30 頃まで）

各パラメーターおよび重決定 R^2 を表 4 に示す．表からも明らかなように，どの温度もほぼ線形を保っており，吸気温度は上部下部ともに a が $2.2 * 10^{-3}$ であることから，同じ上昇率であることが分かる．

一方，CPU 温度データが分散しているように見えるのは，温度情報のオーダーが 1 であるためである．しかしながら，R^2 は 0.9923 であることからほぼ線形変化である．温度上昇率は a が $1.8 * 10^{-3}$ であることから，吸気温度よりもやや鈍い上昇率となっている．

最も上昇率が高いのは排気温度の $2.7 * 10^{-3}$ である．排気は CPU やシステム内の温度を吸収しているための結果だと考えられる．なお，この時間帯（日曜日の 23:00 頃）での CPU 負荷はほぼゼロなので，CPU の温度上昇は吸気温度上昇に依存していると推察できる．

ところで，温度上昇率となる a はサーバー室のエアフローにより決定されると推測される．つまり，a が低いほど良好なエアフローが保たれており空調障害時の耐性が高いと考えられる．

表 4　最小自乗法による結果パラメーター

温度	a (10^{-3})	b	R^2
吸気温度（上部）	2.2	31.287	0.9837
吸気温度（下部）	2.2	26.664	0.9887
排気温度	2.7	41.291	0.9632
CPU 温度	1.8	43.626	0.9923

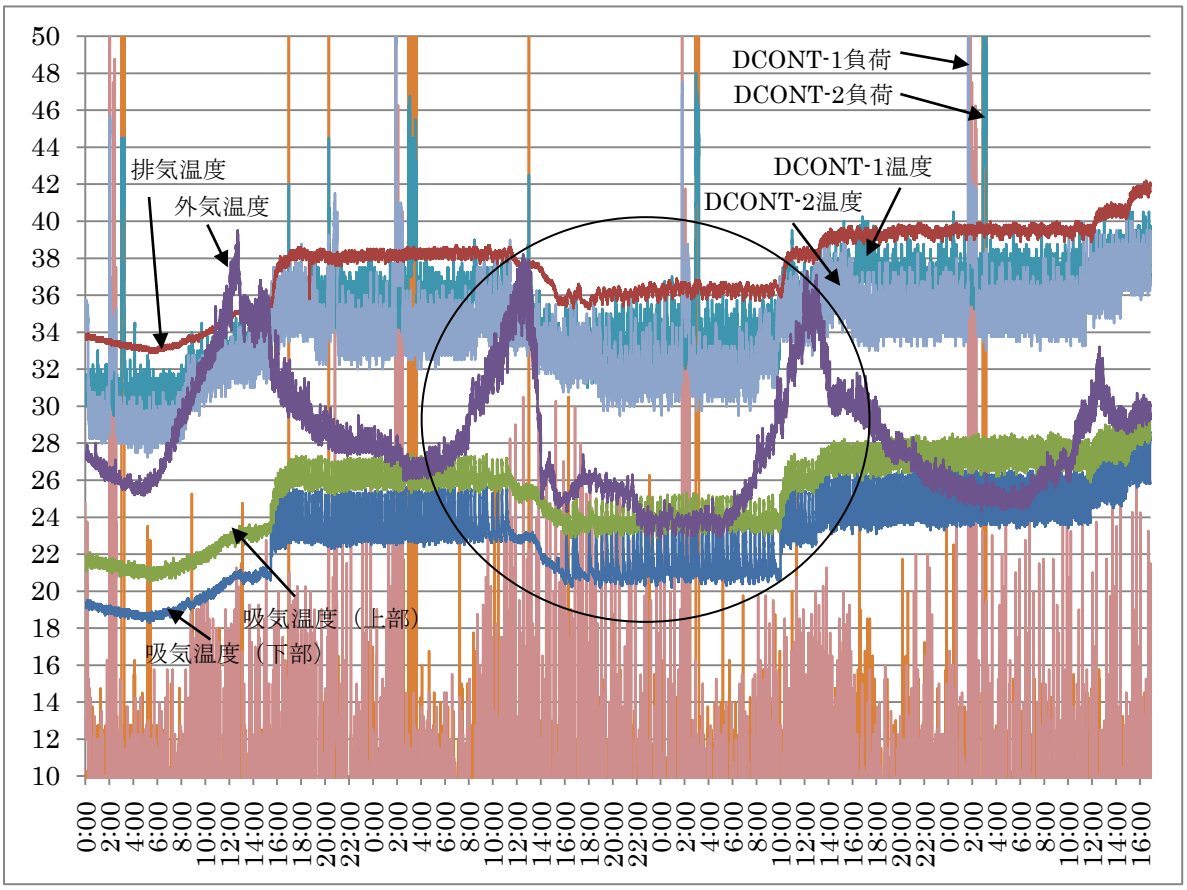


図 13　CPU 負荷を含むサーバー環境温度の統合グラフ（2011 年 6 月 29 日 0 時から 7 月 3 日 16 時まで）

5.3. CPU 負荷を含めたサーバー環境温度

図 13 にサーバーの環境温度に加えて，CPU 負荷も含めたグラフを示す．およそ 4 日間のデータであり，外気温を見るとちょうど 12 時過ぎ頃に温度のピークが記録されている．本来の気温よりもやや温度が高いのは，センサー位置の問題が考えられる．空調室外機の近くであることやコンクリートの照り返しが影響した可能性がある．

吸気温度・外気温度に着目すると，30 日 16 時頃から温度が上昇している．これは空調の設定温度を 23℃としたためである．それ以前は最大冷却の 20℃であった．図中の丸で囲んだ部分は一時的に設定温度を 21℃に変更して温度応答を調べてみたところである．結果としては設定値分の温度下降が確認できた．

その後, 7 月 2 日 12 時頃に温度設定を 25℃としたが同様に各温度は空調設定に追従した．ここで重要なのは，外気温が大きく変化してもサーバー室にはほとんど影響がないことである．つまり，吸気温度はあくまでも空調の温度設定に影響されるということである．

サーバーの安定稼働を考慮した場合，吸気温度が重要なのは明らかである．一般的なサーバーの場合，吸気温度の限界は 34℃である. 今回の調査では空調設定を 26℃にしても十分に余裕があった．

6. まとめ

これまでの温度評価から，サーバー機器の温度管理においては吸気温度がもっとも重要であることがわかった. また, 吸気温度は上部と下部で約 5 ℃の温度差があることから, 高温になる機器は下部に設置するのが好ましい．

また，サーバー排気熱の回り込みは吸気温度を顕著に上昇させることから，サーバー室内の換気口へ直接排出するのが望ましい．しかし，現実としては関連機材の配置やケーブルの取り回しを考慮すると簡単ではないだろう．

サーバー室の空調設定は，エアフローが適切であれば 26℃でも余裕があるが, 本学ではこれまでは常に 20℃としており過剰冷却であった．現在，やや高い環境温度と思われる吸気温度 28℃付近のテストも行っており，これらは別の機会に報告する．さらに，サーバーの節電を考慮した場合は電力の実測が必要であるが，今後は温度調査に合わせて行っていきたい．

参考文献

[1]. 経済産業省，http://www.meti.go.jp/earthquake/shiyosei gen/index.html

[2]. Microsoft 社自動節電プログラム，http://support.microsoft.com/kb/2545427/ja

[3]. ワットチェッカー，http://www.sanwa.co.jp/product/syohin.asp?code=tap-tst5

[4]. PUE 解説，http://www.dir.co.jp/souken/green/keyword/13_pue.html，大和総研

[5]. The Green Grid, “The Green Grid Data Center Power Efficiency Metrics: PUE and DCiE,” Technical Committee White Paper, 2007.

[6]. Malone, C., Belady, C., “Metrics to Characterize Data Center & IT Equipment Energy Use,” Proceedings of 2006 Digital Power Forum, Richardson, TX, 2006.

[7]. Greenberg, S., Mills, E., Tschudi, W., Rumsey, P., Myatt, B., "Best Practices for Data Centers: Lessons Learned from Benchmarking 22 Data Centers," ACEEE Summer Study on Energy Efficiency in Buildings, http://eetd.lbl.gov/emills/PUBS/PDF/ACEEE-datacenters.pdf, 2006.

[8]. Google data centers (Mesurement), http://www.google.com/corporate/datacenter/efficient-computing/measurement.html

[9]. 日本マイクロソフト, “サーバー ルームの節電に関する詳細情報，http://technet.microsoft.com/ja-jp/windowsserver/hh272765

[10]. 4 チャンネル温度 SD カード記録計 47SD，http://www.ureruzo.com/ondo47SD.htm，株式会社佐藤商事

[11]. CoreTemp，http://www.alcpu.com/CoreTemp/

[12]. Intel SERVER PROCESSORS，http://www.intel.com/products/server/processor/index.htm

[13]. Intel® Xeon® Processor E5520 (8M Cache, 2.26 GHz, 5.86 GT/s Intel® QPI)，http://ark.intel.com/Product.aspx?id=40200

[14]. 榎本 寿彦, “空冷ヒートポンプパッケージエアコンの能力曲線,” Refrigeration 83(968), 418-420, 2008.

[15]. 岡田拓也，今井正和，“空間的に密な温度変化を計測するシステムの構築,” 電子情報通信学会技術研究報告. IA，インターネットアーキテクチャ 109(137), 13-18, 2009-07-10.

[16]. 田中公祐 ,佐藤裕樹 ,諏訪敬祐, “ワイヤレスセンサネットワークにおける画像及びデータ計測センサの統合化とデータ収集法に関する研究,” 情報処理学会研究報告. ITS, [高度交通システム] 2006(120), 67-74, 2006-11-16

[17]. 岡本昌幸，小林俊満，赤井光治,“サーバー室空調の省エネに対する取り組み,” 学術情報処理研究 (14), 72-76, 2011

高精細多地点遠隔講義システムの全国運用と開始 2 年の状況

High-Definition multipoint teleconference system at Japan and a report for two years

櫻田　武嗣†，萩原洋一†，古谷　雅理‡
Takeshi Sakurada†, Yoichi Hagiwara†, Tadasuke Furuya‡

take-s@cc.tuat.ac.jp, hagi@cc.tuat.ac.jp, tfuruya@kaiyodai.ac.jp

†東京農工大学総合情報メディアセンター
‡東京海洋大学海洋工学部海事システム工学科

†Information Media Center, Tokyo University of Agriculture and Technology
‡Faculty of Marine Technology, Tokyo University of Marine Science and Technology

概要

本論文では，多地点を高精細映像で結ぶ遠隔講義システムの全国運用と運用開始から 2 年間の状況について述べる．我々は 2009 年から全国 18 国立大学法人を HD 品質の高精細映像，高品質な音声で結び，利用者の負担を減らすための自動化をすすめた遠隔講義システムの設計と構築を行い，運用を行っている．通常はシステムが予約に従い自動起動や自動終了するが，万が一自動起動しなかった場合の復旧を簡単にする仕組みや，予約時間を簡単に延長する仕組みの設計，構築など使いやすくするための改良，調整を続けている．またこの 2 年の間に設置拠点も増え，遠隔の教室を結ぶだけでなく近隣の教室を結んで仮想的な大教室としての利用もされている. 本システムは 1 日約 2 件の遠隔講義や会議で利用されている. 今後も高品質な映像，音声を生かした幅広い活用が期待される.

キーワード

多地点遠隔講義システム，自動制御，遠隔会議システム運用

1. はじめに

近年大学間，地域間連携の流れが進み，複数の大学などを結んだ遠隔講義が行われてきている．東京農工大学（以下，本学と記す）でも SCS(Space Collaboration System)[1]を利用して遠隔講義を行ってきた. SCS は衛星通信を利用するため，天候に左右されて通信が安定しないなどの問題を抱えており, 導入から 10 年以上が経過しているため，機器の故障などがあり，安定的に遠隔講義を行うことは難しくなっていた. 現実に 2008 年 6 月に国立大学法人 12 校を結んで 2 日間行われた集中講義では，天候の問題や機器の問題で衛星回線が途切れ，スムーズな遠隔講義を行うことが難しかった．この回に限らず，安定した遠隔講義ができなくなりつつあり，その解決の

ためにも SCS に替わる新しいシステムが必要とされていた．一方で，ネットワークの広帯域化が進み，ネットワークを利用して映像や音声を配信することで遠隔講義を行うことも可能となった．しかしながら，これらネットワークを利用した多くの遠隔講義システムは一つの大学内の離れたキャンパスを結ぶもの，数大学を遠隔講義の実験として結ぶものがほとんどで，SCS のように多くの大学が定常的に講義で利用するものではなかった．さらにこれまでの遠隔講義システムの画質はアナログテレビ程度の品質以下であるものが大半であり，詳細な資料等を提示しながら高度な教育を行うには不十分なものであり，中には独自規格の製品のため，他の遠隔講義システムと接続できないものもあった．

そこで我々は，多地点を高精細映像で結ぶ遠隔講義システム(以下，本システムと記す)を導入することとし，設計，構築を行い，2009 年から運用を開始した．SCS に替わるものを目標に導入すすめたが，設計開始時には SCS の運用停止が発表され，本システムを運用することがさらに重要なものとなった．

本論文では高精細多地点遠隔講義システムとその予約，自動制御について述べるとともに，全国運用を開始してからの 2 年間の状況と利用傾向について述べる．

2. 高精細多地点遠隔講義システムの設計と構築

2.1. 従来の遠隔講義システムの問題点

これまで利用されてきた遠隔講義システムは，テレビ会議システムをそのまま利用したものが多く，CIF(352×288 画素)サイズの画像を伝送するものが中心であった．アナログテレビ放送は NTSC の場合約 720x480 画素であり，これと比べても画像解像度は十分ではない．資料や模型などを利用して説明が行われる講義も少なくないため，高品位映像を遠隔講義で利用するために様々な取り組みがなされてきた．定常的に授業を行うことを目的にしたものでは，地域の大学間を結び，高品位な映像を用いる北陸地区双方向遠隔授業システム[2,3,4]がある．しかしながらこれは従来品のテレビ会議端末を利用した遠隔講義システムや他社製品との互換性が無い独自規格であり，高価でもあった．

我々も 2006 年から宇都宮大学，茨城大学との間で DVTS(Digital Video Transport System)[5]を用いた遠隔講義の実験を行っていた[6]．DVTS は DV をそのまま送受信するためこれまでのテレビ会議システムに比べ画質が良い．今後一般的な講義室での導入を検討していくため特に帯域制御を行わず実験を行ったが，各大学内で DVTS 以外の通信がバースト的に発生する度にブロックノイズが発生したり，通信断が起きたりした．伝送レートを 25Mbps から 1/2，1/4 などに落としていくと安定度は高くなるが，それでも時々ブロックノイズが発生するなど通常の講義を行うには安定度の面で問題が残るものであった．

これまでの遠隔講義システムでは，高品位映像に対応できないか，対応できたとしてもネットワーク帯域等の問題から独自規格のシステム以外に安定的に運用できないという問題があった．

もう一つの問題として運用時の問題がある．これらテレビ会議システムをそのまま利用した機器の場合には，機器の操作に習熟した人が各拠点で必要になる．遠隔講義の開始時刻前に，機器の起動とテレビ会議の接続を行う必要があり，それができる人の確保が問題であった．

これらの機器の互換性の問題，機器操作者の確保の問題から，多くの遠隔講義システムは導入されてもなかなか活用されるには至らなかった．

2.2. 高精細多地点遠隔講義システムに求められる要件

本システムでは SCS で行われてきたものと同じ形態で遠隔講義ができるだけでなく，安定した接続が可能で，システムの操作が簡易であることが求められる．各拠点に機器操作に習熟した人を配置しなくても講義が可能であることが望ましい．

また本システムの導入にあたっては，全国のすべての連合農学研究科の構成大学を結んだ遠隔講義を行いたいとの要望があった．つまり，本システムでは国立大学法人 18 校(帯広畜産大学，弘前大学，岩手大学，山形大学，茨城大学，宇都宮大学，東京農工大学，岐阜大学，静岡大学，鳥取大学，島根大学，山口大学，愛媛大学，香川大学，高知大学，佐賀大学，鹿児島大学，琉球大学)(図 1)を最低限結ぶ必要があり，SCS の替わりを目指すためには全国の大学を結ばなくてはならない．

連合農学研究科内の講義は遠隔地の学生同士のディスカッションも組み合わせる試みも行われており，配信型の講義スタイル以外に双方向型の講義スタイルにも簡単に対応できる必要がある．

また講義科目の特性上，資料を利用して説明されることが多く，鮮明に資料を伝送・表示できることも求められる．近年は PowerPoint などを利用する講義が増えているため，PC の画面，音声も伝送できる必要がある．

新しいシステム構築のために複数の SCS 利用者から意見の聞き取りを行ったところ，これまでの SCS では機器操作が煩雑で分かりにくいという意見が多かった．構

図- 1 接続する 18 国立大学法人とその位置

築を行う拠点では，利用者の多くが農学系で，機器操作に苦手意識を持っている人が少なくないことが分かったため, 本システムでは, 機器操作をできるだけ簡単にし，通常の対面講義と同程度の準備で遠隔講義ができるようにする必要がある．

本システムは少なくとも 4～5 年は使用することを前提としており，地域連携や国際交流などで初期導入の 18 国立大学法人以外とも遠隔会議や講義を行うため，拡張性があり，独自の規格ではなく，業界標準に基づいた機器を利用する必要がある．

2.3. 本システムの設計と機器選定

遠隔講義システムの多くはテレビ会議システムをベースに構築されるが，その形態はテレビ会議専用端末を用いる方式，Web ブラウザなどを利用したソフトウェア方式の 2 つに大きく分けられる．それぞれの長所と短所を表 1 に示す．ソフトウェア型は初期の導入コストは安く済むが，映像解像度の問題や拠点数の増加などに対応することが難しい．またソフトウェア型は個人同士の小規模の会議向けであることが多いため，大講義室のように映像・音声系統を作り込まなくてはいけない場合に，システム構築が難しいという問題がある．

既に多くの大学や企業でポリコム，タンバーグ，ソニー製の H.323 や SIP に準拠したテレビ会議端末が導入されており，それらとの相互接続性や前述の大講義室でのシステム構築のことを考え，今回はテレビ会議専用端末を利用する方式を選択する．

講義で使用する資料などを高品質で遠隔地で見せる必要があるため HD 品質の映像に対応し，同時に PC の映像を高品質で伝送できるようにする必要がある．初期の

表-1 テレビ会議システムの一般的な特徴

	テレビ会議専用端末型	ソフトウェア型 (Web ブラウザ利用型)
初期導入コスト	高い	安い
多地点の接続	MCU 利用で可能	一定数以上できない
機器拡張性	有り (会議室の AV システムへ組み込み可能)	無し
画質・音質	高品質(HD 対応)もあり	低品質
他社互換性	有り	無し

構築ではベースとなるテレビ会議端末として，他社互換性があり，HD 対応の HDX-8006XL(ポリコム社)を利用する．これは，SD(従来のテレビ品質)，HD 品質で他社製品混在の通信も可能であり，720p/60fps，1080p/30fps，ステレオ 22kHz の音声にも対応しており，RS-232C などで外部から制御可能である．

また本システムでは，初期から 18 大学 23 拠点の接続を想定していたため，多地点接続装置(Multipoint Control Unit，以下 MCU と記す)が必要となる．通常テレビ会議端末に内蔵可能なものは自局を含めて 4～6 拠点である．これでは同時接続可能数が不足するため，MCU (ポリコム社製 RMX2000-MPM+160，HD 対応テレビ会議端末を 40 台まで，通常の CIF 解像度の場合 160 端末まで同時接続可能)を導入する．将来的にさらに接続台数が必要な場合には MCU を追加導入し，カスケード接続により増やすこととする．

本システムのような遠隔講義システムを導入する場合，MCU 単体とテレビ会議システム単体を導入するだけで終わることが多い．単体導入の場合，毎回機器の操作をしてテレビ会議を接続しなくてならず，機器操作が難しい．加えて講義スタイルは一般的な会議スタイルではないため，講師側，受講側が替わる度にカメラ，モニタの配置や機器設定を変更しなくてはならず，手間がかかってしまう．その結果活用されなくなる例が少なくない．

そこで本システムでは，様々な講義スタイルに対応するため，カメラを増設(前方，後方に計 2 台設置)する．さらに大教室でも音声のエコーやハウリングが起きにくくするための対策を行う．このエコーやハウリング対策は，従来はデジタルミキサや専用のエコーキャンセラーを組み合わせて実現することが多かったが，内蔵しているエコーキャンセラーがテレビ会議用にチューニングされている点や遠隔地から機器の状態監視や設定変更が行える点を重視し，それらを 1 台の機器で行える Sound Structure(ポリコム社)を使用する．

操作を簡易にするための仕組みとして，無線式タッチパネル(図 2)を利用し，後述の予約システムと連動させて機器操作の自動化を行う．通常テレビ会議端末は機器付

図-2 無線式タッチパネル画面

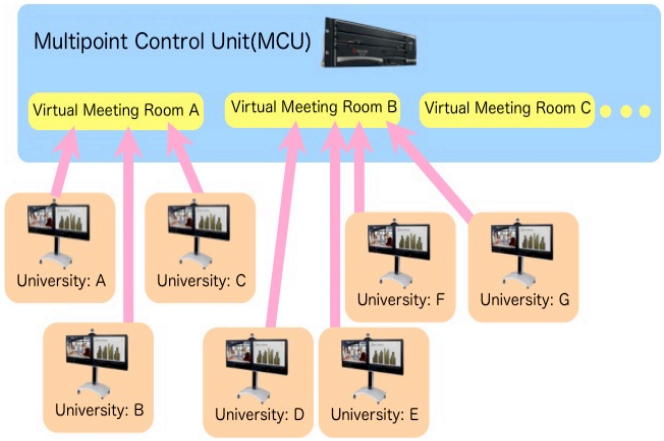


図-4 MCU の利用と仮想会議室

属のリモコンで操作を行うが，リモコン上のボタンが数十にもなり，操作に慣れていなければ使いこなすのは難しい．またテレビ会議システムの利用中に不用意にリモコンのボタンを押してしまい，意図せず会議の通信が切断されたり，機器の設定が変わったり，音声ミュートがかかったりするなどのトラブルが発生しがちである．対策として本システムではテレビ会議システム端末付属のリモコンは使用させず，その代わりに無線式のタッチパネルでテレビ会議端末やカメラ，AV 機器(プロジェクタや大型モニタ，音声アンプ，マトリックススイッチャなど)を同時に操作できるようにする．そのためにシステムコントローラが必要となるが，これには AMX 社製の NI-3100 コントローラを利用することとした．このコントローラは Ethernet からコントロールできるため，予約システムと連動させることで遠隔地からのシステム立ち上げや立ち下げ，遠隔監視・操作を行うことができる．

各大学の拠点に配置する機器を図 3 に示す．映像表示装置は，部屋の大きさや受講人数が各大学で異なるため同一機種ではないが，フル HD 品質対応のプロジェクタまたは大型モニタを各拠点に 2 面配置し，講師(受講者)映像と PC 画面等の資料映像を同時に表示可能にする．これら大型の映像表示装置は普段の授業や講義で有効活用したいという要望が当然出てくる．そのため「機器のリモコンで遠隔講義と通常講義用の入力を切り替えて…」というシステムにすると，いざ遠隔講義となった時にシステムが立ち上がっているが，機器の入力が切り替えられてしまっていたために，映像が映らないで戸惑うということが十分に考えられる．そこで本システムでは，タッチパネルに遠隔講義を使用しない普通の講義用のモードとして「映像・音声のみ使用」という項目を用意した．これを選択することでプロジェクタやマイクだけを簡単に使うことができる．

通常 MCU を使用して多地点を接続する場合には，MCU 内に仮想的な会議室を作成しておき，その会議室にテレビ会議端末を接続させる(図 4). 接続される拠点が常に同じであればあらかじめ仮想会議室を作成しておき，

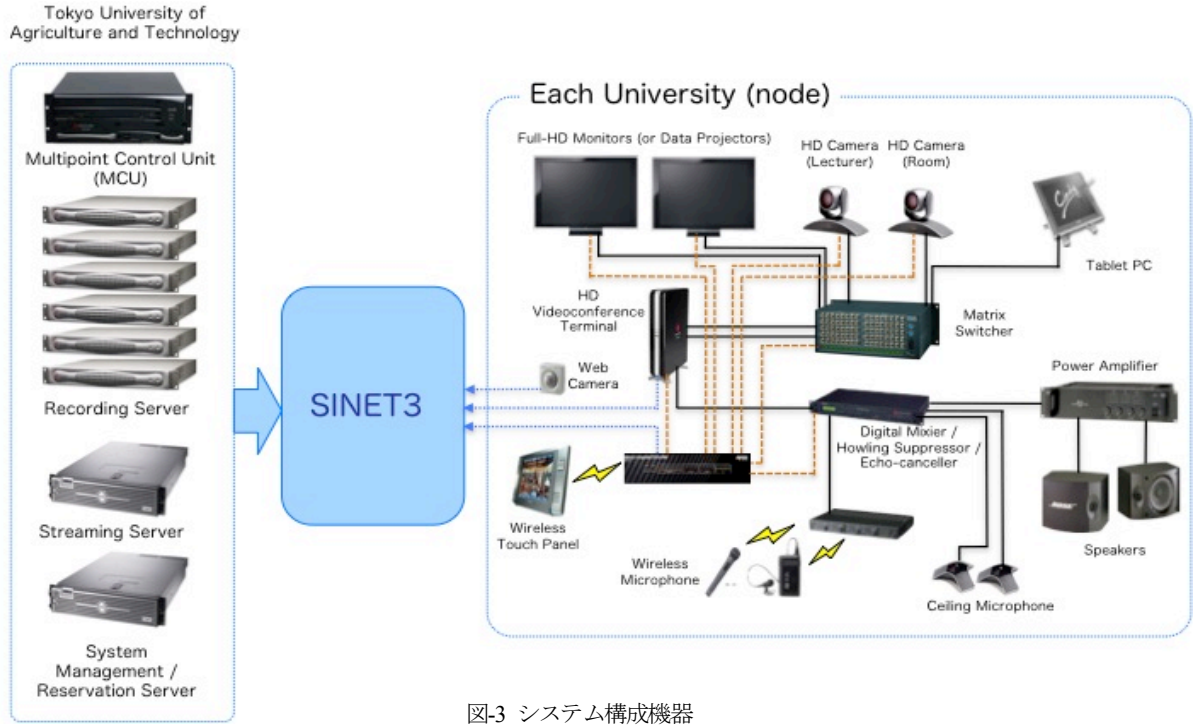


図-3 システム構成機器

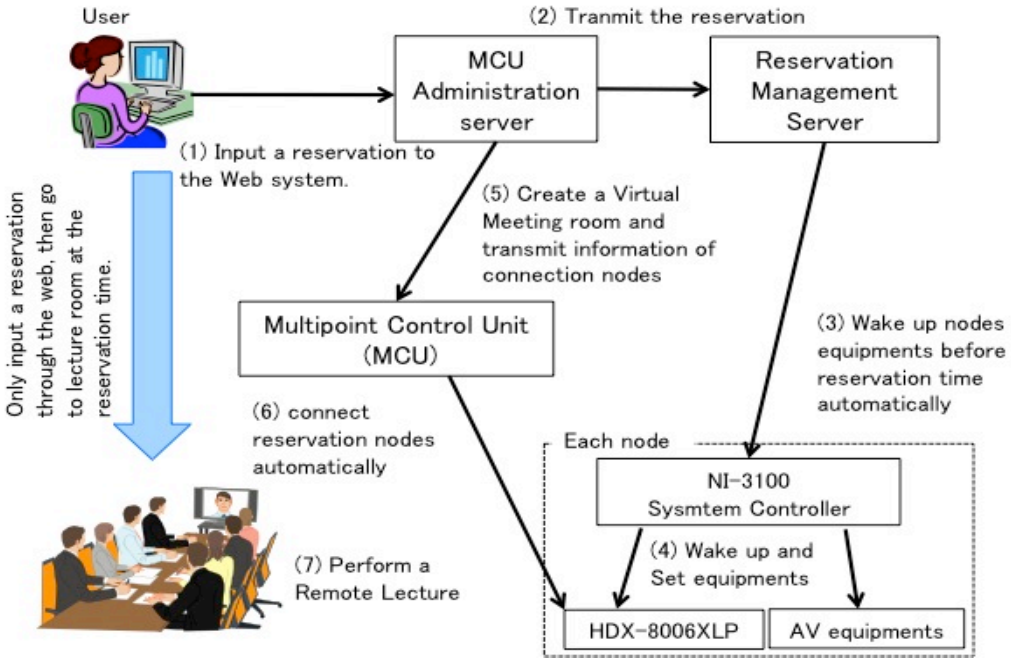


図-5　システムの利用の流れ

その仮想会議室にテレビ会議端末を接続すればよい．しかしながら，本システムでは 2～3 の大学を結んでの会議や遠隔講義，全大学を結んでの遠隔講義等の様々な用途で使用するため，接続される拠点が常に同じではない．また複数の講義が並行して行われることがある．このため講義が行われる度に MCU 内に仮想会議室を作成し，テレビ会議端末を接続する必要がある．毎回作成することで，無断で MCU に接続してリソースを利用される危険性を減らすこともできる．そこで MCU のリソースを管理するための予約管理システムを構築する．

予約管理システム利用の流れを図 5 に示す．利用者は予約管理システムにあらかじめ接続したい拠点，利用する日時を Web インタフェースから入力し予約する．予約時刻の 3 分前になると予約管理サーバが MCU 内に仮想会議室を作成，接続予定の各拠点のテレビ会議端末や AV 装置等を遠隔で起動する．機器の起動には時間がかかるため 3 分前に機器の起動をはじめている．予約管理サーバは各拠点の機器の起動を確認した後，予約された時間に遠隔操作でテレビ会議端末を MCU へ接続する．この自動化により学生，講師は予約時間に各拠点にいくだけで遠隔講義が開始された状態になっている．予約終了時刻 1 分後には自動的に予約管理システムが各拠点のテレビ会議端末を切断し，AV 機器などを含めて自動的に立ち下げる．利用者は機器の操作をすることなく拠点から帰るだけでよい．

予約通りに会議や講義が終われば良いが，実際には講義や会議が予定した時刻になかなか終わらないことがある．Web から予約の変更をしても良いが，講義や会議に集中している中で Web 画面を開いて予約の変更を行うことは難しい．そこで各拠点に設置する無線式タッチパネルの中に「時間延長」のボタンを配置することにした．この「時間延長」を押すことで 10 分間予約終了時間を延長することができる．押す度に 10 分間ずつ延長が可能であるが，次の予約が入っている場合には終了処理を行い，次の予約を実行する．

急な会議や講義にも対応するため，２つの方法を用意した．一つは予約管理システムで，即時会議という選択肢を増やし，それを選択した場合には，即座に予約管理システムが各拠点のシステムを起動し，自動的に接続を行う．もう一つは，あらかじめ用意してある仮想会議室に接続する方法である．これはタッチパネルにあらかじめ用意してある仮想会議室(構築では 3 つの仮想会議室を用意)への接続ボタンを表示し，各拠点ではシステムを立ち上げ，同じ仮想会議室への接続ボタンを押すだけで接続が完了するものである．ただし，選択した仮想会議室が別の会議や講義で使っていた場合には利用できないので，あくまで急な利用に限られる．通常は前述のように予約システムを利用して自動的にシステムを立ち上げる形で利用する．

終了コマンドを予約管理システムが発行したにもかかわらず，何らかの不具合で機器との通信が正常に終了せず，何日も起動したままとなることを防ぐため，夜中に各拠点のシステムのリセットを毎日自動的に行い，電源が入りっぱなしになることを防いでいる．

2.4. 講義の収録と変換

講義収録用にレコーダを用意する．設計時に最大 6 つの講義が同時に行われることが想定されていたので，HD 収録に対応した Polycom RSS-2000 を 6 台用意した．これ

も予約管理システムから制御され，予約時にレコーダを選択すると，自動的にその講義や会議が録画される仕組みとした. 録画したコンテンツを Web にアップロードする際には，WMV 形式ではなくビットレートを抑えた mp4 形式にする必要が多くあるため，簡易的なビデオコーデック変換用のサーバを用意し，予約の録画が終了すると WMV 形式から mp4 形式へ自動的に変換を行う仕組みを構築した.

2.5. 構築・運用開始時の問題点と改良

実際の構築では細かい点も含め多くの問題点が洗い出された．ここでは，今後同様のシステムを構築する際に参考となるである点を述べる.

まずテレビ会議の接続ができない場合，ネットワークの配線，設定ミス，ファイアウォールで利用ポートが開けられていないことが原因として挙げられる．実際にネットワーク配線のミスがあったり，機器設定問題があったりして通信が構築当初はなかなか確立できなかった．具体的には Cisco 製 PIX ファイアウォールのバージョン古く，H.239 の通信が落とされてしまう問題があったり，大学内部で AMX　NI-3100 システムコントローラ制御に使うポートが，ネットワーク監視に使われており，利用を制限していて自動制御ができなかったりして，各大学の担当者に原因調査に協力してもらい，都度回避策を考えつつ対策を行った.

また通信が確立してもある大学は必ず一定時間後，多くは 1 時間もしくは 2 時間後に接続が切れてしまうという問題が発生した．これは該当大学内のファイアウォールのセッション維持時間がデフォルト値 3600 秒または 7200 秒で設定さており，その時間が過ぎると通信を一度切断してしまうのが原因で，デフォルト値を書き換えたり，該当する通信ではセッションを切らないように設定したりしてもらい対処する必要があった. しかしながら，各大学でネットワーク機器の更新があった場合には，セッション維持時間については考慮されていない場合があり，再度問題解決のための設定をファイアウォールに入れてもらうことが毎年起きている.

本稿執筆時はだいぶ安定はしているが，構築当初は使用したテレビ会議コーデック HDX-8006XLP，MCU の RMX-2000MPM+160 が新製品であったため, バグ出しが完全ではなく，ネットワークや設定の問題なのか，機器自体のバグなのかの切り分けが難しい点があった．現在も最新版のファームウェアでは接続や通信が安定しない現象が出ているため，最新版ではなく安定したファームウェアで運用を行っている.

各拠点ではシステム利用時以外は省電力を図るため，外部から電源投入などの制御を受け付けるために必要な最低限の機器だけ常時電源を入れる形とした. このため，各拠点のシステムを起動してから実際にシステムが利用できる状態になるまでに時間がかかってしまう．特にハウリング，エコーキャンセラーのために用いた Sound Structure は高機能ではあるが電源投入から 3 分程度起動に時間がかかってしまう．映像機器の起動の方が速いため，映像が表示される状態になっても Sound Structure が起動中であるため音声が出ない状態となってしまう．利用者は，映像が表示されるとシステムがすべて起動し終わったと思い込み，導入当初に音声が出ないと戸惑う場面が見られた．現在は利用者に対しあらかじめ立ち上げに時間がかかる点を説明するとともに，タッチパネルにプログレスバーを表示し，起動までの目安を表示するようにしたところ，戸惑う状況は見られなくなった.

大学の場合春休みや夏休み，冬休みなど長期の休みがある．この期間，講義棟などの建物丸ごとブレーカを落

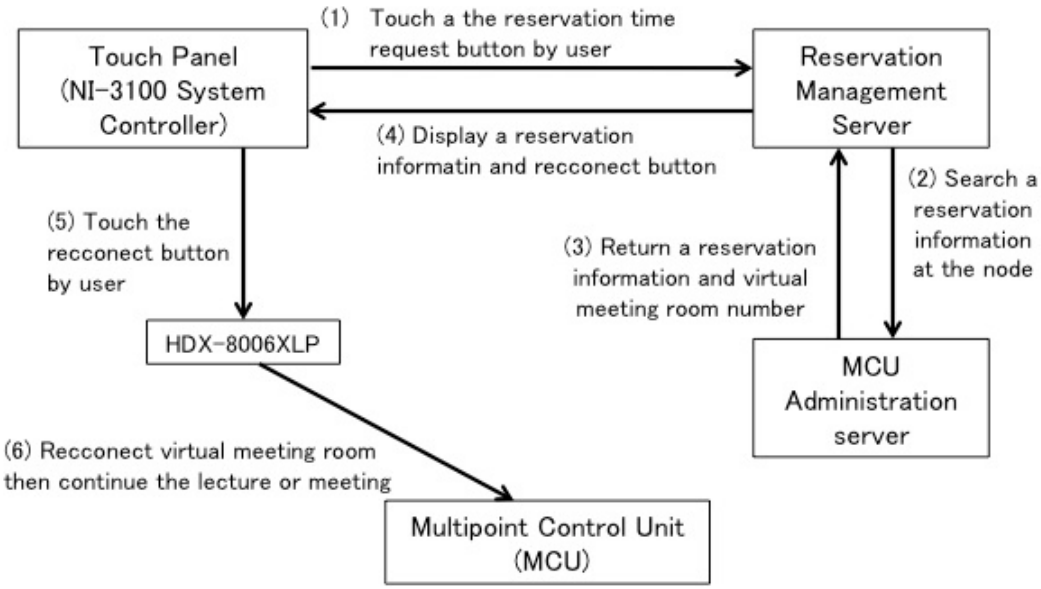


図-6　再接続問い合わせの流れ

としてしまう運用を行っている大学があり，休み明けに遠隔講義を行おうとしたところ，ブレーカを入れ忘れておりシステムが自動起動しないトラブルが起きた．この場合，拠点のシステムは自動起動しないため，ブレーカが入れられたあと，タッチパネルから拠点のシステムを立ち上げる必要がある．拠点のシステムが起動していれば，MCU は予約時間になっても接続できない端末は自動的に一定回数接続を試みるので接続が可能である．しかしながら，その回数を超えると自動的にテレビ会議が接続できない状態となる．

また一度接続が完了し，その後ネットワークの異常などで通信が切れた場合には，MCU 側からは自動的に再接続されないため，復帰の手段が必要となる．誤って接続を切る操作をしてしまった場合も同様である．

これらの停電や通信断の問題に対応するため，予約された遠隔講義へ接続・復帰するための機能を追加する改良を行った．タッチパネル上に予約確認と再接続の項目を追加した．タッチパネル上で「予約確認」ボタンを押すと予約管理サーバへ接続され，タッチパネルの ID からどの拠点からのリクエストなのかを判断する．予約管理サーバは MCU 管理サーバに接続し，リクエストのあった拠点が参加すべき仮想会議室の ID を検索する．該当する仮想会議室の ID があった場合には，タッチパネル側に仮想会議室 ID を転送され，再接続のボタンが表示される．利用者はその再接続ボタンを押すことで遠隔講義に参加・復帰可能となる(図 6).

3. 他のシステムとの接続と拡張

MCU はそれ自体の価格，保守費用が高価である．そのため複数台用意して冗長化することは難しい．テレビ会議システム自体は他システム，製品などと互換性があるため，MCU が故障してしまった際には，他の MCU を借りて遠隔講義を行うことが可能である．その場合には接続の部分の自動化ができないため，タッチパネルから各拠点で接続先の MCU の IP アドレスと仮想会議室番号を入力してもらう必要がある．本稿執筆時までは，幸いにもそのような状況にはなっていない．ただし MCU が故障した大学へ MCU のリソースを貸し出す，遠隔講義イベントで MCU の接続数が足りなかった際にカスケード接続をし，一部リソースを貸し出すなどは行っている．MCU を持っている大学同士で，いざという時の MCU のリソースの相互補完を行うことで，複数台 MCU を所有して冗長化するコストを削減している．

また MCU が故障した場合は前述のように他大学などの MCU を借りる他に，各拠点のテレビ会議端末では自拠点を含め４拠点が接続できるようになっているため，４拠点以内の接続であれば，それを利用して遠隔講義を行うことが可能である．

高精細な映像や音声が双方向で配信できるため，これを遠隔講義や会議以外にも利用する．近隣の教室を本システムで結んであたかも広い一つの教室を作り出す．これによって全員を収容出来る大教室を物理的に作ったり，会場を借りたりする必要はなくなる．2009～2010 年にかけて教室を整備し，既に近隣の教室を結んで大学説明会や新入生オリエンテーションなど年に数回，大人数を収容しなくてはならない時に利用を開始している(図 7).

拠点システムの低コスト化にも取り組んでおり，小さな部屋への展開用に，テレビ会議端末として SONY PCS-XG80，タッチパネルを小型のもにした拠点の設計と構築を行い，テスト利用を始めている

4. システムの保守

連合農学研究科は複数の大学で構成される大学院であり，日常的に離れた大学と講義や会議が行われている．そのため特に本システムは重要なものとなっている．そのため基幹部分に関しては機器の保守契約を行っている．本システムでは遠隔から機器の操作や状態監視が可能であるため，これを利用し，遠隔から毎日機器状態のチェックを行ってもらっている．機器に異常が発生した場合は保守契約会社から電話が入り，各拠点の人が対応するか，修理を手配するかなど行う．これまでの対応で多いものは「無線式タッチパネルが充電器に置かれておらず，電池が空になっている」が多く，希にテレビ会議端末が壊れたり，システムがフリーズしてしまったのでラック全体をリセットするボタンを押したりということがある．遠隔監視で最初の切り分けがある程度できるため，その後の対応が比較的早く行われるのが特徴である．

連合農学研究科では，6 月と 11 月に全大学を結び，数日間遠隔講義を行い続ける．１コマごとに別の大学の先生が講義を行う形となっており，機器の操作はタッチパネルで簡単になったとはいえ連合農学研究科にとっては重要な位置付けとなる講義群であるため，この期間は講

図-7　近隣教室を結んでの使用

義のサポートを業者に依頼している．講義のサポートとして，本学に遠隔監視する部隊を数人派遣し，サーバ並びに各拠点の機器を講義中監視する．万が一通信が切れた場合などは，遠隔から再接続などをする．また，講義を本システムで導入している収録機器で録画し, DVD 等にして終了後にとりまとめの大学へ提出している．また，進行役の大学には連絡調整員として 1 名派遣してもらい，事前のテストやトラブルが発生した場合の進行調整などを行ってもらっている．

トラブルとして多いのは, 2.6 のところにも記したが，大学のネットワークの入れ替えがあった場合などは，その大学の接続が一定時間後に切れてしまうということが多くあり，休み時間中に遠隔からシステムを再起動して講義中に切れないように工夫する，もし切れてしまっても遠隔からすぐに再接続をするなどを行ってもらっている．本システムの問題ではないが，2009 年の集中講義では，SINET の一部地域で障害が起こってしまい，その先につながっている大学がネットワークに接続すらできなくなってしまうということが起きた．この時は，講義を収録していた DVD を SINET の障害が起きた大学へ送り，後日講義を見てもらい，メールやレポートで質疑等を行うという形式がとられた．

またシステムの利用者に対し，年に数回本システムを使って遠隔で利用者講習会を開催している．これは利用したいと考える人が増えている点，各拠点の事務担当者が定期的に入れ替わってしまう点などを考慮してのことである．10〜20 分程度の簡単な説明ではあるが，全く分からないでシステムを触ることに不安を覚えている人が多く，一度でも説明を受けると安心して利用ができるとの意見を得ている．

5. システムの利用状況

システムの利用状況について述べる．構築と試験運用を始めた 2009 年 1 月から 2011 年 6 月までの間に 1245 回予約，使用されている．この他に構築時にテスト運用で 39 回使用されている. 使用された回数を単純に日数で平均すると 1 日平均約 1.5 回使用されている．実際には大学は週末, 夏期休業, 年末年始などは休みであるので，それらを除くと 1 日 2 回以上講義や会議で使用されていることになる．定期的に行われる会議や講義の利用が増えている．月別の予約回数を図 8 に示す．目立った傾向は見られないが，2〜3 月と 9〜10 月の利用が他の月に比べて少ないのが分かる．2011 年 3 月に起きた東日本大震災以降は利用が減っているが，5 月の連休過ぎあたりから以前と同じように講義や会議の予約が入っている．この時期あたりから徐々に各大学も通常の体制に戻りつつ

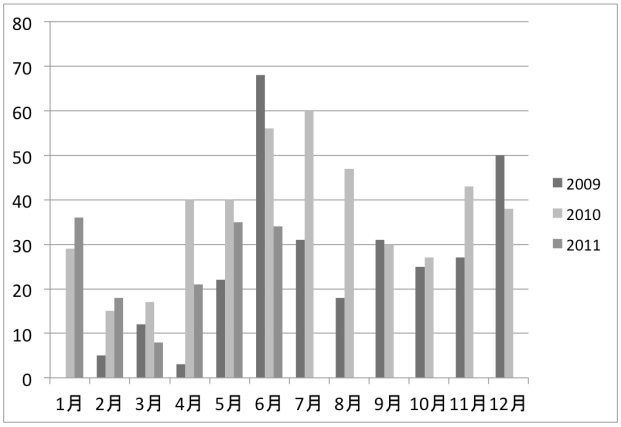


図-8　月別システム利用状況

あることが伺える．

予約時間延長ボタンは運用を開始した当初は何度か利用されているが，徐々に利用が減っており，全体で 10 程度の遠隔講義で利用された．遠隔会議・講義の平均開催時間は約 2 時間 40 分であるのに対し，予約時間は約 2 時間 50 分であるため, 余裕を持った時間で予約をする傾向にあるのが分かった．特に会議の場合は長めの時間予約されていることが多く，会議が終わった段階でタッチパネルからシステムを終了し，予約終了時間に自動的にシステムが終了するのを待っていないことも分かった．

また，多くの拠点を結んで特に会議を行うような場合には，事前に機材チェックや簡単な担当者打ち合わせが行われていることが予約のログから伺える．さらにあまり時間を空けないで複数の会議や講義が入れ替わり行われるような場合には，まとめて連続した時間で予約が行われている．そのため半日程度の予約があった．

1 つの遠隔講義，会議あたりの同時接続拠点数は，平均 4.2 拠点で，最大 24 拠点を結んだものがあった．本システムで導入した拠点以外にも，H.323 などに準拠した端末からも遠隔講義，会議に参加でき，実際に利用されているが，前述の同時接続拠点数にはこれらの数はカウントしていない．このため実際の同時接続拠点数はこれよりも多くなる．

6. おわりに

本論文は多地点を高精細映像で結ぶ遠隔講義システムの設計，構築ならびに運用の状況について述べた．本論文で示したシステムは，北海道から沖縄までの全国 18 国立大学法人を HD 品質の高精細映像，高品質な音声で結ぶものとして設計，構築を開始し，現在 2 年間運用を行っている．本システムは自動化やタッチパネルをするなどし，利用者の負担を減らす仕組みを設計・構築し，運用を行いながら機能の追加などを行っている．利用者は Web から簡単な予約を行うだけで，後はシステム側

が予約時間に自動的に機器を立ち上げ，設定，接続を行うため，利用者は予約時間に教室にいくだけでよい．

さらに現在は，構築するシステムを利用して隣接した教室を接続することで仮想的な大教室を作り出すなど，遠隔地を結んで使用するだけでない新しい使い方にも挑戦している．

運用を開始して 2 年であるが，適切に保守を入れ，利用者講習会を適宜開催していることで定常的な利用が増えてきている．1 日平均 2 件程度遠隔講義や会議で利用されている．また予約の傾向として，多くの大学を結ぶ場合には事前に短い機器テストや打ち合わせが行われていたり，特に会議の場合，予約時間は実際の時間よりも長めに確保されていたりすることなどが分かった．システムの利用状況を集計する際に分かったことだが，予約する際につける講義，会議名は利用者によって特徴が現れていたり，仮想会議室の番号は通常自動で割り当てられるが，指定することもできるので，毎回指定して予約をする利用者がいたりする．仮想会議室番号を毎回指定する利用者のいる拠点は，以前にテレビ会議システムが導入されていたところに多いが，この点なども今後調査していくと面白いと考えられる．

北海道から沖縄までの国立大学法人を大規模に HD 品質で結び，実運用を行う例は過去に無く，徐々に接続拠点も増え，利用も増えている．また本システムで利用している機器は，テレビ会議システムの業界標準に準拠しており，インターネットとも接続されているため，他の大学や研究機関，企業，さらには姉妹校などの海外の大学ともテレビ会議が可能であり，実際の接続も始まっている．本論文で述べたシステムを核として今後も利用が拡大されることが期待される．

参考文献

[1] 近藤喜美夫 : “衛星による大学間コラボレーションシステム(SCS)の開発と評価,”メディア教育開発センター，NIME 研究報告第 18 号，ISSN 1880-2192 (2006).

[2] 田中一郎，堀井祐介，高畠勝之 : “北陸地区双方向遠隔授業システム試行運用から見えてきたこと,”PC カンファレンス 2006 (2006).

[3] 長谷川 忍 : リアルタイム型遠隔講義におけるデザインパターン， システム技術分科会， サイエンティフィック・システム研究会 (2007).

[4] 長谷川忍，但馬陽一，二ツ寺政友，安藤，敏也 : “多様なメディアを利用した同期型遠隔講義環境の構築・実践,”メディア教育研究，投稿研究資料，メディア教育開発センター，Journal of Multimedia Aided Education Research 2006Vol.2，No.2，pp.79－91 (2006).

[5] 杉浦一徳，小川晃通，中村修，村井純 : “民生用 DV を用いたインターネットビデオ会議システム,” 情報処理学会， 情報処理, vol40, No7, 413， pp.698-702 (1999).

[6] 櫻田武嗣，萩原洋一，古谷雅理，江木啓訓，寺田松昭 : “DVTS を用いた遠隔・近接多地点講義教室の構築と運用,”マルチメディア，分散，協調とモバイルシンポジウム，情報処理学会，DICOMO 2006，pp.593-596 (2006).

[7] 学術情報ネットワーク SINET
URL： http : //www.sinet.ad.jp/

[8] 多地点制御遠隔講義システム導入用サイト
URL： http : //jets.med.tuat.ac.jp /

[9] 萩原洋一，櫻田武嗣，川島幸之助 : “全国 18 国立大学高精細遠隔講義システムの設計構築と課題,” 学術情報処理研究論文誌, ISSN1343-2915, No.13, pp40-48 (2009).

ヘルプデスク解析を応用した学生向けの情報提供
Provide Students with Helpful Information based on Helpdesk Analysis

吉冨健一 †, 岩沢和男 †，三戸里美 ‡

Kenichi YOSHIDOMI, Kazuo IWASAWA, Satomi MITO

domi@hiroshima-u.ac.jp, iwasawa@hiroshima-u.ac.jp, mitomito@hiroshima-u.ac.jp

広島大学 情報メディア教育研究センター †
広島大学 社会連携・広報・情報室 情報化推進グループ ‡
Information Media Center, Hiroshima University†
Information Promotion Group, Office of Industry-Academia-Government Collaboration, Community Relations, Public Relations and Academic Information, Hiroshima University‡

概要

広島大学情報メディア教育研究センターでは，利用者からの問い合わせ（ヘルプデスクメール）に着目し，サービスごとに問い合わせ件数を自動で集計するシステムの運用を行った。その結果，特に学生からの問い合わせに関しては，問い合わせ内容から対象となるサービスを逆引きすることに限界があることが明らかとなった。また，端末利用者へのアンケート結果から，わからないことがあった場合に, 問い合わせる学生は全体の４％にすぎず，１割を超える学生がそれを放置してしまうという結果が得られている。今回，学内の学生向けポータルサイト『もみじ』に，“パソコンＱ＆Ａ”という形で情報を掲載する機会を得た。この場を利用して，集計に基づいて前年同時期に多く寄せられた問い合わせ内容を掲載するとととともに，新規サービスの告知に活用した結果，メディアセンターの FAQ と比較して倍以上のアクセス数を得た。『もみじ』の“ パソコンＱ＆Ａ ”に選択的にメッセージを提供することは，学生に特化した情報の提供先として，センター FAQ よりも有用であることを確認した。

キーワード

情報提供，学生向け，問い合わせ, ヘルプデスク, 広報

1　まえがき

情報メディア教育研究センター（以下メディアセンター）では，利用者からの問い合わせ（ヘルプデスクメール）に着目し，毎月の問い合わせ状況をサービスごとに自動で集計するシステムを構築した。得られた集計結果を基に，提供サービスに関して使いにくいと思われる点やホームページによる解説のわかりにくい点などを洗い出そうと努力を行ってきた経緯 [1] がある。利用者数と比較して問い合わせ数の多いサービスは，いわゆる “わかりにくいサービス” であるとして，ホームページの記載事項の変更や，FAQ の充実などを行ってきた。

その結果，ホームページには 15 分野にわたり 167 個の FAQ が掲載される結果となった。FAQ のホームページを開いても自分の知りたい情報が，どこに掲載されているのか探し出すのがが大変で，逆に目的の情報にたどり着きにくい本末転倒な状況に陥っている。

集計システムは，事前に準備したキーワード群をフィルタとして利用して，問い合わせ内容に含まれる特徴的なキーワードから自動で分類し，サービスごとに集

計を行うシステムとなっていた。しかし，学生からの問い合わせに限っては（職員にも皆無ではないが），“メディアセンターのサービスに関する問い合わせ” というよりは “自分の置かれている困った状況” を強く主張する傾向がある。「ログインできません」などのように何のサービスにログインしようとしているのかさえ不明な状況や,「メールが読めません」という問い合わせの内容が，実は端末にログインできないことであったりすることが少なくない。このため特に学生からの問い合わせに限っては，内容から問い合わせの対象となっているサービスをうまく逆引きすることができないケースが多く発生した。

傾向としては，本来はアカウントの継続や変更に関する問い合わせ，および，端末室やネットワークの利用に関する問い合わせ内容が，メールに関する相談として寄せられる場合と，本来ならウイルス対策ソフトのファイアウォール機能によるトラブルが，メールやネットワーク接続に関する相談として寄せられ，提供サービス別にきちんと分類できないことが多いことが挙げられる．

他にも，メディアセンターとは無関係な内容の問い合わせや，対象のサービスが不明で具体的でないなど，再度こちらから質問の真意を問い合わせる必要があるような問い合わせが四年間の平均で 11 %，三ヶ月ごとの集計では最大 20 %に達する期間もあった。

端末室の利用者を対象としたアンケートによると，学生の一部はわからないことがあっても，放置する傾向にあることも判明した。

本論では，学生向けポータルサイトの場を借りて情報発信を行う契機を得たことで，メディアセンターのホームページに掲載する場合とどのような差が出るのか検証を行った結果を示すとともに，学生が知りたい情報をどのように抽出し，我々が伝えたい情報をどのように加工すべきか，あわせて検討を行った結果を示す。

本論の構成としては，２章で研究を行うに至った背景，３章では学生の知りたい情報を抽出するため，過去の学生からの問い合わせから得られる傾向を明らかにし，４章は，３章で把握した傾向をもとに，どのように “パソコンＱ＆Ａ” を作成すべきかの検討を行った結果を示す。５章で実際に『もみじ』に掲載された内容を掲載し，それぞれのアクセス数を示すとともに，メディアセンターの FAQ との比較から広報の効果の検証を行った結果を示す。

2　研究の背景

研究を開始するにあたっては，学生向けポータルサイト『もみじ』に，“パソコンＱ＆Ａ” という形で，メディアセンターからの情報を掲載する機会を得たこと，

図- 1: リニューアルされた『もみじ』の画面例

および端末利用者アンケートから，わからないことがあっても放置する学生の姿が，浮き彫りになったことが挙げられる。

2.1　『もみじ』のリニューアル

広島大学では法人化に先立って，1994 年 12 月に閣議決定された政府の「行政情報化推進基本計画」にもとづき，積極的に事務作業の効率化や電子情報を利用したペーパーレス化などに取り組んできている [2]。この情報化の一環として，2001 年度に学生情報システム『もみじ』 [3] が導入されたことにより，それまで紙面を用いて行われていた学生の履修登録から，教員の成績入力まで様々な事務手続きが，インターネットを介して行われるようになった [4]。

導入から８年を経過した『もみじ』のリニューアルが行われた翌年，2010 年５月に『もみじ』トップに表示されている「学生生活のサポート」というメニュー（図-1）の中に “パソコンＱ＆Ａ” の項目が新設された。ここに学内の情報基盤を利用するにあたっての FAQ(Frequently Asked Questions) を，学生向けに特化した形で掲載する機会を得た。

本学では１万５千人を超える学生が，履修登録や成績確認の際にこの『もみじ』へとアクセスを行う。メディアセンターのホームページを見たことも無く，様々なサービスが提供されていることを知らない学生に対しては，ここに窓口をつくりメディアセンターのホームページへ誘導を行うのが適切と考えた。

2.2 端末利用者アンケートの結果

中間集計ではあるが，2011 年度のメディアセンター端末利用者アンケートの集計結果（内部資料）を，図-2 に示す。端末室の利用者は主に研究室に所属していない，あるいは PC を所持していない学生である。

アンケート結果からは，学生はわからないことがあっても，自力で解決するか友達を頼ったりする程度で，わからないことがあった場合にメールで問い合わせを行う学生は全体の 4 %，その倍以上の 1 割を超える学生は，わからないことやトラブルがあっても放置してしまうという結果が明らかとなった。これは端末室に関することだけではなく，メディアセンターのサービス全般に対して同様の傾向があると考えられる。

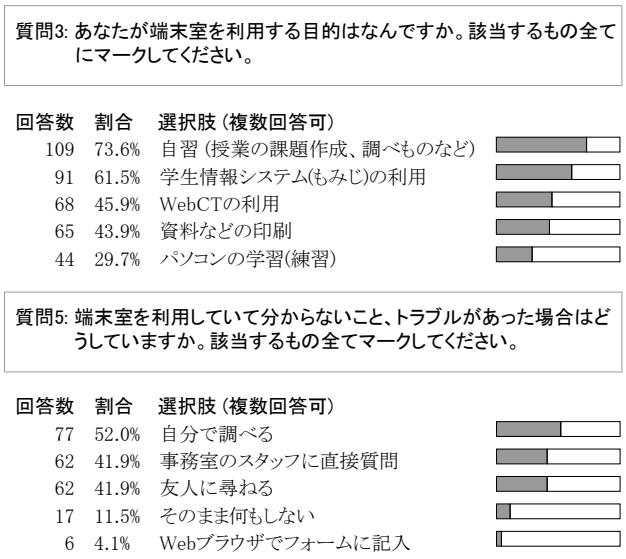


図- 2: 端末利用者アンケート結果

3 過去の問い合わせ

『もみじ』への “パソコンQ＆A” の掲載にあたり，学生が知りたいと思う情報を，作成するための拠り所としては，過去に学生から寄せられた問い合わせ内容以外には考えられない。

そのため，どのような内容を掲示するかという点と，掲載した内容をどの程度の頻度で更新を行うのが適切か，という 2 点について検討を行うため，2006 年度から 2009 年度までの過去 4 年間に，メディアセンターホームページの問い合わせフォームから寄せられた，問い合わせについて集計を行った。年度ごとの問い合わせ件数および質問者の種別を図-3 に示すとともに，集計結果を，問い合わせ数の把握，問い合わせ内容の整理，季節変化に分けて説明する。問い合わせの集計は現在も継続して行っているため，図-3 には 2010 年度の結果も併せて示す。

	問合せ件数	内訳		学生の割合
		職員	学生	
2006年度	686	499	187	27%
2007年度	697	491	206	30%
2008年度	773	560	213	28%
2009年度	703	437	266	38%
2010年度	1,045	709	336	32%

図- 3: フォームからの問い合わせ件数

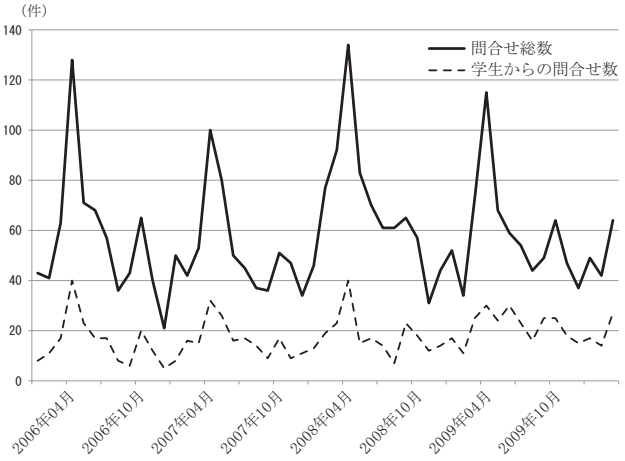


図- 4: 月別の問い合わせ数の推移

3.1 問い合わせ数の把握

メディアセンターへの問い合わせ件数の季節変化を. 図-4 に示す。最も顕著な傾向としては，年度の替わり目にあたる 3 月と 4 月に大きなピークを迎えることが挙げられる。後期の始まる 10 月に再び小さなピークがあり，年末年始に減少するという傾向がみられる。

問い合わせの中から，学生からの問い合わせを選別するにあたっては，職員は数字だけからなる職員番号，またはアルファベットからなるアカウント名を利用しているのに対し，学生は，アルファベット 1 文字＋6 桁の数字からなる学生番号をアカウント名としていることを利用し，自動で処理を行った。

過去 4 年間にメディアセンターに寄せられた問い合わせメールに占める，学生からの問い合わせの割合は，図-3 に示したように年平均でおよそ 3 割から 4 割程度であり，月平均にするとおよそ 20 件前後であった。また，図-4 に示すように，全体の問い合わせ総数とおおよそ比例関係にあり，問い合わせ総数と同様の季節変化

を持つことが明らかとなった。

3.2 問い合わせ内容

2006 年度から 2009 年度までの過去４年間に，学生から寄せられた問い合わせ内容を，前述の理由から手動で内容を確認しながら提供サービスごとに選別した所，

- メール全般に関する相談（17 %）
- アカウントに関する相談（12 %）
- VPN の接続トラブル（10 %）
- Web メールのトラブル（9 %）
- 学内の端末利用に関する相談（9 %）
- 研究室等でのネットワーク接続のトラブル（5 %）
- キャンパスライセンスソフトに関する相談（5 %）
- ウイルス対策ソフトに関する問い合わせ（5 %）
- 学外からのフレッツ接続に関する問い合わせ（4 %）
- 高度科学計算機システムの利用に関する相談（2 %）
- その他（11 %）
- 内容の不明なもの（11 %）

の 10 種類と，その他＋内容の不明なもの，におおよそ区別できることが判明した。括弧内に四年間の総問い合わせ数に占める割合を示す。

3.3 季節変化

10 種類の相談内容に関して，問い合わせ件数の季節による変化を確認した所，季節変動のある内容と，季節にあまり関係しない内容があることが判明した。

それらを整理すると，図-5 に示すように，

- メール全般に関する相談や，Web メールのトラブル，学内の端末利用に関する相談など，季節にあまり左右されない相談内容
- アカウントの引き継ぎや更新など，年度の替わり目に集中する相談内容
- VPN の接続方法など，長期休暇前後に増加する相談内容

など，季節によって寄せられる質問が異なるとともに，その変化に一定のパターンが存在することが明らかとなった。

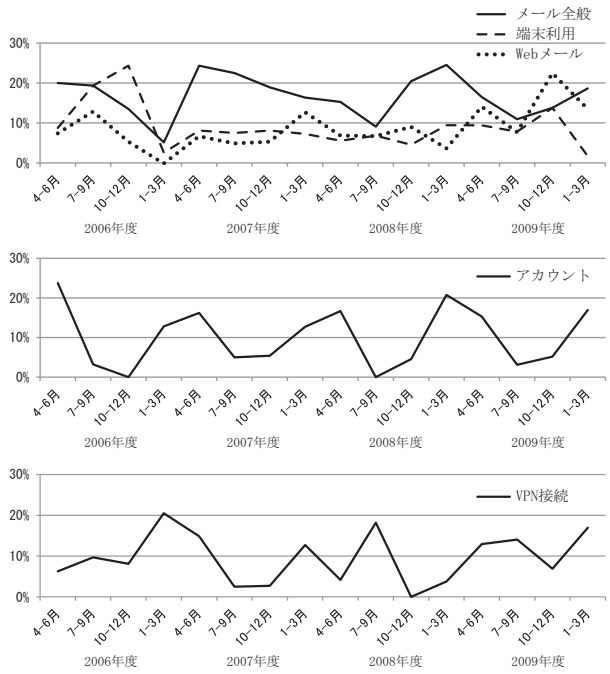


図- 5: 相談内容別の季節変動

4 掲載方法と内容の検討

第３章の解析結果より，学生からの問い合わせは，季節によって変動することが明らかとなった。当然『もみじ』に掲載される “Q＆A” の内容も，季節によって期待される内容が異なることは明白である。

これを実現するために，どのくらいの情報量で，どの頻度で更新を行うのが現実的かということと，過去の問い合わせをどのような方法で “パソコンQ＆A” へ反映するのが最適か，検討を行った結果を以下に示す。

4.1 掲載量の検討

“パソコンQ＆A” がメディアセンターの端末や，学生が通常所持しているノート PC で主に表示されることを考慮すると，縦方向が 600 ピクセルあまりの画面に入りきらない情報は，アクセシビリティが低下する。あまり多量の情報を掲載し過ぎると，こちらが伝えたいことが注目されにくくなるという現実がある。

集計対象とする過去の問い合わせ数が数十件程度であることもあり，メディアセンターの FAQ ページの反省を生かして，掲載するQ＆Aは５件程度とし，“過去の問い合わせ内容頻出トップ５” を “Q＆A” として掲載することとした。

図-6 に，2009 年に学生から寄せられた主な問い合わせ内容を，問い合わせの内容別に三ヶ月ごとに集計した結果を示す。括弧内の数字は問い合わせ件数である。

平成21年度1月-3月期
- ・卒業後, いつまでメールが利用可能ですか(5)
- ・学生から広大職員になる場合のアカウント継続の手続きが知りたい (3)
- ・進学・留年に伴うアカウント継続の手続きについて知りたい(2)
- ・メールスプールの整理の仕方がわからない(2)
- ・VPN接続しようとするとエラーが表示される(2)

平成21年度4月-6月期
- ・メールアドレス変更に関するトラブル(5)
- ・端末にログインするのに時間がかかる(or エラーが表示される)(4)
- ・ActiveMailのメールが全部消えてしまった(3)
- ・VPN接続しようとするとエラーが表示される(3)
- ・WebCTの使い方に関する質問(3)

平成21年度7月-9月期
- ・端末にログインするのに時間がかかる(or エラーが表示される)(6)
- ・VPN接続しようとするとエラーが表示される(5)
- ・ActiveMailのメールが全部消えてしまった(3)
- ・ウイルス対策ソフトがダウンロードできない(2)
- ・アカウントが有効になっていない(2)

平成21年度10月-12月期
- ・サーバエラーでメールが受信できない(or ActiveMailが開けない)(7)
- ・ActiveMailのメールが全部消えてしまった(4)
- ・端末でプロファイルが壊れている, とエラーが表示される(4)
- ・VPNはいつWindows 7に対応しますか(3)
- ・Hinetログイン時にセキュリティ証明書の警告が表示される(2)

図- 6: 過去の問い合わせ内容トップ５

4.2 更新の頻度

時節に応じた内容のものを “パソコンＱ＆Ａ” に掲載するためには，どの程度の期間をあけて更新を行うのが適切なのか。

更新を行うためにはその都度，学生からの問い合わせ内容を集計し，Ｑ＆Ａを作成するという作業が発生する。寄せられる問い合わせの母集団を少しでも多く稼ぐこと，また更新にかかる手間を考慮して，当初は，

- 年度初め
- 夏休み前
- 後期開始時
- 年末年始

と，およそ四半期ごとに年四回ほど更新を行うことが，それぞれの時期に必要な情報を提供できるベストなタイミングであると考えていた。だが，実際に作業を行った結果，過去の問い合わせ内容を集計してもあまり内容に変化がみられない季節のあること，この四半期の境目がちょうど多忙な時期にあたる，などの理由と，もっとも『もみじ』にアクセスが集中するのが，４月と 10 月の履修登録の期間であることなどもあわせて，現在では，３月末と９月末の年２回の内容更新にとどめている。

4.3 Ｑ＆Ａへの反映のさせ方

過去に寄せられた主な問い合わせ内容を参考にして，“頻出トップ５” を FAQ として選出するわけであるが，前述したように，問い合わせ内容は季節によって変化しているため，集計範囲に関しては適切に判断する必要がある。

例えば今年度の４月からの半年間に，“パソコンＱ＆Ａ” として掲載する内容を決める場合に，過去６ヶ月（前の年の 10 月から同じ年の３月まで）の問い合わせ内容から選出するのはあまり意味がない。なぜなら過去の集計結果より季節によって問い合わせられる内容が異なるからである。

よって４月より９月にかけて掲載される内容は，図-7 に示すように前年度（あるいはもっと前の年のデータも参考に）の４月から９月の問い合わせ内容から，作成されるのが望ましい。

5 『もみじ』への掲載

第３章から４章にわたって検討を行ってきた結果をもとに，2010 年の５月より３期に渡って実際に『もみじ』に掲載された “パソコンＱ＆Ａ” の掲載期間と掲載内容，各項目に対するアクセス数を示す。

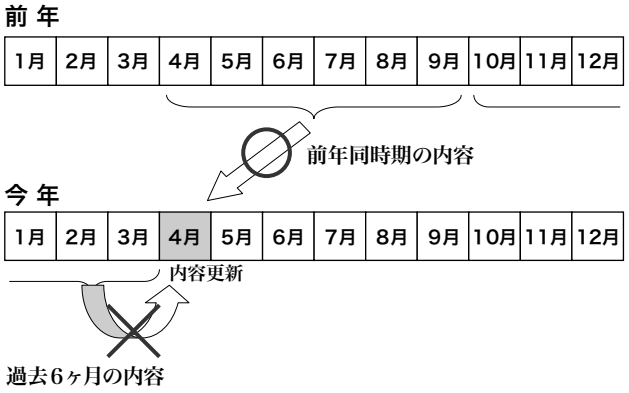


図- 7: 問い合わせ内容のＱ＆Ａへの反映のさせ方

5.1 掲載期間と掲載内容

“パソコンＱ＆Ａ” の掲載期間を，内容更新を区切りとして 2010 年度の前半を第１期，2010 年度の後半に掲載されたものを第２期，2011 年度の４月から６月までのものを第３期として区分した。図-8 に，それぞれの期間における掲載日数と掲載された内容を示す。

掲載項目としては，Ｑ＆Ａ自体は “頻出トップ５” から選出しているため，基本的には５項目であるが，実際に掲載される際には，今一番学生に知っておいて欲しい “お知らせ情報” や “お勧め情報” などが追加されるため，実際に『もみじ』に掲載された内容としては６項目から８項目となっている。

5.2 アクセス頻度

掲載された各項目に対するアクセス件数は，職員が内容確認のために参照を行ったものなども回数として含まれているが，全体としては学生の知りたい情報が何であるのかを反映した結果であると考えている。

それぞれの期間でアクセス回数にかなり差が出ているが，その傾向と考えられる要因について説明する。

第１期 Ｑ３が最も注目されている。実際，ホームディレクトリ容量のクォータ制限にかかった学生が多数存在し，端末にログインするのに非常に時間がかかったり，プロファイルが壊れているなどのエラーが表示されるなどのトラブルが生じていた。

第２期 Ｑ７の注目度が高くなっている。これは年末年始や春休みなどの長期休暇中で，大学から離れた際にも『もみじ』や図書館の文書検索など学内限定の情報にアクセスしたいと考える学生が増えたことが原因と考えられる。またＱ１は，2010 年度の後期より，利用者が明示的にサービスを開始するまでメールを利用できない仕様へと変更になったために追加された項目である。

第３期 Ｑ１へのアクセス件数が極めて高い。これはマイクロソフト社との包括ライセンス契約により，Microsoft Office が利用できることの周知を目的として掲載を行ったものである。予想を超えて多数のアクセスが発生したことは，ポスター等で学内に周知を行ったつもりの包括ライセンス契約も，依然として知らない学生が多くいたことが想定される。第２期と同様，Ｑ４およびＱ６も依然として注目度が高い。

5.3 メディアセンター FAQ との比較

メディアセンターの FAQ のページに掲載されている内容を，アクセス数の多かった順に５項目ほど図-9 に示す。こちらも 2010 年 11 月にリニューアルしたため，アクセス数として比較できるのは,『もみじ』の第３期にあたる部分のみとなっている。掲載量も掲載内容も異なるため単純な比較はできないが,「Microsoft 社のソフトウェアがもらえると聞いたのですが。」と「ウイルス対策ソフトがもらえると聞いたのですが。」の部分が,『もみじ』の「ウイルスバスターと Microsoft Office 提供のお知らせ」に内容的に該当する。メディアセンターの FAQ のページでは，同期間のアクセス数が２項目を合計しても 600 に満たない数であるのに対し,『もみじ』へ掲載内容に対しては倍以上に伸びていることがわかる。

『もみじ』が倍以上のアクセス数を稼ぐ背景として，サービスの存在すら知らなかった学生が「ん？なんだこれは」とアクセスする可能性が高いことを示していると考えられる。また，メディアセンターの FAQ ページは，実際にサービスの存在を知っていて，かつうまく利用することができなかった利用者のみがアクセスするページであることが挙げられる。

6 まとめ

利用者からの問い合わせ（ヘルプデスクメール）に着目し，キーワード群をフィルタとしてサービスごとに自動で問い合わせ件数を集計するシステムを運用した結果，特に学生からの問い合わせに関しては，内容からサービスを逆引きすることに限界があることが明らかとなった。

端末利用者へのアンケート結果から，わからないことがあった場合にメールで問い合わせを行う学生は全体の４％で，その倍以上の１割を超える学生はわからないことがあっても放置してしまうという結果がでている。

わからないまま放置している学生への救済策として，学生向けポータルサイト『もみじ』を利用して，“パソコンＱ＆Ａ” に季節に応じたメッセージを選択的に提供

掲載期間	掲載内容	アクセス回数	一日あたりのアクセス回数
第1期 2010.5.19 ～ 2010.9.30 （134日）	Q1．サーバエラーでメールが受信できない，またはActiveMailにログインするのに時間がかかりすぎる。	216	1.6
	Q2．Active!Mail のメールが全部消えてしまった。	250	1.9
	Q3．ICE 端末にログインするのに時間がかかる，またはプロファイルが壊れている，とエラーが表示される。	597	4.5
	Q4．メールアドレスを変更したい。	78	0.6
	Q5．自宅からネットワークを利用したい。	126	0.9
	Q6．無線LANアクセスポイントを使いたい。	171	1.3
	Q1～Q6のアクセス数の合計	1,438	10.7
	パソコンQ&Aトップページへのアクセス	3,264	24.4
第2期 2010.10.1 ～ 2011.4.11 （192日）	Q1．メールの利用開始手順が知りたい。	652	3.4
	Q2．Active!Mailからメール着信通知が携帯電話に届かなくなった。	339	1.8
	Q3．携帯電話に転送をするためにアドレスを入力したのに有効にならない。	221	1.2
	Q4．端末室の端末を利用するには学生証が必要になります。	144	0.8
	Q5．ICE端末からの印刷が有料化されました。	285	1.5
	Q6．端末利用時にICカードをかざすとエラーとなる。	145	0.8
	Q7．自宅からもみじなど学内限定の情報にアクセスしたい。	1,085	5.7
	Q8．無線LANアクセスポイントを使いたい。	495	2.6
	Q1～Q8のアクセス数の合計	3,366	17.5
	パソコンQ&Aトップページへのアクセス	5,682	29.6
第3期 2011.4.12 ～ 2011.6.12 （61日）	Q1．ウイルスバスターとMicrosoft Office提供のお知らせ	1,382	22.7
	Q2．情報セキュリティ・コンプライアンスって何？	171	2.8
	Q3．アカウント年度更新のフォローアップ試験って何？	306	5.0
	Q4．新入生の方がメールを発信するには手続きが必要です。	476	7.8
	Q5．端末室の端末を利用するには学生証が必要になります。	85	1.4
	Q6．自宅からもみじなど学内限定の情報にアクセスしたい。	433	7.1
	Q7．無線LANアクセスポイントを使いたい。	255	4.2
	Q1～Q7のアクセス数の合計	3,108	51.0
	パソコンQ&Aトップページへのアクセス	3,869	63.4

図- 8: 『もみじ』への掲載内容と項目別アクセス数

集計期間	FAQのアクセスランキングTop５	アクセス回数	一日あたりのアクセス回数
2011.4.12 〜 2011.6.12 (61日)	迷惑メール振分サービスで、ホワイトリストを設定する方法を知りたい。	283	4.6
	Excelのブック全体を両面印刷する場合。	280	4.6
	Microsoft社のソフトウェアがもらえると聞いたのですが。	248	4.1
	私のアカウントは何でしょうか？。	237	3.9
	ウイルス対策ソフトがもらえると聞いたのですが。	225	3.7

図- 9: メディアセンター FAQ への項目別アクセス数

して掲載を行った。その結果，メディアセンターの FAQ として掲載されている情報と比較して倍以上のアクセス数があり，学生に特化した情報提供の方式として非常に有効であることが検証できた。

その方法とは，年に２回，履修登録のために学生が必ず『もみじ』にアクセスする時期にあわせて，前年同時期に多く寄せられた問い合わせ内容や，新しく開始されたサービスを告知しておくことである。これにより，サービスの存在さえ知らなかった学生や，聞きに行くのはめんどくさいという学生に対し，少しでも有用な情報が目に触れる機会や参照先を提供することができたと考える。

学生専用のページに情報を掲載するという今回のような機会があるまで，メディアセンターに寄せられる問い合わせを十把一絡げにして取り扱ってきた。しかし，今回集計に基づいて広報を行うという社会実験を行ったことで，職員と学生では情報の周知のされ方や，サービスの使い方がわからなかった時の対応がまるで異なることに気がついた。これを機に，メディアセンターとしては一方的に情報を発信して終わり，ではなく，誰に聞いて欲しいのかを明確にした上で，きちんと相手に届くような広報の仕組みを検討すべきである。

謝辞

研究の遂行にあたり，学生情報システム『もみじ』を通して学生向けに情報を発信する貴重な機会を与えて頂くとともに，アクセスログをご提供頂いた社会連携・広報情報室情報化推進グループの皆様に深く感謝する。

引用文献

[1] 吉冨健一, 岩沢和男, 宮原俊行，西村浩二. “ヘルプデスク解析のサービスの評価への応用”，学術情報処理研究，Vol.13，pp.49-56，2009.

[2] 広島大学広報グループ. “広島大学：これまでの事務情報化への取組”，http://www.hiroshima-u.ac.jp/top/intro/jyoho-ka/bur/p_4a0aba.html.

[3] 広島大学教育室. https://momiji.hiroshima-u.ac.jp/momiji-top/index.shtml.

[4] 北村 充. “学生情報システム「もみじ」とは”, 広大フォーラム，no.375，2003.

学内監視カメラシステムの運用と今後の展開

Using of Surveillance Camera System and Next Development

古谷雅理†，櫻田武嗣‡，萩原洋一‡
清水さや子†，吉田次郎†
Tadasuke FURUYA†, Takeshi SAKURADA‡, Yoichi HAGIWARA‡
Sayako SHIMIZU† and Jiro YOSHIDA†
tfuruya@kaiyodai.ac.jp, take-s@cc.tuat.ac.jp, hagi@cc.tuat.ac.jp
smz@kaiyodai.ac.jp, jiroy@kaiyodai.ac.jp

†東京海洋大学情報処理センター
‡東京農工大学総合情報メディアセンター

†Information Center, Tokyo University of Marin Science and Technology
‡Information Media Center, Tokyo University of Agriculture and Technology

概要

近年，監視カメラは多くの場所に設置され，防犯などに利用されている．監視カメラは少人数で広範囲を監視できるという利点があるが，従来は専用機器を必要とする高価なシステムであった．そこで我々は 2001 年頃から IP カメラを利用した監視カメラシステムの開発をしてきた．このシステムは民生用ネットワークカメラ(HTTP,FTP 対応の IP カメラ)を利用しており，蓄積画像検索機能や携帯端末への通報機能を有している．さらに狭帯域のサテライトキャンパス監視に向けた拡張システムを開発している．このように学内の監視カメラの増設，システムの改修を続けてきたが，ネットワーク管理部門である総合情報メディアセンターの役割はシステムの構築と運用であり，学内監視は別部門の役割である．今後は他部門での利用を考えた運用，改修をおこなう必要がある．本稿ではこれまで構築してきた監視カメラシステムの概要と他部門運用に向けた今後の展開を述べる．

キーワード

監視カメラ，IP カメラ

1. はじめに

近年，施設の状況記録，防犯に監視カメラシステムが多く利用されている．監視カメラシステムの導入は，小人数で広範囲を監視，運用することが可能なため非常に有用である．

専用機器を利用したシステムの代表的なものに CCTV システム[1][2]がある．複数カメラの映像は，画像分割装置

等を利用しモニタに出力する，あるいは長時間録画可能なタイムラプスビデオに記録する．このシステムではカメラ，制御装置間をほぼ一対一で接続する必要がある．また，制御装置の映像入力数にも制限があるため広範囲を監視するには，多くの設備費用がかかる．さらに，記録装置としてビデオテープレコーダを利用する場合，テープの交換作業が必要であり，一時的に録画を止めなければならないだけでなく，長時間の磁気テープへの保存は画像が荒く鮮明さに欠ける．ハードディスクレコーダを利用することでこれらの問題は解消できるが，非常に高価である．運用面でも，異常に即時対応するためには多くのモニタを同時に監視するための人的コストが必要となる．また，カメラの増設，設置場所の変更が容易に行えない．これらのような問題から専用機器を利用した監視カメラシステムは容易に導入できないか，導入しても有効活用されないことが多い．

ネットワークに接続可能な IP カメラ[3][4]の登場により，これらを利用したいくつかの監視システムが利用されている．これらのシステムはインターネットや携帯電話を利用し，ネットワークカメラのライブ画像を確認するだけのものがほとんどである．松下電器の KH-HNP11[5]のようにネットワークカメラの画像を記録し，後に動画像を作成できるシステムも提供されているが，他メーカの IP カメラの接続は対応していない．また，異常時にメールで管理者に知らせるシステムはあるが，異常を知らせるテキスト，異常検知時の静止画像メールでは，状況を判断することは難しい．

我々はこれらの問題を解決するために 2001 年頃から IP カメラを利用した監視カメラシステムの開発をしてきた．さらに狭帯域のサテライトキャンパス監視に向けた拡張システムを開発している．このように学内の監視カメラの増設，システムの改修を続けてきたが，ネットワーク管理部門である総合情報メディアセンターの役割はシステムの構築と運用であり，学内監視は別部門の役割である．今後は他部門での利用を考えた運用，改修をおこなう必要がある．本稿ではこれまで構築してきた監視カメラシステムの概要と他部門運用に向けた今後の展開を述べる．

2. 監視カメラシステム構築の経緯

従来の監視カメラシステムでは，常時人が監視して異常を発見するか，センサーを利用して異常を感知し，異常発生時刻，発生場所を通知する．これらは，メール，静止画像，音声を利用した異常通知が主であり，異常時の状況を把握することが難しい．また，専用機器を利用するため多くの設備費用，運用費用が必要であり容易に導入できないか，導入しても有効活用されないことが多い．本システム開発当初の 2002 年頃は，ネットワークに接続可能な IP カメラの登場により，これらを利用したいくつかの監視システムが利用されていた．IP カメラは高解像度，低価格化した製品が提供されており，設置・設定が容易に行えるといった利点がある．しかし，これらを利用したシステムの多くは，設置できるカメラの台数に制限があるため，広範囲を監視できない．また，異常時にメールで管理者に知らせるシステムはあるが，異常時の状況を的確に伝えることができないといった問題があった．そこで，これらの問題を解決するために IP カメラを利用した新しい監視カメラシステムを構築した．30 台以上のカメラで撮影された画像を 1 セットの PC サーバに蓄積し管理する．これらは，ネットワークの整備された学校等において大規模監視カメラシステムを従来の方式よりも低コストで構築･運用できるシステムであり，そのシステムを実際に構築し運用[6][7]した事例について既に紹介している．

監視効果やコスト面で一定の効果を挙げているが，1 つの拠点でのみ安定して利用でき複数拠点への対応が難しい点，携帯端末で監視画像を簡便に検索したいという点で課題があった．

そこで，われわれは，運用中のシステムにこれらの課題，要望を反映させた，拡張型ネットワークカメラシステムの開発・構築[8]を示した．これらの方式を備えた拡張型ネットワークカメラシステムについて評価を行い，遠隔地に設置できるカメラの台数とネットワーク帯域の関係，利便性の主観評価によりシステムの有用性を示した．

下記に，これまでの監視カメラシステム構築状況を示す．

2002/06　IP カメラのテスト
2002/10　プロトタイプ試作(1 Server+カメラ 8 台)
2002/12　画像検索システム構築開始
2003/02　画像検索システム提供
2003/06　IP カメラの性能テスト(赤外光カメラ導入)
2003/09　カメラ 36 台に増設
2003/11　新サーバ導入(Apple XServe)
2003/12　自動動画像生成システム開始
2004/01　侵入通知システム提供開始
2004/09　IP カメラの性能テスト
2004/11　PDA による過去画像検索実験
2005/04　無線 LAN 携帯電話による検索実験
2006/08　カメラ 59 台に増設
2006/09　IP カメラの性能テスト
2006/10　FM 唐沢山試験撮影

2007/05　FM 唐沢山定点観測、IP カメラ 3 式
2009/03　新サーバ導入(Apple MacPro)
2009/06　カメラ 98 台に増設，サーバ機 2 機増設
2009/07　画面転送実験開始
2010/04　集約画像による画像検索実験開始

3. システム概要

学内監視カメラシステムは，2 地区の校内を監視するキャンパス監視と遠隔地にあるサテライト施設を監視するサテライト監視に分けられる．それぞれについて次節以降で述べる．

3.1. キャンパス監視

キャンパス監視は，約 100 台の IP カメラの撮影画像を 4 台のサーバに蓄積する．ファイル自動管理機能，動画像自動生成機能，画像検索機能，侵入通知機能の 4 つの機能を提供する．動画像作成機能以外は機能を分散可能である．検索端末では，画像の検索・閲覧のための Web ブラウザ，動画再生環境があればよく，特別なソフトウェアは必要としない．

3.1.1. 機器構成

図 1 に本システムのシステム構成図を示す．本システムは，可視光用 IP カメラ 91 台，赤外光用 IP カメラ 7 台の計 98 台のカメラ，画像サーバ 4 セット，ネットワークから構成されている．

IP カメラは，画像サーバに対して 1 秒間隔で撮影された画像を転送できる機能を有し，任意の文字列と撮影時刻をファイル名とすることができる必要がある．撮影画像は，VGA サイズ以上の Jpeg ファイルとする．また一部のカメラには，後述する異常検知機能を提供するため，外部センサーの I/O 端子とメール送信機能を有する必要がある．本システムでは，表 1 の IP カメラを利用している．

画像サーバは IP カメラから配信される撮影画像を安定して保存でき，自動処理，遠隔地からリモート接続出来る必要がある．また，動画像が自動作成でき，動画像の配信機能があることが望ましい．主な動画像配信ソフトとしては，リアルネットワークス社の Helix Server[9]があるが，動画像が容易に自動作成でき，携帯電話で再生できる形式の動画像が容易に作成できる必要がある．本システムでは，幅広い配信手段に対応している MPEG-4[10]ファイルを作成でき，動画作成用に QuickTime

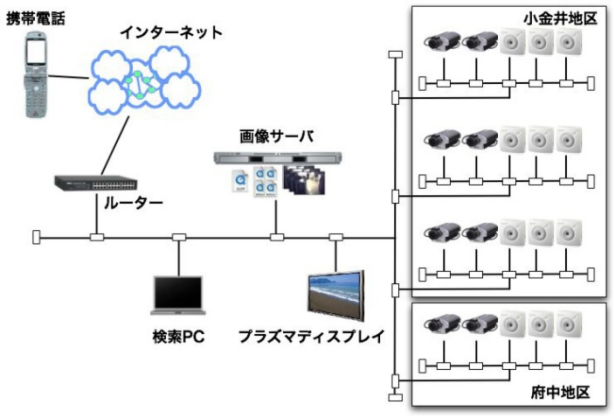


図 1　システム構成

表 1　IP カメラ構成

	メーカ	製品名	台数
1	Panasonic	KX-HCM1	20
2	Panasonic	KX-HCM2	6
3	Panasonic	BB-HCM310	1
4	Panasonic	BB-HCM310	18
5	Panasonic	BB-HCM527	6
6	Panasonic	BB-HCM527	27
7	Panasonic	BB-HCM581	13
8	AXIS	AXIS 2420	7
合計			98

表 2　サーバ機構成

	メーカ	製品名	用途
1	Apple	XserveG4 ・MacOS XServer10.3 ・PowerPC G4 2GHz Dual ・Memory 4096MB ・Hardware RAID5 3.2TB	画像蓄積
2	Apple	XserveG5 ・MacOS XServer10.3 ・PowerPC G5 2GHz Dual ・Memory 4096MB ・Hardware RAID5 3.2TB	画像蓄積 動画配信
3	Apple	MacPro ・MacOS X10.5 ・Quad-core Intel Xeon 2.8GHz Dual ・Memory 4096MB ・Hardware RAID1 1.0TB	画像蓄積
4	Apple	MacPro ・MacOS X10.5 ・Quad-core Intel Xeon 2.8GHz Dual ・Memory 4096MB ・Hardware RAID1 1.0TB	画像蓄積

エンコーダと動画像配信用に QuickTime Streaming Server[11]を標準で装備している Apple 社製 XserveG5 を利用している．サーバ機構成を表 2 に示す．

IP カメラは, 建物内各階に設置された 10/100/1000 Base スイッチングハブに接続する．各階のハブはギガビットイーサネットスイッチで束ね，画像サーバに接続する．

3.1.2. システム機能

撮影画像を蓄積するだけでなく，監視カメラシステムとして重要な画像の検索，通知機能を提供する．

撮影された画像からタイムコードを付加した動画像を自動生成する．これらは，ネットワークに繋がった PC から容易に確認することが可能である．さらに，異常発生後に異常発生前後の動画像を生成し，携帯電話で確認できるシステムを提供する．これは異常感知直後に携帯電話用動画像を作成することが可能である．携帯電話から監視カメラのライブ画像を閲覧できるシステムは既にあるが，1 台の PC サーバで画像の蓄積，動画像生成，携帯電話等への動画像配信まで行うシステムは他にはない．また，作成する異常発生時の携帯電話用動画像は，1 台のカメラで撮影された画像だけでなく，複数のカメラで撮影された画像から 1 つの動画像を生成することも可能である．

また、巡回中に過去に撮影された（数時間前の）画像を見られるように，簡単に検索指定が可能であり，学外からでもキャンパス内でも同様の携帯端末から利用できるようにした．携帯端末での閲覧は，無線 LAN 対応携帯端末での閲覧を考慮し，画像を携帯端末で閲覧できる形式の動画にエンコードする機能，QR コードとの組み合わせによる URL 入力の省略および閲覧者の認証を実現した．

3.2. サテライト監視

サテライトの撮影画像を直接キャンパスに転送せず，サテライトに蓄積する．この方式では，撮影画像の検索時に，検索結果画像の送信のためのトラヒックが生じるが，撮影画像を常時全て転送する量と比較すると少ないため，ネットワーク帯域を圧迫しないと考えられる．撮影画像を常に画像サーバに送信した場合はカメラ 1 台につき常に約 320kbps の帯域が必要となるが，本方式では指定時間分の画像を画像サーバに送信すれば良いため，検索時以外の帯域消費をゼロにすることが可能である．

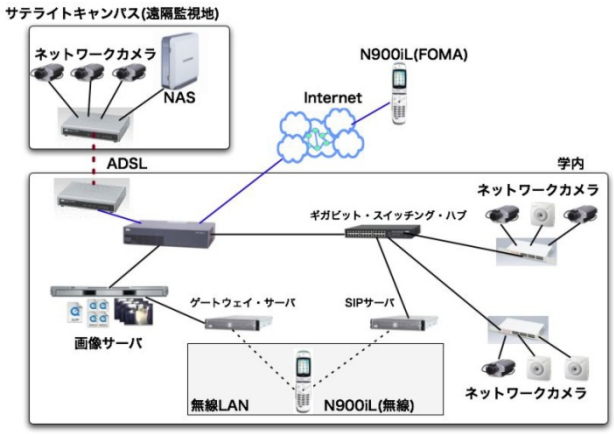


図 2　サテライト監視システム構成

表 3　サテライト監視用機器構成

	種別	メーカ	製品名	台数
1	IP カメラ	Panasonic	BB-HCM310	3
2	NAS	Buffalo	HD-HG120LAN	1

3.2.1. 機器構成

遠隔監視地システムは, ネットワークカメラ, ルータ, ネットワークストレージアプライアンス(NAS)，小型 UPS から構成されている．ルータ，NAS，重要な場所を撮影する最低限のネットワークカメラは UPS に接続する．ネットワークカメラは前述の機能要件を満たすものを利用し，NAS1 台あたり 3 台のネットワークカメラを接続することを想定している．

NAS は，リモートでストレージ内のディレクトリ操作が可能であり，FTP サーバ機能を有する機種でなければならない．本システムでは，遠隔監視地の撮影画像を 10 日間保存することにしたので, NAS はそれに足る容量のものを選ぶ必要がある．3 台のネットワークカメラで VGA 画像を 1 秒間隔で保存する場合，1 日で消費する容量は約 10GB なので, 一般的に普及している NAS を利用した．

3.2.2. システム機能

サテライトへの対応は，キャンパスとサテライトの環境の違いを考慮し，NAS を利用した構成とした．ネットワーク帯域を考慮し，ネットワークの利用者が少ない時間に蓄積画像を一括送信する機能，検索時に検索対象期間を検索条件としキャンパスへの転送画像を減らす機能，検索画像をキャンパス内サーバでキャッシュすることによる帯域節約機能，複数画像を高速で切り替えることによる検索画像の閲覧利便性を実現した．

4. 運用

通路等の夜間も監視すべき場所には，赤外線ライトをつけた赤外光用 IP カメラを，それ以外の場所には可視光用の IP カメラを設置している．設置場所により 24 時間もしくは夜間 12 時間画像を撮影し，毎秒 1 枚の間隔で画像サーバに蓄積している．必要のない時間帯の画像を転送しないことでサーバへ蓄積する画像データ量を削減する．撮影された画像，1 時間毎の動画像は 1 週間画像サーバに蓄積する．それ以前の画像データは自動的に消去する．

通常，蓄積画像は，登録された IP アドレスの PC から画像サーバに接続し画像を閲覧するだけとし，パスワードによる保護と合わせて，セキュリティーを確保した．

異常が発生した場合，携帯電話へ作成された動画像の URL が書かれたメールが自動的に送信され，管理者は携帯電話から画像サーバに接続し動画像を確認する．全て自動化されているのでメンテナンスは通常必要ない．

キャンパス内の画像サーバは，NAS に対して NFS クライアントもしくは FTP クライアントとして接続し，管理作業を行う．まず画像サーバは，6 時間毎に遠隔地の NAS に対して ping による平均応答時間を計測する．6,20 時の平均応答時間が過去 3 日間の平均値の 1.5 倍以下の場合に本部地区の画像サーバはこの時間に NAS にアクセスし，蓄積画像を日付毎に分類し，10 日間保存した撮影画像を削除する．平均値の1.5倍よりも大きい場合は，次の 6 時間後に再度平均値と応答時間の差分を計算し，管理作業を行うか否かを判断する．これらは全て自動処理である．ネットワーク障害などで NAS にアクセスできなかった場合，画像サーバは管理者に作業未完了のメールを送信し，次の指定時間に管理作業を行う．全て自動化されているのでメンテナンスは通常必要ない．

機器の故障は，IP カメラとサーバ機によるものである．IP カメラは，パン・チルトカメラのギヤ破損による修理を 10 回程度，応答不能状態が半年に 1 度程度で起きていた．初期に導入した IP カメラにこのような症状が多く現在は安定稼動している．サーバ機の故障状況を表 4 に示す．主にハードディスクの故障であり交換後は安定して稼動している．セキュリティー・アップデート以外は特にメンテナンスを必要としない．

5. 今後の展開

学内監視の専門部門がこれまで提案してきたシステムを使用する場合，ハードウェアの運用と監視業務を切り分ける必要がある．

表 4　サーバ機器故障

	故障月	故障部品
1	2005/4	XRAID 用 Disk（交換）
2	2005/10	XServe 用 HDD（交換）
3	2006/8	XRAID 用 Disk（交換）
4	2011/3	MacPro 用 Disk（交換）

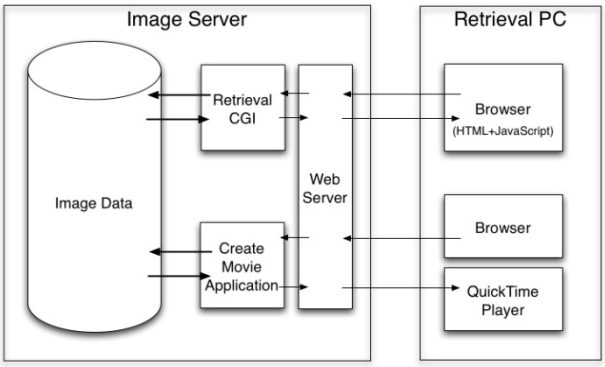


図 3　サテライトシステム画像検索

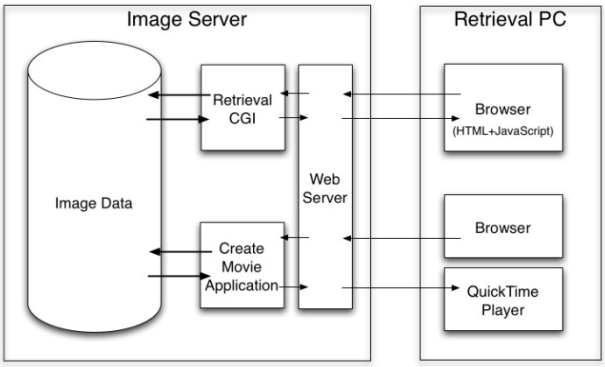


図 4　キャンパス監視システム画像検索

これまでは，システムの構築，特に撮影画像の蓄積が主目的であったが，これからは検索，ライブ表示機能の充実をはかる必要がある

5.1. 低速回線地域の監視画像確認

サテライト施設において，事件事故が起きた時だけでなく，定期的に監視場所の映像を閲覧し，変化を確認したいとの要望があった．これまでのサテライト監視方式では，1 日の変化を確認するためには，すべての映像を転送することが必要となるので膨大な時間を要する．そこで，映像を全て転送することなく長時間の変化を確認する手法を検討する必要がある．

5.1.1. サテライト監視システムの画像検索

高速回線サービスが提供されていないサテライトでの監視システム図3では，管理コストを削減するためNASを利用した．ただし，撮影画像検索方法は従来の検索システム図4とは異なる．遠隔地の撮影画像検索には従来システム同様ウェブブラウザを用いるが動画像生成，配信はおこなわない．利用者は，本部地区内の検索PCのウェブブラウザから本部地区の画像サーバに設置した検索CGIに接続し，ユーザIDとパスワードによる認証成功後に検索したい時間帯とカメラを指定する．検索CGIは指定されたカメラに対応する遠隔地のNASにアクセスし，指定された時間帯のうち画像サーバに蓄積されていない撮影画像を取得する．この時，連続表示できる撮影画像の枚数を制限することによりネットワークへの負荷を軽減するとともに，NASから画像サーバへ転送された撮影画像は本部地区内の画像サーバに一定期間キャッシュする仕組みを採り，短時間に同じ画像を再度検索する場合のネットワーク負荷も軽減している．検索対象の期間が30秒の場合，遠隔地から取得する必要のある画像の合計サイズは約1200KBである．プロトコルオーバヘッドを無視した場合，9.6Mbpsの帯域節約効果がある．撮影画像を全て取得すると，検索CGIは保存先ディレクトリ，画像連続表示用JavaScriptを含んだHTMLが自動生成されるのでウェブブラウザで画像を確認する．この手法ではあらかじめ検索条件がわかっている場合は有効だが，たとえば1日分の撮影画像を確認する場合は，全ての撮影画像をキャンパスに転送する必要がある．

全画像を転送するには，利用する遠隔拠点の回線を評価し，適切な転送手法を検討する必要がある．本システムの遠隔拠点と本部地区とはADSL回線で接続されている．この回線の帯域測定結果は，平均723kbpsであった．次に，遠隔拠点の3台のカメラ画像を直接本部地区の画像サーバへ転送した時の遠隔拠点と本部地区との回線の遅延時間のばらつきを測定した．測定には，遠隔拠点内のPCから本部地区サーバに100ms間隔で1000バイトのデータを500回送信した．これら測定結果から1〜2台のカメラ画像を直接本部の画像サーバに転送できるが1秒間隔で転送できないことがわかった．さらに，この回線は監視カメラ専用ではなく，業務にも利用しているので業務時間帯に利用できる帯域は狭い．

以上のことから，遠隔地内で数台のカメラで撮影した長時間分の確認するためには，撮影画像もしくは撮影情報を圧縮し転送，表示する手法が必要である．

5.1.2. 検索画像の自動生成

重要な画像を自動検出，表示することで，短時間で撮影場所の状況を把握することができる．これに関連した研究として，背景差分により侵入者などの動物体の検出する手法[12]，背景差分をより頑健にし，動物体の検出精度に向上を目的にした手法[13]，得られた人物像の振る舞いパターンの学習を用いることによる認識手法[14]が提案されている．これら手法は，動物体の自動認識を目指しており，さまざまな撮影環境に対応することは困難であり，検出漏れや誤認識を完全に避けることが難しい．

そこで，我々は動物体の検出ではなく長時間分の撮影画像の情報圧縮，表示手法として，階層的集約画像生成手法[15]を提案した．背景が動かない場所に設置されている視野固定式のカメラを対象として，撮影された画像を一定時間ごとに区切り，それぞれの時間範囲について1枚の静止画像に情報を集約する．この一定時間を集約時間，作成する静止画像を集約画像と呼ぶ．この集約画像を確認することで撮影場所の一定時間の状況を短時間で把握できる．この集約画像の生成には，撮影環境ごとにパラメータの設定を必要としない．現在，この集約画像を利用した新しい検索サーバを構築している．集約画像の作成を図5，集約画像の例を図6に示す．集約時間が

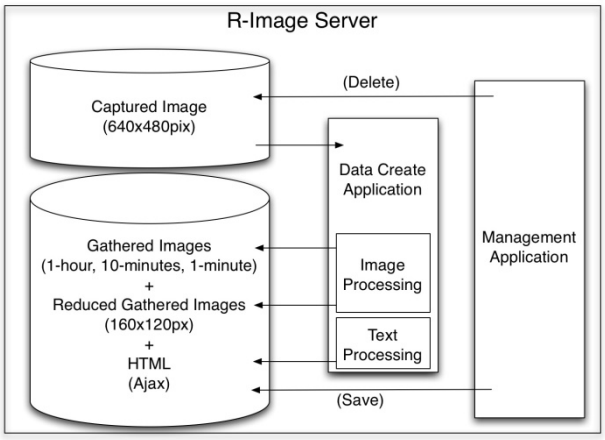


図5　集約画像の作成

図6　集約画像（10分間の撮影画像から生成）

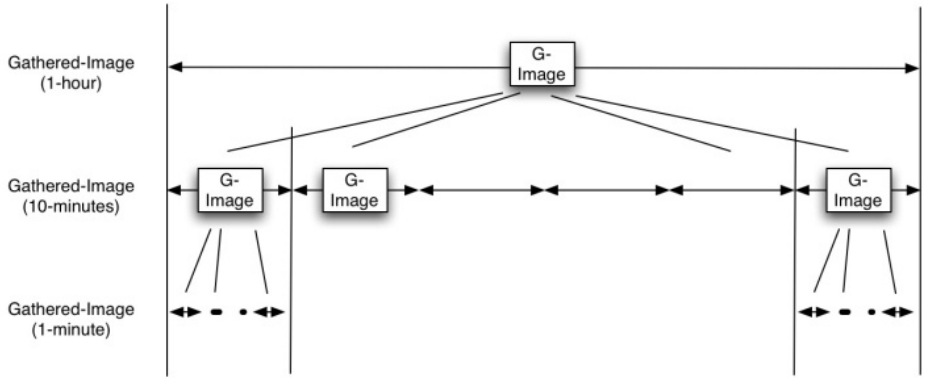


図 7　集約画像の階層表示

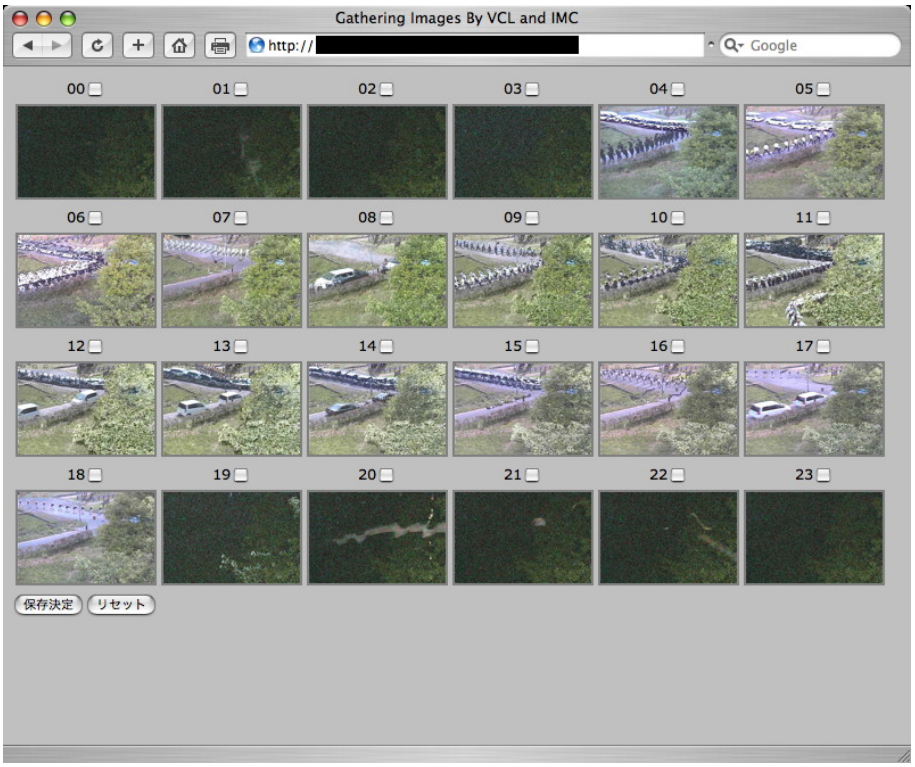


図 8　24 時間分の集約画像

長いと集約画像に情報が埋め込まれすぎて詳細な状況を把握できない．そこで，より詳細な情報を得るために，集約時間の異なる集約画像を生成し，これらを階層的に管理する（図 7）．集約時間が長い上位階層の集約画像において，埋め込まれた動物体情報が密な場合は，下位の階層の集約画像を確認することで詳細を確認する．

1 時間単位の集約画像 24 枚（図 8），10 分単位の集約画像 144 枚，1 分単位の集約画像 1440 枚を生成する．1 分単位の各集約画像は上位の 10 分単位の集約画像，10 分単位の各集約画像は上位の 1 時間単位の集約画像の下に階層的に管理する．1 日の撮影状況を確認する場合，最初に 1 時間単位の集約画像を確認し，詳細な情報を確認する必要がある場合は，下位の階層の 10 分単位，1 分単位の集約画像を確認する．上位階層の集約画像に変化

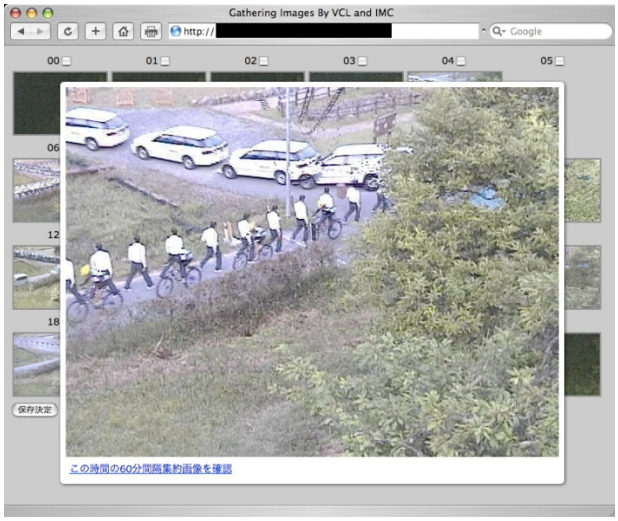


図 8　集約画像の選択

がないときは，下位階層の集約画像を観察する必要はない. したがって, わずかな枚数の画像を確認することで, 長時間の状況を効率的に把握することができる.

現在は, 24 時間に 1 度しか生成していないが今後短時間で生成できるように改修をおこなう予定である.

5.2. 監視カメラ画像の配信

IP カメラには，撮影画像転送機能以外にライブ映像表示機能がある．Web ブラウザを利用し，現在の様子を確認することが出来るが，アクセス数に限りがある．映像を数カ所に配信しながら，画像サーバへのデータ転送は IP カメラに負荷がかかり過ぎ，蓄積画像が欠損する，もしくはライブ表示が出来なくなる場合がある．そこで映像配信ユニットを利用した映像配信をおこなう．本手法は, 1 台の PC にライブ画像を表示し, その画面を転送する．これにより個々のカメラへの負荷を軽減する．本システムでは，Apple 社製 Mac mini に Contec 社製の FlexNetViewer を接続し利用している．Mac mini 内で IP カメラのライブ映像一覧 HTML を表示し, その画面を転送する．転送先は，機器動作確認のため総合情報メディアセンター（図 9），映像確認のため事務室と守衛所（図 10)）である．IP 一覧画面から個別の IP カメラの拡大映像を確認することは出来ない. 図 11 のように 1 本のポールに複数台カメラが設置されている場所がある．このような場合に容易に個別のライブ画面への切り替えられる手法を検討する必要がある.

図 9　IP カメラ一覧表示（センター）

図 10　IP カメラ一覧表示（守衛所）

6. おわりに

本稿では，ネットワークの整備された学校等において大規模監視カメラシステムを従来の方式よりも低コストで構築・運用できるシステムの構築事例とその運用，今後の展開について述べた．本システムは実際に既存のネットワーク回線, 汎用の PC, 約 100 台のネットワークに接続可能なカメラを利用して構築し, 現在運用している. 常に過去約 1 週間分の画像が蓄積された状態で運用しており，これらの画像はシステムを止めることなく，Web ブラウザを利用し検索が可能である．さらに異常検知時には，異常場所が映っているカメラの画像から自動的に異常の起きた前後の動画像を作成し，携帯電話に通知するシステムを開発したことにより，第 3 世代携帯電話で異常が起きた前後の動画像を確認することを可能とした. 電話が通じるところならば管理者がどこにいてもよいことになり，運用面でも管理者の負担を大幅に軽減するものとなった.

今後の展開として，ネットワークに低負荷で長時間分

図 11　学内監視カメラ

の撮影画像の状況確認手法を提案した．本手法はネットワーク回線の細い環境だけでなく全ての環境で利用可能であり，長時間の状況把握に時間が掛かった従来の検索方法と比べ，利便性が格段に向上した．朝には，前日の1日分の撮影状況を確認することが可能である．

現在，約100台のIPカメラを利用している．これらカメラで撮影された画像は膨大な枚数となるため，効率よいデータ管理，検索機能が重要となる．本システムは現在運用中であり，監視部門の意見を採り入れながら日々改良を進め，より使いやすいシステムにすべく開発を行う予定である．

参考文献

[1] ビクターCCTV システム URL: http://www.jvc-victor.co.jp/pro/cctv/

[2] 三菱電機 CCTV システム URL: http://www.mitsubishielectric.co.jp/cctv/

[3] 松下電器産業ネットワークカメラ製品 URL: http://panasonic.biz/products/secmoni/index.html

[4] アクシス(Web カメラ) URL: http://www.axiscom.co.jp/

[5] 松下電気産業ＢＢ-ＨＮＰ11URL: http://panasonic.biz/netsys/netwkcam/lineup/hnp11.html

[6] 古谷雅理, 櫻田武嗣, 瀬川大勝, 萩原洋一:NCS(ネットワークカメラシステム)による監視システムの構築と運用, 情報処理学会論文誌, Vol.46, No.4, pp.965-973, 2005.

[7] 古谷雅理,櫻田武嗣,萩原洋一:PDA を利用した監視画像検索システムの構築, 情報処理学会 DSM 技報, 2005-DSM-36, pp.55-59. 2005.

[8] 萩原洋一，古谷雅理，大島浩太，櫻田武嗣，瀬川大勝，萩原洋一，並木美太郎，中森眞理雄:ネットワークカメラを用いた監視システムの拡張, 情報処理学会論文誌, Vol.48, No.4, pp.1665-1673, 2006.

[9] Helix Server URL: http://www.jp.realnetworks.com/products/helix/media/server_proxy.html

[10] MPEG-4 規格 URL: http://www.m4if.org/

[11] アップルコンピュータ QuickTime Streaming Server URL:http://www.apple.com/jp/quicktime/products/qtss/index.html

[12] C.Jacinto and M.Jorge.:Performance Evaluation of Object Detection Algorithms for Video Surveillance, IEEE Transaction on Multimedia, Vol.8, No.4, pp.761-774, 2006.

[13] 波部 斉, 大矢 崇, 松山 隆司:動的環境における頑健な背景差分の実現法, 情報処理学会コンピュータビジョンとイメージメディア研究会画像の認識・理解シンポジウムMIRU'98, pp.467-472, 1998.

[14] F.Gian, M.Lucio, and R.Carlo.:Automatic Detection and Indexing of Video-Event Shots for Surveillance Application, IEEE Transction on Multimedia, Vol.4, No.4, pp.459-471, 2002.

[15] 阿久津渡,古谷雅理,宮村(中村)浩子,斎藤隆文:監視カメラ画像閲覧のための階層的画像集約手法, 情報処理学会グラフィクスと CAD 研究報, CG-124, pp.43-48, 2006.

仮想化技術を用いたサーバ集約と演習端末室の構築

Consolidation of Servers and Development of Educational Terminal System by Virtualization Technique

瀬川大勝，辻澤隆彦，辰己丈夫

Hirokatsu SEGAWA, Takahiko TSUJISAWA, Takeo TATSUMI

hiroka@cc.tuat.ac.jp, t-taka@cc.tuat.ac.jp, tttt@cc.tuat.ac.jp

東京農工大学総合情報メディアセンター
Information Media Center, Tokyo University of Agriculture and Technology

概要

東京農工大学における教育研究用情報システムは 5 年間のリース期間が 2011 年 1 月 31 日を以って終了することから，新システムへの移行を進めてきた．教育研究用情報システムは演習端末室システム，インターネット情報システム，統合管理運用システム，サーバーファームシステム，図書館システムなど多岐にわたるサブシステムから構成されている．新システムでは仮想化システムを積極的に導入し，スペースの削減と消費電力の削減を目標に構築を進めてきた．本論文では，2011 年 4 月から本格運用を開始した教育研究用情報システムの全体構成と演習端末室システムについて詳細に述べるとともに，Cisco Systems の IA サーバ，EMC ストレージ，VMware の組み合わせによるプライベートクラウドの構築を通して明らかとなった有効性及び今後の課題について報告するものである．

キーワード

仮想化，VDI，サーバ集約，省エネルギー

1 はじめに

東京農工大学における教育研究用情報システムは 5 年間のリース期間が 2011 年 1 月 31 日を以って終了することから，新システムへの移行を進めてきた．教育研究用情報システムは教職員・学生約 11000 名が利用するシステムであり，演習端末室システム，インターネット情報システム，統合管理運用システム，サーバーファームシステム，図書館システムなど多岐にわたるサブシステムから構成されている．従来システムでは，アプリケーションやサービス毎の管理が必要であったが，こうした管理上の負荷を軽減するため，新システムでは仮想化システムを積極的に導入した．具体的には，演習端末室システムやインターネット情報システム，図書館システム，統合管理運用システムなどの大学固有のシステムを仮想化技術によるプライベートクラウドシステムとして実現し，電子メールシステムをパブリッククラウドで実現する手法を採用した．プライベートクラウドシステムは，Cisco Systems の IA サーバ，EMC ストレージ，VMware の組み合わせにより実現しており，個別の最適化から，プライベートクラウド全体の最適化を目標に構築を進めると同時に，スペースの削減と消費電力の削減を狙ったものとなっている．

一方，学生の PC 所持率が高くなっていることが報告されており [4]，演習端末室システムの構築に当たっては学生或は教員が端末室に PC を持ち込んだ場合でも同じデスクトップ環境で利用できることを想定した設計が必要な時期に来ているものと考えられた．また，端末室だけでの利用ではなく，自宅や図書館など，どこからでも同じデスクトップ環境を利用できることも重要になると

考えた．周知の通り，演習端末室システムについてはこれまでに種々の方式が適用されてきている [1, 2, 3]．本学においても前システムでは Mac OS X を OS としたネットブート方式を採用していたが [5]，上述したように，持ち込み PC への対応や場所を意識しない利用に向けてはクライアント環境を仮想デスクトップとして VMware 上に集約した VDI (Virtual Desktop Infrastructure) 方式が適しているものと判断し [7]，VDI 方式による構築を進めた．

システムの更新に先立って行った要望調査からは Windows 演習環境の導入や，3 次元 CAD の演習を可能とすることなどが必要であることが明らかになった．3 次元 CAD 演習を想定した場合，サーバ 1 台当たりに動作する仮想 PC 台数が課題になるが，事前検証結果 [7] を基に，端末利用率を 50 %と仮定することで，47 台として構築した．

既に述べた IA サーバ，EMC ストレージ，VMware を使った VDI 方式により Windows 環境を実現する場合，個人の私的利用を想定して作られてきた Windows システムとまったく同等の機能性を有することは極めて難しい．特に，ストレージの個人領域は十分な容量を確保するために NAS 領域に配置することから，本システムの構築に当たっては，利用者に対してどのように個人領域を見せていくかが課題となった．著者らは，Windows の機能である移動プロファイル機能及びフォルダリダイレクト機能を利用し個人領域を NAS 領域に配置する方式を採用した．そこでは，ドライブレターを個人領域に割り当て，ユーザの利便性確保や多種にわたるアプリケーションの動作検証を行っている．

本論文では，2011 年 4 月から本格運用を開始した教育研究用情報システムの全体構成と演習端末室システムについての詳細を述べるとともに，Cisco Systems の IA サーバ，EMC ストレージ，VMware の組み合わせによるプライベートクラウドの構築を通して明らかとなった有効性及び今後の課題について報告するものである．

2　更新システムの設計と構成

2.1　設計の背景

大学における演習端末室システムには，多種多様な要求があり，限られた予算と人員で構築・運用してゆくことは非常に困難である [1]．本学は，2010 年度まで Mac OS X を中心に据えた Netboot を用いた演習端末室システムを運用してきた（以下，前システムと呼ぶ）[5]．前システムは，目標としていた管理コストの低減を達成するなど，一定の成果を挙げたが，いくつかの問題もあった．また，導入から五年間の運用を経て，時代の変化とともに，利用者側と管理者側双方から新たな要求が出てきた．

前システムが抱えていた主要な問題は次の通りである．

起動時間の増大
パッチの適用やアプリケーションの追加などによりブートイメージのサイズが大きくなり，運用の終盤では端末の電源投入から利用可能になるまでに二分以上待たされることもあった．

Windows 専用アプリケーションの存在
クライアント環境として Mac OS X を採用したが，CAD に代表される専門的なアプリケーションの一部に，Windows 向けにのみ提供されているものがあった．そのため，別途 Windows 2003 Server をリモートデスクトップサーバとして用意し，端末室の iMac から RDP で接続することで利用していた．また，専門的なアプリケーションの中には，リモートデスクトップ上では，意図通りに動かないアプリケーションも存在し，それらの導入はあきらめざるを得なかった．

故障端末の増加
導入当初からロジックボードと液晶ディスプレイの故障が多発していた．予備機の増強により運用していたが，予想外に運用コストが増大した．

また，利用者と管理者からの主要な要求をまとめると次の通りである．

基本となる環境は Windows としたい（クライアント OS として，Windows を利用したい）
前システムの Mac OS X は，学生には抵抗なく受け入れられた感触があったが，教員側からはやはり Windows で講義・演習を行いたいという要望があった．

Windows 専用の専門的なソフトを利用したい
前システムにおいて，リモートデスクトップサーバで提供されていたアプリケーションは，引き続き利用したいという要望があった．加えて，前システムで，リモートディスクトップの制約で動作しなかったアプリケーションも利用したいという要望もあった．

前システムに引き続き，異なる端末でも個々の環境（Windows であればでデスクトップ環境など）を再現して欲しい
個人領域の提供はもちろん，ある程度のカスタマイズが許された個人環境を提供して欲しいという要望があった．

図書館の端末室コーナーに代表される自習環境を充実させたい
前システムで導入した図書館の端末室コーナーが好評であり，空席待ちとなることが度々あったので，そのような環境を充実させる要求があった．また，それらをさらに発展させて，講義室や研究室などからも環境を利用したいという要求や，将来に向けて，教育用だけでなく，いわゆる事務部門にも端末を展開できると良いという要求もあった．

持ち込み PC を利用できるようにしたい
これまでは，端末の配置は固定的であり，端末室に代表される物理的な場所に束縛されていた．このため，特別講義や一時的な再履修者の増加などによる利用者増加への対応が難しかった．また，管理上，あらかじめ用意された端末以外からのリソースの利用は積極的に禁止していたが[1]，自宅や研究室のマシンで作成した資料やプログラムなどが，端末室に導入されているソフトウェアとの些細なバージョンの違いで意図通りに動作しないなど，データのやり取りに問題が出る場合があった．さらに，1 章で述べたように，PC の普及率の増加から，自宅や研究室などのマシンで端末室環境を利用できるようにしたいとの要求も出てきた．この要求は，前項の自習環境の充実の問題とも関連が深く，端末室に拘らずに「いつでも・どこからでも」リソースや環境が利用できるようになることを理想として，解決が求められた．

個人領域（いわゆるホームディレクトリ）の容量を増やして欲しい
アプリケーションデータや講義資料などの容量は年々増加していて，不足気味になっていた．また，いわゆるリッチコンテンツの増加により，キャッシュなどの一時的な使用容量も無視できない大きさになってきた．

管理コスト軽減のために多種多様なサーバを集約したい
これまで，サーバはアプリケーションやサービスごとに存在していたが，できるだけ集約することで管理コストの軽減を図りたい．また，単純に集約するだけではなく，リース期間（五年間）中のさまざまな変化に対応すべく，仮想化技術を積極的に用いて，物理サーバに束縛されない，柔軟な構成をとりたい．ただし，集約化することで，万が一の故障などでサービスが全滅することは避けたいので，必要に応じてパブリッククラウドの利用も検討する．

設置空間の削減を図りたい
近年では各部局からの要求で空調と非常用発電機を備えているサーバ室の利用ニーズが高まっている．また，教育システム以外の自前の運用および実験システムも多種多様なものがあり，恒常的に手狭な状態となっているが，サーバ室の改築は困難である．さらに，機器を効率的に配置することで発熱量を押さえ，空調を含めた消費電力の削減を図りたい．

2.2 設計方針

削減され続ける予算の中で，前節で述べた課題をできるだけ解決するために，新しい演習端末室システムは，次のような設計方針とした [7].

端末室には，シンクライアントを配置し，VDI を用いてクライアント環境（Windows 環境）をサーバ上の仮想環境に集約する．つまり，利用者が操作するのは，シンクライアントであるが，実際には，サーバ上の仮想化された OS にネットワークを通じて接続し，それを利用する．OS やアプリケーションの実行はサーバ上の仮想環境上で行われ，利用者にはその画面が転送されることから画面転送型シンクライアントシステムとも呼ばれる（図 1）[6].

さらに，端末室に設置されたシンクライアントだけでなく，個人が持ち込んだ PC が仮想マシン上のクライアント環境へアクセスすることを念頭に置いている．このことが従来の演習端末室システムとは異なり，特徴的である．

具体的には，ネットワークの入口として，演習端末室システム専用の Firewall と VPN 装置を用意し，VPN 接続できようにしている．また，持ち込み PC 専用の仮想リソースプール (仮想マシンの集合) を用意し，それに対して適切な設定を施すことで，ライセンスやサーバリソースなどを制御することとした．

演習端末室システムには，端末利用者の目に見えるデスクトップ環境以外にもさまざまなサービスが必要とされる．それらについても，可能なものは積極的にサーバ上の仮想環境を利用する設計とした．

2.3 更新システムの構成

初めに更新システムの全体概要を図 2 として示す．本節ではこの中の演習端末室システムを中心に述べる．

システムの中核をなすサーバは，Cisco UCS 5108 シャーシに搭載された 30 台の B200M2 ブレードサーバ

[1] 一部，資料の提示などのために教員が個人 PC を持ち込むことはあったが，それらは，プロジェクタの利用などに限られていて，設置端末とは明確に区別されていた．

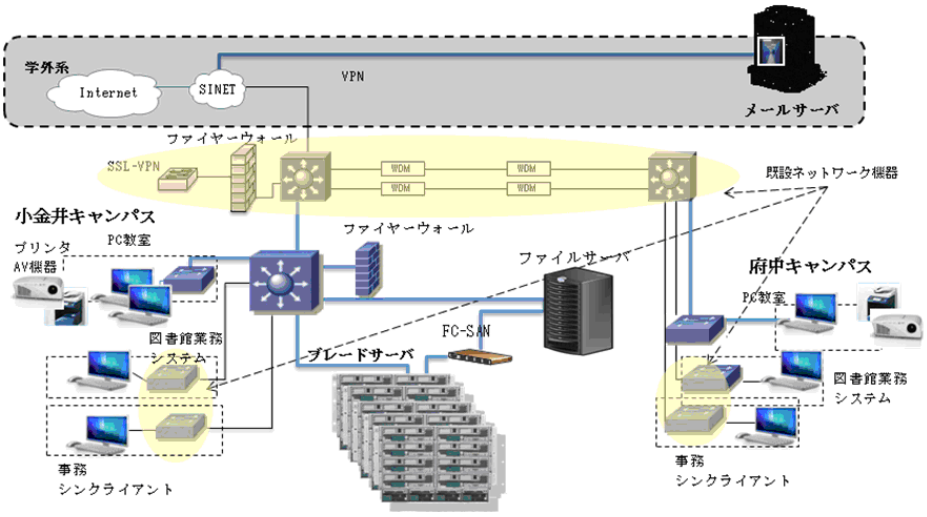


図- 2: 更新システムの全体概要図

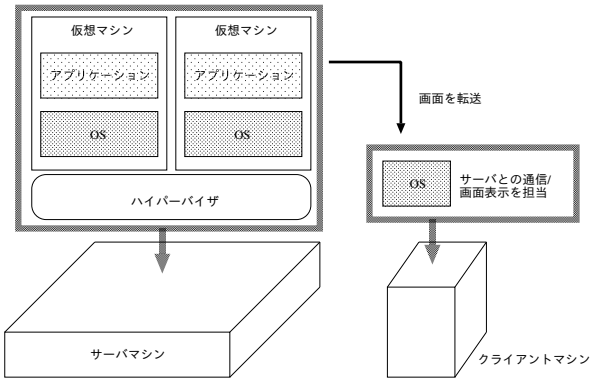


図- 1: VDI の概念図

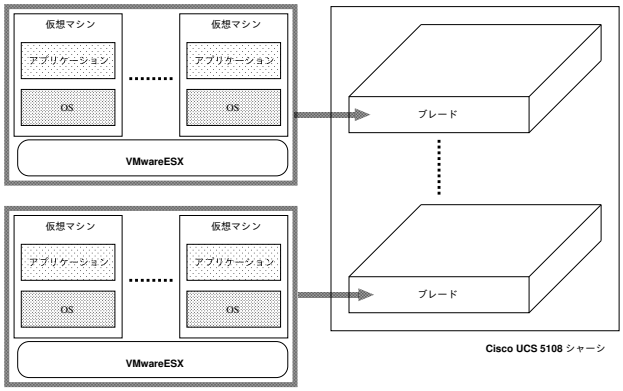


図- 3: ブレードサーバと ESX サーバの関係

群からなる．提供するサービスの性質に応じて，ブレードサーバ一枚をそのまま物理サーバ一台として用いる場合とブレードサーバ内に複数の仮想マシンを構築する場合で使い分けている．

後者の仮想マシンの構築には，VMware ESX を用いている（図 1 のハイパーバイザに対応する）．本稿では，こちらを物理サーバに対応して，ESX サーバと呼ぶ（図 3）．演習端末室システムには，12 台のブレードサーバを割り当て，530 台のクライアントをホストしている．

なお，ブレードサーバ B200M2 は，いわゆる IA サーバであり，目的に応じて仕様の異なる三種類が混在している．物理サーバ用の仕様を表 1（ブレードタイプ A : 11 台），演習端末室システム用以外の ESX サーバの仕様を表 2（ブレードタイプ B : 7 台），演習端末室システム用の ESX サーバの仕様を表 3（ブレードタイプ C : 12 台）として示す．さらに，これら三種類のブレードサーバ構成の概念図を図 4 として示す．

また，ストレージシステムについてであるが，演習端末室環境における個人領域を初めとして，さまざまなシステムのデータを収納するので，高性能と高信頼性の両立が必須となる．さらに，複数のプロトコルでのアクセスに対応している必要がある．

更新システムでは，ストレージシステム EMC Celerra NS-480 をブレードサーバと Fibre Channel で接続し，SAN (Storage Area Network) を構成した （図 2 の FC-SAN）．また，通常のネットワークを用いて，NAS (Network Attached Storaqge) としても振舞うことができる構成となっている．表 4 にストレージシステムの仕様を示す．

RAID 6 構成を採用し，SAN 上にシステム領域として約 46 TB，NAS 上にデータ領域として約 43 TB の容量を確保した．これにより，演習端末室環境における個人領域は，前システムの三倍である一人当たり 300MB を提供できることになった．

加えて，前システムでは独立していた学習用 LMS (moodle) や Web サーバのデータ領域などを集約することができた．また，事務部門のための共有ストレージ

表- 1: 物理サーバ（ブレードタイプ A）

プロセッサ	Xeon E5540 2.53GHz 1P/4C × 2
メモリ容量	8GB
ディスク容量	内蔵ディスクなし（SAN 領域にディスク容量確保）
NIC	UCS M81KR Virtual Interface Card/PCIe/2-port 10Gb

表- 2: ESX サーバ（ブレードタイプ B）

プロセッサ	Xeon E5540 2.53GHz 1P/4C × 2
メモリ容量	24GB
ディスク容量	内蔵ディスクなし（SAN 領域にディスク容量確保）
NIC	UCS M81KR Virtual Interface Card/PCIe/2-port 10Gb

サービスを新たに提供することが可能となった．表 5 に NAS ストレージの容量設定を示す．

2.4 ラック構成と消費電力

ブレードサーバ群とストレージシステムを中心とする更新システムの基幹部分は，本学総合情報メディアセンター内にあるサーバ室に設置されている．サーバ室の耐荷重は 400 Kg/m^2 であるため，8 本のラックに分散して配置した．

ブレードサーバの採用が設置空間の削減につながり，前システムと比較してラック当りの実装密度が下がり，熱的に有利な構成となった．ラック構成を図 5 として示す．

更新システムに対する要求の一つとして消費電力の削減があるが，定格消費電力合計（最大想定）を 22,254 W として構築し，UPS の負荷率から計測した実際の消費電力合計は 10,510 VA であることが確認できた．前システムではメールサーバやそのための負荷分散装置もサーバ室内に設置していたため，一概に消費電力の比較は残念ながらできないが，前システムの消費電力は設計上 35,430 W （内メールサーバ関連 1,880 W）であり，

表- 3: ESX サーバ（ブレードタイプ C）

プロセッサ	Xeon X5650 2.66GHz 1P/6C × 2
メモリ容量	96GB
ディスク容量	内蔵ディスクなし（SAN 領域にディスク容量確保）
NIC	UCS M81KR Virtual Interface Card/PCIe/2-port 10Gb

表- 4: ストレージシステム（EMC Celerra NS-480）

シェルフ	NS4-4PDAE × 16
プロセッサ	Xeon 2.8GHz × 2
メモリ容量	8GB × 2 （SP あたり 8GB）
ディスク搭載数	FC 148GB × 5, FC 600GB × 189, SATA 1TB × 2
I/F	10GbE NIC × 4, FC Port × 2
入力電力	100 ～ 240 VAC 単相電源
高さ	53U（基本筐体 8U, シェルフ 3U × 15）

表- 5: NAS ストレージの容量設定

教育用端末	事務部門共有	Web サーバ
16TB	8TB	1TB
LMS	教職員用	その他
10TB	3TB	5TB

メールサーバ分を除いた場合を比較すると 33% 程度の低消費電力化（設計値比較）ができているものと考えている．

2.5 シンクライアント

端末室に配置されるシンクライアント Wyse C90LEW ThinClient（以下，Wyse 端末と呼ぶ）の仕様を表 6 として示す．

Wyse 端末上では，Windows Embedded Standard (Windows XPe) が利用者には書き換え不可能な状態で動作していて，通常は，制限されたユーザですでにログインされた状態で起動している．ここで，仮想マシンに接続するためのソフトである VMware View Client を起動し，認証を経て仮想マシン上で動作する Windows 7 に接続される．なお，Windows XPe の機能である FBWF (File-Based Write Filte) を積極的に用いることで，Wyse 端末上でもいくつかのアプリケーションを動作させることが可能であるが，現在は VMware View Client のみを利用している．

Wyse 端末の Windows XPe は，20 秒ほどで起動し，およそ一分弱で仮想マシン上の Windows 7 が利用可能になる．ネットブートを用いた前システムと比較して，30 秒程度短縮されている．今のところ，利用者から強い不満の声は挙がっていない．

Wyse 端末の仕様上の平均消費電力は，7 W であり（表 6），前システム iMac G5 (M9844J/A) の 80 W と比較すると[2]大幅な削減となった．

[2]iMac G5 の仕様上の最大消費電力（連続使用時）は，180 W である．

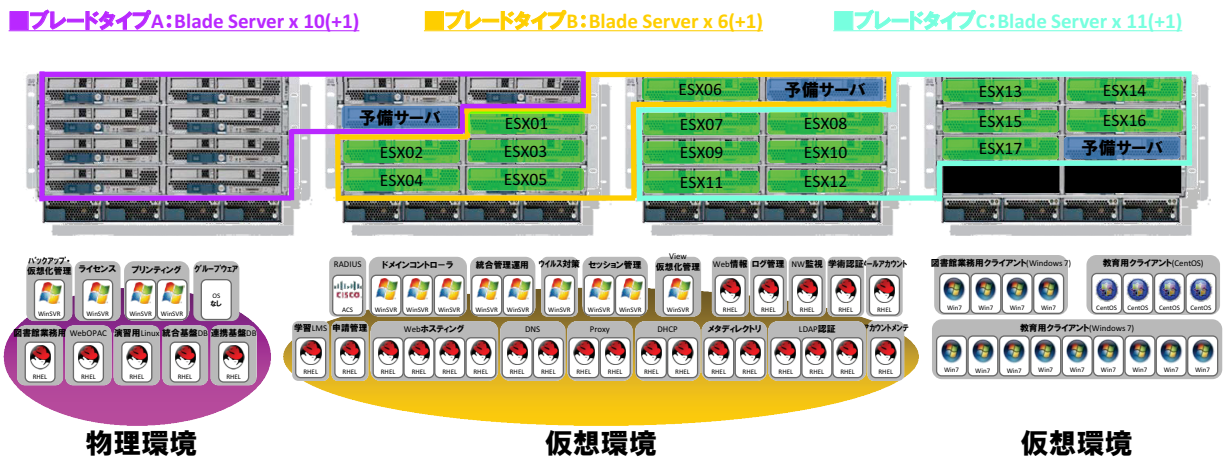


図- 4: ブレードサーバ構成概念図

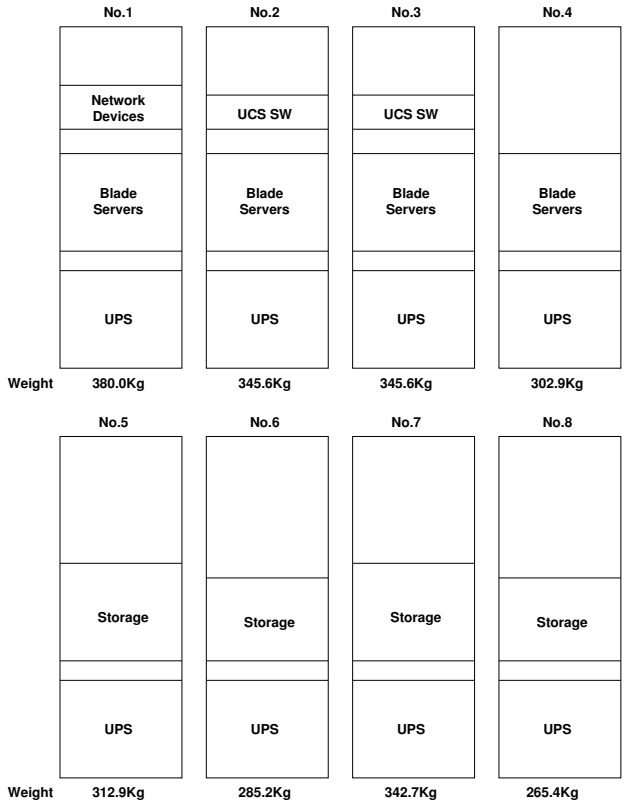


図- 5: ラック毎のシステム構成

表- 6: Wyse 端末の仕様

プロセッサ	Via C7 ULV 1.0GHz
メモリ容量	2GB Flash / 1GB DDR2 RAM
USB ポート	USB 2.0 ポート × 4
NIC	10/100/1000 Base-T
外形寸法	177 × 121 × 34mm
重量	約 612 g
平均消費電力	7 W

画面転送型シンクライアントシステムは，一般に動画再生などの高い描画能力を要求される処理が苦手とされていたが [6]，最近では，その問題を緩和するための支援機能が利用できることがある．採用した Wyse 端末では，Wyse TCX Multimedia（動画再生）や Wyse TCX Flash Acceleration（Flash 動画高速化）と呼ばれるものがあり，今のところ，懸念していた CAD ソフトの利用などで，大きな不満の声は出ていない．

Wyse 端末では，Wyse TCX USB Virtualizer と呼ばれる，USB 機器が直接仮想マシンに接続されているように見せかける機能（仮想 USB）を持っている．今のところ USB 機器の利用に対して特別な制限は設けていないので，仮想マシンの Windows 7 上にドライバが用意されていれば，一般ユーザでも利用可能である．実際に USB メモリが広く利用されているようである．実用上は，仮想マシンにログインした状態で仮想 USB の機能を有効にする操作が必要であるが（有効にするボタンをクリックすることで機器が認識される），特に不満なく受け入れられているようである．

3 個人環境・個人領域の提供

Windows 7 システムでは，ユーザの個人領域となるホームディレクトリ（ホームフォルダ）がシステムと完全には分離されておらず，標準構成では C:\Users\<ユーザ名> に配置される．ここにユーザが作成したデータとともに，プロファイルと呼ばれる環境設定が保存される．このままではホームディレクトリが仮想マシンに依存してしまい，多数の仮想マシンを利用する演習端末室環境には向いていない．

なお，仮想マシンを採用したことで，理論的には，ユーザ毎に専用の仮想マシンを容易することも可能である．しかし，入学や卒業に伴うユーザの入れ替わりや障害時の復旧，OS のライセンスの管理などの問題があり，現実的ではではない．したがって，VMware View Client からの接続要求があると，VMware View Connection Server と呼ばれるセッション管理サーバが適切な仮想マシンを選択し，そこに接続する方式を取っている．つまり，ユーザは接続する仮想マシンを選ぶことができないので，個人領域をシステムから分離する必要がある．

仮想化の有無に関わらず，演習端末室環境では，容量を十分に確保しつつ管理を容易にするために，個人領域を NAS 上に配置することが一般的である．しかし，Windows システムの場合は，主として個人の私的利用を想定して作られているアプリケーションが多数存在し，それらは標準構成以外では意図通りに動作しない．つまり，単純に分離しただけでは，問題が起こることがあり，ユーザデータとプロファイルの配置は，少なくとも見かけ上は Windows の標準構成に準拠している必要がある．

また，Windows システムが一般に広く普及した結果，演習端末室環境においても，家庭や研究室で慣れ親しんだ標準の構成であることが利用者から求められている．

このような前提を踏まえて，いくつかの方法を検討した結果，移動プロファイルとフォルダリダイレクトを組み合わせた方式を採用することとした．検討した個人領域の提供方法を表 7 として示す．具体的には，Windows が提供する移動プロファイルの機能を用いて個人領域をシステムから分離する．しかし，それだけでは，ログインとログオフ時に NAS と仮想マシンの間で大量のデータがやりとりされることになるので，デスクトップなどのユーザデータ部分については，フォルダリダイレクトを用いて直接 NAS にアクセスすることとした．

ただし，この方式では，フォルダリダイレクトを用いた部分をリダイレクト前の C:\Users\<ユーザ名> ではなく，リダイレクト後の NAS 上を指す UNC (Universal Naming Convention) パスで認識してしまうアプリケーションがあり，ユーザが混乱することが懸念された．また，そのようなアプリケーションの中には，意図通り動作しないものもあった．そこで，この部分に改めてドライブレターを割り振った．使用可能な任意の文字で良いが，更新システムでは Y ドライブとし，ユーザデータがそこからアクセス可能であることを周知している．事前にこの措置を取ったことにより，今のところ大きな混乱は起きていない．

4 おわりに

本論文では 2011 年 4 月から本格運用を開始した教育研究用情報システムの全体構成についてと，演習端末室システムの構築について述べた．

更新システム導入の基本的な方針は，スペースの削減と消費電力の削減にあり，仮想化技術を積極的に導入した．前システムとの完全な比較はできないが，消費電力としては前システムに比べ約 33%（設計値比較）の低下となっている．

演習端末室システムの構築では，システム構築に先立って行った調査から，クライアント OS として Windows の利用要望が多く，端末室にシンクライアントを配置した VDI 方式を採用した．仮想マシン上に集約された Windows 環境では，システム部分から個人領域を分離するために移動プロファイルを用いる必要があったが，ファイルサーバやネットワークへの負荷を考慮して，フォルダリダイレクトを併用した．これにより，どの仮想マシンにログインしても同一のプロファイルが利用可能であり，仮想マシン毎に全ユーザのプロファイルを置かなくて済むようになった．さらに，リダイレクト先の領域に改めてドライブレターを割り振ることで，パスの認識に問題があった一部のアプリケーションの対応した．導入したシンクライアントシステムの平均消費電力は 7 W であり，端末単体としての低消費電力化も達成できたものと考えている．

今後，持ち込み PC による演習端末室環境（クライアント環境）利用の本格展開を検討している．これにより，教材準備や自習環境の充実などの利便性の向上に加えて，これまで対応が難しかった，突発的な受講者増加に対する有力な解決手段となることが期待される．そのためには，PC の必携化を前提にライセンス管理方式を明確化することと，利用者教育や利用時間拡大に伴うメンテナンス体制の見直しなどのいくつかの運用上の問題を解決する必要があるが，それらは今後の課題としたい．

参考文献

[1] 桝田秀夫ほか：特集 大規模分散ネットワーク環境における教育用計算機システム，情報処理，情報処理

表- 7: 個人領域の提供方法

		移動プロファイル				ローカル
		個別プロファイル		共通プロファイル		プロファ
フォルダリダイレクト		使用	未使用	使用	未使用	イル
保存場所	設定	NAS	NAS	保存不可能	保存不可能	仮想マシン
	ユーザデータ	NAS	NAS	NAS	保存不可能	仮想マシン
負荷		低い	高い	低い	低い	低い
個人設定の保存		可能	可能	不可能	不可能	可能
複数の仮想マシンからの利用		可能	可能	可能	可能	不可能

学会，Vol. 45, No. 3, pp. 225–281 (2004).

[2] 丸山伸，最田健一，小塚真啓，石橋由子，池田心，森幹彦，喜多一：Virtual Machine を活用した大規模教育用計算機システムの構築技術と考察，情報処理学会論文誌，情報処理学会，Vol. 46, No. 4, pp. 949–964 (2005).

[3] 関谷貴之，安東考二，尾上能之，田中哲郎，山口和紀：NetBoot による端末を用いた教育用計算機システムの開発と評価，情報処理学会論文誌，情報処理学会，Vol. 48, No. 4, pp. 1651–1664 (2007).

[4] 三菱総合研究所：大学生等への消費者啓発方法に関する調査研究，平成 18 年度内閣府請負事業，資料 4，p. 10，<http://www.consumer.go.jp/seisaku/caa/shohishakyouiku/kyouikukaigi2/file/shiryo4-1.pdf> (2007).

[5] 瀬川大勝，櫻田武嗣，萩原洋一，川島幸之助：Mac OS X による Netboot を用いた端末室環境の運用，第 12 回学術情報処理研究集会，学術情報処理研究集会，Vol. 12, pp. 81–85 (2008).

[6] 只木進一，田中芳雄，松原義継，日永田泰啓，江藤博文，渡辺健次：仮想デスクトップ・画面転送型シンクライアントによる演習室端末システム (佐賀大学の新しいシステム紹介)，情報処理学会研究報告，インターネットと運用技術 (IOT)，Vol. 2010-IOT-11, No. 3, pp. 1–5 (2010).

[7] 櫻田武嗣，萩原洋一：シンクライアントと持ち込みノート PC による端末室デスクトップ環境の設計，情報処理学会研究報告，インターネットと運用技術 (IOT)，Vol. 2011-IOT-13, No. 18, pp. 1–6 (2011).

第 15 回学術情報処理研究集会

対外接続の冗長化運用とその評価

Redundancy Operation of External Network and It's Evaluation.

平沼賢次†，柳沼匠†，清水悦郎†
Kenji HIRANUMA†, Takumi Yaginuma†, Etsuro SHIMIZU†

kh@ xi.kaiyodai.ac.jp, yaginuma@m.kaiyodai.ac.jp, shimizu@ kaiyodai.ac.jp,

†東京海洋大学情報処理センター

† Information Processing Center, Tokyo University of Marine Science and Technology

概要

旧東京商船大学（現：海洋工学部）と旧東京水産大学（現：海洋科学部）が，2003 年 10 月に統合して誕生した東京海洋大学では，学外への対外ネットワーク接続に，学術情報ネットワーク SINET3 を利用している．大学の立地条件や統合時の対外接続用回線の契約状況等の様々な問題のため，対外接続回線はキャンパスごとに保有し利用している．そこで，対障害性の向上，回線の有効活用を考え，現在，学外と 2 つのキャンパスとの接続には，冗長化による対障害性の向上を目的とした三角形の接続方式を用いている．これは国立大学法人では東京海洋大学のみの接続方式である．本稿では，この冗長化方式の構築と，対障害性の実証実験，及び今後について述べる．

キーワード

冗長化，対障害性

1. はじめに

近年進む電子化などの社会の情報化に伴い，電子情報やその運用システムの重要性が益々増している．特に情報集約と発信の拠点のひとつである大学では，メールやブラウジングは，授業，研究以外にも，学生の就職など広く利用されている．そのため基盤となるネットワークは安定した運用と高い信頼性が求められる．しかし，実際には様々なネットワーク障害が発生しており，特に本年発生した東日本大震災に代表される地震や津波などの大規模災害よる通信施設の破損・停電等による情報通信網の切断などの被害によって，ネットワークの維持やその早期回復が困難な状況が現実に発生している．また，近年の国公立大学を取り巻く状況は，法人化や予算減少に伴う経費節減ため，ネットワークの運営環境は厳しいものになってきている．東京海洋大学では，ネットワークの安定運用・高信頼性等のため, 2005 年以降の 6 年間, のように，対外接続用ネットワークを冗長性化することで，情報通信網の切断等障害後の早期復旧による対障害性の向上や諸問題に対応してきた．本稿では，この冗長化方式とその構築法について述べるとともに，実際の大学のネットワーク用いた実験と運用実績から，この方式の冗長性と対障害性を示す.

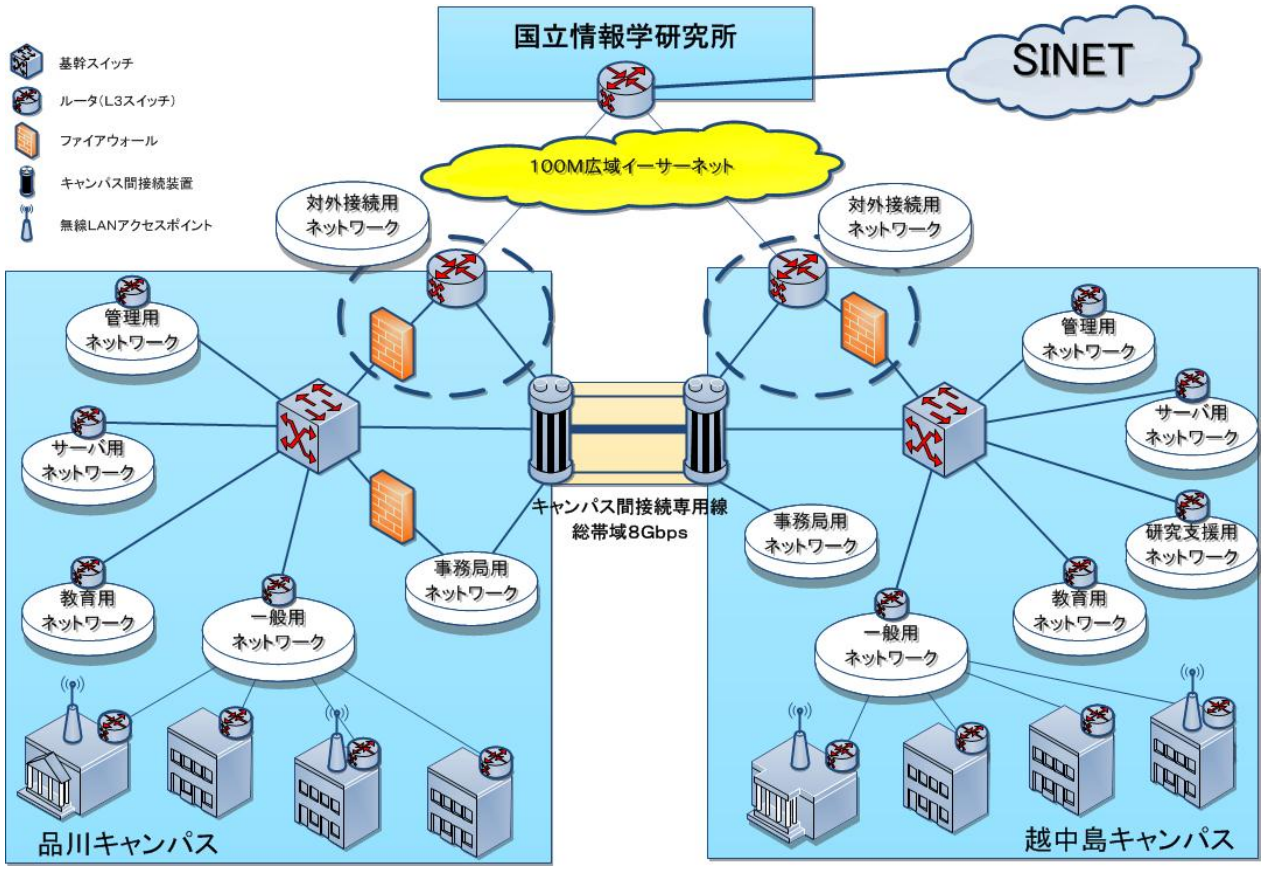


図 1：ネットワーク構成図

2. 従来のネットワーク構成と問題点

東京海洋大学のような複数のキャンパスを持つ大学の場合，経費や保守管理などの都合上，図 2 のような対外接続 1 ラインの大学が多い．このような場合，上流のキャンパスが工事や障害等で対外接続が停止した場合，下流のキャンパスは対外接続を失うことになる．一方，このようなことは，下流が工事などの場合では発生しないので，情報通信に関するキャンパス間格差という問題も含むことになる[1]．このような接続方式による問題点以外にも，東京海洋大学には，立地など地理的問題が存在している．越中島・品川，両キャンパスとも東京湾に面し，四方を河川や運河に囲まれた島状の埋立地に立地している．このため，地震等の災害により，橋脚が損傷すると孤立する危険性がある．また，そのような緊急災害時において大学は，災害対応の拠点（越中島：江東区指定広域避難所，品川：東日本大震災時，帰宅困難者受け入れの実績）となるため，情報通信手段の確保はより重要な案件となる．

他にも，異なる別々の大学が統合した東京海洋大学特有の課題が存在する．学生証などは統合時に統一化が進められたが，教育用情報機器は契約期間の関係により統合後もしばらくの間はそれぞれ別仕様のものを使用していた．

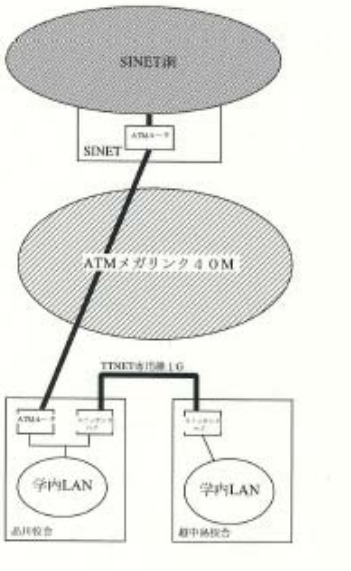


図 2：第 1 期対外接続図（1 ライン）

その後，情報ネットワークは管理や経費圧縮も兼ね，統合が進められた．統合前は，それぞれ対外接続は直接 SINET に接続していたが，統合後は，図 2 のようにネットワークの統合が行われ，SINET への接続は，統一した対外セキュリティーポリシーのファイヤーウォール（以

後：FW）を用いた 1 ライン方式に変更された（第 1 期構成）．それまで，各キャンパス別に対外接続（計 2 ライン）を行ってきたものが，同じ回線速度の 1 ラインに統合されたため，1 本の対外接続を 2 キャンパスで共用することになり，多少の通信速度低下などが生じた．また，それ以上に，共通のセキュリティーポリシーでの運用が問題となった．元々別大学でありセキュリティーポリシーやその利用方法などで多くの点が異なっていたため，共通の FW の利用を始めたところ，それぞれの授業・研究等に支障がでるなどの様々な問題点が明るみになった．

2005 年の学内情報機器の更新による学生証と情報機器の統合を機に，限られた予算や設備で，これらの課題に対応して，利用者に情報網の維持と品質を提供する必要があった．

3. 対外接続の冗長化

3.1. 冗長化方式の構成

前述したような様々な問題を考慮した検討の結果，2005 年の第 2 期構成（図 3）では対外接続の冗長化をベースに，これらの問題の解決にあたることにした．対外接続の冗長化には様々な方式があるが，以下のようなことから，冗長化の方式を決定し，その設計をおこなった．

元々スタンスの異なる別々の大学であった各キャンパスを，同時に全ての統合することが困難であるならば，統合する部分と，別にする部分とにあえて分離することにした．更新により導入される統合認証システムと深くかかわる学生証（IC カード型）や教育用端末機などは同じ仕様に統合し，異なるセキュリティーポリシーに関わる FW を 2 つ分けて，それぞれをキャンパス別の仕様を設定した．これによりシステムの共通化を進めつつ，ポリシーの違いによる課題に対応することにした．回線は上流の品川キャンパスで分岐し，その下流に FW を配置するのが，最も安価であるが，先に述べた地理的問題やキャンパス間の格差や災害等などの様々な障害に対応する必要があった．そこで，図 3 のように統合以前と同じく，各キャンパスがそれぞれ SINET に接続することによって，片方が対外接続を失う状態になったとしても，もう一方は接続を保てるようにした．また，これまで用いてきた高価で専用大型機器を用いる ATM（asynchronous transfer mode：非同期転送モード）と比較して，技術向上よって非常に安価で構成できる高速なイーサネットに切り替えた．これにより，学内外のネットワークは，速度が 40M→100Mbps に増速，通信品質は 100TX と向上した上，ネットワーク費用を大幅に圧縮することができた[2].

これにより，SINET 側に設置していた，ATM ルーターを 100TX の L3 スイッチに変更した．各キャンパスにおける対外接続用スイッチも同様の 100TX の L3 スイッチを設置し，その下に，FW を置いた．更に既存のキャンパス間ネットワーク（1000SX×8 本）の内，1 本用いて，両キャンパスの対外用 L3 スイッチを接続して，図 3 のように三角形のネットワークを構成した（第 2 期構成）．

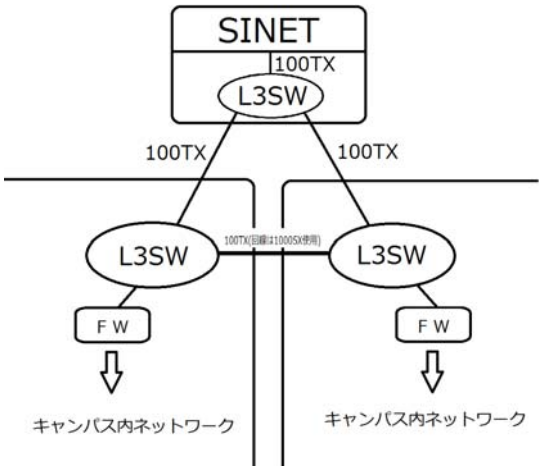


図 3：第 2 期構成（冗長化）

このように設計された三角形構成は，片方のキャンパスのネットワーク障害時にも，他方のキャンパスでは，問題なくネットワークを利用できる上，更に片方の対外接続に障害が発生して学外ネットワークが切断されたとしても，キャンパス間接続を用いて他方のキャンパスを迂回して，対外接続を維持する冗長性を持つ方式である．

迂回路は各 FW の上流にあるので，それぞれの対外セキュリティーポリシーを保ちながら迂回すること可能となる．また，両キャンパス間での通信は，FW 内の既存のキャンパス間ネットワーク（1000SX×7 本）を用いる．

また，既存の学内設備の変更を最小限に止めることによって，経費を抑えることができた．東京海洋大学はこの冗長化の方式を採用した構成により，対外接続の対障害性が向上することができた．

3.2. 運用と改修

第 2 期構成に移行後，運用により何点かの問題が浮かびあがった．その一つは，経路の探査・管理の方式として通信業者が強く推進めた PING を用いた業者方式の問題であった．業者方式は，通常の通信網で実績があり多くの利点を有する方式であるが，実際に大学の対外接続で運用したところ，各キャンパス間で通信速度差異，通信速度のバラつき，仕様やテストと異なる障害時の切り替え時間（数時間から数日）などが判明した．また，システム業者が納入した L3 スイッチや PING 方式の切り替

えシステム等が完全にブラックボックスとなっていた．このことは，大学でのネットワークやそれらを用いた他の研究等において支障を生じた．そこで，2006 年の SINET の仕様変更（1000T 対応）を機に，更なる効率的なルーティング・プロトコルを使用して，効率的な経路制御を目指した改修をおこなった．また，これにより，将来の回線の増速対応を考慮してスイッチをギガ対応の MRV 製 L3 スイッチに変更した（第 3 期構成）．

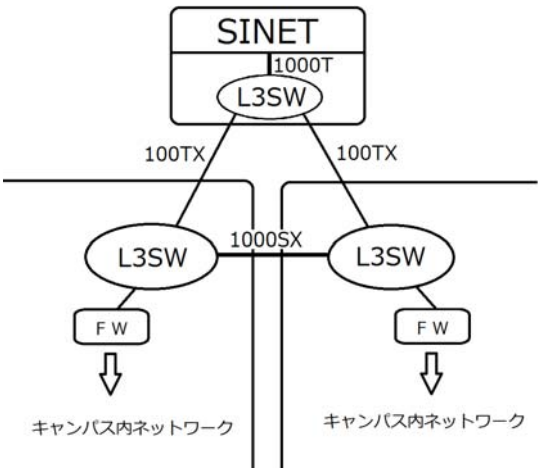


図 4：第 3 期構成

第 3 期構成は MRV 製 L3 スイッチを，SINET・越中島キャンパス・品川キャンパスにそれぞれ 1 台設置した計 3 台で構成される．通信速度は SINET（一橋）と SINET 側の L3 スイッチ間が 1000T，SINET 側 L3 スイッチと各キャンパス間は 100TX，キャンパス間は 1000SX で接続されている．各キャンパスのスイッチの下流に，FW を通して学内ネットワークに接続されている．SINET 側の規格の変更に対応して交換した L3 スイッチが，ギガ対応になったため，これまでより余裕ができ，SINET と両キャンパス間の通信が安定するようになった．このため，それまでやや不安定であったこの通信が安定することで，100TX でも十分な通信をおこなうことができるようになった．これによって，SINET と両キャンパス間のメトロイーサの契約を，料金が高い 1 Gbps に切り替えることなく，従来の 100TX の契約を継続することによって，通信経費を抑制することに成功した．また経路のネットワーク探査・感知・管理の方式には，研究の自由度をあげるため，ブラックボックス化した業者方式に換えて，OSPF（**Open Shortest Path First**）を用いた方式に変更したところ，障害時の切り替え時間（切断時の回復：10 秒程）も大幅に短縮され，システムのブラックボックス化も解消された．この OSPF において 3 つの L3 スイッチは，互いにネイバーとして情報を交換している．その後，2011 年 2 月の学内情報機器更新まで，大きなトラブルもなく，接続を維持して有効に機能した．その後，2011 年 2 月の学内情報機器更新により，三角形対外接続の内，キャンパス間接続の機器の入れ替えが行われたが，対外接続の基本構造は維持された（第 4 期）．

4. 実験と考察

4.1. 対障害性の実験

今回，2011 年 2 月の情報システム更新による新システムでのネットワークを用いた，対障害性の実験をおこなった．方法は，実際に対外接続を行っている状態で，その接続経路情報データをモニター&記録し，各キャンパスで通常（図 5）の対外接続に用いられている対外用 L3 スイッチ上の SINET への直接回線を物理的に取り外すことで回線切断障害（図 6）を発生させ，迂回ルートの構築（図 7 **エラー! 参照元が見つかりません。**）などへの自動切り替え動作や，回線を元にはめ戻すことによる障害復旧後の動作について実験をした．

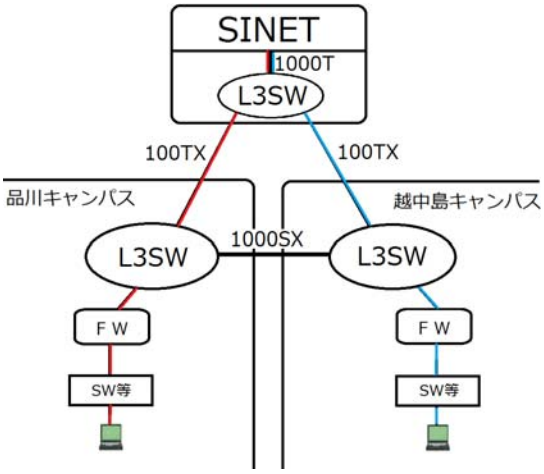


図 5：対外接続（通常）

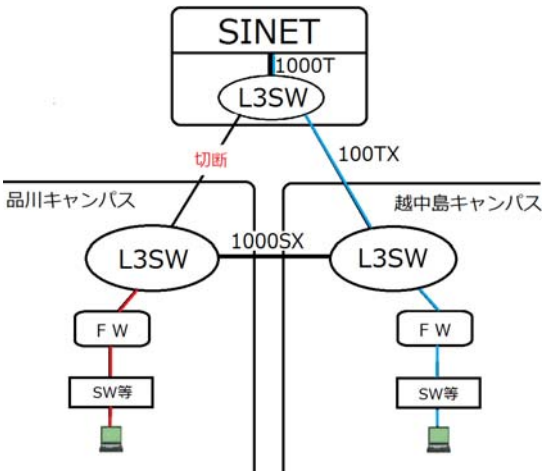


図 6：対外接続 1 ライン切断

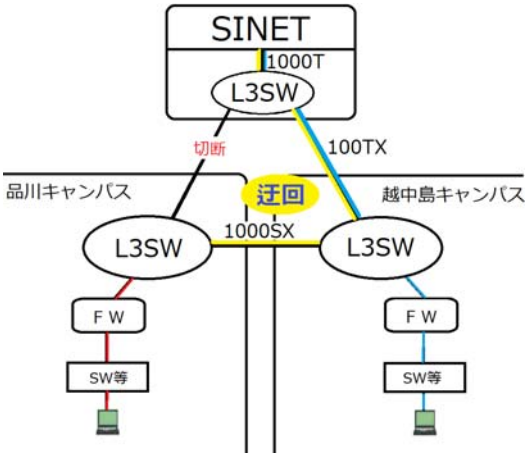


図 7：迂回経路

4.2. 結果と考察

結果の一例をあげる．品川キャンパス側の対外接続を図 6 のように切断した場合, 平均 15 秒ほどで**エラー! 参照元が見つかりません。**のような迂回経路に自動で切り替えて接続は回復した．また，図 5 のように品川側の対外回線が回復後は，迂回経路による対外接続を維持した状態で，回線回復後 20 秒ほどで，元の通常経路である SINET 直接回線に自動で切り替わった．この切り替えは瞬時に行われ，WEB サイトの閲覧をおこなっている利用者には，切り替えを気づかせることなく切り替わったことが確認された．(実験の一部は, 昼休みに行われたが, 情報処理センターには，接続できないなどのネットワークの不調を示す報告はなかった．)

このことから障害時・復旧時の切り換わり時間も十分な速さであることが確認することができた．この実験結果より，本稿で用いた冗長化方法の実用での有効性が示された．

5. 今後の予定

本稿で述べた冗長化方式は，実験においても，実運用においても良好な結果を示しているので，この方式は実用に耐えうる対障害接続法式といえる．このような実績より，2010 年の学内無線 LAN 本格運用開始，2011 年 2 月の学内情報機器更新においても，この方式は引き続き用いられた．また，2011 年 3 月 11 日の東日本大震災時においても，対外ネットワークは切れることなく維持をした．だが，近年は，通信インフラの整備が進み，また技術の開発・向上による機器の機能向上と価格低下，

IP の有料化，大学予算の減少による情報経費の削減などから，来年度からの SINET 4 切り替えを機に対外回線の 1 ライン化が検討されたが，東日本大震災やその後の電力事情による停電への対応などを考慮して引き続き同じ冗長性方式を用いることが決定した．しかし，SINET 4 では，SINET 側に L3 スイッチを設置できないため，図 8 のような構成となる．この場合スイッチ同士の通信が必要な OSPF が利用できないため，これまでの対障害性のための冗長方式用いることができない．そこで OSPF の代わりになる冗長化方式を検討中である[3].

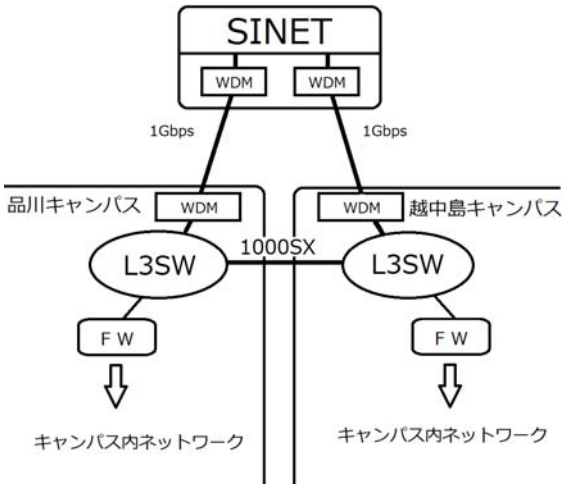


図 8：次期構成案

その他にも，学外からの VPN を使った学内サービスを利用するシステムの導入などが検討中であり，将来予想される通信量の増加にも対応していく予定である[4].

このように，実際に導入・運用されて，対障害性，大学統合による課題の解決，コスト削減，通信速度向上など安定的な運用と高い信頼性確保し，実現してきた実績は，ネットワーク技術に貢献してきたと考える．この冗長方式を元に，新たな要望や現在の電力事情と学内のポリシーを踏まえ，次期システム構成に活かしていく予定である．

参考文献

[1]山井成吉，岡山聖彦，金　勇，河野圭太，大隅淑弘：岡山大学における地域 IX と SINET を利用したネットワーク冗長化，情報処理学会研究報告 4, 113-118, 2009

[2]漆谷重雄，松方純，阿部俊二，計宇生，福田健介，鯉渕道紘，中村素典，山田茂樹：多様なサービスを支える sinet3 の詳細ネットワーク設計，電子情報通信学会論文誌 B Vol. J91-B No10 pp. 1136-1146, 2008

[3]鳩野逸生，伴好弘，佐々木博史：神戸大学におけるネットワークシステムの構築，情報処理学会研究報告 7 No1, 1-5, 2009

[4]曽根直人, 林 秀彦, 菊地 章:Proxy サーバによる HTTP トラフィックのルーティング，鳴門教育大学情報教育ジャーナル 5，1-6，2008

仮想サーバとクラウドサービスを活用した演習室クライアントシステム構築の一例
A client system for education using server virtualization and cloud services

本田　修啓
Naohiro Honda
nhonda@gw.fukushima-u.ac.jp

福島大学総合情報処理センター

Fukushima University Information Network Center

概要

福島大学総合情報処理センターでは,平成 22 年度に演習室システム(教育・研究用電子計算機システム)設備更新を行い,平成 23 年 3 月 1 日よりサービス提供を開始した.リースによる調達であり期間は 5 年間である.本報告では仮想サーバとクラウドサービスの活用に特徴を有するこのシステムについて概要と運用状況を紹介する.

キーワード

ネットブート,シンクライアント,クラウドサービス,仮想化サーバ

1. はじめに

演習室システムは,数百台のクライアント PC への効率的なセキュリティ更新対応や,追加ソフトウェア導入を迅速かつ効率的に行う必要がある.またサーバにおいては,講義時に集中する大量の負荷に対応できる必要がある.これらは一般のコンピュータシステムとは異なった特徴であり,情報処理センターの演習室システム固有の難しさであろう.

今回の更新では,クライアント PC ではネットブート型シンクライアント化による迅速性の確保と,作業負担の軽減を目指し,サーバにおいては仮想化サーバ技術およびクラウドサービスを活用することで,集中的な負荷に対応可能なサーバシステムを,実サーバ台数を圧縮しコスト削減を図りつつ実現することを目指した.

2. システム設計の基本方針

2.1. ユーザフレンドリーなクライアント PC

最新のクライアント OS (Windows7, MacOS X Snow Lion)を採用し,画面アスペスト比 16:9 の液晶ワイドスクリーン型を採用した.加えてディスプレイ一体型とし,作業スペースを最大限確保する.

2.2. 高セキュリティ

セキュリティ更新の迅速な適用を可能とするネットブート型シンクライアント端末とする.セキュリティソフトを導入し,マルウェア感染を抑制する.

2.3. 運用負担の少なさ

メールシステムはインターネットクラウドサービスを

利用することとし,メールサーバ廃止等で管理するサーバ台数を削減する.ネットブート型シンクライアント採用により,セキュリティ更新作業負担の軽減を行う.

2.4. 省エネルギー

仮想サーバ方式を採用し,実サーバの台数を最小限に抑えることで空調に要する電力も含め省電力をはかる.

2.5. レンタルサーバ化による可用性向上

www 情報発信サーバについては,クラウド型仮想専用レンタルサーバとし,本総合情報処理センターのメンテナンス作業時あるいは停電時サービス継続性を確保する.

3. システム構成

3.1. 全体構成

全体のシステム構成を**エラー! 参照元が見つかりません。**に示す.本センター設備に加え附属学校コンピュータ設備も仕様に加え一括調達を行った.

3.2. クライアント PC

クライアント PC は Windows7 クライアント 396 台,Macintosh クライアント 60 台である.

Windows7 PC は Coreboot(NTT データ製)によるネットブート型シンクライアント（iSCSI ブート）であり,Macintosh PC は Xserve によるネットブート（Apple 社製）を採用した.両者アスペクト比 16:9 のワイドスクリーンを採用した液晶ディスプレイ一体型 PC である.(図-1)

図-1 クライアント PC

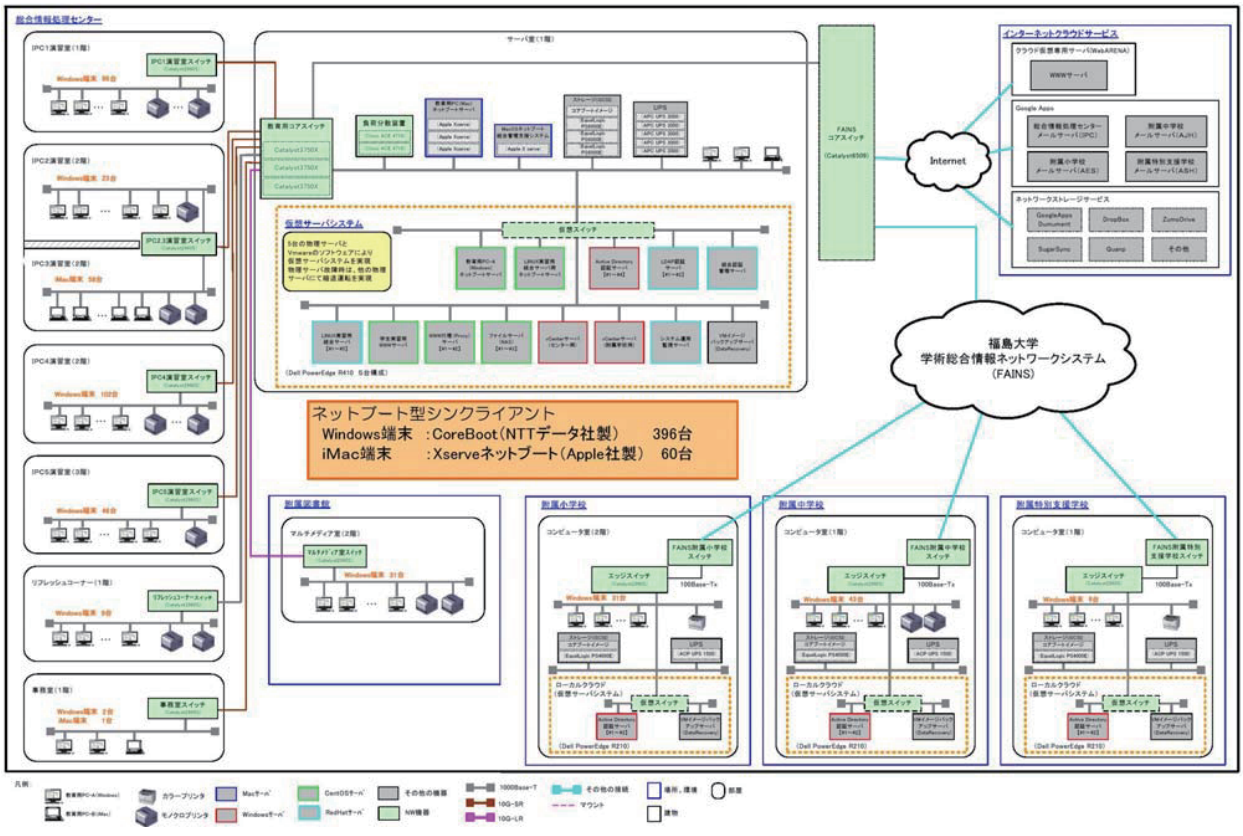
3.3. ネットワーク構成

ネットワークは,サーバを置くサーバ室とクライアント PC を設置する各演習室間を 10G Ethernet で接続し,各演習室ではクライアント PC を Gigabit Ethernet (1G)でスター型に接続している.スイッチは CISCO 社の Catalyst スイッチを採用した.

ただし,附属学校については,WAN(100M)経由で接続している.

ネットワーク論理構成は,運用系と管理監視系に分け独立して設計した.

運用系ネットワーク論理構成図を**エラー! 参照元が見**



つかりません。に示す.

クライアント IP ネットワークを演習室毎に分けず,全体として 1 つの IP ネットワークとして設計した.また,ネットブートシステムの高速性確保を優先し,ネットブートサーバ,NAS サーバおよび iSCSI ストレージをクライアントと同じ IP ネットワークに配置している.

また,サーバ用 IP ネットワークはセキュリティを考慮し,機能ごとに 3 つに分離した構成としている.

冗長性確保および負荷分散のため,複数台のサーバを負荷分散装置で負荷分散する構成としている.サーバは演習室クライアント以外の学内システムにサービスを提供するため,負荷分散装置は,演習室側とインターネット側に配置する構成としている.この目的では CISCO 社の ACE の仮想デバイス機能が有効であった.

管理監視系ネットワークは,安全に ssh,VMware,VNC 等のリモートメンテナンスおよび SNMP 監視を行うためのネットワークである.各サーバは原則として,運用用と管理監視用のネットワークインタフェースを持つ.

3.4. サーバ構成

実サーバ 9 台で構成している(表- 1,図- 1).

5 台の PC サーバでは VMware 環境を導入し 21 台の仮想サーバを運用している.(表- 2)

表- 1 実サーバー一覧表

サーバ機種名	台数	用途
Mac Xserve	4台	Macintosh netbootサーバ他
Dell PowerEdge R410	5台	VMware vSphere

表- 2 VMware 仮想サーバー一覧表

VMware仮想サーバ	台数	用途	OS等
Corebootサーバ	1	Windows7ネットブート	Linux,Coreboot
ActiveDirectory認証サーバ	4	Windows7認証	Windows Server 2008
LDAP認証サーバ	2	Linux,Macintosh認証	Linux,OpenLDAP
統合認証管理サーバ	1	Unicorn ID manager	Linux,Unicorn ID manager
WWW代理サーバ	2	WWW Proxy	Linux,Squid, DrWeb AV
ファイルサーバ(NAS)	4	ユーザファイル保存	Linux,samba
学生実習用WWWサーバ	1	WWW情報発信	Linux,apache
学生実習用Linuxサーバ	5	Linux実習用	Linux
システム運用監視サーバ	1	運用監視(Zabbix)	Linux, Zabicom

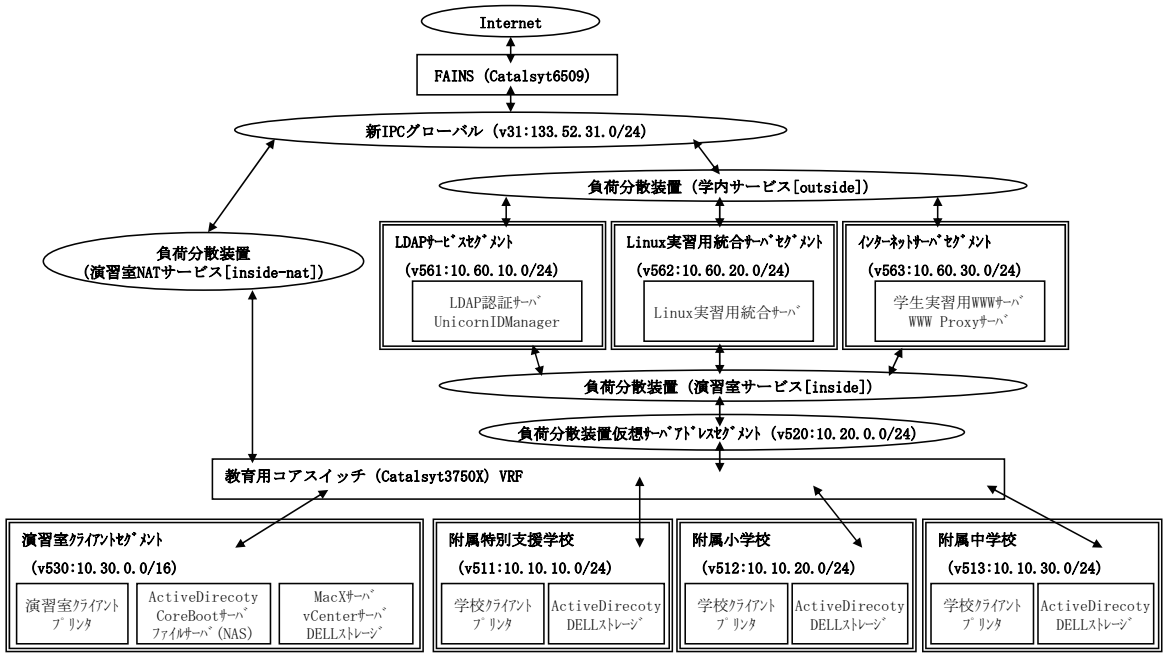
図- 2 サーバ設置状況

3.4.1. Mac X serve (4 台)

3 台を Macintosh ネットブートサーバ,1 台をネットブート管理サーバとして構築している.これらについては仮想化されていない.

3.4.2. Windows7 ネットブートサーバ(Coreboot)

Windows7PC がネットブートするための情報を提供するサーバである.OS イメージそのものは,iSCSI ストレージから直接転送されるので,このサーバがクライアント PC に転送するデータ量は小さい.附属学校クライアント



PC へのネットブート情報提供も行っている.

VMware に構成された仮想サーバである.

3.4.3. Active Directory 認証サーバ (4 台)

Windows7PC のドメイン認証,ユーザ認証を行う認証サーバである.DNS サーバ機能も担っている.

3.4.4. LDAP 認証サーバ(2 台)

学生実習用 WWW サーバ,学生実習用 Linux サーバのユーザ認証および Macintosh PC のユーザ認証を行うサーバである.

3.4.5. 統合認証管理サーバ(1 台)

OSStech 社製 Unicorn ID Manager により,管理者による Active Directory サーバ,LDAP サーバ,および GoogleApps にユーザアカウントおよびパスワードの同時登録,同時変更,同時削除が行えるほか,学生ユーザ自身によるパスワード変更機能を有している.

付加機能として,学生ユーザ向けにパスワードリマインダー用質問と解答情報登録機能,パスワード初期化機能,Windows プロファイル初期化する機能を提供しており,教員ユーザ向けに,臨時アカウント発行機能を提供している.

3.4.6. ファイルサーバ(4 台)

iSCSI ストレージをマウントし,samba により Windws7PC ユーザへファイル保存用領域を提供し,NFS により Macintosh PC および学生実習用 Linux サーバ,WWW サーバへファイル保存領域を提供している.

提供領域は,Windows7 用 2G, Macintosh 用 2G, Linux 用 2G を上限としている.各 OS 用の領域は重複させていない.

3.4.7. WWW 代理サーバ(2 台)

Squid による代理サーバ機能を提供している.

マルウェア検出遮断ソフトウェアを有しており,Squid と連携して動作する.Windows7PC および Macintosh PC はこのサーバを利用して,安全なインターネット利用が行える.このサーバは DNS キャッシュサーバ機能も有している.

3.5. メールシステム(Google Apps)

GoogleApps を採用し,ipc.fukushima-u.ac.jp ドメインで利用できるよう構成した.ユーザ名,パスワードについては,Unicorn ID Manager により,Windows Active Directory および LDAP サーバと同時登録・修正・削除する方法で同期が取られる.

ユーザ認証は本学の SSO 認証サーバに問い合わせるのではなく,GoogleApps に保存された情報で行われる.

Webmail としての利用だけでなく,pop3,imap での利用も可能となっている.

3.6. 学生実習用 Linux サーバ

Linux 実習については,5 台の学生実習用 Linux サーバを VMware 仮想サーバとして用意し,PC 端末から VNC クライアントソフトあるいは ssh クライアントを利用し,GUI あるいは CUI で利用できる環境を提供している.

負荷分散装置経由でこのサーバにアクセスするため,1 台のサーバに見えるため,学生は 5 台の実サーバを意識することなくサービスを利用することができる.

管理面においては,1 台にセキュリティ更新を実施することで,他の 4 台にも更新が行われるよう工夫されており,運用負担が軽減される.

3.7. WWW サーバ

WWW サーバについては,これまでの 1 台のサーバを総合情報処理センターの情報を発信するサーバと学生実習用のサーバに分離し,総合情報処理センター情報発信サーバはレンタルサーバを利用し,学生実習用 WWW サーバのみ,VMware 仮想サーバとして本センターで運用することとした.WWW サーバソフトとして Apache を利用し,NetCommons, Geeklog の CMS を導入した.

総合情報処理センターWWW サーバについては,仮想専用サーバ方式のレンタルサーバとして実現し,全学 DNS サーバとしても活用している.

4. ネットワークストレージサービス

クラウドサービスとして個人向けネットワークストレージサービスが提供されており,1-2GByte の容量を無料で提供しているサービスも多い.

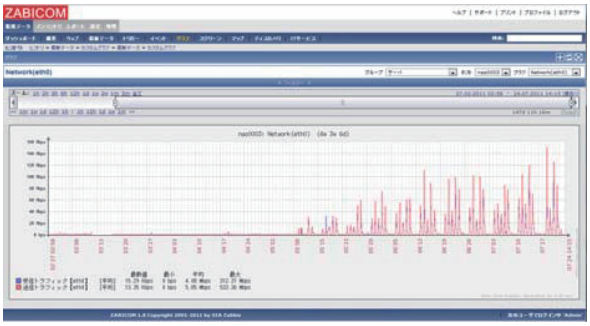
学生用に提供しているファイルサーバの保存領域は 2Gbyte であるが,保存領域が不足することも想定し,クライアント PC には,ネットワークストレージ用クライアントソフトを導入した.

学生が個人としてネットワークストレージサービスに利用登録を行うことで,クライアント PC からこのサービスが利用可能となり,容量不足の解決の他,自宅のパソコンとのデータ交換や,異なる OS とのデータ交換に有効に利用できると考えている.

5. 運用管理支援システム

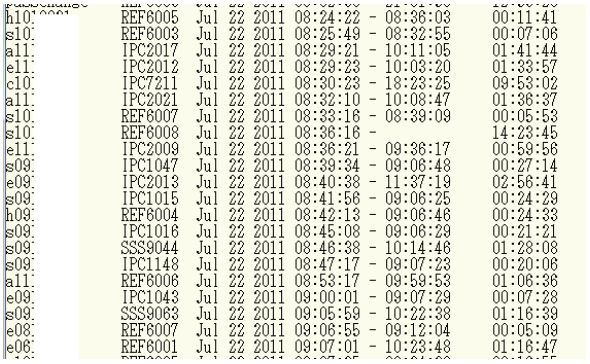
ネットワーク機器とサーバを同一のユーザインタフェースで監視するため,ZABBIX の商用版である ZABICOM 監視サーバを VMware 仮想サーバとして構築した.ZABICOM により,ネットワーク流量の他,サーバについては CPU 負荷,ディスクおよびメモリ利用状況把握が容易であり,設定値を超えた場合,メールで管理担当に通知することが可能である.

図-3 ZABICOM によるネットワーク流量監視



Windows7PC 利用については,Coreboot サーバログにログオン,ログアウト時刻情報が記録されるので,この情報を利用することで,PC 利用状況を容易に把握することができる.

図-4 Windows7PC 利用状況



h10	REF6005	Jul	22	2011	08:24:22 - 08:36:03	00:11:41
s10	REF6003	Jul	22	2011	08:25:49 - 08:32:55	00:07:06
a11	IPC2017	Jul	22	2011	08:29:21 - 10:11:05	01:41:44
e11	IPC2012	Jul	22	2011	08:29:23 - 10:03:20	01:33:57
c10	IPC7211	Jul	22	2011	08:30:23 - 18:23:25	09:53:02
a11	IPC2021	Jul	22	2011	08:32:10 - 10:08:47	01:36:37
s10	REF6007	Jul	22	2011	08:33:16 - 08:39:09	00:05:53
s10	REF6008	Jul	22	2011	08:36:16 -	14:23:45
e11	IPC2009	Jul	22	2011	08:36:21 - 09:36:17	00:59:56
s09	IPC1047	Jul	22	2011	08:39:34 - 09:06:48	00:27:14
e09	IPC2013	Jul	22	2011	08:40:38 - 11:37:19	02:56:41
s09	IPC1015	Jul	22	2011	08:41:56 - 09:06:25	00:24:29
h09	REF6004	Jul	22	2011	08:42:13 - 09:06:46	00:24:33
s09	IPC1016	Jul	22	2011	08:45:08 - 09:06:29	00:21:21
s09	SSS9044	Jul	22	2011	08:46:38 - 10:14:46	01:28:08
s09	IPC1148	Jul	22	2011	08:47:17 - 09:07:23	00:20:06
a11	REF6006	Jul	22	2011	08:53:17 - 09:59:53	01:06:36
e09	IPC1043	Jul	22	2011	09:00:01 - 09:07:29	00:07:28
s09	SSS9063	Jul	22	2011	09:05:59 - 10:22:38	01:16:39
e08	REF6007	Jul	22	2011	09:06:55 - 09:12:04	00:05:09
e06	REF6001	Jul	22	2011	09:07:01 - 10:23:48	01:16:47

6. 運用状況と評価

6.1. 東日本大震災の影響

3 月の運用開始後 4 ヶ月経過したが,3 月 11 日に東日本大震災が発生した.サーバへの影響は幸いなことにほとんどなかったが,クライアント PC の机からの落下による破損が多発した.ディスプレイ一体型の PC は重心が高いせいか,地震の際,机から落下しやすいようである.クライアント修理に 2 ヶ月以上の時間が必要であった.

6.2. ネットブート性能

Windows7,Macintosh とも電源投入後 90 秒程度で起動し,起動失敗はほとんどなく快適である.

附属学校クライアントは,本センターに設置された Coreboot サーバから WAN(100M)経由で起動用情報を得て現地設置の iSCSI ストレージから直接 OS イメージをダウンロードして起動するが,特に問題は発生していない.

6.3. ファイルサーバ性能

ファイルサーバについては若干の機能不足があり,ログオン時の遅延等が発生している.これらの不具合については,サーバへの割り当て資源の見直し等で改善できる見込みである.

6.4. 省エネルギー

仮想サーバ化およびクラウドサービス活用の目的の一つは,実サーバ削減による省エネルギー効果である.

講義開始後の 5 月および 6 月の本センターの使用電力については約 3 割の省エネルギーが達成できている.

表-3 電力使用量(単位 kWh)

年度	3月	4月	5月	6月
2010年	38,220	43,590	31,710	40,190
2011年	25,180	22,890	23,860	26,870

6.5. セキュリティ更新作業

Windows7PC についてはマイクロソフト社からの月例セキュリティ更新提供にあわせ実施している.

前システムのマルチキャストによるディスクイメージ配信作業は,ほぼ 1 週間の作業期間を要したが,ほぼ 1 日の作業に短縮されている.

7. おわりに

本センターは,技術職員が配置されておらず,専任教員 1 名と業務委託職員および本来技術が専門でない少数の事務職員とで協力しシステムの運用を行っている.そのような事情から,サーバ数を削減,運用負担の軽減による管理負担の軽減は,セキュリティ対策に手を抜けない状況をも考慮して必要なことであった.

そのような事情から,メールシステムのクラウド化が必要であったし,認証においては運用負担が大きい,SSO 認証サーバの構築・運用を回避し,認証情報はクラウド側

にも置く方式をとった.

3 月に大震災に見舞われたが,本センターが停電等で停止した場合でもメールが利用でき,情報発信が行える必要性を痛感したが,今回紹介したシステムは,この意味でも有効であると感じた.

8. 謝辞

新システムの基本仕様を策定するにあたり,見学の機会を提供いただき,また貴重なご意見をいただいた,群馬大学総合情報メディアセンターの皆様,学習院大学計算機センターの皆様に感謝いたします.

9. 参考文献

[1] http://www.coreboot.jp/ Coreboot ホームページ
[2] http://www.osstech.co.jp/product/unicorn Unicorn ID manager ホームページ
[3] http://www.zabbix.jp/ ZABBIX-JP ホームページ

横浜国立大学におけるネットワークトラフィック監視

Network Traffic Monitoring in Yokohama National University

志村　俊也
Toshiya Shimura

tshimura@ynu.ac.jp

横浜国立大学　情報基盤センター

Information Technology Service Center, Yokohama National University

概要

ネットワークトラフィック監視はネットワーク運用管理の基本業務の 1 つである。本学では、MRTG と RRDtool を利用し、学内各所のネットワークトラフィックを常時監視している。監視は 5 分平均の大局的なトラフィックを MRTG で行い、5 秒平均の瞬間(短時間平均)トラフィックを RRDtool で行っている。本稿では、学内の代表的な 3 つの監視ポイントにおける、5 分平均と 5 秒平均それぞれで得られたトラフィックの特徴について報告する。

キーワード

ネットワークトラフィック監視, MRTG, RRDtool

1. はじめに

学内ネットワークのトラフィック監視はネットワーク運用管理の基本業務の 1 つである。ネットワークトラフィックの振舞いを常時把握することにより、ネットワーク異常・障害・不正利用・不正通信の検知、及びその発生箇所・原因特定を速やかに行うことができる。このため、本学では、学内各箇所のネットワークトラフィックを常時監視している。監視ポイント総数は 1141 箇所であり、学内各建物のネットワークトラフィックに関しては各フロアまでの送受信トラフィックを、サービスサーバ群に関しては、各サーバの送受信トラフィックを監視している。

トラフィック監視に利用しているのは、フリーソフトウェアの Multi Router Traffic Grapher (MRTG) と Round Robin Database Tool (RRDtool) である。 MRTG は、5 分平均のトラフィックを 1 ピクセルとして過去 400 ピクセル分(33 時間 20 分) のトラフィックを 1 つのグラフとして可視化するソフトであり、学内各所のネットワークトラフィックの約 1 日分の振舞いを一目で把握することができる。このため、ネットワーク異常・障害・不正利用・不正通信の検知、及びその発生箇所・原因特定を行う上で、この MRTG で得られた 5 分平均のグラフが非常に役に立つ。

RRDtool も MRTG 同様にトラフィックの時間的な推移を 1 つのグラフとして可視化するソフトである。RRDtool には MRTG が持つグラフ自動作成機能は搭載されていないので、利用者側でグラフ作成スクリプトを作成しなくてはならないが、取得するトラフィックの平均時間を 1 秒まで下げることができるという利点がある。

このため、MRTG では得ることができない瞬間（短時間平均）トラフィックを把握することが可能であり、MRTG 同様にトラフィック監視の強力なツールとなっている。

実際のトラフィック監視においては、1141 箇所全てに対して MRTG(5 分平均)による監視を行い、かつ、その中でも瞬間トラフィックを把握する必要がある最重要監視ポイント(SINET との接続点やコアスイッチ内の各ポート等)に対しては、MRTG に加えて RRDtool による瞬間トラフィックの監視も行なうという方法をとっている。RRDtool で監視するトラフィックの平均時間については、短く取り過ぎるとネットワーク機器が受ける SNMP アクセス負荷が大きくなり、またグラフ全体の表示時間が短くなってしまう。このため、本学では 5 秒平均の値を 1 ピクセルとして、過去 800 ピクセル分(約 1 時間) のトラフィックを 1 つのグラフとして表示するように設定している。

本稿では、最重要監視ポイントの内、代表的な 3 箇所を例に挙げて、MRTG (5 分平均)と RRDtool (5 秒平均)それぞれで監視したトラフィックの特徴について報告する。

2. トラフィック

本稿で紹介するトラフィック監視ポイントのネットワーク上の配置を図-1 に示す。

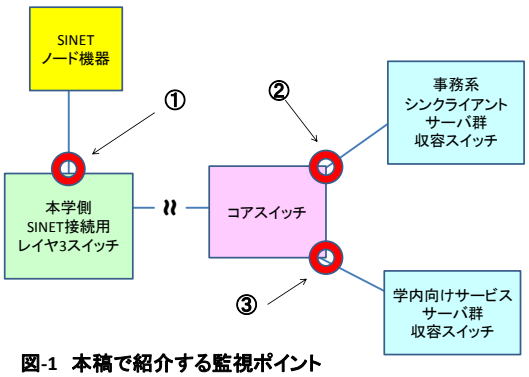


図-1 本稿で紹介する監視ポイント

図-1 中の◎で示した箇所、具体的には、

① SINET ノード機器←→本学側 SINET 接続用レイヤ 3 スイッチ
② コアスイッチ←→ 事務系シンクライアントサーバ群収容スイッチ
③ コアスイッチ←→ 学内向けサービスサーバ群収容スイッチ

の 3 箇所のトラフィックの特徴を以降の章で説明する。

なお、以降で出てくる図-2～図-4 において、MRTG のグラフの時間推移方向は、『右→ 左』であり、RRDtool のグラフの時間推移方向は、『左→右』であることを注記しておく。(MRTG と RRDtool では時間の推移方向が逆になっていることに注意して頂きたい。)

2.1. SINET ノード機器←→本学側 SINET 接続用レイヤ 3 スイッチ 間のトラフィック

本学は SINET ノード校であり、SINET 側の設備が本学情報基盤センター内に設置されている。そのため、SINET ノード機器に対して、民間のキャリア回線を使用せずに直接 1000BASE-T で接続することが可能となっている。図-2 は、『SINET ノード機器 ←→本学側 SINET 接続用レイヤ 3 スイッチ』間のトラフィックである。上が 5 分平均(MRTG) 、下が 5 秒平均(RRDtool) のトラフィックを示している。5 分平均のトラフィックは 2011 年 7 月 19 日 23 時 ～7 月 21 日午前 9 時のものである。5 秒平均によるトラフィックは、 上記の時間帯の 7 月 20 日 15 時 10 分 ～ 16 時 10 分の間の詳細トラフィックを示している。 グラフより、学内への受信トラフィックが学外への送信トラフィックよりも圧倒的に多いのがわかる。これは、通信の大部分が ウェブアクセスによる学外から学内へのデータ・コンテンツのダウンロードであることを示している。学内への受信トラフィック量は、午前 6 時前後が最少であり、その後、時間とともに増加していき、12～17 時にかけて最大となり、その後次第に減少するという振る舞いとなっている。教職員・学生が学内で行う各種業務（教育・研究・事務）とほぼ同じリズムでトラフィックが増減しているのがわかる。 MRTG(5 分平均)による監視では、トラフィックの最大値は 28MB/s (224Mbps)程度であるが 、RRDtool (5 秒平均)による監視では、それを上回る 40～50MB/s (320～400Mbps)が計測されており、SINET との接続帯域(1Gbps) が有効に活用されていることが RRDtool によって明確に示されている。

2.2. コアスイッチ ←→ 事務系シンクライアントサーバ群収容スイッチ 間のトラフィック

本学の事務系職員用 PC の大部分は、ネットブート型シンクライアント PC である。シンクライアント PC の総数は 400 台であり、 事務局庁舎、学務部庁舎、各部局の事務棟など学内各所に配置されている。ネットワーク的には、24bit のグローバルサブネット 3 個を使用し、ブートサーバと PC を同一サブネットに収容し、ブートサーバ←→PC 間通信はルーティングせずに行なえる構成

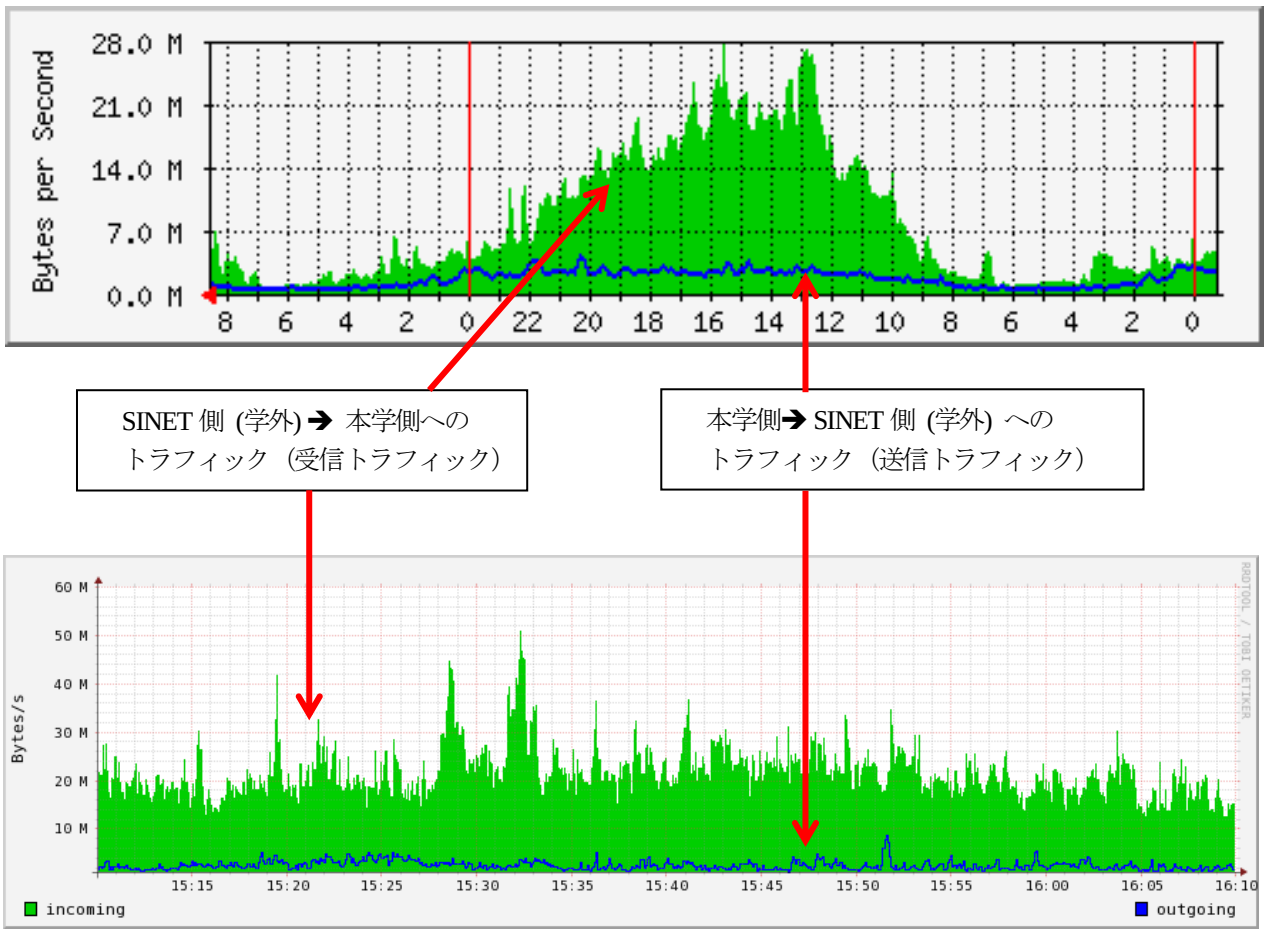


図-2　『SINET ノード機器 ←➔本学側 SINET 接続用レイヤ 3 スイッチ』間のトラフィック。
上図が 5 分平均 (MRTG) 、下図が 5 秒平均 (RRDtool) のトラフィックを示す。

としている。PC400 台の内 239 台は、毎起動時にブートサーバから OS のイメージ配信を受ける標準型ネットブートであるが、残り 161 台は、初回のイメージ配信を受けた後、利用したイメージを PC 側の内蔵 HDD にキャッシュし、2 回目以降の起動は差分イメージだけが配信される ReadCache 型ネットブートである。ブートサーバ群は、標準型 6 台と ReadCache 型 4 台で構成されている。

図-3 は標準型ネットブートのサーバ群 6 台が収容されている『シンクライアントサーバ群収容スイッチ←➔コアスイッチ』間のトラフィックを示す。上が 5 分平均 (MRTG)、下が 5 秒平均 (RRDtool) のグラフである。5 分平均のトラフィックは、2011 年 7 月 13 日 午前 6 時 ～ 7 月 14 日 15 時 のものである。5 秒平均のトラフィックは、上記の時間帯の 7 月 14 日 午前 8 時 05 分～9 時 05 分の詳細トラフィックを示している。5 分平均のグラフからわかるように、事務系職員が出勤する午前 8 時 30 分前後に『収容スイッチ➔ コアスイッチ』に対して非常に多くのトラフィックが出ている。これは、出勤した事務系職員が、自身の利用する PC を次々と起動し、ブートサーバ群から集中的に OS イメージの配信が行われるためである（配信されるイメージは PC1 台あたり約 50MB）。ブートサーバ群からのトラフィックの最大値は、MRTG の 5 分平均では約 56MB/s (448Mbps) 程度であるが、RRDtool による 5 秒平均値では、約 110MB/s (880Mbps) まで達しており、帯域上限値である 1Gbps 近くまで利用されていることがわかる。なお『コアスイッチ➔収容スイッチ』方向のトラフィックは『収容スイッチ➔ コアスイッチ』のトラフィックに比べて非常に小さいため、グラフ上には表れていない。

2.3. コアスイッチ ← ➔ 学内向けサービスサーバ群収容スイッチ間のトラフィック

学内向けサービスサーバ群収容スイッチ配下には、全学教職員・学生(約 13,000 人)を対象とした各種サービス提供サーバ群が接続されている。具体的には、DNS サーバ 4 台、認証サーバ(Active Directory, LDAP, Radius) 4 台 、

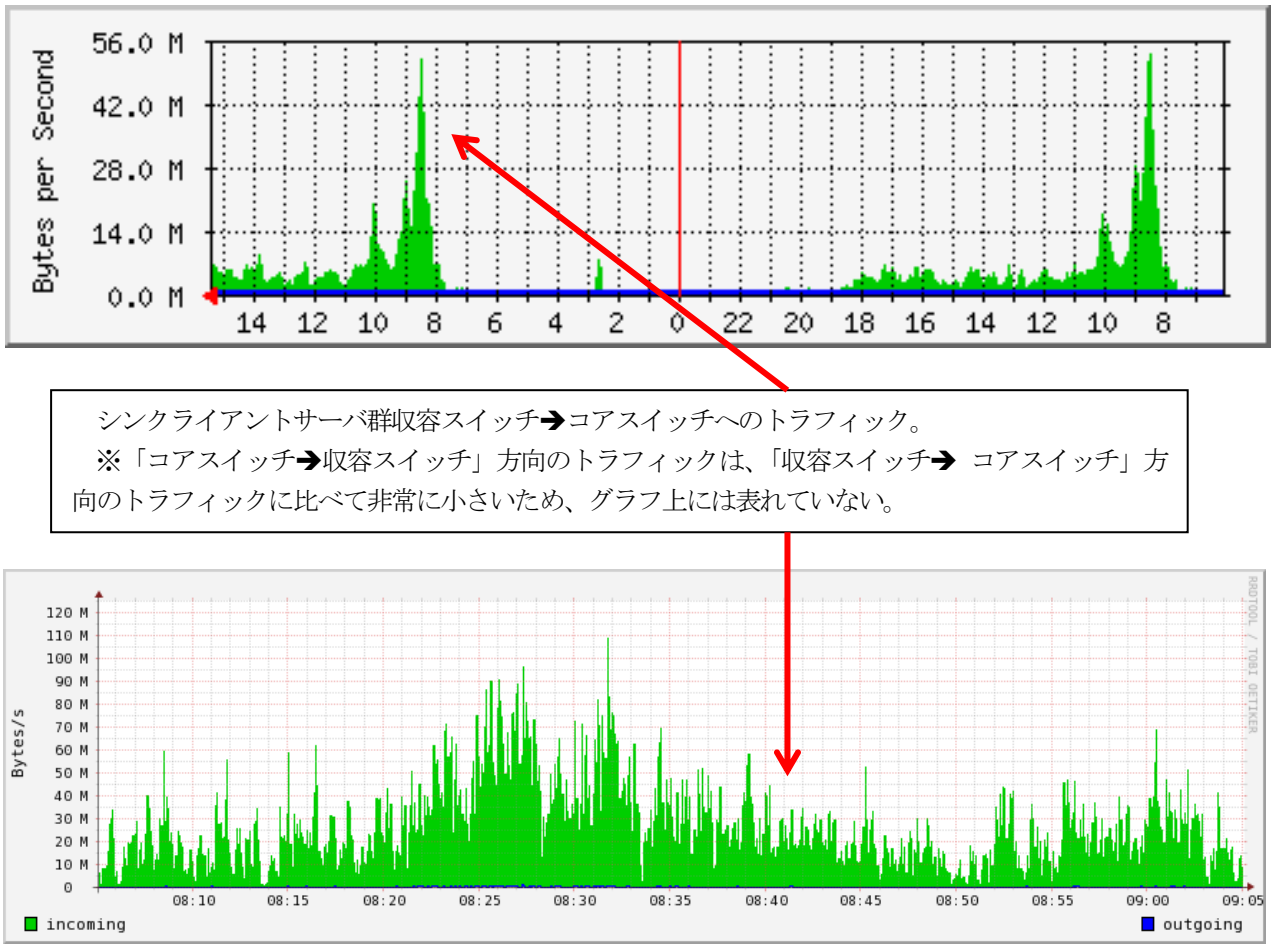


図-3　『シンクライアントサーバ群収容スイッチ➔➔ コアスイッチ』間のトラフィック。上図が 5 分平均(MRTG) 、下図が 5 秒平均 (RRDtool) のトラフィックを示す。

メールサーバ 1 台、メール中継サーバ(学外から配信されてくるメールを一旦受信し、メールサーバに受け渡すサーバ)1 台、ウェブメールサーバ 1 台 、メーリングリストサーバ 1 台である。

図-4 に示すのは、『コアスイッチ➔➔ 同サーバ群収容スイッチ』間のトラフィックである。上が 5 分平均(MRTG)、下が 5 秒平均(RRDtool)のグラフである。MRTG のトラフィックは、2011 年 7 月 25 日午前 4 時 30 分～7 月 26 日 13 時 50 分の間のトラフィックである。RRDtool によるトラフィックは、上記の時間帯の 7 月 26 日午後 12 時 45 分～13 時 45 分の間の詳細トラフィックを示している。MRTG(5 分平均)で計測した『サーバ群収容スイッチ➔ コアスイッチ』のトラフィックの振舞いとしては、午前 2 時～6 時の間は量的には非常に少なく、午前 6 時以降から徐々に増加し、業務時間帯である午前 9 時～18 時の間は、平均して 500 kB/s (4Mbps) 前後のほぼフラットな形状となり、その後徐々減少するという特徴を示している。一方、RRDtool (5 秒平均)で計測した業務時間帯のトラフィックでは、1～2MB/s (8～16Mbps) 程度のショット状のトラフィックが多数計測されており、MRTG(5 分平均)によって表示されているフラット形状とは様相が異なっていることがわかる。

MRTG(5 分平均)で計測した『サーバ群収容スイッチ➔ コアスイッチ』方向のトラフィックの内訳は、DNS サーバの寄与が 4 台で 30kB/s 程度、 メーリングリストサーバの寄与が 10kB/s 程度であり、残りの大部分がメールサーバとウェブメールサーバによるものである。認証サーバ 4 台の寄与は無視できるほど小さい。メール中継サーバは、メールサーバに対する学外からの SMTP 接続のゲートウェイサーバとして機能するため、『サーバ群収容スイッチ➔コアスイッチ』へのトラフィックには寄与しない。

『コアスイッチ➔サーバ群収容スイッチ』の業務時間時間帯のトラフィックが概ね 300kB/s 程度であるのに対して、『サーバ群収容スイッチ➔ コアスイッチ』のトラフィックが 500kB/s 程度となっているのは、『コアスイッチ➔ サーバ群収容スイッチ』の通信が、「学内 PC からメールサーバへの SMTP 接続」と「ウェブメールサーバ

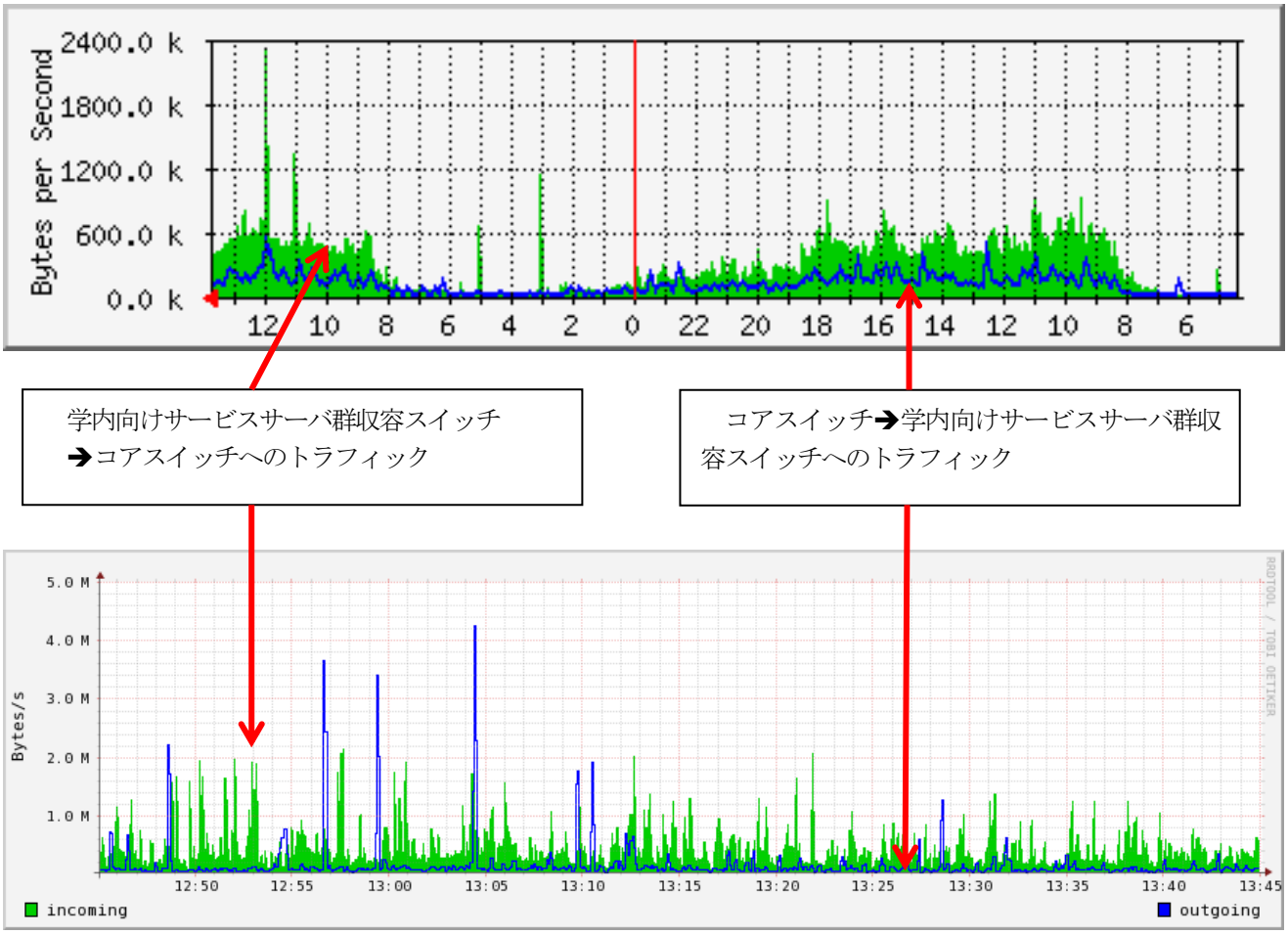


図-4 『学内向けサービスサーバ群収容スイッチ←→コアスイッチ』間のトラフィック。上図が 5 分平均 (MRTG) 、下図が 5 秒平均 (RRDtool) のトラフィックを示す。

に対する HTTPS 経由でのメール送信」によるものが主であるのに対して、『サーバ群収容スイッチ ➔ コアスイッチ』の通信は、学内 PC のウェブメールサーバに対するウェブアクセスによって発生するウェブコンテンツ（ウェブメールサーバへのログイン画面、ログイン後の受信メール一覧画面等）のダウンロードが主であることに起因する。本学では、事務系職員の場合、メールの送受信はウェブメールを利用する決まりとなっている。学生・教員の場合は、そのような制限はないが、それでも、多くの利用者がウェブメールを利用している。このため、業務時間帯のウェブメールサーバへのアクセスは大変多く、ウェブメールサーバからウェブコンテンツが頻繁にダウンロードされる。その結果として、5 分平均の MRTG のグラフにおいて、常時 500kB/s 程度のトラフィックが計測されているのである。

3. 終わりに

本稿では、本学のネットワークトラフィック監視の現状について代表的な監視ポイント 3 箇所を例に挙げて紹介した。MRTG と RRDtool の双方を利用することで、大局的(5 分平均)及び瞬間(5 秒平均)トラフィックをリアルタイムに把握できるようにしているため、学内ネットワーク管理上、非常に役に立っている。

なお、本稿では説明を省略したが、本学のネットワーク監視において、測定可能な機器に対しては、トラフィックだけでなく、CPU 使用率、メモリー使用量、接続セッション数も MRTG で監視している。また別のソフトウェアを利用して、全機器に対する死活監視も行っている。ネットワーク異常・障害の検知の際には、トラフィックだけでなく、これらの情報を総合して、発生箇所・原因の特定を行っている。本学の取り組みが他大学の参考になれば幸いである。

岡山大学における認証・ロケーションフリーネットワークの構築

Construction of Location-free Network with Authentication in Okayama University

岡山 聖彦, 山井 成良, 大隅 淑弘, 河野 圭太, 藤原 崇起, 稗田 隆

Kiyohiko Okayama, Nariyoshi Yamai, Yoshihiro Oosumi, Keita Kawano, Takaoki Fujiwara, Takashi Hieda

{okayama,yamai,oosumi,keita,hieda-t}@cc.okayama-u.ac.jp
fujiwara-t4@adm.okayama-u.ac.jp

岡山大学情報統括センター
Center for Information Technology and Management, Okayama University

概要

岡山大学では，2009 年度に旧キャンパス情報ネットワークを更新し，2010 年 6 月から新ネットワーク (ODnet2010) の運用を開始した．ODnet2010 では，ネットワークの高速化・高信頼化に加え，新機能としてフロアスイッチにおけるネットワーク認証とロケーションフリー (認証 VLAN) 機能を導入している．本稿では，セキュアネットワークへの移行の第一段階として構築した，「生活系ネットワーク」と称する認証・ロケーションフリーネットワークについて報告する．生活系ネットワークは，本学の全構成員が利用可能な共通的なネットワークであり，主に講義室や会議室などの共用スペースでの利用を想定している．

キーワード

認証スイッチ, ロケーションフリー, Web 認証, MAC アドレス認証

1 はじめに

岡山大学 (以下，本学という) では，キャンパス情報ネットワークを更新し，2010 年 6 月から新ネットワーク (以下，ODnet2010 という) の運用を開始した．

旧ネットワークは 2002 年 1 月から稼働を開始したものであるが，導入から 8 年が経過して老朽化が進み，ネットワーク機器の故障が頻発するようになっていた．また，旧ネットワークは基幹 1Gbps・支線 100Mbps のネットワークであるが，クライアント PC のネットワークインタフェースがギガビット化し，上位の SINET が 10Gbps 化しようとしている状況では，教育研究を支えるインフラとしての性能不足も懸念されるようになってきた．さらに，旧ネットワークは基本的にグローバル IP アドレスで運用しており，ネットワーク機器が認証機能を持たないため，ネットワークの不正利用や学外からの攻撃に対して無防備であることも問題であった．

このような状況を受け，ODnet2010 では，以下に示す 4 つの目標を掲げて導入を進めた．

1. ネットワークの高速化
2. 信頼性の向上
3. セキュリティの強化
4. 利便性の向上

これらのうち，ネットワークの高速化と信頼性の向上については物理的な特性であり，基幹に 10GbE（支線は 1GbE）を導入し，さらに，ネットワーク機器および回線の冗長化を図っている．

また，セキュリティの強化については，機器をネットワークに接続する際の認証機能を備えたフロアスイッチや，仮想網によるネットワークの分割機能を持つコア

スイッチなど，不正利用を防止とセキュリティインシデントの局所化が可能な機器を導入した．一方，セキュリティの強化はユーザから見ると利便性の低下に繋がるため，本学で導入している統合認証基盤システムとの連携による認証 VLAN 機能や，SSL-VPN サーバの導入により，学内外を問わずロケーションに依存しないアクセス環境の実現を目指した．

フロアスイッチを利用したネットワーク認証機能およびロケーションフリー機能の導入は，本学では初の試みである．ネットワークに接続する際に，ユーザ名およびパスワードの入力が必要であったり，事前に MAC アドレスを登録する必要があったりするなど，従来の利用方法と大きく異なるため，各部局が使用する従来のネットワーク（以下，既設研究系ネットワークという）に全面展開しようとすると，大きな混乱が生じる可能性がある．このため，我々は，本学の構成員全員が利用可能な (共通的な) ネットワークを用意して，講義室や会議室などの共用スペースと，当センターが管理する全学無線 LAN に適用すること移行の第一段階とした．このネットワークは，ある程度の制約があっても，メールや WWW などの一般的なサービスを安心・安全に利用することを想定したものであり，研究のために自由度の高い環境を用意するものではないことから,「生活系ネットワーク」と称している．

一方，生活系ネットワークの適用場所として共用スペースを選んだのは，旧ネットワークでは必ずしも共用スペースの情報コンセントが活用されていなかったためである．旧ネットワークでは，部局からの要望に応じて，建物の各居室のみならず多くの共用スペースにもフロアスイッチからの事前配線（以下，情報コンセントという）を施している．共用スペースの情報コンセントは部局管理としたが，これを教職員や学生などに安全に利用させようとすると，別途認証システムの導入が必要となるなど，情報コンセント活用の妨げとなっていた．このような情報コンセントに対して生活系ネットワークを適用すれば，クライアント PC の接続時にフロアスイッチで認証を行うため，部局から見て余計なコストをかけることなく共用スペースの情報コンセントを利用者に開放することができる．

以下，本稿では，ODnet2010 の概要について述べた後，我々が構築した生活系ネットワークと，構築にあたって生じた技術的課題とその解決策について述べる．

2 ODnet2010 の概要

ODnet の物理構成を図 1 に示す．この図に示すように，ネットワークの高速化に関しては，基幹ネットワーク（コアスイッチ・建物集線スイッチ間，コアスイッチ・データセンタースイッチ間および津島・鹿田キャンパスコアスイッチ間）は 20Gbps （10Gbps × 2 回線），建物内のフロア間（建物集線スイッチ・フロアスイッチ間）は 2Gbps（1Gbps × 2 回線），フロア内の支線ネットワーク（フロアスイッチ以降）は 1Gbps の帯域を確保した．また，信頼性の向上に関しては，コアスイッチの筐体内モジュールの二重化，建物集線スイッチの二重化，基幹ネットワークおよび建物内のフロア間での回線二重化により，主要箇所での単独故障に耐えうる構成になるように設計を行った．

フロアスイッチはいわゆる認証スイッチであり，Web 認証，MAC アドレス認証，IEEE802.1X 認証の機能を有する．Web 認証は主として利用者が接続する端末を認証する場合に用いる．この場合，利用者名としては「user-ID」あるいは「user-ID@VLAN-ID」の形式を用いることができ，前者の場合には標準の VLAN （多くの利用者に対しては生活系 VLAN），後者の場合には指定された VLAN（選択可能な VLAN は利用者毎に異なる）に接続される．一方，MAC アドレス認証はサーバやプリンタなど Web 認証を行えない機器を認証する場合に用いる．この場合には MAC アドレス毎に指定された VLAN に接続される．なお，現時点では IEEE802.1X 認証は利用していない．

3 生活系ネットワークの構築

3.1 旧キャンパスネットワークの問題点

以前のキャンパスネットワーク OUnet3 では，VLAN 機能こそ利用可能であったが認証機能はなく，また VLAN（サブネット）単位で部局に管理権限を委譲していたため，以下に示すような様々な問題が生じていた．

- 各部屋に設置されている情報コンセントに任意の機器を接続して利用できるため，部外者が施錠されていない部屋に侵入し，無断でネットワークを使用する場合があった．
- 無断使用を防ぐためには VLAN 管理者が認証機器を導入する必要があり，導入コストや管理コストの面で普及が進まなかった．特に，共用スペース（講義室や会議室など）の情報コンセントは部局が管理しており，その多くが事実上利用できないように設定されていた．
- 誰が，いつ，どこから，どのような端末を利用しているかを把握することが困難であったため，インシデントが発生した場合に IP アドレスからトラブル発生源となった端末を特定するのにかなりの時間を要した．

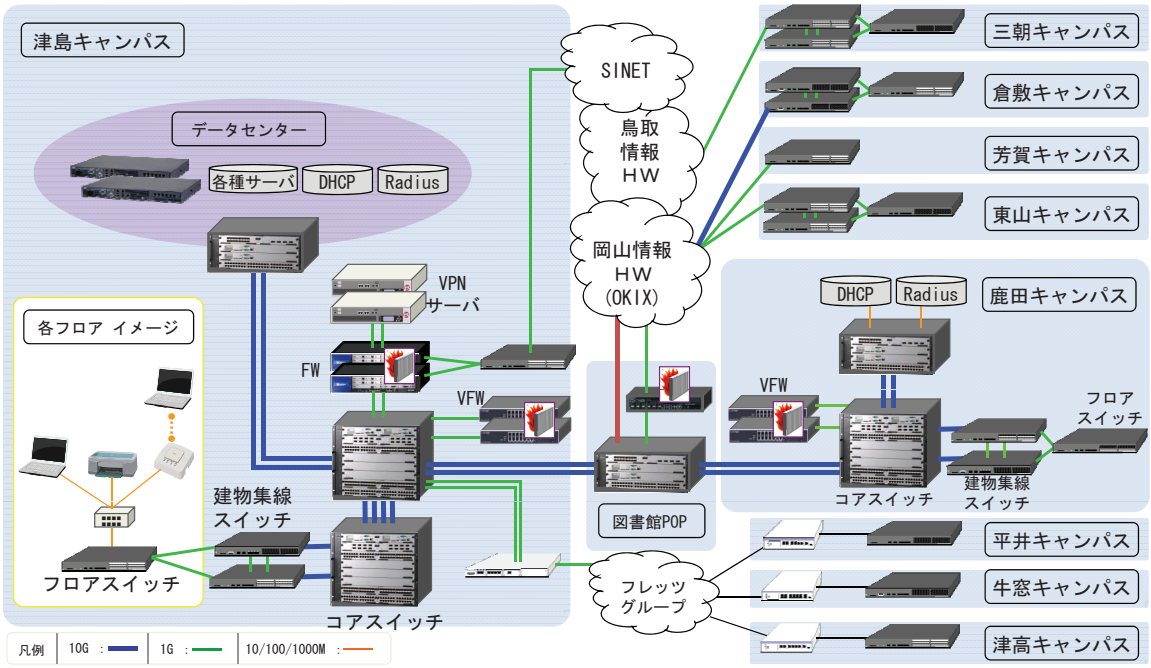


図- 1: ODnet2010 の物理構成

- 基本的に各サブネットにはグローバル IP アドレスを配布していたため，学外から利用者端末に直接アクセスすることができ，ファイアウォール機器があるとはいえ攻撃の対象になっていた．
- 外部からの攻撃に対する安全性を高めるため，部局が独自に NAT ルータを導入してプライベート IP アドレスで運用する場合が増加した．その結果，インシデントが発生した場合に IP アドレスからトラブル発生源となった端末を特定することがさらに困難になった．

これらの問題は，特に管理者がそれほどネットワークに精通していない部局では顕著であり，しばしば問題を引き起こしていた．

3.2 生活系ネットワークの設計

前節で述べた問題点を解決するために，ODnet2010 では新たに生活系ネットワークを構築することにした．生活系ネットワークはプライベート IP アドレスで運用し，IP アドレスは DHCP で自動的に割り当てられる．したがって，生活系ネットワークは部局のネットワーク管理者が関与することなく利用できるようになっている．部局のネットワーク管理者の唯一の役割は，どの部屋で生活系ネットワークを利用できるようにするかを決定することである．

生活系ネットワークでは 10.0.0.0/8 のプライベート IP アドレス空間を用い，次の 4 つのカテゴリーのネットワークを用いている．

- 教員用ネットワーク
- 学生用ネットワーク
- ゲスト用ネットワーク
- 学内共通ネットワーク

これらのうち，教員用ネットワーク，学生用ネットワーク，およびゲスト用ネットワークでは Web 認証が必要で，アクセス可能範囲をキャンパスネットワーク管理者がカテゴリー単位で設定できるようになっている．また，これらのカテゴリーでは利用者の身分および所属により認証後に接続される VLAN が決定されるようになっている．したがって，IP アドレスを見ればサーバではクライアント PC 利用者の所属を判別でき，サーバ側で所属に応じた細かなアクセス制御を行うことができる．

従来の OUnet3 では部外者向け情報コンセントシステム [1] を用い，部外者に対する学内限定情報へのアクセス制御機能を提供していた．これに対して，ODnet2010 では同様の機能をネットワーク側で提供し，生活系ネットワークが利用できる部屋であればどこでも同様のサービスを提供できるようになっている．ただし，従来の部外者向け情報コンセントシステムではクライアント IP アドレスが学内用（150.46.0.0/16）かどうかで学内からのアクセスかどうか判定していたため，サーバの設定は原則として変更する必要がなかったが，ODnet2010 ではどのプライベート IP アドレスがどの身分・所属に対応しているかをサーバ管理者が把握し，適切なアクセス許可範囲になるように設定を変更する必要がある．

一方，学内共通ネットワークはサーバやプリンタなど，Web 認証が困難な機器を収容するもので，MAC アドレス認証を用いる．このネットワークでは接続される機器に応じた VLAN が提供され，たとえばプリンタが接続されている VLAN ではプリンタとは無関係の通信が制限されるなど，機器に応じたアクセス制御が行われる．

4 構築にあたっての課題と解決方法

ODnet2010 の構築にあたり，特に生活系ネットワークが関連する課題がいくつか発生した．本章では主要な課題とその解決方法について述べる．

4.1 ループ検知設定に伴う通信障害

ODnet では生活系ネットワークとして多数の VLAN がキャンパス全体で利用されているため，一部の VLAN でループ接続が発生すると影響がネットワーク全体に波及する可能性が高い．そのため，STP (Spanning Tree Protocol) 等を用いたループ検知機能を活用する必要がある．

ところが，当初の設定では全てのレイヤ 2 スイッチにおいて全ての VLAN に対するループ検知機能を有効化していたため，（レイヤ 2 スイッチ台数× VLAN 数）分のループ検知フレームが全てのレイヤ 2 スイッチに伝送されるようになっていた．その結果，各レイヤ 2 スイッチでは大量のループ検知フレームにより帯域が圧迫されるだけでなく，これらのループ検知フレームの MAC アドレスが全て FDB(Forwarding Database) に登録され，他の端末の MAC アドレスが FDB に登録されなくなり，通信が不安定になる現象が発生した．

この問題に対処するため，我々は当初目標としていた任意箇所でのループの検知を断念し，同一フロアスイッチ内での検知のみを行うように設定した．これにより，ループ検知フレームが他のレイヤ 2 スイッチに中継されないようになり，FDB のオーバフローを抑えることができた．なお，複数のレイヤ 2 スイッチ間を跨ぐループの検知については，STP の代わりにストームコントロール機能を用いて実現している．

4.2 VLAN の切替え

ODnet2010 では前述のように「user-ID@VLAN-ID」の形式で利用者名を指定すると標準以外の VLAN に接続することができる．この機能を有効に活用するには，現在使用している VLAN との接続を一旦終了する機能（ログアウト機能）が必要になる．

ODnet2010 で導入したスイッチでは標準でログアウト機能を有しているため，当初はこの機能をそのまま利用する予定であった．ところが，この機能を利用するには，現在接続している VLAN 内でアクセスできる IP アドレスをスイッチが持つ必要があるにも関わらず，1 台のスイッチで指定できる IP アドレス数に制限があったため，全ての VLAN に IP アドレスを持たせることは不可能であった．

そこで，我々はログアウト専用の Web ページを別に提供することにした．ログアウト処理は以下の手順で行われる．

1. クライアントの IP アドレスをもとに，レイヤ 3 スイッチの ARP テーブルを検索してクライアントの MAC アドレスを特定する．
2. 認証ログをもとに，クライアントが接続されているレイヤ 2 スイッチを特定する．
3. クライアントが接続されているレイヤ 2 スイッチに管理者権限で接続し，当該クライアントの認証を強制的に無効化する．

また，これとは別に，クライアント側ではこれまで割り当てられていた IP アドレスを解放して認証用 VLAN 用の IP アドレスを新たに取得する必要がある．これには利用者側の操作が必要となるが，これを行うプログラムをログアウト用ページで提供し，事前にダウンロードできるようにしている．

4.3 Web 認証と MAC アドレス認証の併用

生活系ネットワークでは特に必要ではないが，研究系ネットワークの中には Web 認証や MAC 認証では不十分で，より強力な認証を必要とするものがある．これは，単なる Web 認証ではパスワードの漏洩に耐性がなく，また単なる MAC アドレス認証では端末を誰が使用したか特定できないためである．そこで，Web 認証と MAC アドレス認証の両方に成功した場合に限りネットワークアクセスを認める認証機構を一部の研究系ネットワークに導入するようにした．

ODnet2010 で導入したレイヤ 2 スイッチではこのような認証（多段認証）に対応できない[1]ことから，我々は認証システムに一部修正を加えてこの機能を実現した．このようなネットワークに接続可能な端末は MAC アドレスの事前登録時に接続先として特別な VLAN を割り当てる．この VLAN は実在しないものであり，結果として MAC アドレス認証には失敗して Web 認証に移行するが，その際に端末の MAC アドレスが認証シス

[1] 最近のレイヤ 2 スイッチでは対応済み

テムに通知される．その後，接続先 VLAN が多段認証を必要とするものであれば，Web 認証時に認証システムが MAC アドレスの照会を行い，接続の可否を決定する．

5　まとめ

本稿では岡山大学新キャンパスネットワーク ODnet2010 において新たに導入した「生活系ネットワーク」の構築方法に関して報告した．生活系ネットワークはキャンパス内のどこからでもアクセスが可能なネットワークであり，身分や所属に応じたキャンパスワイドの VLAN を構成することにより実現している．2011 年 7 月 14 日現在，フロアスイッチのポート数で 501 個のポートが生活系ネットワークに移行しており，これは使用済みポート数の約 1 割にあたる．今後は生活系ネットワークへの移行を進めるとともに，旧研究系ネットワークの移行も順次進めていきたい．

参考文献

[1] 山井成良, 岡山聖彦, 木澤政雄, 土居正行, 河野圭太, 大隅淑弘: 部外者からの組織内限定サービスへのアクセスを保護する LAN アクセス制御システム, 情報処理学会論文誌, vol.48, no.4, pp.1573–1583 (2007-04).

信州大学認証ネットワーク「セキュアネット 2010」における認証スイッチの拡張と整備

Expansion of the Authentication Switch for Shinshu University User Authentication Network System “Secure-Net 2010”

鈴木　彦文†，永井　一弥†，浅川　圭史†，今井　美香†，不破　泰†
Hikofumi SUZUKI†, Kazuya NAGAI†, Yoshifumi ASAKAWA†,
Mika IMAI†, Yasushi FUWA†

h-suzuki @shinshu-u.ac.jp, kznagai @shinshu-u.ac.jp, asakawa @shinshu-u.ac.jp,
mika_imai @shinshu-u.ac.jp, fuwa@shinshu-u.ac.jp

†信州大学総合情報センター
† Shinshu University Integrated Intelligence Center

概要

信州大学では平成 12 年より光回線を用いた Gigabit Ethernet ネットワークを構築してきた. そして 2004 年に本学全域に対してユーザ認証可能な認証ネットワークシステムとして「信州大学セキュアネット 2004」を構築した．本ネットワークシステムは Private IP Address と NAT をベースとし，Web 認証システム，統合認証システム，ポータルサイトと連動する認証ネットワークシステムである．その後，マルウェア，P2P 対応，不正なアクセスを行ったユーザの特定，ネットワークの利用を前提とした学生ノート PC 購入など，認証ネットワークに対する大幅な機能追加と性能向上が要望された．これらに対応するため新認証ネットワークシステムとして「セキュアネット 2010」を構築し 2010 年 4 月より運用を開始した．本ネットワークシステムにより，安全性の高い認証ネットワークを大規模化させるだけでなく，本学におけるセキュリティ上の対応や，ユーザ個々の追跡など高度な分析や制御が可能となった．しかしながら，一部において大量のユーザが同時に認証ネットワークへ接続し認証を行った場合に障害が発生した．これに対応するための方法を述べる．

キーワード

認証ネットワーク，セキュリティ，ユーザ挙動監視，ネットワーク構築運用管理

1. はじめに

信州大学は全学で利用可能な認証ネットワークとして「セキュアネット 2004」を構築し運用してきた．「セキュアネット 2004」では Class B 程度のネットワークに関してゲート認証を行ってきた．しかしながら，認証ネットワークに対し，多くの機能拡張や性能向上の必要性が高まってきた[1].

更に，本学においては学内外合わせて公式な拠点だけでも 43 拠点(2011 年 7 月現在)を有する遠隔講義・会議

システム SUNS(Shinshu Ubiquitous-NetSystem)を運用している[2,3]．従来であれば遠隔講義・会議システムは認証ネットワーク内に設置することはなかったが，現在では安全性の確保のために認証ネットワーク内への設置が進んでいる．遠隔講義・会議においては定常的にネットワークの帯域を必要とする上，安定している必要がある．また，本学はほぼ全ての学生にノート PC の購入を促しており，授業や実験実習においても活用されている．そして授業においては認証ネットワークより本学 e-Leaning システムである eALPS [4,5]が参照される．

このよう認証ネットワークの安定運用は，授業や実験実習を実施するにあたりおいて欠くことのできない要素となっている．これは教育の質的保証においても重要であり，安定性の高いネットワークを設計，構築し運用することは業務として責任を持って遂行しなければならない．

このような要望を満たすネットワークとして信州大学では「セキュアネット 2010」を構築した．「セキュアネット 2010」では，Class A 規模の Private IP Address ネットワークを構築しつつ，更に Class B の Global IP Address も包含するトータルな認証ネットワークとして構築された．更に 2010 年度より「高速高信頼性ネットワーク」(3 年計画)構築に伴い，初年度信州大学主要 5 キャンパス(松本，長野(工学)，長野(教育)，上田，南箕輪)の全てのキャンパス内建物間光回線の整備とキャンパス間ネットワーク整備を実施した．2 年目以降の計画において，「セキュアネット 2010」全ての建物にて利用可能とするため拡充を行っている．

本稿では「セキュアネット 2010」の運用と拡充において発生した問題とその解決方法として実施した認証スイッチの拡張と整備について報告する．

2. 信州大学ネットワークと認証ネットワーク「セキュアネット 2010」

信州大学は松本，長野(工学)，長野(教育)，上田，南箕輪の主要 5 つのキャンパスからなる大学であり，各キャンパス間は 1C/8C の光回線(SM 9.5/125 μm)にて接続されている(図 1)[6]．また 2010 年度より「高速高信頼性ネットワーク」の構築を開始し，信州大学ネットワークのリプレースを実施している．認証ネットワークである「セキュアネット 2010」は総合情報センターにおける「教育用計算機システム」の一部として 2010 年度から運用を開始し，更に「高速高信頼性ネットワーク」の構築において認証機能を全ての建物に対し拡充する(前者にて 60%程度の建物に供給したので，後者にて 100%へ拡充する)．

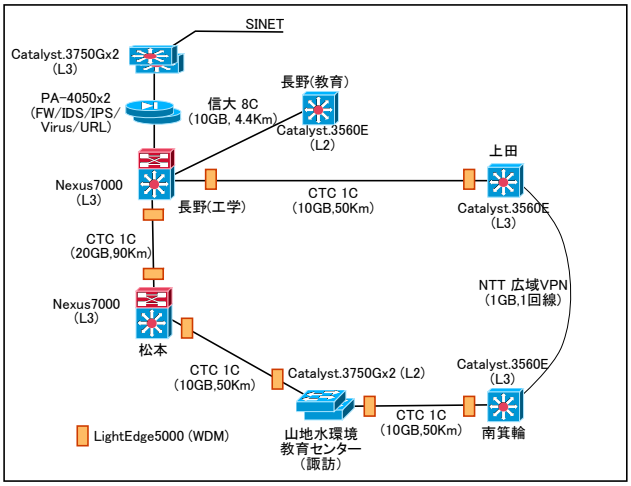


図 1 信州大学キャンパス間ネットワーク構成概要

図 1 に示す信州大学キャンパス間ネットワークにおいて，「セキュアネット 2010」構築における基本コンセプトは次に示す通りである[1].

1. 信州大学全域に対する広域サービス
2. 広域化に伴う性能の低下最小限化
3. 導入，運用コストの低減
4. DHCP サービスと適切な割当対処
5. Web/MAC 認証の実施と柔軟なポリシー適用
6. 信大ポータルサイトや各種サーバと連携
7. UTM(Unified Threat Management) との連携
8. IP Address/MAC Address/ユーザ単位でのトラフィック制御と統計情報の取得
9. P2P アプリケーションやゲーム，マルウェア等の挙動監視と制御
10. 長期不使用 IP Address の洗い出し

上記ポリシーに基づき構築した認証ネットワーク「セキュアネット 2010」の概要は図 2 となる．本認証ネットワークの最大のポイントは，L2 認証とゲート認証(Captive Portal 認証)，及び，ポータルサイト認証を同時に行うことにより，ユーザからはポータルサイトにログインする動作だけで全ての認証が完了している認証ネットワークである点である．これにより上記 1.～10.目標達成が可能となった．

3. 「セキュアネット 2010」の問題と課題

「セキュアネット 2010」の運用を実施した 2010 年度において，運用から問題や課題が発生した．詳細は参考文献[1]に示すが，とりまとめると次のようになる．

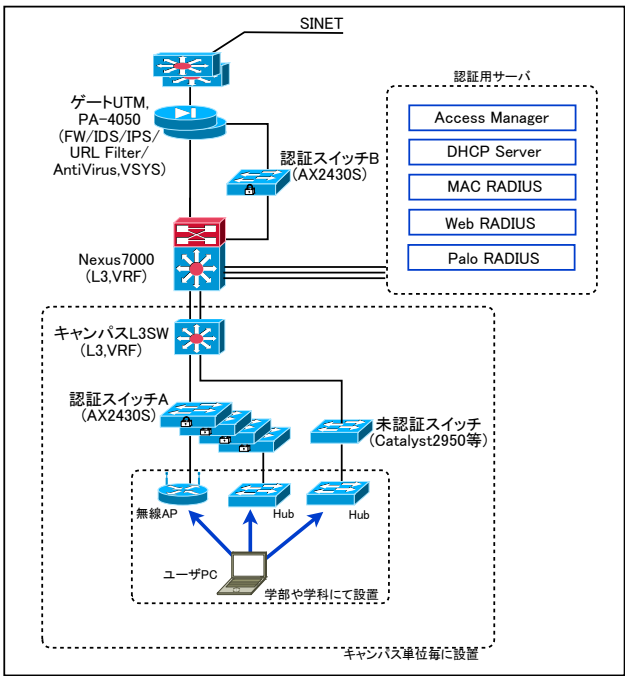


図 2 セキュアネット 2010 ネットワーク構成概要

1. Global IP Address のネットワークへの適用とポリシーの拡大

現在は Private IP Address ネットワークのみに認証を適用しているが，今後は Global IP Address ネットワークにも適用する．

2. 同時 login 性能の向上

600 人が同時に login した場合，全てのユーザにおいて 10 秒以内に処理を完了する．

3. 認証連動部分の改善

認証スイッチや UTM (PA-4050) では，最終的にバックエンドにある Web/Palo RADIUS に認証情報をエントリする必要がある．現在，このエントリ情報の共有は https にてユーザ PC と認証が必要(エントリ情報が必要)な装置間で逐次的に交換しているが，バックエンド内で閉じて共有する仕組みを構築する．

4. 非正規に設置された NAT や DHCP サーバ機能を持つ機器への対応

セキュアネットに限らずネットワークを運用する上で発生する重要な障害の 1 つとして，非正規に設置された NAT 機器と DHCP サーバがある．これを検出する仕組みを構築することにより，授業実験を安定して開催できる．

5. ユーザへの情報提供

希望するユーザ対し，当該ユーザ ID の情報をベースとしたトラフィックの状況等をユーザ単位で供給する．こともできるため，例えばマルウェアの挙動等を個々人でも確認することができる．

6. メーカーへの要望

UTM 機器の Palo Alto Networks 社製 PA-4050 において，ユーザ認証機構である Captive Portal が http でしかできない．これにより認証フローが複雑化しているため改善を要望している．また，認証スイッチの ALAXALA Networks 社製 AX-2430 において，認証待ちにおける処理が滞留する状況の改善を要望している．

本稿では上記の問題や課題から特に 2.同時 login 性能の向上に関して，設計と取り組みについて述べる．

4. 「セキュアネット 2010」における同時 login 性能向上計画と設計

前章にて提示した同時 login 性能において，最も性能的にボトルネックとされたのは，ゲートに設置されている UTM による Captive Portal 認証やポータルサイトではなく，L2 認証スイッチにおける同時認証性能である．今回投入した AX2430 シリーズでは，L2 認証における同時認証処理能力が実効で 40 以下である．また，本スイッチにはそれ以外の問題点として，不要に認証待ちとなった場合のセッション切断までの時間が長い等，認証処理そのものに関する問題があったが，これらは適宜ファームウェアが改善されてきた．しかし，同時処理等基本性能に関わる部分についてはファームウェアの改善では対処できない．

このような根本的なボトルネックの問題を解消するため，L2 認証スイッチの構成を変更することで大量の同時 login が発生しても耐えうる構成を考案した（図 3）．

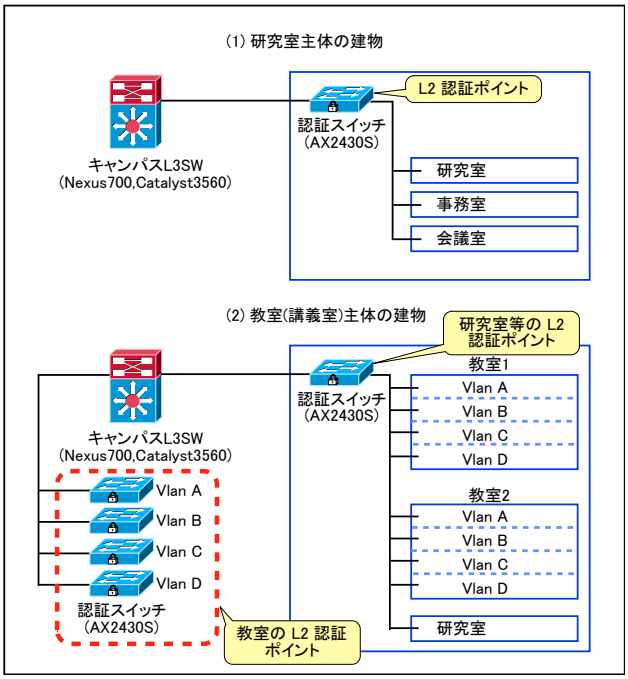


図 3 認証スイッチの設置形態と認証ポイント
(1)研究室主体の建物の認証と，(2)教室(講義室)主体の建物への L2 認証スイッチの設置と認証ポイント

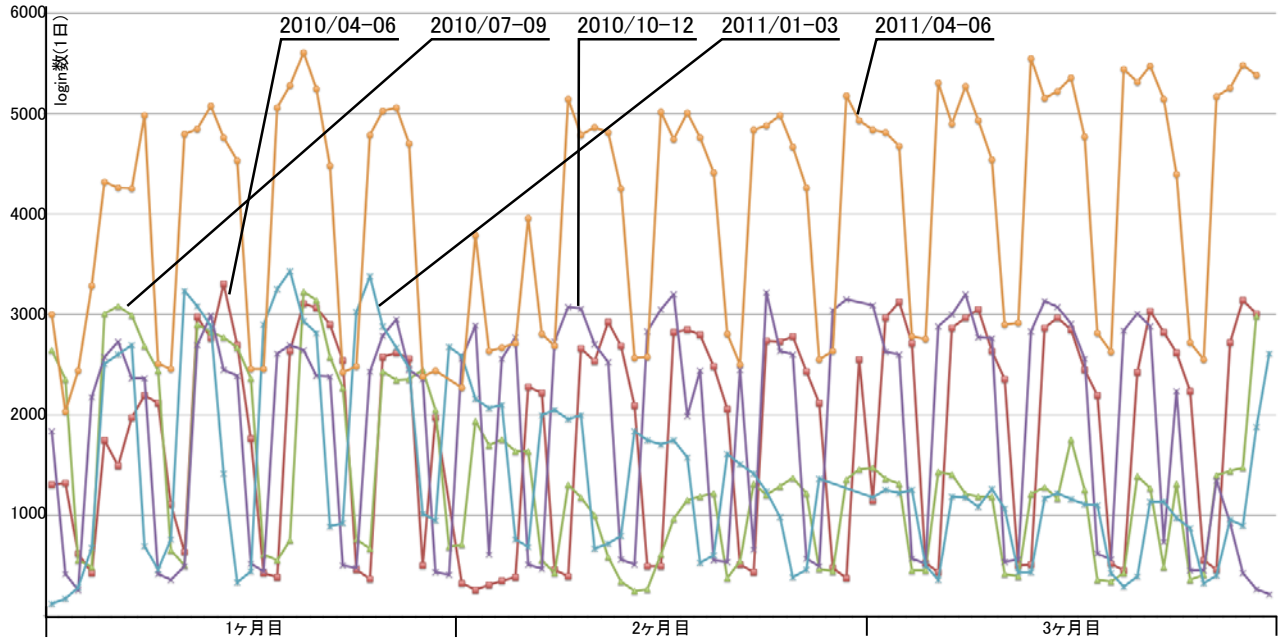


図 4 「セキュアネット 2010」 認証数(login 数)の推移 (四半期ごと 2010/04 ～ 2011/06)

図 2 の(1)は通常の研究室主体の建物に対する L2 認証を表している．研究室主体の建物の場合，認証スイッチは建物に 1 台設置され，同一建物内の L2 認証をすべて実施する．この場合，認証ネットワークに同時に多数のユーザが login することは稀であり，AX2430 の同時認証処理が 40 セッションであることは問題にならない．

問題は教室や講義室主体の建物の場合である．特に 1 年生向けの授業では，学部等で指定されたノート PC(持ち込み PC)を利用した場合，画面を説明しながら 1 ステップずつ授業が開催される．また，生協主催の購入 PC 説明会等でも 300 台近いノート PC の基本的な操作説明が，やはり画面を説明しながら 1 ステップずつ説明される．この場合，40 台以上のノート PC が同時認証する事態が発生し，L2 認証が困難となった．2010 年の 4～5 月において頻繁に発生した障害の多くは L2 認証スイッチのこの問題によるものが少なくなかった．

そこで教室や講義室主体の建物に対応すべく，図 2 (2) のような接続方法を考案した．図 2 (2) の例では教室 1,2 を 4 エリアに区切り，それぞれに Vlan を設定する(1 つの VLan あたり 20～30 人の学生がノート PC を接続すると想定)．そしてその Vlan 毎に認証するスイッチをキャンパスセンタースイッチ側に設置し，L2 認証機能のみを提供するのである．ボトルネックを解消するための重要な点は，同時に認証が発生した場合に分散させることである．つまり，教室 1 や 2 において認証ネットワークを利用する授業があったとしても，全く同じタイミングで認証が同時にかからない限り本構成で問題ない．これは教室の数が多くなれば異なる教室で同時に認証が発生する可能性が高まるが，現在の運用においては，松本キャンパス(7600 人)では 8 台，長野(工学)キャンパス(2700 人)では 6 台の AX2430 を認証分散のために設置されている．

5. 認証ネットワークのトラフィックデータと運用状況

前章で述べた設計を実施したのは 2010 年 10 月からである．また，図 4 は「セキュアネット 2010」における login 数を四半期毎にまとめたものである．2010 年度においてはピークでも 3000 login であり，特に 2010 年 9 月までは授業の方法によっては同時認証の問題が発生していたが，前章の対策が完了して以降，「セキュアネット 2010」における同時 login 時における L2 認証の問題は発生していない．特に図 4 では 2011 年度に入り最大 login 数のピークが 6000 login 近くまで増加した．それにも関わらず，認証関係の障害に関しては L2 認証においても，Captive Portal 認証においても，またポータルサイトの認証においてもほぼ発生していない．

図 5 は「セキュアネット 2010」における 2010 年度の総認証回数(login 数)を時間にて集計したグラフである．昨年度のピークは 9～16 時であるが，これは主に学部学生が利用する時間であり，認証ネットワークの拡充と共に認証数やピーク時間が変動する可能性がある．

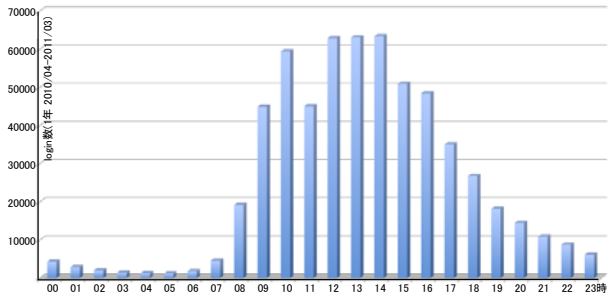


図 5「セキュアネット 2010」年間認証数(login 数)
2010/04 – 2011/03

6. 結果と今後の課題

教室(講義室)主体の建物に関して，認証スイッチをキャンパスセンタースイッチにまとめて収容し，教室を Vlan で分割し対応する認証スイッチにて認証させる方法で同時認証の問題が解決した．認証のピークが倍増した(図 4)今年度において, 本対策が完了していたため認証に関わるトラブルは発生していない．更に授業において同時に login 操作をさせる授業の担当教員(特に昨年度障害が発生した授業を中心)に，今年度の障害状況に関する問い合わせを実施したところ，授業の進行には全く問題がなかったとの回答を得たことから，本対策が非常に有効であったと考えられる．

また，通常の設計であれば，教室にて同時認証の問題が発生した場合，教室側に大量の認証スイッチを設置することとなるが，センタースイッチ側に認証スイッチをまとめる本対策は費用対効果や HA の面でも非常に優れており有効な対策であると考えられる．

7. まとめ

本稿では大学として必要性が高まってきた認証ネットワーク「セキュアネット 2010」の同時認証における障害対策として認証ネットワークを有効に拡張するための設計を行い構築した経緯をとりまとめた．

認証ネットワークは安全性や管理者に取っての利便性だけを考慮するのではなく，利用者の利便性の向上が重要であると考えている．教職員が授業の運営で工夫しなくとも，ストレス無くあたりまえのように利用できるシステムとして, 今後も「セキュアネット 2010」を拡充させる予定である．

更に，「セキュアネット 2010」は今後の認証ネットワークの拡充を見据え，更に完成度を高めるために 600 人同時 login を 10 秒以内に達成する目標を 2011 年 9 月までに達成する予定である．

謝辞

「セキュアネット 2010」の設計や構築，及び，本稿にて提示している認証やトラフィックのデータ解析に関して，ネットワンシステムズ株式会社に支援をいただきました．ここに感謝の意を表します．

参考文献

[1] 鈴木彦文,永井一弥,浅川圭史,今井美香,不破泰:UTM を用いたユーザ認証ネットワーク「セキュアネット 2010」の構築;学術情報処理研究,No.14,pp.21-30,2010

[2] 森下孟,茅野基,鈴木彦文,永井一弥,新村正明,矢部正之:高等教育コンソーシアム信州における大学間遠隔講義システムを活用した遠隔講義「K3 茶論」の実践;学術情報処理研究,No.14,pp.105-116,2010

[3] 森下孟, 新村正明, 茅野基, 鈴木彦文, 永井一弥, 矢部正之, “大学間遠隔講義システムの構築と試行”，日本教育工学会，第 25 回全国大会, P1p-FLS-17, Sep. 2009.

[4] 五月女雄一,鈴木彦文, 新村正明, “複数の教育支援システムの相互利用とシステム間の情報共有を実現する教育基盤システムの構築と運用”,教育システム情報学会研究報告, 23, (7), pp.118-123, Mar. 2009.

[5] 五月女雄一, 鈴木彦文, 新村正明, “教育支援システムの疎結合で構成される教育基盤システム「eALPS2.0」”,情報処理学会研究グループ報告, 第10回 CMS 研究発表会, pp.1-4, Dec. 2008.

[6] 山崎洋一，“ネット構築の現場から”，日経 NETWORK, 2010 年 7 月号(第 123 号), pp.56-59.

岡山大学における生涯 ID を実現する統合認証システムの構築

Construction of Integrated Authentication System to Realize Permanent ID in Okayama University

河野 圭太，藤原 崇起，大隅 淑弘，岡山 聖彦，山井 成良，稗田 隆
Keita KAWANO, Takaoki FUJIWARA, Yoshihiro OOSUMI, Kiyohiko OKAYAMA, Nariyoshi YAMAI, and Takashi HIEDA

keita@cc.okayama-u.ac.jp, fujiwara-t4@adm.okayama-u.ac.jp,
{oosumi, okayama, yamai, hieda-t}@cc.okayama-u.ac.jp

岡山大学情報統括センター
Center for Information Technology and Management, Okayama University

概要

近年, シングルサインオンの実現による利便性の向上と認証機能の一元化による ID 管理コストの削減および安全性の向上を目的として, 各大学において統合認証システムの導入が進んでいる. 岡山大学においても, 従来より，ID 一括管理システムや LDAP を利用して学内情報システムの ID とパスワードの統一を進めてきたが，全ての学生および教職員を包含する ID 体系が存在しないことや，進学の度に ID が変更されてしまうことが課題となっていた．本稿では，全構成員に対する統一的な ID 付与に加えて，付与した ID の生涯利用を実現するシステムとして平成 22 年 6 月より運用を開始した岡山大学統合認証システムの概要について報告する.

キーワード

統合認証，シングルサインオン，生涯 ID，認証一元化

1. はじめに

近年，シングルサインオンの実現による利便性の向上と認証機能の一元化による ID 管理コストの削減および安全性の向上を目的として，各大学において統合認証システムの導入が進んでいる[1]-[4].

統合認証システムの導入により，利用者は，利用するシステムごとに ID とパスワードを使い分けなければならない手間から解放され，一度の ID・パスワード入力で複数のシステムを利用することが可能になる．また，連携システムの管理者は，ID 管理を含む認証機能を統合認証システムに委託することにより，本来の業務である提供サービスの充実に専念できる.

岡山大学においても，従来より，ID 一括管理システムや LDAP を利用して各種情報システムの ID とパスワードの統一を進め，学内における利用者・連携システム管理者双方の ID 管理コスト削減に取り組んできた.

しかしながら，ID の利用に課金をしていた経緯も

あり，情報統括センターが発行する ID(センターID)を保持していない教職員もいたため，センターID のみで各種情報システムの統合認証化を進めることができなかった．その結果，センターID による統合認証を基本としつつも，学務システムの ID による統合認証，教員評価システムの ID による統合認証が同時に運用される状態となっていた．

また，学生に付与する ID は学生番号に基づいて発行されていたため，進学の度に新しい ID が作成され，それに伴いメールアドレスが変更されること，個人データが引き継げないことが課題となっていた．

本稿では，これらの課題を解決するため平成 22 年 6 月より運用を開始した岡山大学統合認証システムの概要について報告する．

2. 要求条件と構築方針

統合認証システムの構築にあたり，以下の要求条件を満足することが求められた．

(1) 全構成員に対する統一的な ID 付与を実現すること．
(2) ID の生涯利用を実現できること．
(3) 既存の運用に与える影響を最小限に抑えること．
(4) 効率的な ID 管理を実現すること．

まず，要求条件(1)および(4)を実現するため，認証情報は学務システムおよび人事システムとの自動連携によりマスタデータベースに集約して生成することを基本とした．また，集約された情報をセルフメンテナンス等により分散的に維持・管理できる管理システムを構築することにより，要求条件(4)の実現を目指した．

さらに，要求条件(1)および(2)を実現するため，ID 体系の見直しを行った．従来の ID 体系では，学生に対しては学生番号に基づく ID を，教職員に対しては希望に基づく任意文字列の ID を発行し，それをメールアドレスとしても利用していた．新しい ID 体系では，学生番号が変更された場合や学生が教職員として採用された場合にも継続して利用できる ID として，ランダムな英数字による ID（システム ID）を生成することとした．

ただし，要求条件(3)を考慮し，利用者がシステムへログインする際に入力する ID（岡大 ID）やメールアドレスとして利用する ID についてはそれぞれ独立に変更可能とし，統合認証システムの運用開始時には従来のセンターID を引き継ぐこととした．

図 1 にシステム ID と岡大 ID の関係をまとめた．

3. システム構成

図 2 にシステム構成を示す．

学務システムおよび人事システムを発生源とする構成員の情報は，大学情報データベースを経由して統合認証マスタデータベースに登録される．マスタデータベースの情報は統合認証管理システムにより管理され，各種システムに提供される．

また，電子証明書による認証を実現する岡山大学認証局に加えて，各種情報システムへのシングルサインオンおよび認証機能の一元化を実現するためのシングルサインオンシステムが導入されている．

以下に統合認証管理システム・統合認証マスタデータベースおよびシングルサインオンシステムの詳細を述べる．

3.1. 統合認証管理システム・統合認証マスタデータベース

前述したように，全構成員に対する統一的な ID 付与を効率的に実現するため，学生の情報を保持する学務システムと，教職員の情報を保持する人事システムとの自動連携による ID 発行を実現した．学務システムおよび人事システムに登録された構成員情報は，夜間のデータベース連携により，大学情報データベースを経由して統合認証マスタデータベースに登録される．

名称	用途	割り当てルール	割り当て例
システムID	個人を識別するために付与するID	ランダムな英数字	p12qr345
岡大ID	システムにログインするために利用するID	個人が設定した文字列 (初期値は上記と同じランダムな英数字)	okadai-taro (初期値：p12qr345)

図 1　システム ID と岡大 ID

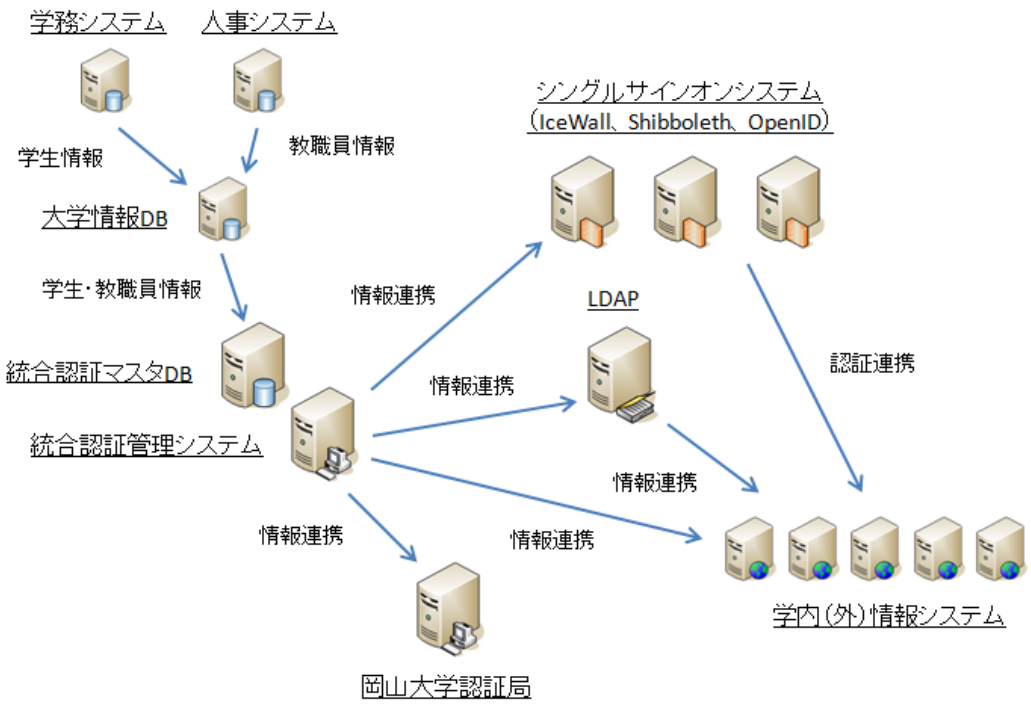


図 2　システム構成

また，統合認証マスタデータベースが保持する利用者の属性情報を管理するための統合認証管理システムでは，ロールに基づく権限管理やワークフローの機能が実装されており，管理者だけでなく，利用者自身による属性情報の変更や，利用システムの申請ができるようになっている．さらに，それらの属性情報は CSV 連携もしくは LDAP 連携により各種情報システムに提供することが可能であり，学内における ID 管理コストの削減を実現している．

図 3，図 4 に統合認証管理システムの個人属性変更画面，メール設定変更画面を示す．利用者は岡大 ID で統合認証管理システムにログイン後，権限の範囲内で岡大 ID や所属等の個人属性を変更し，連携システムに反映させることや，メールアドレスのエイリアスを設定すること等が可能である．

3.2.　シングルサインオンシステム

1 章で述べたように，過去に ID の利用に課金をしていた経緯もあり，センターID を保持していない教職員が存在した．正確には，教員については平成 21

図 3　個人属性変更画面

図 4　メール設定変更画面

年度より大学付与メールの運用を開始し，全教員がセンターID・パスワードを保持するようになっていたが，既存のメールアドレスへの転送も許可したため，センターID・パスワードが完全に浸透しているとは言い難い状況であった．

そこで，要求条件(3)を考慮し，シングルサインオンシステムについては既存の認証機能と並行して運用を開始することとし，当面は従来の方法でもシステムが使える状態を継続させることとした．

このため，リバースプロキシ型のシングルサインオン製品である日本 HP 社の IceWall を導入し，運用開始時には，教員評価システム，学務システム（教員向け），Web 購入システム，学内教職員専用ページとの連携を実現させた．

一方で，リバースプロキシ型のシングルサインオン製品には負荷集中の問題があるため，今後統合認証を実現するシステムについては，対応が困難なものを除き，Shibboleth または OpenID による認証連携を進めることとした．特に，現在，国立情報学研究所が主体となって進めている学認において，Shibboleth による組織間での認証連携が成功を収めつつあることもあり，本学においても Shibboleth を中心とした統合認証を進めている．

平成 23 年 7 月現在，30 を超えるシステムが岡大 ID で利用可能になっている．

4.　生涯 ID の実現

前述した ID 体系の見直しにより，学生番号が変更された場合や学生が教職員として採用された場合に ID の再割り当てを実施する必要が排除された．

しかしながら，ID の発行については要求条件(3)，(4)を考慮し，学生番号および個人番号に基づいて学務システムおよび人事システムとの自動連携で実施することとしたため，名寄せの実現が課題となった．

幸い，本学の学務システムでは，システム内部に個人を一意に特定する ID を保持していたため，この ID をキーとして名寄せを実施することにより，進学に伴う ID の引き継ぎ処理を自動化した．

一方で，教職員についても非常勤職員が常勤職員として採用された場合などに個人番号が変更されるが，人事システムには個人を一意に特定する内部 ID が存在しないため，自動での名寄せを断念した．

現在，学生から教職員への身分変更，非常勤職員から常勤職員への身分変更等については本人の申告に基づく手動での ID の引き継ぎを基本としており，システムとしての対応はカナ氏名と誕生日を用いた重複確認による気づきの提供にとどまっている．

このような生涯 ID の実現に伴い，Gmail を利用した学生向けのメールサービスについても，在学期間

中の継続利用が可能になった．ただし，要求条件(3)を考慮し，アドレス付与ルールの変更に伴うメール送信者側の混乱を避けるため，当面は従来の学生番号に基づくメールアドレスも，エイリアスとして持たせることにした．

5. 運用開始後の課題

平成 22 年 6 月の運用開始以降，以下のような課題が発生している．

まず，3.2 節で述べたように，本システムには 3 種類のシングルサインオンシステムが導入されており，相互の認証連携は実施されていない．そのため，シングルサインオンドメインが異なるシステムを利用しようとした場合，再度 ID とパスワードの入力が求められることになり，ネットワークを利用するための認証も含めると，1 日に複数回の ID・パスワード入力が必要になる．

費用の関係もあり，導入時には対応を見送った課題ではあったが，実際に運用を開始すると利用者からの問い合わせも多く，何らかの改善策が必要な状況となっている．

現在，文献[5]を参考に，ネットワーク認証，IceWall 認証，Shibboleth 認証の連携を実現するよう，検討を進めている．

また，前述したように，要求条件(3)，(4)を考慮した結果，岡大 ID は現時点の学生番号または個人番号と 1:1 に紐づくように定義されている．名寄せの実現により，ID の継続利用は可能な状態となっているが，正規生かつ非正規生であるため複数の学生番号を持つ場合や，学生と教職員を兼ねているため学生番号も個人番号も持つ場合には ID を引き継ぐことができず，個人に対して複数の岡大 ID が発行されてしまう．

この問題については，文献[6]のように，個人がログインに利用する ID をいずれかの岡大 ID に統一するような仕掛けの検討が必要であると考えている．

さらに，本システムの導入により，学生にとっては個人が任意に指定するアドレスによるメールサービスの継続利用が可能となったが，メールを受信する教職員にとっては From から学生番号が特定できないことが問題であるとの報告も寄せられている．

この問題については，必要に応じて 4 章で述べた従来のアドレス付与ルールに基づくエイリアスを From としても利用する運用の実現を検討している．

6. まとめ

本稿では，全構成員における統一的な ID 付与に加えて，付与した ID の生涯利用を実現するシステムとして平成 22 年 6 月より運用を開始した岡山大学統合認証システムの概要について報告した．

今後は 5 章で述べた課題の解決に加えて，残課題となっている学務システム（学生向け）や生涯メールとの認証連携を実施する予定である．

参考文献

[1] 沖野 浩二，布村 紀男，“富山大学における認証基盤の整備による業務軽減評価，”学術情報処理研究，no.14，pp.31-39，Sept. 2010.

[2] 桝田 秀夫，“Shibboleth を含んだ統合認証システムの導入～京都工芸繊維大学の 2010 年導入事例～，”第 4 回統合認証シンポジウム，pp.15-18，Dec. 2010.

[3] 松平 拓也，“Shibboleth による金沢大学統合認証基盤の構築と今後の展開，”第 4 回統合認証シンポジウム，pp.33-48，Dec. 2010.

[4] 松浦 健二，“徳島大学における SSO の実現と課題，”第 4 回統合認証シンポジウム, pp.49-66, Dec. 2010.

[5] 藤村 喬寿，西村 浩二，相原 玲二，“大規模キャンパスネットワークにおける SSO 認証の設計と実装，”電子情報通信学会 IA 研究会技術研究報告，pp.13-18，Nov. 2009.

[6] 江原 康生，村尾 靖子，山口 文雄，“大阪大学における新全学 IT 認証基盤システムの構築と移行，”情報処理学会 IOT 研究会研究報告, pp.1-6, Feb. 2011.

必携ノートパソコンによるＷｅｂ履修登録の試み

Trial of Web-based Learner's Applicaion System using mobile PC

佐々木正人†，松村譲‡，田村純久‡，竹下佳‡，久保山明彦‡，
松浦良典‡，正木茜†，石黒克也†，斎藤卓也†，豊永昌彦†
Masato Sasaki†, Yuzuru Matsumura‡, Yoshihisa Tamura‡, Kei Takeshita‡, Akihiko Kuboyama‡,
Yoshinori Matsuura‡, Akane Masaki†, Katsuya Ishiguro†, Takuya Saito†, Masahiko Toyonaga†

† 高知大学総合情報センター
‡ 高知大学研究協力部学術情報課

† Integrated Information Center, Kochi University
‡ Academic Information Section, Kochi University

概要

高知大学では，２０１１年度１学期の共通教育および専門教育の履修登録を，１年生をはじめ全学生が所有するノートパソコンを用いて実施した．これまで１年生は，１学期開講の必修科目「情報処理」の授業の中でセキュリティ対策や学内ネットワークに接続するための設定を実施していたが，２０１１年度は授業開始前にセルフ形式で実施した．

キーワード

Ｗｅｂ履修，ノートパソコン必携，セキュリティ対策，教育支援

1. はじめに

高知大学では，2009 年度２学期分から Web システム（KULAS: Kochi University Learner's Application System）による履修登録を開始した．学生は，必携ノートパソコンを学内ネットワークに接続し，Web システムにアクセスして履修登録を行った．１年生は１学期に開講される必修科目「情報処理」の授業でウイルス対策ソフトの確認・導入などのセキュリティ対策や学内ネットワークに接続するための設定を行っており，在学生を含め全学生が必携ノートパソコンで履修登録が可能であった．

2010 年度１学期の履修登録では，「情報処理」の授業前に生協でパソコンを購入した人文学部と農学部の１年生（約 350 名）に対してはセキュリティ対策とネットワーク設定をした後履修登録を行った．また，他学部の１年生(約 600 人)は，２日間の履修登録期間を学部・学科別に作業時間を分けて，総合情報センター教育端末室のデスクトップパソコン（６０台）で履修登録を行った．

１回目の履修登録結果の公開と同時に，優先登録（空き定員のある科目を早い物勝ちで登録する）が可能となるため，教育端末室のある建物の前には，長蛇の順番待ちの列（約 400 メートル）ができ，開館と同時に教育端末室に学生が殺到した．

ノートパソコン必携による情報教育や Web 履修登録等の教育の情報化の責任母体である「全学教育情報委員会」では，この状況を改善するため，2011 年度は１学期

の履修登録を必携ノートパソコンで行うことを検討し，履修登録期間前（もちろん授業開始前）に１年生が自分のノートパソコンで Web 履修できるよう事前準備や実施の協力要請が総合情報センターにあり，その企画・実施を研究協力部学術情報課の協力を得て実施した．

本稿では，１年生へのＷｅｂ履修事前準備の周知から実施･Web 履修登録の支援までの試みについて報告する．

2. Web 履修登録に利用される設備等

Web 履修登録で使用する必携ノートパソコンの内訳，総合情報センターが提供している教育用パソコンやネットワーク環境について説明する．

2.1. 必携ノートパソコン

高知大学では，平成９年度より「ノートパソコン必携による情報教育」を実施している．学生は，大学の推薦する生協パソコン（以下，生協ＰＣ）やパソコンショップ等で購入したパソコン（以後，持込ＰＣ）を入学時に準備することになっている．また，パソコンが準備できない学生に対しては，大学でパソコンを貸与している．2010 年度と 2011 年度のパソコンの内訳を表１に示す．

	2010 年度	2011 年度
生協ＰＣ	56.3 %	66.0 %
持込ＰＣ	42.5 %	32.7 %
貸与ＰＣ	1.2 %	1.3 %

表１．新入生ノートパソコン内訳

入学時点での学生のノートパソコンのスキルは，毎年教育情報委員会がアンケート形式で調査(「パソコン活用自己診断テスト」）している（表２参照）．困った際に支援するスタッフを配置すれば，マニュアルを見ながらパソコン操作できるスキルは持っていると思われる．

操作内容	可能(率)
日本語入力ができる	97%
ワープロで簡単な文書が作成できる	80%
Web ページ閲覧（リンク・URL）	85%
お気に入り・ブックマークの利用	85%
ファイルの整理(複写・移動・削除)	80%

表２．パソコン活用自己診断テスト（抜粋）

2.2. 総合情報センターデスクトップＰＣ

総合情報センターで準備しているデスクトップパソコンは，教育用６０台，研究用５台，マルチメディア対応５台のみである．教育用は，主に専門教育の授業で使用されており，授業外は自習可能としている（農学部のある物部キャンパスには２０台）．

2.3. ノートＰＣ接続環境とウイルス対策

学内にはノートパソコンをネットワークに接続して利用する環境を整備している．

(1) 情報コンセント教室

DHCP 環境を整備した共通教育棟の教室で，授業の開始・終了時に授業担当教員が電源を On/Off する．

(2) 情報コンセントコーナー

全学認証ＩＤによる利用認証後ネットワーク接続できる環境で，総合情報センター（図書館）や自学自習室等に設置されている．

さらに，ノートパソコンのセキュリティ対策を確実に実施するため，総合情報センターでウイルス対策ソフト（McAfee）を提供している．在学生は，４月初めに年度更新処理を学内ネットワークに接続して行うことで，在学期間内は継続して使用できる．

3. Web 履修登録処理のスケジュール

2011 年度の入学式は４月３日（日曜日），Web 履修登録は４月６～７日（在学生は５日から），授業は４月１１日（月）より開始された．つまり，Web 履修登録の事前準備を，入学式から Web 履修登録日の前日までの３日間で実施することが今回の条件となる．

4. １年生への事前準備の周知

１年生に各自のノートパソコンで Web 履修を行う必要があること，それぞれのパソコンによって事前準備が異なることなどを周知するため,「ノートパソコンチェックシート」と説明文（学務課作成）を入学式で配布し説明した．

この「ノートパソコンチェックシート」では，(1)生協で購入，(2)生協以外で購入，(3)貸与パソコン希望から該当するものを選択し，(1), (2)についてはウイルス対策ソフトを(a)自分で購入，(b)大学提供ソフト使用を選択することで事前準備として何が必要であるかが分かるように工夫した．

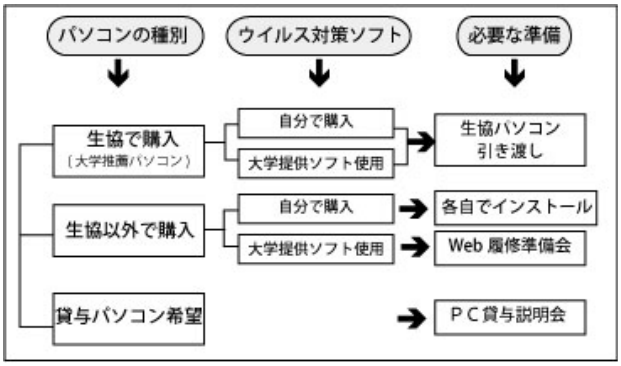


図１．Web 履修に必要な事前作業の確認

一部の「情報処理」のクラスにおいて実施したアンケートでは，入学式での説明やチェックシートの内容は，ほぼ理解されていたことが分かる．

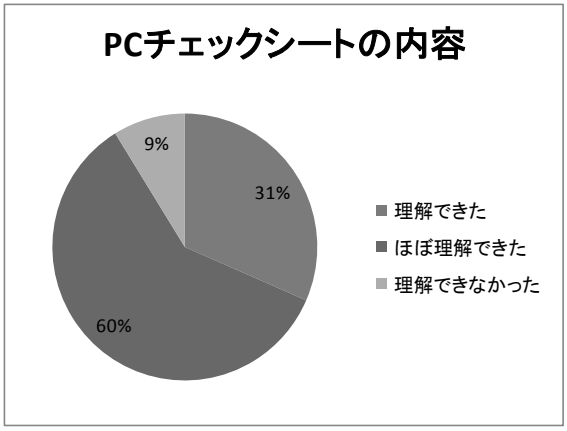


図２．パソコンチェックシートの内容の理解

5. 事前準備の概要

チェックシートにより誘導する４つのパターンの事前準備の内容と作業支援の結果について説明する．

5.1. 生協パソコンの引き渡し

生協では，パソコンの引き渡しの際に，簡単なパソコン操作説明，学内ネットワークに接続するための設定などを行った後，総合情報センターで準備したマニュアルとインストールＣＤにより大学提供版ウイルス対策ソフトのインストール作業を実施した．４月３日・４日の午後に合わせて６１６台（全体の 66%）の引き渡しが完了した．だたし，自分でウイルス対策ソフトを購入した学生に対しては，Web 履修が終わるまでは大学提供ウイルスソフトを使用させ，授業開始後に入れ直してもらうこととした．

5.2. Web 履修準備会

持込ＰＣのうち，ウイルス対策ソフトを自分で購入していないパソコンを対象に，(1) お試し版ウイルス対策ソフト導入状況を確認，(2) 導入されていた場合はアンインストール方法を説明，(3)大学提供ソフトのインストール，(4)学内ネットワーク接続に必要な設定を実施した．前年度までの実績から該当するパソコンは２５０台程度と予想していたが，生協で購入したパソコンが増え結局約２００台（全体の 22%）であった．この作業の担当者と支援の内容は次のとおり．

(1) 総合情報センター（教員１名）
お試し版の確認・学生スタッフへの作業指示
(2) 学術情報課（２～３名）
お試し版の確認・削除支援
(3) 総合情報センター学生スタッフ（３～５名）
お試し版の削除支援（指示に従って）
(4) 富士通ＳＥ（１～２名）
お試し版の確認・削除支援

5.3. ＰＣ貸与説明会

授業料免除申請者は，貸与希望を出し，後日大学が準備するノートパソコンを貸し出すこととなっている．このため，Web 履修登録は総合情報センターの教育用ＰＣの使用を許可した．なお，2011 年度は東日本大震災によりパソコンの準備が遅れた学生に対しても，教育用ＰＣの使用を許可した．

5.4. 自分で購入したウイルス対策ソフト

持込ＰＣで，ウイルス対策ソフトを自分で購入した場合，Web 履修までに各自でインストールしてもらうよう指導した．また，総合情報センターにサポート窓口を設置し，不安のある学生の支援・相談を実施した．

なお，学内ネットワークに接続するための設定は，Web 履修会場ではじめて接続する際にマニュアルを見て各自で設定してもらった．

5.5. インストール作業の支援

生協パソコンの引き渡しおよび Web 履修準備会でのウイルス対策ソフトのインストール作業は，セルフ方式（マニュアルやＣＤを学生に渡し，マニュアルを見ながら各自で操作）で実施してもらったが，不明な点やトラブルが発生した際にサポートする環境があれば初心者でも十分作業できた．このことは，その後実施されたアンケート調査からも分かる（図３）．

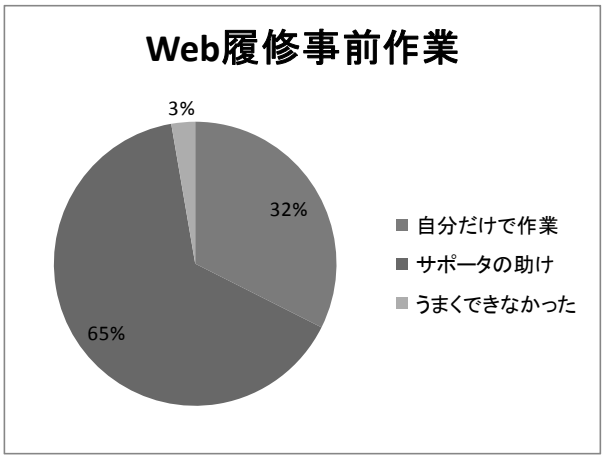


図３．Web 履修事前作業について

6. Web 履修登録期間の利用状況

４月６～７日（在学生は５日から）の履修登録期間，４月８日の履修登録結果の確認および優先登録日の利用状況は次のとおり．

6.1. Web 履修登録期間（4/6～4/7）

2010 年度は，教育用端末６０台が常に使用されていたが，2011 年度は使用を制限しノートパソコンで履修登録するよう指導した結果，１年生を含むほとんどの学生が各自のノートパソコンで作業した．なお，１年生は共通教育棟の１つの教室に集め履修に関する質問にも対応できる環境で履修登録処理を実施した．一方在学生は，他の共通教育棟の情報コンセント教室や，学内の情報コンセントコーナーで接続して作業を行った．また，パソコン修理中の学生や貸与希望者など自分のパソコンが使用できない学生のみ教育用ＰＣを利用して行った．

6.2. 履修確認と優先登録（4/8）

履修登録結果は４月８日１３：００より公開され，同時に優先登録（空き定員のある授業を早い者勝ちで登録する）が実施された．公開時刻の１時間前頃から込み始め，２時間後には混雑が解消された．

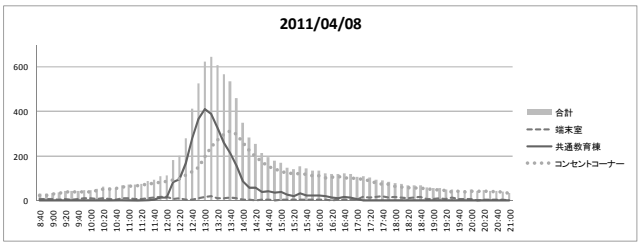


図４．優先登録日の利用状況

例年この優先登録に学生が殺到し，2010 年度は教育用端末室前から約 400 メートルの行列ができた．2011 年度は，共通教育棟の情報コンセント教室にノートパソコンを接続したため，多少混雑は解消されたが教室に入りきれない学生の行列ができた．

その後のアンケート調査では，Web 履修登録の学外からの利用を希望する学生が多く，現在そのために必要なシステム変更等の検討を教育情報委員会で行っている．

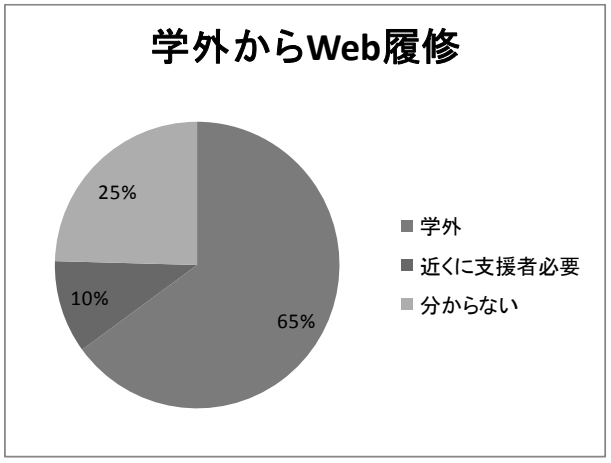


図５．学外からの Web 履修登録について

7. まとめと今後

高知大学では，授業開始前にすべての１年生が所有するノートパソコンに対し，セキュリティ対策および学内ネットワーク接続のための設定を実施し，Web 履修登録処理を行い，大きな問題もなく無事終了した．

しかし，Web 履修に関する事前準備について，１割の学生が入学式での説明が理解できておらず，会場間違え等で多少混乱した．さらなる周知徹底が必要である．

持込ＰＣのお試し版ウイルス対策ソフトのアンインストールについては，その操作方法を直接指導しなければいけないが，それ以外の操作については，マニュアルを見ながら学生自身で作業できた．

持込ＰＣでウイルス対策ソフトを「自分で購入」した学生のパソコンについては，今回全く確認等を実施していない（自己申告により接続許可）．今後はこのパソコンに関する支援・確認が必要である．

来年度も今回の結果を踏まえ，必携ノートパソコンを用いた Web 履修登録を行う予定である．現在，学外からの履修登録や成績参照の実現を含め，今回の試みで得られた課題や問題に対して検討を行っている．

金沢大学での共通教育における情報教育と必携PCの活用

Information Education and Use of PC Owned by Students in Education in Liberal Arts and Science in Kanazawa University

佐藤正英，森祥寛，松本豊司

Masahide Sato, Yoshihiro Mori, Toyoji Matsumoto

sato@cs.s.kanazawa-u.ac.jp, mori@el.kanazawa-u.ac.jp, matsumoto@wave.kanazawa-u.ac.jp

〒 920-1192 金沢市角間町金沢大学総合メディア基盤センター
Information Media Center, Kanazawa University, Kakuma-machi, Kanazawa 920-1192

概要

金沢大学では，平成 18 年度より入学時に入学生全員にノート PC を用意してもらう取組 (以下では，PC 必携化と呼ぶ) を続けている。約 1800 名程度の入学者がいる理系，医系，文系からなる総合大学ではまだそれほど例は多くない。入学時には，情報倫理，学内外での情報活用，およびいわゆるリテラシーを教育内容として含んでいる科目として情報処理基礎を必修化している。また，共通教育での情報教育を企画担当する教員組織の情報グループと総合メディア基盤センターが連携して，共通教育での発展的な情報教育科目についても企画している。本発表では，これらについて，情報処理基礎でのアンケート結果を踏まえつつ報告する。

キーワード

情報基礎教育, PC 必携化, ポータルサイト

1 はじめに

金沢大学では，平成 18 年度から新入生全員に入学時にノート PC を準備させる取組を進めている。これは，(i) もともと学内の総合メディア基盤センター内の実習用 PC の台数が十分ではなく，学生全員に情報処理の基礎的な科目を履修させることが困難であったこと，(ii) 実習用 PC のレンタル期間を 5 年間を選択したため，入学年度によっては，旧式の PC や OS で学習しなくてはならない学生もいたこと，さらに (iii) 大学での教育以外にも学生生活全般や卒業後に社会に出てからも情報機器を活用する能力がますます求められている。というような状況を考えたものである。

現在では，ノート PC の必携化は大して目新しくないかもしれない。しかし，理系，医薬系，文系からなる 1800 名規模の国立大学で全学規模で行っている例はあまりない。さらに，本学ではノート PC の必携化とともにポータルサイトの充実やソフトウェアの包括ライセンスなども行っており，ノート PC の必携化があるから進められている取組もある。

以下では，ノート PC の必携化とともに始まった情報の基礎科目である情報処理基礎と，金沢大学における共通教育における情報教育の現状を報告する。

2 必携PCについて

金沢大学で PC の必携化の取り組みを行っていることは，募集要項により受験希望者に知らせている。また合格後，入学予定者への通知で PC を準備する際の注意点を知らせている。また，大学としては大学オリジナル PC を選定し，金沢大学生活協同組合 (以下，金沢大学生協) を通して販売している。ただし，この PC はあくまでも 1 つの目安になるように学生に提示するものであり，学生は基準を満たしている PC ならば何を準備し

てきてもよい。大学が求める基準も，ネットワークに接続が可能であること，持ち運ぶことができること，マイクロソフト社のオフィス製品またはそれと同等なソフトウェアが無理なく利用できること，ウィルス対策ソフトがインストールされていることなど，この数年間内に販売されている大抵のノート PC ならば問題ない範囲を要求している。

学生は，すでに所有している PC や新たに PC を購入して準備し，入学前に行われるノート PC のセキュリティ点検会に参加する。これは，金沢大学生協と大学が協力して 3 月末に行うものである。この点検会で大学の基準を満たしているか，ウィルス対策ソフトなど必要とされているソフトウェアなどが準備されているかを点検する。入学前に学生に手間をかけるが，大学内のネットワークへのウィルスの持ち込みを未然に防ぎ，学生が加害者にも被害者にもならないようにする必要性から行わざるを得ない。約 1800 名程度の学生全員に対して数日で行うことは大変な労力であるが，金沢大学生協が全面的に協力してくれることにより実施できている。

3　情報処理基礎の授業内容について

情報処理基礎は，本学が入学生全員に必修として行っている共通教育の情報科目である。学生は入学前に様々な水準の情報教育を受けて入学することが予想される。様々な学生に対して，必要最低限の内容は教えて，底上げを行うことを目的として開講している。

始めの 4 回は総合メディア基盤センターの教員が手分けをして全ての学生に対して講義を行う。情報モラルの基本的な内容，学内でのネットワーク利用方法，ポータルサイト (アカンサスポータルと呼ばれている) と全学で利用している学習管理システム (Learning Management System: LMS) の利用方法などを教える。続いて，図書館の職員が図書館の使い方や情報検索方法について 2 回 (もしくは 1 回) 担当し，残りは各学類が学類独自の内容も含めつつ授業を行っている。

下記では，総合メディア基盤センターが担当する 4 回に焦点を絞り報告する。情報処理基礎は，新入生が初めて自分で用意した必携 PC を活用する授業であるが，事前にセキュリティ点検を実施していることもあり，出荷状況の PC を初めて立ち上げて一番初めの OS の設定で授業が進まないということはない。

この科目では，授業中には主として必携 PC を用いた実習に加え，情報モラルに関してを e ラーニングを用いて学習する。1 回目の授業では，主に本学が学生を含めた全教職員に提供しているポータルサイト (アカンサスポータル) へ接続し，基本的な使用方法を試してみることが大きな目的となる。学生は，このポータルサイトを通じて大学の事務や教員からの連絡などを多く受けることになる。また，ポータルから授業の履修登録を行ったり，ポータルが LMS への入口となっていることもあり，第 1 回目の授業でポータルの利用方法に慣れることは学生にとって極めて重要である。

1 回目の宿題としては，金沢大学のセキュリティポリシーについての学習をすることである。教材は e ラーニング教材として用意されている。この数年の調査により入学時には 90 %以上の学生が自宅やアパートなどからインターネットに接続できる環境を持っている。学内に準備されている無線 LAN の設定についてはまだ学習していないが，この段階において，有線 LAN で接続が可能な環境が用意されているので，それを用いて学内で学習可能となっている。学生は LMS 上に用意してある e ラーニング教材で学習したのち，同様に LMS 上に用意してある e ラーニング教材で学んだ内容について試験を受ける。試験問題は多数用意してあるものから 10 問程度ランダムに出題される。きちんと学習した学生にとっては非常に用意であることに加え，繰り替えし受験ができることもあるため，9 割できないと合格にならない。

2 回目の授業としては，学内に設置してある無線 LAN の利用について行う。金沢大学においては，総合教育棟 (主な共通教育が行われる建物) やその他の建物のロビー，ラウンジや食堂などで学生が利用できる無線 LAN が用意されてる。これらの無線 LAN は安全性のために若干複雑な認証を経てから使用する必要がある。そこで，有線 LAN, 無線 LAN を問わずに学内で自由にネットワークが利用できるようにする。また，宿題ではネットワークセキュリティについて学習する。

3 回目では，メールの書き方，送り方を中心にしたネットワーク上のマナーについて，金沢大学で提供している Web メールである Active mail!を例にとり学習する。これは，学生がメールやポータルメッセージを介して学生が大学教職員や大学以外の一般社会の人ととやり取りをする際に最低限のマナーを守れるようにするためである。また，宿題では知的所有権やネットワーク上のマナーについて学習する。

4 回目の授業では，1〜3 回目でできなかった内容，例えば，金沢大学で行っている包括ライセンスなどについて触れる。また，著作権については，違法なダウンロードやソフトウェアの違法使用などが無いように授業中でも改めて触れる。

取り扱っている内容が最低限知っていてほしい無いようなので，4 回修了までに各回の宿題として出していた確認テストに合格していなかった学生には，改めて集めて昼休みなどを利用して合格させるまで学習させる。

4 アンケート結果

情報処理基礎では，授業開始時と 4 回目の授業修了時および 15 回目の授業が修了した時にアンケートを実施してる。アンケートは必携 PC に関するアンケートに加えて，これまで受けてきた情報処理教育や今後受けたい情報教育などについて聞いたものである。以下では，そのいくつかについて報告する。新入生 1813 名に対して，第 1 回アンケートでは約 99 %の学生が回答し，4 回目の授業修了時のアンケートには約 92 %の学生が回答をしている。アンケートの収集には LMS を利用した。

4.1 PC 必携化について

まず，本学の行っている PC の必携化について質問した結果をまとめる。

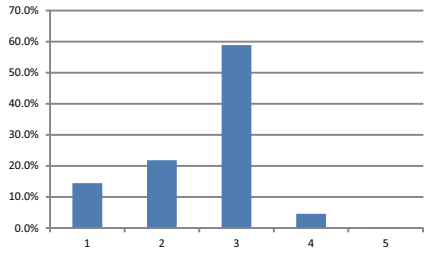


図- 1: PC 必携化をどのように知ったか？

図 1 は，ノート PC の必携化についてどのように知ったかを聞いたものである。グラフは左から (1) 志望校として選択する前から，(2) 志望校として選択した時。(3) 金沢大学に合格し，送られてきた「金沢大学入学予定者へのお知らせ」を見た時。(4) 大学に入学手続きに来た時。(5) その他である。半数程度の学生が合格した時に初めて知っており，金沢大学を志望校として選択する際に大きな要素になっていないことが分かる。

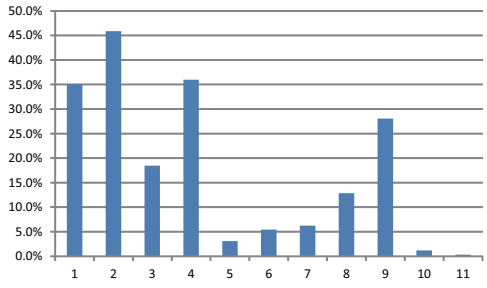


図- 2: PC 必携化をどう思うか

図 2 は，PC 必携化をどのように思うかを聞いたものである。左から，(1) 金沢大学の特徴として良いことである。(2) どうせ大学生になったら PC を買うので必携でかまわない。(3) PC 必携化のために入学時にすぐに PC が得られてうれしい。(4) PC を活用する生活は大学生として望ましい。(5) もっと上級生になってから自分で好きな PC を準備する方がよい。(6) 自宅にデスクトップ型 PC があれば十分である。(7) 学内に共用 PC が準備されていればそれで十分である。(8) 入学時の金銭的な負担が大きくなり経済的につらい。(9) 今更珍しくないのでわざわざ騒ぐことでもない。(10) その他。(11) 未回答。で，複数選択可能として聞いたものである。全体的にみると，(1) から (4) の PC 必携化に好意的な選択肢が多く選ばれている。さらに (9) に挙げた今更珍しいないも比較的多く選択されている。図 1 に挙げた結果と合わせると，学生は入学時に初めてノート PC の必携化について知るが，当然のごとく受け入れ積極的に活用しようとしていることが分かる。

4.2 入学時前の情報の学習について

次に，入学生がどのようなまず，本学の行っている PC の必携化について質問した結果をまとめる。

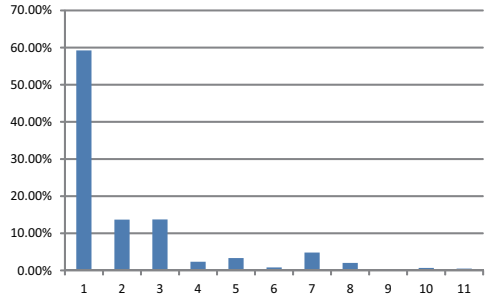


図- 3: 高等学校で習った教科「情報」について

図 3 は高校で習った教科「情報」について聞いたものである。複数選択可能とした時の回答をまとめたものである。グラフは左から，(1) 情報 A を習った。(2) 情報 B を習った。(3) 情報 C を習った。(4) 情報の時間，他の科目を習った。(5) 情報の時間自体が存在しなかった。(6) 情報処理等の科目 (専門科目を含む) を習った。(7) 授業の区分が不明。(8) わからない，覚えていない。(9) 留学生なので区分が違う。(10) その他 (11) 未回答となっている。多くの学生が，情報 A を中心に学習していることが分かる。一部の学生が (4),(8) のような選択をしている。高等学校における情報の位置づけは，一部の高校ではあまり高くなく，学生の記憶に残らなかったとか，情報の学習の上で他の教科の素材を活用する (例えば，歴史についての研究発表をするためのプレゼンテーションの資料を作成する。) などをしているためではないかと推測している。

図 4 は高校で習った教科「情報」について聞いたものである。複数選択可能として回答を求めた。グラフは左から (1)1 年生。(2)2 年生。(3)3 年生。(4) 習ってい

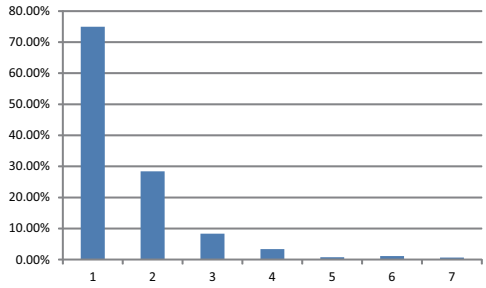


図- 4: 高等学校で教科「情報」を習った学年について

ない。(5) 留学生である。(6) 未回答。(7) 受講時期が不明。の回答数を表している。ほとんどの学生が 1 年生の時に情報を学習している。情報で学習していることが，高等学校の授業でどの程度活用されているかについては不明である。また，複数回答可としているので，1 年生の時に学習しただけではなく，高学年でもした場合も考えられる。しかし，情報が受験に関連しない科目であるために，1 年生の時に学習したまま情報については一切学習しない可能性もあると思われる。

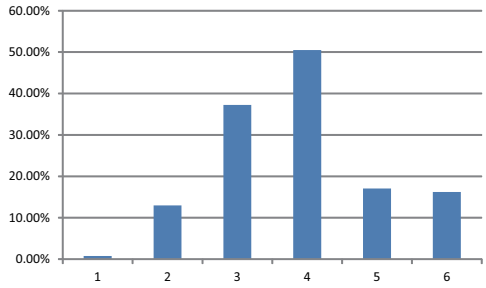


図- 5: 情報モラルの学習について

図 5 は大学入学時までの情報モラルについての学習状況を複数選択可で聞いたものである。(1) 小学校低学年で習った。(2) 小学校高学年で習った。(3) 中学校で習った。(4) 高等学校で習った。(5) 習っていない。(6) 言葉の意味を知らない。という回答の回答数を表している。多くの学生が高等学校で学習しているが，習っていない。情報モラルという言葉の意味が分からないという学生も無視できない程度いることが分かる。

図 4 と図 5 から，すでに学習した情報モラルなどについて忘れていたり，少し古い内容しか知らなかったりする学生，さらに，学習していない学生も無視できない程度存在すると思われる。全体の水準を引きあげる科目としての情報処理基礎のような科目が必要といえる。

4.3 入学後の学習について

また，実際に 4 回目までの授業を受けた感想および，今後どのようなことについて学習したいのかについても聞いた。

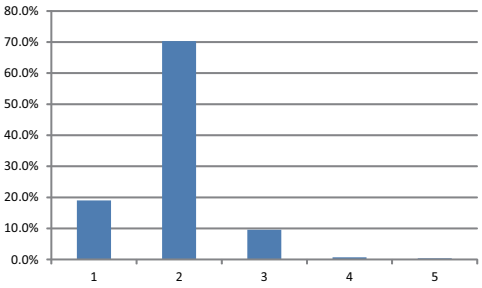


図- 6: 授業の有益性について

図 6 は授業の内容が有益かどうかを聞いた結果である。(1) 非常に有益だった。(2) 有益だった。(3) あまり有益ではない。(4) 無意味だった。(5) 未回答という回答で,, 9 割近い学生が有益またはとても有益だったと回答している。

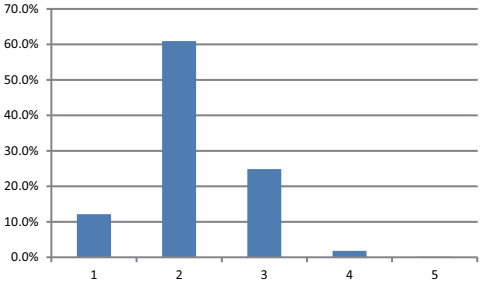


図- 7: 授業の難易度について

図 7 は授業の難易度を聞いた結果である。回答は，左から (1) とても簡単だった。(2) 簡単だった。(3) 難しかった。(4) とても難しかった。(5) 未回答である。6 割近い学生が簡単だったと回答している。

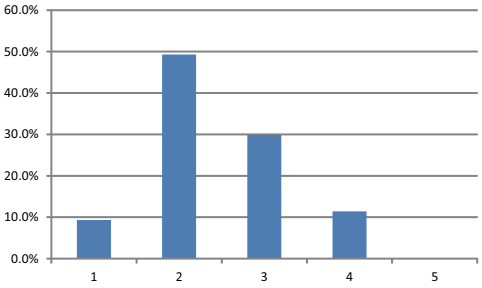


図- 8: 学習内容について

図 8 は情報モラルについて学習した内容について，授業前にどの程度知っていたかを聞いたものである。(1)9 割程度知っていた。(2)6 割程度知っていた。(3)3 割程度知っていた。(4) ほとんどしらかかった。(5) 未回答という回答で，6 割程度の学生が 6 割〜9 割で知っていたと回答している。図 7 と 8 の結果は情報処理基礎が「底上げ」の意味を持たせた科目であることを考慮に入れると仕方がない面があるが，学習内容の水準について

検討する必要があることを示している。

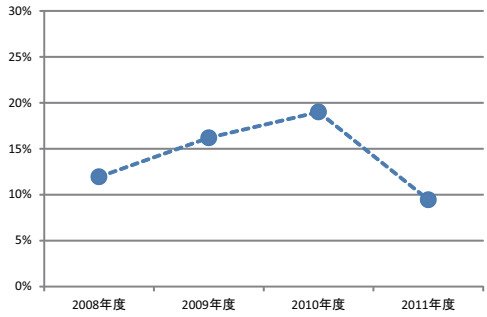


図- 9: e ラーニングについて

図 9 は，過去 4 年間での e ラーニングの学習方法の経験の有無について聞いたものである。経験者の割合は 10〜20 %の範囲内で推移している。本年度について経験者の割合が減少している。昨年度までは，事前に準備した動画教材を授業中に見せ，テストについてはネットワークを介して受けるようにしていた。これに対して，今年度からはビデオ教材の視聴もネットワークを介して受けるように変えたことが，影響しているのではないかと推測している。

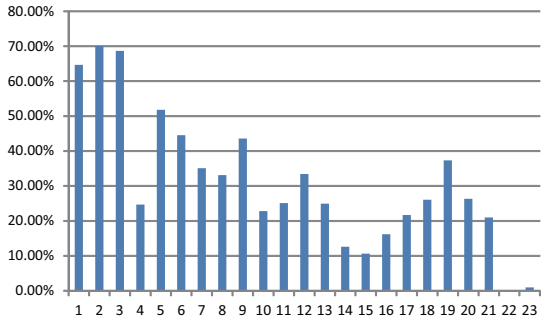


図- 10: 今後学習したい内容について

図 10 は今後学習したい内容について聞いたものである。回答は複数選択可の条件で聞き，(1) ワープロの応用的操作。(2) 表計算ソフトの応用的操作。(3) プレゼンテーションの技法。(4) 電子メールのマナーやモラル。(5) タッチタイピング。(6) プログラミング。(7) サーバ管理。(8) ネットワーク構築。(9) ハードウエアの知識。(10) モデル化とシミュレーション。(11) データベース。(12) 画像処理とマルチメディア。(13) ホームページ作成。(14) ブログの開設。(15)SNS や Twitter などのコミュニティへの参加。(16) 動画配信。(17) 著作権。(18) 個人情報とプライバシー。(19) 情報セキュリティ。(20) メディアリテラシー。(21) 情報関連資格取得。(22) その他。(23) 未回答。である。文書作成，表計算，プレゼンテーションの要望が多いのに加えてタッチタイピングやプログラミング，ハードウェアの知識，情報セキュリティなどが多くなっていることが分かる。

5 まとめ

最後に，情報処理基礎以外の情報に関する共通科目についてまとめる。現在，金沢大学では，下記のような科目を開講している。(1) 情報科学 A，(2) 情報科学 B，(3) 一歩進んだ PC 活用講座，(4) プログラミング演習 A，(5) プログラミング演習 B，(6) プログラミング演習 C，(7)ICT 素材作成術，(8) 情報発信リテラシー，(9) ○○系のための情報処理 (○○系には文，理工，医薬保健が入る。)。

図 10 の学生の要望と比較してみると文書作成，表計算，プレゼンテーションについての要望は (3) や (9) などの科目が満たしている。また，プログラミングについての要望については，(4)〜(6) で満たしている。(1) や (2) はいわゆる講義形式の授業でああるが，ハードウエアの知識等につい手の要望も満たしていると言える。また (8) などで個人情報とプライバシー，情報セキュリティなども満たされてると思われる。これに対して比較的多いにも関わらずネットワークの構築やサーバ管理などについては開講科目がないことも分かる。

現状では，情報処理基礎のように広く浅く底上げをする科目をなくすことは難しい。一方で情報処理基礎ですべての要望に応えることは難しいことも事実である。今後は，多様な要望に応えるように検討中である。

謝辞

本発表をするにあたり，科学研究費補助金 (基盤研究 C 21500930, および基盤研究 C 22500914) の支援を受けた。ここに記し謝辞とする。

サーバ室電力系統二重化による無停止運用と経過報告

Redundant Electric Power System for Main Server Room

杉浦 徳宏† 伊藤 篤†
Tokuhiro SUGIURA†, Atsushi ITO†

sugiura@cc.mie-u.ac.jp, itoa@cc.mie-u.ac.jp

†三重大学総合情報処理センター
† Center for Information Technologies and Networks, Mie University

概要

大学において，保守のための停電は避けられないものであるが，インターネットの普及によりネットワークの停止ができるだけ避けるべきものと認知されるようになってきている．特に，停電そのものは不可避であるものの，停電時に停電エリア以外についてネットワークが不通となるべき状態はできる限り避けるべきものである．また，サーバ室内において停電からの復電は，さまざまな障害が集中的に発生する引き金となるため，停電自体を排除できれば理想的である．これら二つの問題を解決し停電の影響を最小化するために，当センターの基幹サーバ室について，２つの異なる電気室から電力を引き込む電力系統の二重化と，保守点検方法を変更することで無停止運用を実現した．本発表では，その経緯と導入後の経過について報告するものである．

キーワード 無停止運用，停電

１．はじめに

大学において，停電は避けられないものである．キャンパスネットワークにも保守が必要であるように，普段，なにげなく使っている電力系統ネットワークにおいても保守停止が必要であり，一部はより厳格に法的に定められている．また，電気室については電力容量増化のための工事停電なども，耐震改修工事の多数行われている昨今不可避のものとなっている．また，ごくまれに事故による停電が発生することがある．実際に 2005 年度にセンターの電気室で事故停電が発生し，大規模障害事案となった．しかし，一方でキャンパスネットワーク及びインターネットのコモディティ化が進み，必須インフラとなったことによって，ネットワークの停止が困難な時代となりつつある．特に，停電しない箇所においてネットワークが不通となることは，できるだけ避けて欲しいとの声がよく聞かれる．また，センター内のコアスイッチや基幹サーバを設置しているサーバ室の停電について考えてみると，停電復旧時に障害が集中的に発生し，その対応に非常に苦慮していた．

これら諸問題に対し，停電エリアとネットワーク不通エリアの一致化と，電力系統二重化によるサーバ室の無停止化という取り組みによって，実質的に，停電によるネットワーク停止が顕在化しないように対策を行った．2008 年度から現在まで無停止運用を継続して

おり，大変有効に機能している．以下では，その方策の具体的な説明と導入後の経過について報告する．

２．停電の分類と要因

まず，停電はその影響範囲により大きく３種類に分けることができる．(1)全学停電，(2)電気室停電による部分停電，(3)低圧電気設備法定点検による建屋停電，である．

(1)全学停電は，電力会社の停電と学内の特高変電所の停電の２つの要因に分類できる．電力会社による停電要因としては，雷や事故，最近では電力不足による計画停電の可能性があげられる．特高変電所は，電力会社からの電力受け口となっており，学内の電気室による電力ネットワークの上位に位置し冗長性はないため，特高変電所の停電時には全学停電となる．いずれの全学停電の場合にも，雷等の短時間停電であればUPS により耐えることが可能であるが，長時間にわたる場合には，発電機等の別電源を手配する以外に対策はない．ただし，基本的に定期的な停電は発生しないものと想定することができる．

(2)電気室停電による部分停電は，停電要因により計画停電と事故停電の２つに分類できる．計画停電では，年一回実施される定期的な受変電設備点検による停電と，電気室内工事による停電の場合がある．電気室内工事停電では，容量増化工事や，高効率トランスへの更新工事などがある．事故停電としては，猫や蛇の侵入による事故，浸水による事故，また，人為的な工事作業ミスによる事故などが過去に発生している．

(3)低圧電気設備法定点検による建屋停電では，建屋内の分電盤のブレーカーごとに下流側の絶縁測定を行うため，停電が発生する．年一回，定期的に実施される．

以上により，大学内の一般的な箇所において停電は年間最低２回発生することになるが，(2)の受変電設備点検による電気室の停電と，(3)の低圧電気設備法定点検による停電を同日に設定することによって，停電発生を一回に抑えることができる．本学においては基本的にそのように計画され実施されている．

３．停電の間接的影響

停電時には，間接的な影響を受ける場合がある．例えば，コアスイッチのあるセンターが停電になる場合には，全学においてキャンパスネットワーク及びインターネットが停止することになる．また，上流となるエリアの停電によって，停電とはならない下流のネットワークが間接的に不通となる場合もある．結果として，本学では，センター以外の場所については最低年２～３回のネットワーク不通状態が発生することとなっていた．

３．１　センター外での間接的影響

ここで問題となるのは，停電対象ではないエリアについてネットワーク不通となることである．そこで，停電エリアとネットワーク不通エリアが一致するようにネットワークトポロジの改修を行ってきた．具体的には，電力の必要なスイッチ類による中継を避け，できるだけセンター内のコアスイッチと各建屋を光ファイバにより直結するよう変更を行ってきた．この改修によって，学内のほとんどの箇所において，センター停電時以外では，そのエリアの停電時のみネットワーク不通となることで実害が発生しないようになった．

しかし，センター停電時に，全学においてネットワーク不通となる問題については，対策が取られないままであり，インターネット時代が進むにつれて，この問題が大きくクローズアップされることとなってきた．

３．２　サーバ室内での間接的影響

キャンパスネットワーク用のコア装置類及び基幹サーバ類は，センター内のサーバ室に集約して設置されている．従来，停電時には発電機などによる電源確保は行わず，すべての装置類は UPS 連動によって自動停止し，復電後，自動復旧する形態をとってきた．なお，どちらの場合も基本的に立会はなしである．しかし，近年の装置類の増加によって自動復旧時の障害が頻発するようになり，その対処に非常に苦慮することとなってきていた．実際に発生する障害内容は，ハー

ドディスク故障，電源故障，ファン故障，UPS のバッテリ不良など，日常的にも発生する頻度が高いものである．これらの問題は，連続運転時よりも起動時，特にコールドブート時に問題が発生する可能性が高く，それが年一回の停電復電時に集中することでより大きな問題となって現れる．さらに，停電はその影響が小さくなるよう土日などの休日に設定されているため，障害が発生した場合には休日出勤するか，もしくは，休日出勤したとしても対応する業者側も休みであることが多いため，結局月曜日までなすすべがないという状況が発生し，障害継続時間が非常に長くなる傾向があった．

４．無停止化への取り組み

３章で述べたように，学内について停電時には停電エリアのみネットワークが不通となるという停電影響の最小化状況を達成し，また，サーバ室の停電復旧時の障害発生の顕在化を解消するためには，根本的にサーバ室の停電が発生しないようにできれば理想的である．サーバ室の停電は，２章で述べたとおり，電力供給元である電気室の停電によるものと，低圧電気設備法定点検による停電の２つに要因よって発生する．通常これらは同日に行われるため，年間の定期停電回数は一回である．これら２点についてそれぞれ電力を無停止とすることができれば，サーバ室の無停止運用が可能となる．以下，それぞれについて無停止化の方策を述べる．

４．１　電気室停電対策（電気室の二重化）

2005 年度にセンターの電気室で漏電事故が発生し，平日昼間長時間にわたってセンターが停電となる大規模障害が発生した．事故発生直後は全学停電していたものの，すぐに復旧し，問題となっていたセンターの電気室のみ停電が継続したことで，よりセンターの停電の影響が浮き彫りとなった．この事故を機に，危機管理として再発防止策を講じるべき，という声が学内からあがり，実現可能な方法を検討することとなった．まず，一般的な方法として停電時にはレンタル発電機によって電源を確保する方法が考えられるが，即時調達できるわけではなく突発的な事故に対応することができない．次に，自家発電装置の導入についても，初期導入費及び継続的なメンテナンスが必要である等，実現が容易ではないことがわかった．そこで，最終的に，従来の電気室（メイン電気室と呼ぶ）に加えて，もう一つ別の電気室（サブ電気室と呼ぶ）から電力を引き込み，必要に応じて切り替えるという電力系統二重化を実施することにした．

具体的な工事内容について，図１に系統図を，図２に切替 BOX 内の全体写真を示す．図１のとおり、200V（三相三線式）100A を２系統（１系統は空調用），同 75A を２系統，100V（単相三線式）100A を１系統の計５系統について，ダブルスローと呼ばれる切替機とブレーカーが設置されている．実際に，サブ電気室から引いた電線は，200V 系，100V 系それぞれ３本の計６本である．工事費は約 450 万円であった．尚、この仕組みにおいて，ランニングコストは全く不要である．

ネットワーク停止による直接及び間接的損失を計上することは困難であるため，具体的な費用対効果を計算することは困難ではあるが，仮に発電機によって無停止を実施する場合には，当センターの場合，レンタル費用は約 30 万円/日であるため，15 回の停電で費用を回収できることになる．

４．２　低圧電気設備法定点検による停電対策

次に，低圧電気設備法定点検による停電対策について検討を行った．この点検は建屋の分電盤内のブレーカー直下において絶縁抵抗を計測するもので，この際にブレーカーを落とすことによって発生するものである．この作業は，従来，建屋単位でまとめて行われていたため，建屋全体の電力を停止し数時間の停電として実施されてきた．しかし，実際には一つのブレーカーあたり十数秒で検査が完了するため，建屋ごと停電させる必要はない．十数秒間であれば，十分に UPS によって電源供給が可能であるため，点検実施方法を変更することで，実質的に無停止とすることが可能である．

４．３　停電時の運用

実際に，計画停電が実施される場合の作業について説明する．電気室の停電については，ほぼ土日に設定されているため，金曜日までに電力系統をサブ電気室に切り替え，月曜日にメイン電気室に戻す作業を行う．実際の切り替え作業は，分電盤側ブレーカーを遮断，切替機によるサブ側への切り替え，ブレーカー通電，の順に行う．この作業は数秒以内で実行可能であり，その間は電力供給が断たれることになるが，UPS によって電力供給されることで無停止運用を続けることが可能である．

低圧電気設備法定点検は，従来休日に実施されていたものを平日昼間に設定し，点検作業に当センタースタッフが立ち合いながら順にブレーカーを落とし，点検作業を進めていく．

５．効果と経過報告

2008 年度から無停止運用を開始し，2011 年 8 月現在 3 年以上が経過したが，引き続き無停止運用を継続している．この 3 年間において，メイン電気室について 3 回の定期停電以外に 7 回もの工事停電があった．また，2009 年に特高変電所の 30 時間にわたる計画停電があったが，この際には発電機を利用した．施設部によると，特高変電所は 15 年に一回程度，保守のため定期的に停電するとのことであったが，2010 年に大規模改修工事を行い，今後この定期停電は発生しないとのことであった．

電力系統の切替作業について，前述のとおり，数秒の停止にて切り替えを実行することが可能であるが，UPS のバッテリ不良発見のため，意図的に 15～20 秒程度停止させるようにしている．これは，電力無停止運用を継続したことによって UPS 自体の不良が発見し難くなっており，落雷や配線変更などのために短時間停電した際に，UPS 不良が発見されるということがしばしば起こったためである．UPS には，バッテリの自己診断機能が備わっているが完璧ではなく，問題の早期発見のためには，実際に負荷試験を行うことも必

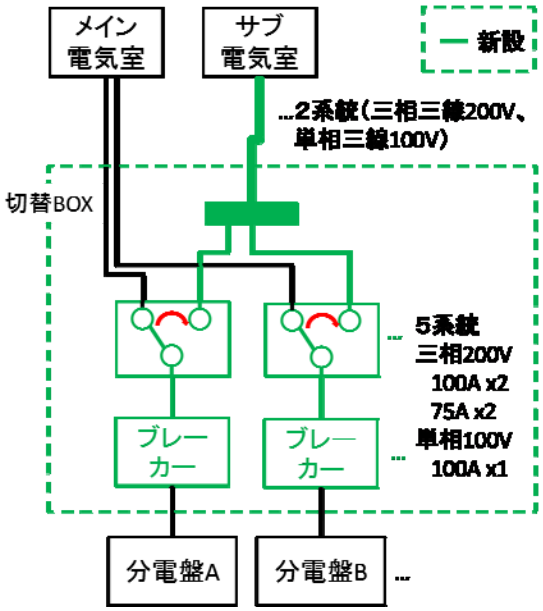


図１．電気室切替器系統図

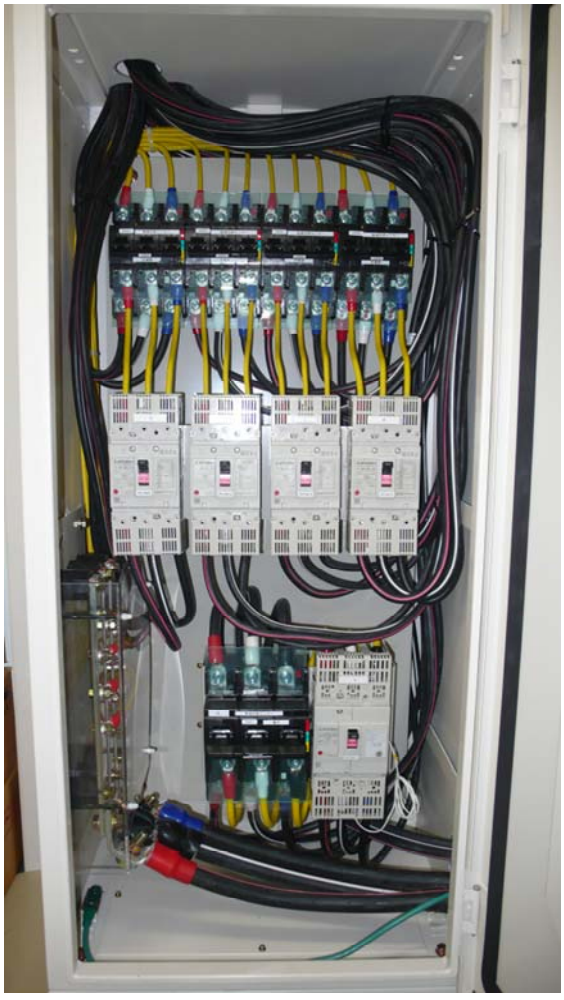


図２．電気室切替 BOX

要であると考える．

また，従来，不定期に行われる工事停電は，連絡を受けてから実施までの猶予が短い場合が多く，担当する施設部や学内との調整に大変苦慮する場合があったが，二重化後は気軽に停電に応じられるようになり，非常に円滑に工事停電を進めることが可能となった．

６．まとめ

本発表では，キャンパスネットワークの継続運用という観点から，大学における停電とその間接的な影響について明らかにした．次に，停電による影響を最小化するためには，停電エリアとネットワーク不通エリアを一致させることが必要であり，そのためには，まずネットワークのトポロジを変更し，学内の各電気室の停電によって，間接的な不通状態が発生しないようにした．次に，キャンパスネットワーク及びインターネットの停止を引き起こすセンターの基幹サーバ室について無停止運用ができるよう対策を行った．具体的には，電気室停電対策として，２つの電気室から電力を引き込み切り替え可能とする電力系統の二重化工事を行った．また，低圧電気設備法定点検による建屋停電対策として，点検実施方法を見直すことで停止時間を十数秒に抑え，UPS によるバックアップによって無停止運用を可能とした．以上により，サーバ室については完全無停止運用が可能となり，その結果，学内の各所についても，基本的に年一回の停電が発生するだけで，見かけ上ネットワークの停止は発生しないという最小化状態を実現できた．また，サーバ室については，停電復電時に顕在化していたトラブルが分散されることで，大幅な負担軽減となった．

謝辞

本件を実現するにあたり，本学施設部施設管理チームの宮崎典氏を始め同チームの諸氏には多大なるご尽力をいただき，深く感謝する．

センター紹介

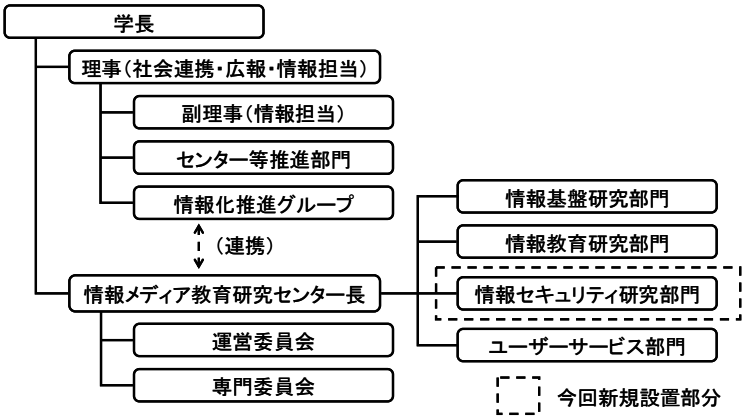
広島大学情報メディア教育研究センターに新研究部門を設置

副理事（情報担当）・情報メディア教育研究センター長　相原　玲二
情報メディア教育研究センター情報セキュリティ研究部門長　西村　浩二

1.　情報セキュリティ研究部門の設置

国内の多くの大学と同様に、広島大学においても情報セキュリティインシデントや構成員による著作権違反と疑われる行為が多数発見されており、情報セキュリティ・コンプライアンスの強化および啓発などの教育を含む多角的な対応が求められている。これを受けて本学では、学長（CEO）および理事（CIO, CISO）を頂点とする情報環境ガバナンス体制を再構築することにより、大学運営の効率化や情報セキュリティの強化などの適切な情報環境の整備を行うとの方針が示された。

これまで本学では、情報メディア教育研究センター（以下、メディアセンター）情報基盤研究部門（教員）と社会連携・広報・情報政策室情報化推進グループ（職員）が協力し、情報セキュリティインシデント等に対応する体制をとっていたが、上記の方針を具体化し状況改善の効果を上げるためには、取り組みに対する企画立案と実現、管理・運用、啓発教育の推進などを担当する中核的組織を常設する必要があるとの結論に至った。そこで平成 23 年 4 月より、当該分野に精通し、既存組織との連携を含めて組織運営に長けた教員を長とする教員組織「情報セキュリティ研究部門」を新規に設置し、メディアセンターの既存部門および社会連携・広報・情報政策室情報化推進グループなどが連携する組織体制を構築した（右図参照）。



2.　情報セキュリティ・コンプライアンス教育の実施

2.1.　フレッシュマン講習

①　受講対象者

広島大学では情報環境ガバナンス体制構築のひとつとして、平成 23 年度から在籍 1 年目の学生を対象としたフレッシュマン講習を開始した。対象は学部 1 年次生、大学院博士課程前期・後期の 1 年次生および編入学生、研究生等で、約 1 時間の座学と WebCT によるオンライン講座の受講が必須となっている。ただし本学から進学した大学院生については座学の受講が免除、また学部 1 年次生のうち教養教育（情報科目）または教養ゼミを履修している者はそれを座学に代えることができる（下表参照）。平成 23 年度の受講対象者は 4,312 名であった。

対　象　者		授業（座学）	講習（座学）	オンライン講座
学部1年次生	・前期に開講する教養教育（情報科目）を履修する学生	情報科目	－	○
	・後期に開講する教養教育（情報科目）を履修する学生 ・教養教育（情報科目）を履修しない学生	－	○	○
	・経済学部, 経済学部夜間主コースの学生	教養ゼミ	－	○
大学院M1年次生 大学院D1年次生	・他大学から進学した学生	－	○	○
	・本学から進学した学生	－	－	○
平成23年度編入学生		－	○	○
平成23年度からの非正規生（研究生等）		－	○	○

② 受講状況

座学を実施するにあたり、全学共通で使用する講義資料を作成した。講義資料は日本語版のほか、英語版、中国語版を用意した。4 月からの教養教育（情報科目）、教養ゼミで 18 回をそれぞれの授業担当教員が実施し、5 月からの講習会 11 回（うち英語と中国語による講習が各 1 回）および 6 月からの補講講習 3 回を情報セキュリティ研究部門が実施した。これらにより、座学受講対象者 3,094 名のうち 2,809 名（90.8%）が受講を完了した。一方 285 名の未受講者の多くは社会人学生で、スケジュール的に座学に出席することが困難であることから、講習会を収録したビデオ教材を WebCT でオンライン受講させることとした。

オンライン講座のオンライン教材には、教養教育（情報科目）で使用するオンライン教材（フル版）を抜粋したダイジェスト版を使用し、座学と同様に日本語版のほか、英語版、中国版を用意した。オンライン講座対象者は 2,800 名であり、9 月末までに受講して、修了テストで 60 点以上を獲得することを受講完了の条件としている。

2.2. フォローアップ講習

① アカウントの年度更新

メディアセンターでは、管理状態の悪いアカウントや長期間に渡って使用されていない遊休アカウントを撲滅するため、すべてのアカウントに有効期限を設け、継続して使用するためには年度更新が必要である。年度初めの 3 か月間（猶予期間を含む）に年度更新を行わない場合はアカウントがロックされ、メディアセンターの全サービスが利用できなくなる。平成 22 年度までは注意事項等の確認と利用規定の承諾を更新の条件としていたが、平成 23 年度からは在籍 2 年目以降の学生に対してフォローアップ講習を実施した。フォローアップ講習は、WebCT によるオンライン教材でフレッシュマン講習の内容を復習する形式となっており、受講後の確認テストで 80 点以上を獲得すると年度更新が可能となる。

② 受講状況

平成 23 年度の対象者数は 11,658 名であり、7 月 19 日現在、9,731 名（83.5%）が年度更新を完了している。平成 22 年度と比較すると、フォローアップ講習の必須化による進捗の遅れが若干見られるが、最終的には例年と同様に 10%程度のアカウントが未更新として残ると思われる。確認テストの受験に要した時間は 10 分程度であり、オンライン教材による学習時間（10～20 分を想定）を含めても対象者の負担は限定的であると考えられる。

2.3. 今後の課題

フレッシュマン講習における座学の開講スケジュールは、もともと過密スケジュールである新入学生の履修状況を考慮して調整を行う必要があるため困難を極めている。また、大学院生や研究生等は電子掲示版（学生ポータル上）を見る習慣を持たない者が多いため、指導教員を通じた周知が必要である。留学生に対する対応として英語版、中国語版の資料を作成し、外国語による座学も各 1 回開講したが、回数としては不足している。ただし担当教員の負担が大きいため、留学生受け入れ部局の積極的な協力が不可欠である。一方、フォローアップ講習については、今後教職員への対象拡大を検討しているところである。

3. 情報環境ガバナンス構築に向けて

今回の新研究部門設置にあたって教員増は認められず、准教授から教授へのポストアップおよび既存研究部門教員の異動で対応した。既存業務も依然増加傾向にあり、総業務量に対する人的資源の供給が追いついていない。また、本学における CIO の役割や権限が十分に明文化されておらず、情報環境ガバナンス体制の再構築に関する課題は山積しているが、安全かつ快適な情報環境の全構成員への提供を目指して一歩ずつ前進することが肝要である。

情報基盤センター

Information Technology Center

ITC

国立大学法人
電気通信大学

ご 挨 拶

電気通信大学における情報基盤センターは、その前身である情報処理センターの発足以来30年を経ています。この間、学術情報ネットワーク西東京地区のノード・ポイントとしての役割を担いつつ全学ネットワークの1Gbpsを実現するなど、大容量データ処理能力を備えた高速ネットワーク環境の整備を進めてまいりました。

一方、大学を取り巻く社会環境は技術革新の進展とともに高度なITを創造し、また自在に駆使することができる人材を強く求めており、電気通信大学はその要請に応えていくことを基本命題として、2010年度より情報理工学部を骨格とする新たな大学経営へと大きく舵を切りました。

従来、本学における高速ネットワークの整備にあたっては、情報基盤センターとして以下の事柄を念頭において取り組んでまいりました。

学生の皆様が学習・研究を進めるために、使い易く効率的なネットワークシステムを提供すること。教職員の皆様のためには効率的で質の高い有効なシステムであること。

教育・研究活動支援のためだけでなく、教務・財務・人事・総務など大学経営の基礎を担う部門においても効率的に活用できるネットワークシステムを実現すること。

学内のすべての人々がいつでも必要に応じて様々なアプリケーションを利用でき、またそれぞれ迅速なレスポンスが得られること。

ネットワークシステムを取り巻く大学内外からの不当な侵入や攻撃などに耐え得る安全・安心なセキュリテイ・システムが備えられていること。

これらは今後とも引き続いて取り組むべきことですが、大学における情報基盤整備事業の主たる内容は、「学内共同利用施設としてコンピュータネットワークを中心とする学術情報基盤の整備とそれらの維持管理」が基本業務であり、これに加えて「教育研究支援」、「学術情報サービス」、「情報技法教育」、「付属図書館関係」、さらに「学務事務処理システム」などきわめて多岐にわたる事業を推進することが期待されています。

特に法人化後の大学においては経営効率を高めるために、従来のいわゆる縦割り方式を廃した情報システムの構築や組織の統合化への必要が高まっています。これら増大する一方の需要に対して年々縮減する一方の大学運営予算のもとでは、情報基盤センターの人員・体制も限定的とならざるを得ず、日々の対応に相当な工夫と努力を重ねるほかありません。当センターとしては、大学外部において進行しつつある様々な情報基盤（たとえばSINET4、GakuNin、あるいはクラウドコンピューティング等々）サービスの利活用も考慮しつつ、皆様の需要にお応えできるよう一所懸命に努めてまいります。
そのためにも学内教職員・学生利用者の皆様の深いご理解とご協力をお願いいたします。

2010年10月

情報基盤センター長　　小池　英樹

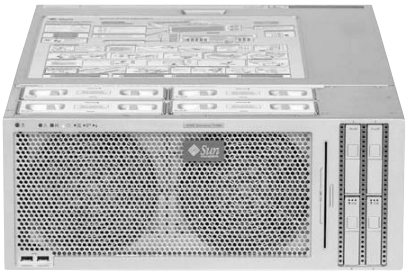
システム紹介

教室利用者環境

教室系端末

Apple Mac mini 300台を設置。
Mac OS X上に仮想環境による Windows Vistaを用意することで幅広い情報教育へ対応しています。
また個人領域としてひとりあたり 20 GByteを提供しています。

教室系バックエンド



利用者用の端末である Apple Mac miniから、UNIX計算機システム(Sun SPARC Enterprise T5440)をリモートで利用できます。

ネットワーク

高速ネットワークの提供

学内にあるほぼすべての棟間は 10 Gbpsで接続するようにネットワーク帯域の高速化をはかりました。また情報基盤センター内にある基幹ネットワークも H3C S5820X 4台の仮想化ルータの実現により 40 Gbpsへと高速化しました。

対外セキュリティの更なる強化として攻撃に対してダイナミックに接続を遮断するためにIDS / IPSを導入しています。
<IPS: Intrusion Prebention System　不正侵入阻止のため侵入を検知すると接続遮断などの処理をリアルタイムにおこなう機能を有する装置>

認証システムの多方面での利用促進

情報基盤センターで導入の LDAP認証システムは研究・教育系、図書館のほか e-Learning、学務情報システムなど広くカバーしています。

無線LANの一元管理

学内全域を網羅した無線LANではリモート管理を実現して管理を簡素化、より安全・安定した運用を目指しています。

研究系計算機環境

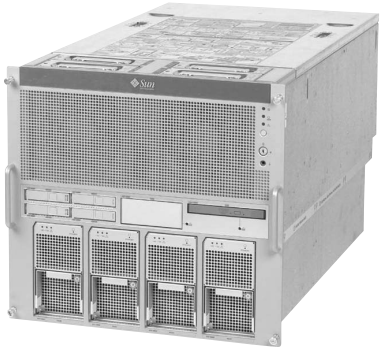
大型RAIDディスク装置の導入

研究系利用者の個人領域はひとりあたり 50 GByteを提供しています。

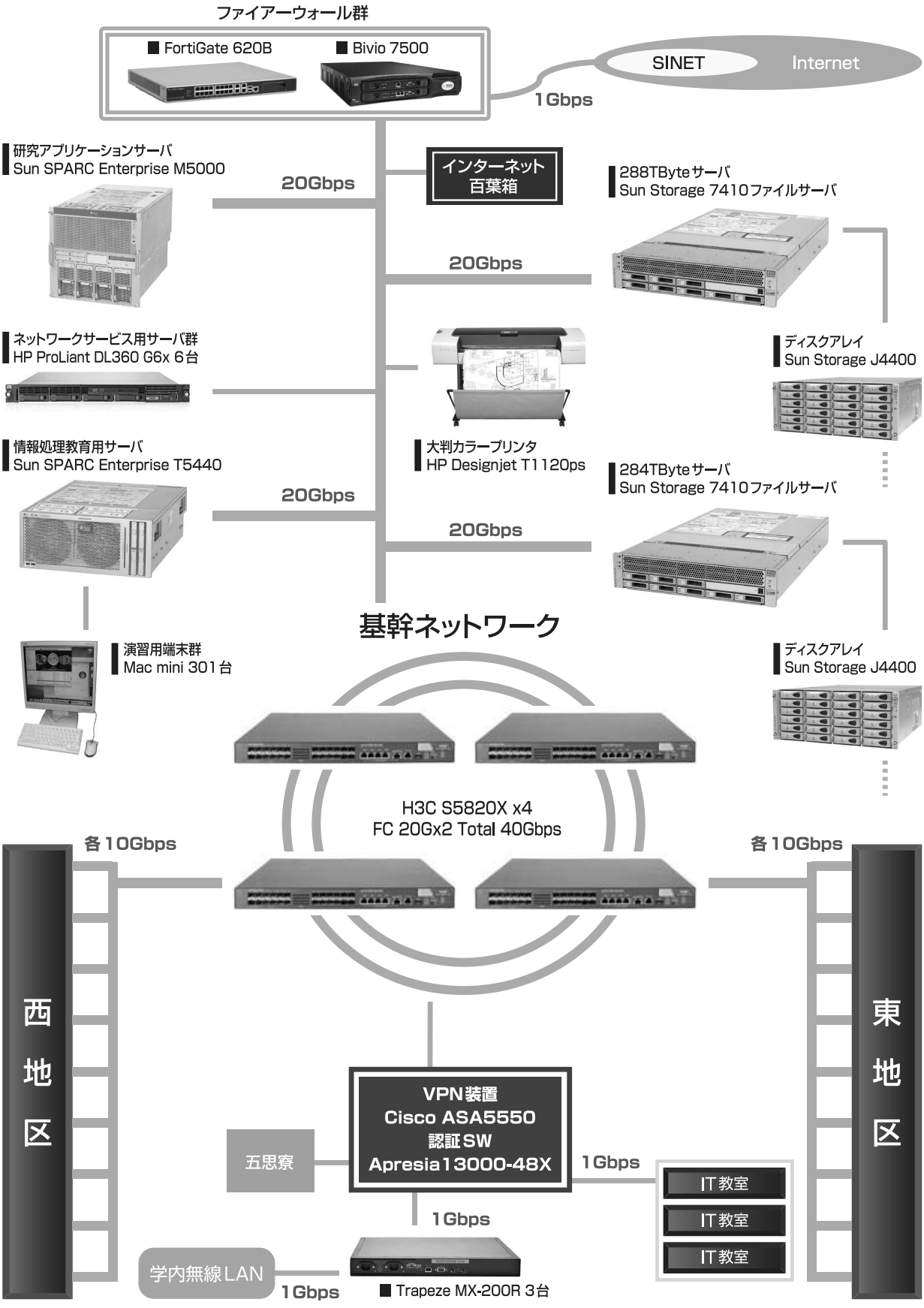
全学メールゲートウェイの強化

メールサーバー4台の協調により、処理能力の増強をはかっています。

■Sun SPARC Enterprise M5000系を中心とした利用者環境の充実



情報基盤センターシステム構成略図



利 用 環 境

主なユーティリティソフトウェア、アプリケーションソフトウェアのサービス

IMSL Fortran ライブラリ
Gaussian09
Maple
Unigraphics NX（Nastran プリポスト機能付、教育用システムと共用）
IMSL C ライブラリ
AVS/Express Developer
Verilog-HDL（教育用システムと共用）
Matlab、Simulink、Toolbox（教育用システムと共用）

貸し出しソフトウェア

アンチウィルスソフト ---------- Symantec Endpoint Protection（For Windows）、Sophos Anti-Virus（For Mac）
数式処理ソフト ---------- Maple
数値解析ソフト ---------- MATLAB（Toolbox,Simulink etc.）、Gaussian09
UNIX 用仮名漢字変換 ---------- Wnn（Linux/UNIX）

その他のサービス

バーチャルサーバ

DNS、メール、Web サーバなどの仮想環境を学科・研究室向けに用意してあります。またバーチャルマシンの提供も予定しています。詳細は以下の URL をご参照ください。

► http://www.cc.uec.ac.jp/network/virtual.html

インターネット百葉箱

気象情報、新宿方面の静止画などのリアルタイムでの提供のほか過去のデータ等も参照できます。詳細は以下の URL をご参照ください。（学外へも公開）

► http://weather.cc.uec.ac.jp/

Webメール

学外などからのメール利用も容易にする Web メールを提供します。アクセスはつぎのとおりです。

► https://webmail.cc.uec.ac.jp/

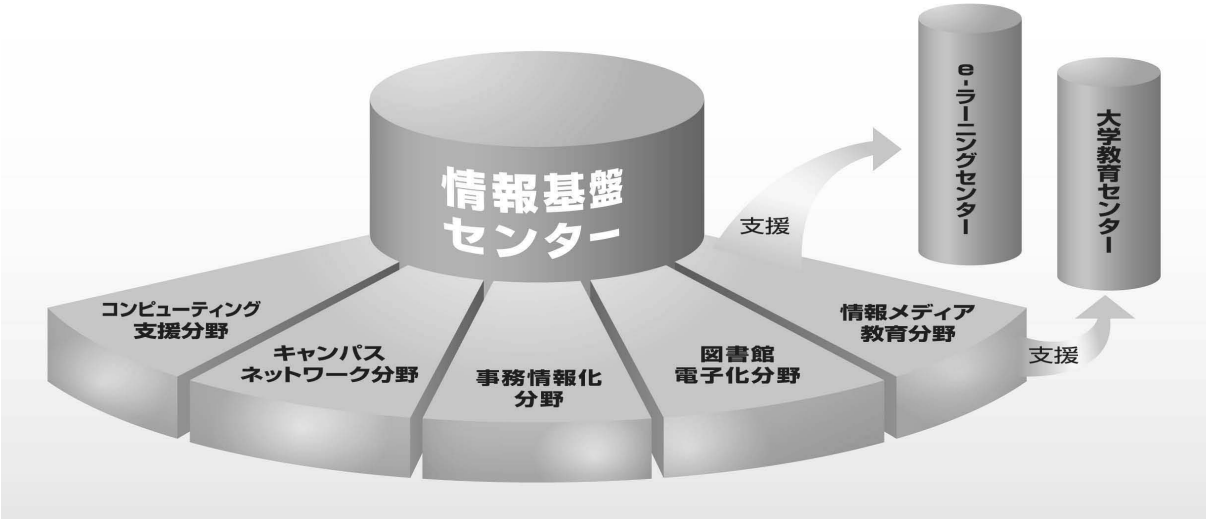
無線LAN

学内ネットワークの常時利用を可能とする無線 LAN 環境を提供します。学会等の来訪者も利用できます。eduroam も予定しています。

全学統一メールアドレスの提供

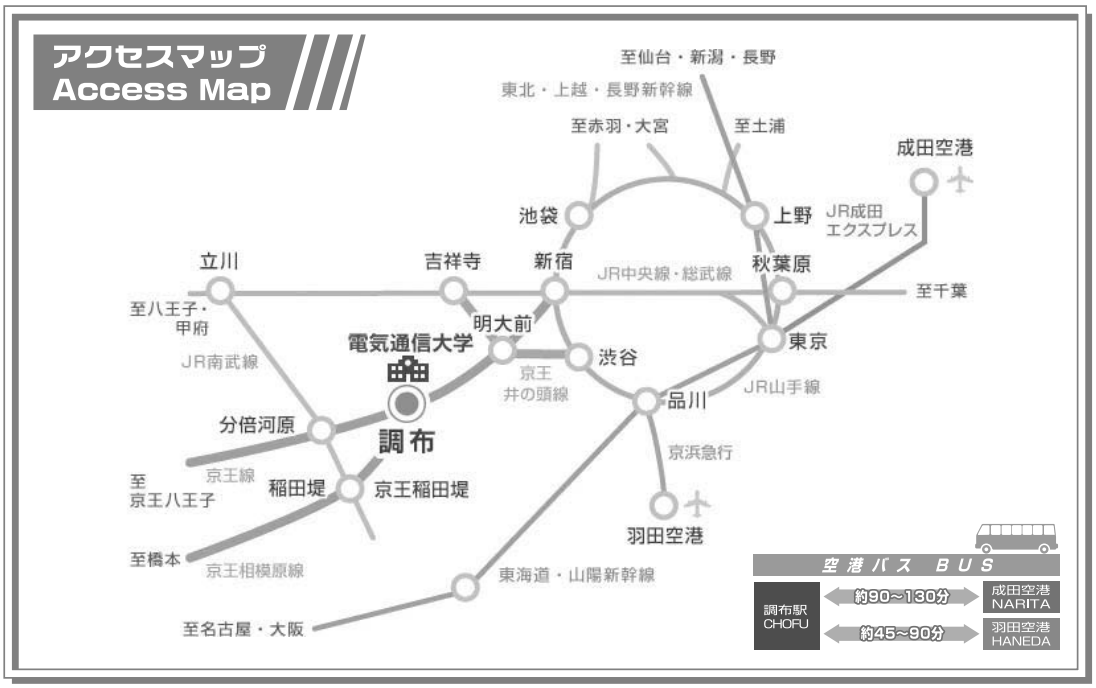
- 学生および教職員すべてが同一ドメインでのメールを利用できる環境を提供します。（現在準備中）
- 学内、学外を問わず前述の Web メールの利用により、より継続的な利用を可能にします。

組 織 概 要



センターのあゆみ

昭和39年	(1964)	OKITAC5090C稼動開始、電子計算機室発足
昭和49年	(1974)	データステーション建物竣工 HITAC8250(128KB)稼動
		東大大型計算機センターとのリモートバッチ(2400bps)開始
昭和54年	(1979)	HITAC M-170システム稼動
昭和55年1月	(1980)	情報処理センター発足
		土方克方 物理工学科教授 センター長に就任
昭和55年2月		大学間ネットワークTIPサービスを全国で初めて開始
昭和55年10月		大学間ネットワークサービス開始
昭和57年	(1982)	HITAC M-180システム稼動
昭和58年	(1983)	HITAC 8644 光ファイバーネットワークテストシステム導入
昭和60年	(1985)	HITAC M-260 システム稼動 光ループネット開始、JUNET開始
昭和62年	(1987)	熊本芳朗 電子工学科教授 情報処理センター長に就任
平成元年5月	(1989)	学内共同教育研究施設・総合情報処理センターを設置
平成元年6月		熊本芳朗 電子工学科教授 総合情報処理センター長に就任
平成 2年	(1990)	BITNET開始、IBM3090-18Sシステム稼動
平成 3年	(1991)	学術情報ネットワーク西東京地区ノード校になる
平成 4年	(1992)	インターネットバックボーン(SINET)運用開始
平成 6年	(1994)	CRAY-EL98システム稼動
平成 7年	(1995)	伊藤秀一 IS教授 総合情報処理センター長に就任
平成10年3月	(1998)	SGI Origin2000システム稼動
平成11年3月	(1999)	全学研究室及び教室に情報コンセントを設置
		全学100Mbps化
平成11年6月	(1999)	箱崎勝也 IS教授 総合情報処理センター長に就任
平成13年7月	(2001)	全学ネットワーク 1Gbps完成
平成14年3月	(2002)	SGI Origin3400稼動
平成14年8月	(2002)	総合研究棟(コミュニケーションパーク)に移転稼動
平成15年6月	(2003)	尾内理紀夫 情報工学科教授 総合情報処理センター長に就任
平成17年7月	(2005)	尾関和彦 情報通信工学科教授 総合情報処理センター長に就任
平成18年3月	(2006)	Sun E25Kシステム稼動
平成18年4月		情報基盤センター設置
平成18年9月		建屋内各階に 1Gスイッチ設置
平成20年4月	(2008)	藏信行理事 情報基盤センター長に就任
平成22年2月	(2010)	春日正好理事 情報基盤センター長に就任
平成22年3月		Sun M5000システム稼動
平成22年10月		小池英樹 IS教授 情報基盤センター長に就任



センターのスタッフ

センター長[兼任]	小池 英樹	先任技術専門員	才木 良治	技術専門職員	山口 昭男	技術支援員	井桁 正人
准教授 [専任]	高田 昌之	先任技術専門職員	岡野 豊	事務補佐員	朝倉 雅子	技術支援員	岸本 創
准教授 [専任]	土屋 英亮	技術専門職員	服部 修二	技術支援員	緒方 優	技術支援員	田中 英人
准教授 [兼任]	桑田 正行	技術専門職員	石井 和広	技術支援員	神原 誠	技術支援員	西尾 奈恵
助 教 [専任]	矢崎 俊志	技術専門職員	大西 邦弘	技術支援員	松橋 拓人		

国立大学法人 電気通信大学 情報基盤センター 業務室 ☎042-443-5718
〒182-8585 東京都調布市調布ヶ丘1-5-1 京王線調布駅北口下車 徒歩5分 http://www.cc.uec.ac.jp/

報告

第５回国立大学法人情報系センター長会議議事要旨

○開催日時：平成２２年１０月２２日（金）　１４：００ ～ １７：００
○開催場所：ホテル日航奈良　羽衣の間（４階）

○出席者（敬称略）：
　文部科学省研究振興局情報課学術基盤整備室長　飯澤隆夫
　文部科学省研究振興局情報課学術基盤整備室学術情報第一係長　井上裕幸
　国立情報学研究所学術ネットワーク研究開発センター長　山田茂樹
　国立情報学研究所学術基盤推進部学術ネットワーク課　特任専門員　平原孝明
　奈良先端科学技術大学院大学副学長（附属図書館長）　木戸出正繼

北海道教育、室蘭工業、帯広畜産、旭川医科、北見工業、弘前、岩手、宮城教育、秋田、
山形、福島、茨城、筑波、筑波技術、宇都宮、群馬、埼玉、千葉、東京学芸、東京農工、
東京工業、東京海洋、お茶の水女子、電気通信、一橋、横浜国立、新潟、長岡技術科学、
上越教育、富山、金沢、福井、信州、北陸先端科学技術大学院、山梨、岐阜、静岡、
浜松医科、愛知教育、名古屋、名古屋工業、豊橋技術科学、三重、滋賀、滋賀医科、
京都教育、京都工芸繊維、大阪教育、神戸、奈良教育、奈良女子、和歌山、
奈良先端科学技術大学院、鳥取、島根、岡山、広島、山口、徳島、鳴門教育、香川、愛媛、
高知、福岡教育、九州工業、佐賀、長崎、熊本、大分、宮崎、鹿児島、鹿屋体育、琉球
以上７３大学のセンター長（代理者を含む）

○配付資料：
　資料１　第５回国立大学法人情報系センター長会議
　資料２　学術情報基盤等に関する最近の動向等について（文部科学省説明資料）
　資料３　ＳＩＮＥＴ４および学認について（国立情報学研究所説明資料）
　資料４　ＮＡＩＳＴにおける情報科学センターから総合情報基盤センターへの展開
　資料５　第２２回情報処理センター等担当者技術研究会について
　資料６　第５回国立大学法人情報系センター研究交流・連絡会議及び第１４回学術情報処理研究集会について
　資料７　大学ＩＣＴ推進協議会の設立とその参加意義等に関する紹介
　資料８　国立大学法人情報系センター協議会総会／センター長会議／研究交流・連絡会議　開催校一覧および運営規約

○会議内容：

１　配布資料の確認

当会議の総合司会である、奈良女子大学の外嶋総務･企画課長から、配付資料の確認があった。

２　日程等説明

外嶋総務･企画課長から、本日の日程等の説明があった。

３　開会

外嶋総務･企画課長から、開会宣言があった。

４　来賓紹介

外嶋総務･企画課長から､来賓である文部科学省研究振興局情報課の飯澤学術基盤整備室長、国立情報学研究所学術ネットワーク研究開発センターの山田センター長及び奈良先端科学技術大学院大学の木戸出副学長の紹介があった。

５　当番校挨拶

当番校である奈良女子大学の野口学長及び加古総合情報処理センター長から挨拶があった。

６　文部科学省説明

飯澤学術基盤整備室長から、挨拶の後、学術情報基盤等に関する最近の動向等について、資料２に基づき以下の説明があった。

１）科学技術・学術審議会学術分科会研究環境基盤部会学術情報基盤作業部会における審議状況

科学技術・学術審議会研究環境基盤部会の下に置かれている学術情報基盤作業部会において、平成１８年３月に『学術情報基盤の今後の在り方について』という報告がまとめられているところであり、そのフォローアップとして、第４期の学術情報基盤作業部会においては、情報基盤センターの在り方及び学術情報ネットワークの今後の整備の在り方について審議され、平成２０年１２月に『学術情報基盤整備に関する対応方策等について（審議のまとめ)』が出されている。平成２１年２月からは、図書館の整備、学術情報流通のあり方を中心に審議している。昨年の秋以降は、特に「大学図書館の機能・役割及び戦略的な位置付け」「大学図書館職員の育成・確保」を中心に審議しており、とりまとめに向けた最終段階に入っている。

平成２２年９月末に行われた作業部会において、法人化後の国立大学は財政的にも

制度的にも非常に変化している中で、大学図書館に求められている役割・機能は何なのかということを整理している。また、図書館職員に求められる資質・能力、及び育成のあり方について取りまとめる方向で議論している。

これらの議論は、今年末を目途に取りまとめをして、公表する方向で考えている。

2）次期学術情報ネットワークに関する検討

先に紹介した学術情報基盤作業部会の審議まとめを受け、次期学術情報ネットワークの具体的な整備方策について検討するために文部科学省内に検討会を設けて審議を進め、本年７月には『次期学術情報ネットワークの整備について（意見のとりまとめ)』と題した取りまとめが行われたところである。本まとめの概要として、次期学術情報ネットワークは、高度化、環境の向上、経済性の向上、持続的な整備方策の検討という整備の基本方針のもと、先進性、優位性を確保するため、引き続き国立情報学研究所の一元的な整備を図っていくことが適当であると述べられている。

基本的な構成については、ネットワーク需要の拡大へ適切に対応するために、高速で高信頼のコア回線を導入するとともに、上位レイヤ機能の実現、さらには、先端学術基盤格差を解消することなどが必要であり、その整備にあたっては、より一層の大学等関連機関との連携･協力の強化が求められることなどが述べられている。今後は、引き続き、学術情報ネットワークの役割、特別なニーズや新たなニーズを伴う場合を含めた経費負担の在り方などについて検討する必要があることなどが述べられている。

3）平成２３年度概算要求

平成２３年度の概算要求は、各省一律１０％減となっている中で、「元気な日本復活特別枠」として、各省の判断で１０％以上の削減をすることにより、その３倍の要望が可能となっており、文部科学省全体として、要求・要望額は、対前年度比４．３％増となっている。この特別枠の要望事項については、今後、政務ヒアリング、政策コンテストなどを経て決定していくことが想定される。

情報系センターに関連するものとして、大学からの要望に基づく学内ＬＡＮ等の整備に係る経費を要求しているほか、国立情報学研究所の学術情報ネットワーク（ＳＩＮＥＴ）については、平成２３年度にＳＩＮＥＴ４への移行により、高速化・高度化を実現する新たなネットワークを構築することとして、約７９億円（１７億円増）を全て要望枠で要望している。

情報系センターに係る概算要求については、７月の情報系センター協議会でもお話ししたとおり、法人としての基盤の必要性などについて引き続きご検討いただき、各大学における検討を踏まえて、文部科学省にご相談いただきたい。

4）第４期科学技術基本計画策定に向けた検討

総合科学技術会議基本政策専門調査会において、「科学技術に関する基本政策につい

て」の報告がまとまっている。この中で、研究情報基盤の整備という事項が立てられ、ネットワークの整備や運用、研究成果の保存、発信など着実な推進が図られてきた。

一方、財政事情等が厳しい状況にある中、個々の機関においては研究情報基盤の整備が困難な状況になりつつあるため、国として研究成果の情報発信と流通体制のより一層の充実に向けて、基盤強化に向けた取り組み、具体的にはオープンアクセスの推進、デジタル情報資源及び流通システムの整備、電子ジャーナルの効率的な整備などを推進していくことの必要性について指摘されている。

7　国立情報学研究所説明

山田学術ネットワーク研究開発センター長から、ＳＩＮＥＴ４および学認について、資料３に基づき、以下の説明があった。

1）ＳＩＮＥＴ４について

来年４月からスタートするＳＩＮＥＴ４の主な特徴として、エッジノードの高安定化・学術基盤格差の解消・上位レイヤサービスの展開があげられる。結果的に、以下のネットワーク構成の変更を行っている。

- コアノードのデータセンターを８拠点に集約、最適化
- エッジノードは大学キャンパスからデータセンターへ移行。ノード未設置県には新しく設置する。来年度は山形県、福島県、奈良県、宮崎県の４県の予定
- ネットワークの回線の高速化
- データセンターは、どのキャリアのアクセス回線でも同様な接続を可能にし、計画停電等による電源供給停止がない環境を整えることで、ＳＩＮＥＴの信頼性を向上する。

なお、ＳＩＮＥＴ３から４へは、一度に切り替えるのではなく、段階的な移行を考えている。ただし、遅くとも平成２７年度末には非ノード校の回線がすべてエッジノードに直接収容される形態になるように進めていく。

（ア）ＳＩＮＥＴ４運用開始までのロードマップ

ＳＩＮＥＴ４は来年４月以降の運用開始に向けて現在作業中である。今年度当初からの第１期アクセス回線の共同調達はある程度達成した。来年も第２期の調達を実現できるように努力しているが、予算状況によっては見直しもあり得る。また、ＳＩＮＥＴ３から４への移行時期は、大学の入試シーズンと重なって迷惑をかけると思われるが、ご協力いただきたい。

（イ）ＳＩＮＥＴ４運用開始後について

ＳＩＮＥＴ４運用中、大学キャンパスに配置した小型レイヤ２スイッチ経由の加入機関との接続については、既存アクセス回線の 1Ｇｂｐｓまでの増速、ＶＰＮの新規

接続は可能とするが、ＳＩＮＥＴ４が終了するまでに、小型レイヤ２スイッチ経由による接続はなくす予定である。

（ウ）ＳＩＮＥＴ４運用終了後について

ダークファイバーを使った接続の場合、ノード校と非ノード校の構成が基本的に同じになるため、どの機関が経費負担すべきかが検討課題と考えられる。ＳＩＮＥＴ４の運用期間内に、いろいろ検討・相談しながら対応していきたい。

２）学認について

「学認」は、将来的に、マッシュアップサービスのような形に展開できるという点で、非常にメリットが大きい。

２００８年度からテスト環境下での利用が始まり、本年度は本格的な運用を始めている。使えるサービスは増加しており、大学独自で活用しているケースもある。ＮＩＩではシボレス構築研修も行っており、好評を得ている。

今年８月に情報サービス連携コンソーシアムを設立した。これは主に産業界と連携し、「学認」のプロジェクトを強力に推進するのが目的である。

「学認」の本格運用が始まり、タスクフォースチーム・研修などを通し、普及の努力を進めており、それらの活動・新しい情報などをなんらかの形で報告する予定である。

８　基調講演

奈良先端科学技術大学院大学の木戸出副学長から「ＮＡＩＳＴにおける情報科学センターから総合情報基盤センターへの展開」と題した基調講演が行われた。その概要は次のとおりである。

１）奈良先端科学技術大学院大学の紹介

けいはんな学研都市にある、独立系の学部を持たない大学院である。情報・バイオ・物質の３研究科からなり、教職員約４００名及び学生約１１００名で構成されている。

２）総合情報基盤センターの設立

平成２２年７月より、附属図書館と情報科学センターを統合し、総合情報基盤センターを設立した。ＣＩＯを設定し、大学全体の学術情報に関するコンテンツから情報ネットワークシステムを一体で管理運営することをコンセプトとしている。また来年、開学２０年を迎えるのを機に、組織やサービス、人事管理上の問題点を挙げ、それぞれ円滑にしようとしている。

具体的には、センター内に次世代研究グループ（教員により構成）、情報基盤技術サービスグループ（教員と技術職員により構成）、学術情報サービスグループ（事務職員により構成）の３つのグループを作り、組織化し、ヒト・モノ・カネを集約管理して

いる。

3）全学情報基盤について

全学情報環境を「曼陀羅システム」と呼んでいる。過不足のない、充実した環境提供をしたいということからである。この設計・導入・運営するにあたっての、コンセプトを最先端のプラットホーム、インフラの準備、運営の効率化とした。全学一体運営のため、図書館のデジタル化システムを含めて、曼陀羅システム上にすべて乗せようとしている。曼陀羅ネットワークは、有線ネットワークと、キャンパス内で接続可能な、無線ネットワークで構成されている。

端末は、約１５００名（教職員および学生）の構成員に対し、１台ずつ対応している。３研究科の現場において使い方は様々である。個人のファイル、研究用ファイルを総合情報基盤センターで高い信頼性のあるシステムファイルサーバを使用することを考えている。ディスク容量全体はペタの単位である。

4）電子図書館について

基本は、デジタル化、電子化したものを端末で検索する形である。全ての情報は、使いやすいように検索機能、サービス機能を付け、端末上に表示させている。今後必要なら一般公開も考えている。

授業のアーカイブ等、大学から発信する情報をいかに上手く電子化し、学内学外利用できるようにするか、上手く利用できるように電子図書館システムも曼陀羅内で動かそうとしている。図書館業務も電子化され、図書管理システムとして動いている。これから追加を試みようとしているのが、博物館機能である。大学の歴史がまだ２０年と浅いため、過去を含めこれから起こるべきことを全て電子化することを想定している。

5）総合情報基盤センターのこれからについて

大学全体のエネルギー管理、情報管理、人員管理等の様々なことを管理運営できるサービス機能をセンターで明確に構築し、運営しようとしている。扱うべきデータが多様化していく中で、どのように対応していくか枠組みを作る必要がある。また、人材育成、人材教育も具体的に行いたい。大学全体の効率化促進の道筋を付けていけるよう現在検証中である。

9　議長選出

奈良女子大学の加古総合情報処理センター長が議長として選出された。

１０　議　事

議長の議事進行のもと、次の議題について協議を行った。

（１）報告事項

ア　第２２回情報処理センター等担当者技術研究会について

技術研究会当番校である名古屋工業大学の松尾情報基盤センター長から、資料５に基づき、次の報告があった。

第２２回情報処理センター等担当者技術研究会が、平成２２年９月１６日（木）及び１７日（金）に開催され、９１名が参加した。発表者は１７名だが、聴講のみの方が５２名の非常に懇親的で活発な会となった。技術職員の交流会の形で行われ、研究発表が６件、現状報告が１１件、意見交換会の後、名古屋工業大学の施設見学をした。

次回は室蘭工業大学で開催される。

イ　第５回国立大学法人情報系センター研究交流・連絡会議及び第１４回学術情報処理研究集会について

研究交流・連絡会議当番校である和歌山大学の河原システム情報学センター長から、資料６に基づき次の報告があった。

第５回情報系センター研究交流･連絡会議及び第１４回学術情報処理研究集会を、９月９日（木)、１０日（金）に県民交流プラザ・和歌山ビッグ愛を会場として開催した。参加大学は５９大学、連絡会議は９５名、研究集会は１００名が参加した。センター長や技術職員の方々が研究発表を２２件行い、そのうち原著論文数が１４件であった。参加人数は年々少しずつだが増加している。

議題は、１日目にＩＣＴ推進協議会、学認、ソフトウェアアライアンスの取扱い、マイクロソフトのライセンス契約、国立大学の情報システムの開発ライフサイクルなど、実際の運用に係わる議論を行い、２日目に個別の研究テーマについての討議が行われた。

会議の中で、参加しているメンバーや議題の中身がセンター長会議など他の会議と重複しているものが多いので、整理が必要ではないかという指摘があった。この意見は、次の議題で討論していただきたい。

今回の連絡会議及び研究集会は、非常に活発に切実な問題が話し合われたので、ノウハウの交流会という意味で十分機能していた。

（２）議　　題

ア　第５回国立大学法人情報系センター研究交流・連絡会議における要望について

本議題については、報告事項イの内容と重複したため、報告事項イにも出たとおり、各種会議において重複内容が多いため、整理を行った方がよいのでは、という話題に基づき、議長から、センター長会議、研究交流・連絡会議、研究集会開催及び研究会誌の発行について、当番校及び担当者選任に係るこれまでの例が挙げられた。千葉大学土屋総合メディア基盤センター長から、従来どおり委員を決定するよりも、議題の順序を変更して一通り議論を済ませてから、その議論の結果を元に、次期開催校及び委員の選任の議論に入ってはどうか、という動議があり、拍手により承認された。この議題に関しては、議題最後に、議題オと関連付けて話し合われることとなり、本件の審議を終了した。

イ　情報サービスとユーザーを最適に結びつける枠組みについて

議題提案校の東京外国語大学から、情報系センターの活動範囲の考察、ＮＩＩの「学認」を視野に入れて、各センターが維持管理するネットワーク資源、計算資源、蓄積資源、サービス資源等の整理と、組織内で提供する資源、組織外へ提供できる資源の区分、及び提供の仕方（情報系センターが、学内外で資源提供能力を向上する施策も含む）について伺いたいとの要望があったが、佐野総合情報コラボレーションセンター長が欠席のため、審議保留となった。

ウ　大学ＩＣＴ推進協議会の設立とその参加意義等に関する紹介

初めに、熊本大学の中野総合情報基盤センター長から、今後の情報共有や技術協力、政府への働きかけ等に大きな意味を持つことが期待される、大学ＩＣＴ協会（仮称、日本版ＥＤＵＣＡＵＳＥ）の設立とその参加意義等に関する紹介をしたいということで、名古屋大学の阿草情報基盤センター長から次のとおり説明があった。

自分たちの情報化投資が妥当な方向に向いているか協議する場として、アメリカのＥＤＵＣＡＵＳＥのように、高等教育機関における情報技術の活用のためのコミュニケーションとインフォメーションのマネジメントをするための組織を日本に設立するため、大学ＩＣＴ推進協議会の設立を計画した。情報基盤を整備し、大学の教育研究・経営を強化し支えるのが目標である。具体的には、共通の基盤をどのように作るか、職員のＩＣＴ利活用のレベルアップ、情報スタッフのキャリアパスの整備である。事業内容として、ＩＴベンチマーキングや、さまざまな会議で議論しているような内容や情報を交換できる場を作りたいと考えている。

この説明に対し、千葉大学の土屋総合メディア基盤センター長から、大学ＩＣＴ推進協議会へ参画するにあたっての費用負担や、メリットについて質問があり、阿

草情報基盤センター長から、大学の規模と人員構成等からその情報化投資が妥当であるか､その活用レベルがどこにあるかを大学間でベンチマーキングできる､また、ソフトウェアアライアンス交渉の際に交渉力を強化できる等、との回答があった。

次に、奈良先端大学の木戸出副学長から、大学ＩＣＴ推進協議会に参加する実働メンバーについての質問があり、阿草情報基盤センター長より、大学ＣＩＯレベルの参加が望まれる、ＣＩＯレベルではＩＣＴについてわからない場合もあるが、情報を交換できる場がまずは必要である、との回答を得て、本件の審議を終了した。

エ　情報系センターのアウトソーシング化の現状と課題について

島根大学の小林准教授から、情報系センターあるいは大学規模でアウトソーシングしている大学があれば、その内容・利点・課題・コスト・運用状況などを教えてほしい。特に、静岡大学の状況が知りたいとの要望があった。

これに対し、静岡大学の長谷川情報基盤副センター長から、今年３月に行われた基盤更新では､｢安い計算リソース､見えないリソース､サーバにさわらなくていい｣というキーワードのもとクラウド化を行った、また１０月に、商用のクラウドを主メモリで３０４ＧＢ調達し、希望者には自由なメモリ配分（0.5, 1.0, 2.0, 3.0,4.0GB Linux/Windows）で無償で割り当てを行っていること、学内のサーバはなくす方向で進めている、コストメリットは確実にあるとの報告があった。

また議長から、奈良女子大学ではサーバのメンテナンスを外部委託している、外部に委託したほうがセキュリティ・運用停止について安心な面もある、との意見が出された。

オ　次期開催校について

佐賀大学の只木総合情報基盤センター長から、現在行われているセンター長会議・連絡会議等の内容重複の整理をするためのワーキンググループを組織したいとの提案及びその承認の要望があり、これに対し次のとおり意見が出された。

・任期のこともあるので早急に対応できないか
・センター長会議は、大学のＩＣＴマネジメントの方向性を議論する場所なので、ワーキンググループは、センター長会議の開催の有無を議論するのではなく、センター長会議で話し合うべき内容を議論してほしい
・只木総合情報基盤センター長にワーキンググループの設置やメンバー選出を含めて一任してはどうか。ただし、個人に負担をかけることになるので、それなりの見返りは必要なのでは？
・次回の協議会のアンケートを充実させ、それをもとに価値ある内容の議論をすれ

ば、一部の方々に負担をかけなくても、今まで行われてきた会議開催作業の流れの中で収拾できるのではないか？

これらの意見交換の後、議長から今後のセンター長会議について検討するワーキンググループを、只木総合情報基盤センター長が中心となり立ち上げること、メンバーに関しては只木総合情報基盤センター長に一任すること、また、来年度はセンター長会議を開催することについての確認があり、拍手多数で承認された。

最後に、議長から来年度のセンター研究交流・連絡会議開催校として三重大学、センター長会議開催校として宮崎大学が担当すること、また、運営委員会及び編集委員会については今年度開催校と次年度の開催校で委員を担当するということについて諮られ、拍手多数で承認された。

カ　その他

報告・議題の提案はなかった。

１１　閉会

外嶋総務･企画課長から､情報交換会等についての連絡及び会議の閉会宣言が行われ、本会議を終了した。

（以上）

第 5 回国立大学法人情報系センター研究交流・連絡会議 報告

和歌山大学システム情報学センター長　河原英紀

開催日時：平成 22 年 9 月 9 日（木）13：30 ～ 17：00
開催場所：県民交流プラザ 和歌山ビッグ愛
参 加 者：計 61 大学 96 名

配布資料：

1. 第 5 回国立大学法人情報系センター研究交流・連絡会議議事次第
2. 第 14 回学術情報処理研究集会プログラム
3. 第 5 回国立大学法人情報系センター研究交流・連絡会議及び
   第 14 回学術情報処理研究集会出席者名簿
4. 学術及び総合情報処理センター　センター超会議，研究交流・連絡会議　開催校一覧
5. 第 6 回国立大学法人情報系センター研究交流・連絡会議及び
   第 15 回学術情報処理研究集会にかかる委員（案）
6. 第 5 回国立大学法人情報系センター研究交流・連絡会議資料
7. 学術情報処理研究No.14

会議次第：

1. 開会
2. 開会の挨拶　和歌山大学 システム情報学センター長　河原英紀
3. 開催校挨拶　和歌山大学 副学長・附属図書館長 竹内昭浩
4. 議事 1
   1. 大学 ICT 協会(仮称、日本版 EDUCAUSE)について
   2. ソフトウェアライセンスの取り扱いについて
   3. マイクロソフト社の包括ライセンス契約について
   4. 国立大学法人における情報システムのライフサイクル管理について
   5. 情報セキュリティに関する予算の捻出について
   6. 学術認証フェデレーション：GakuNin の現状と活用について
5. 議事 2
   1. 教育面に関するアンケート結果説明と意見交換
   2. 研究面に関するアンケート結果説明と意見交換
   3. サービス面に関するアンケート結果説明と意見交換
   4. 運営面に関するアンケート結果説明と意見交換
5. 第 5 回国立大学法人情報系センター長会議への要望
   第 6 回国立大学法人情報系センター研究交流・連絡会議／第 15 回学術情報処理研究集会
   及び第 6 回国立大学法人情報系センター長会議の開催校について
6. 閉会

議事内容：

議事１では，これまでの情報系センター会議とは若干異なる形式であるが、事前に議題提案を募り，提案者にご説明を頂いた。それぞれの情報系センターが現在抱える問題について実際の事例を通してご紹介頂いたことで討論が活発になされた。特に事例紹介では、具体的なライセンス管理や学内システム構築に関するコンサルティングなどを進めるにあたり重要となるノウハウに関して情報交換がなされた。議事２に関しては、基本的に集計結果に基づく傾向を概説し、意見交換を実施した。

第 5 回国立大学法人情報系センター長会議への要望

「第 6 回国立大学法人情報系センター研究交流・連絡会議／第 15 回学術情報処理研究集会」については、三重大学が開催を担当することが決定された。また、「第 6 回国立大学法人情報系センター長会議」については，宮崎大学が開催を担当することが決定された。但し、一部からは本研究交流・連絡会議がセンター長会議など他の会議と重複している部分があり、アンケートについても類似のものが多く、重複して参加・回答しなければならないため負担が大きいという声が上がった。

第 14 回学術情報処理研究集会 報告

和歌山大学システム情報学センター長　河原英紀

開 催 日 時 : 平成 22 年 9 月 10 日（金）9：30～17：00

開 催 場 所 : 県民交流プラザ 和歌山ビッグ愛

研 究 発 表 数: 22 件（発表 12 分、質疑応答 3 分）

参 加 者 数 : 計 60 大学 97 名

議事内容 :

各種新技術を備えたシステムの導入事例が多く行われた。導入システムに対する運用コストや具体的な効果、導入計画や導入期間などに関する議論が活発になされた。

学術情報処理研究投稿規定

平成11 年5 月13 日改定
（平成10 年4 月16 日制定）

１．本誌に掲載する記事は未発表のもので、その分野と種類は以下のとおりとする。

分野

（１） 学術情報処理の研究・開発、教育に関するもの

（２） 学術情報処理施設の設計・管理・運用に関するもの

種類

（１） 査読付き論文

（２） 学術情報処理研究集会予稿

（３） 解説

（４） 報告

（５） その他

２．投稿者は、原則として大学の総合情報処理センター及び情報処理センター関係者・利用者とするが、必ずしもこれに限るものではない。

３．査読付き論文の場合、投稿者は原稿2 部（1 部はコピー可）を編集委員会に届けるものとする。

その他は、そのままオフセット印刷ができる形の原稿を1 部提出するものとする。

また、それとは別に電子的媒体（電子メール、FTP、フロッピー等）による原稿も1 部提出するものとする。

４．査読者は、編集委員会の議を経て、編集委員長がその該当分野の専門知識を有するものに依頼する。1 名による査読者が掲載不可と判断した場合、更に2 名の査読者の判断をもって掲載の可否を決定するものとする。

５．本誌に掲載された著作物の著作権は、すべて編集委員会に属することとする。

６．本誌は冊子体で配布するほか、同じ内容がWWWにより公開される。

７．査読付き論文の場合は有料で別刷り50 部を最低とし、それ以上は50 部単位で受け付ける。

８．著作校正は1 回とする。校正の際に原文を大きく改変することは許されない。

９．原稿は原則として返却しない。返却希望があれば、返信料を添えて投稿時に申し出ること。

１０．原稿の分量は以下の文字数を目安とする。

査読論文	・20000 文字程度（A4 40 行×43 文字で ～12 ページ程度）
研究集会予稿	・10000 文字程度（A4 40 行×43 文字で 2～5 ページ程度）
記事等	・10000 文字程度（A4 40 行×43 文字で 4～5 ページ程度）

１１．その他の詳細は、別途「原稿の作成の手引き」によるものとする。

編集後記

「学術情報処理研究」は今回で第 15 号を刊行するに至りました。本誌は査読付きの学術論文誌であり，著者の熱意が伝わる高いレベルの論文が掲載されております．取上げられているテーマは，「災害対策」や「省エネルギー施策」，「サーバ集約」など時代背景を反映したものに加え，日頃直面している課題であるセンター業務の「コスト削減」や「セキュリティ」の充実など，広範にわたっています。近年特に，各センターに対するユーザからの要望は質・量共に多様化・複雑化の一途を辿っております。この「学術情報処理研究」は，それら要望に応える智慧を共有するための貴重な論文誌であるものと思われます．

このような本論文誌の編集と刊行は，編集委員をはじめとする多くの先生方・職員の皆様方の努力に支えられております。本論文誌が無事に刊行され，皆様にお届けできたのは，それらの方々のご協力の賜物です。お忙しい中，貴重な時間を割いてご尽力くださった先生方・職員の皆様方に心より御礼申し上げます。

昨今，大学内におけるセンター業務の重要性は増しており，特に学内インフラや業務システムの整備・効率化が強く求められていると感じております。学内業務の効率化を目的とした最新技術の導入は，逆に一歩間違えればユーザからの反発や業務の非効率化にも繋がりかねません。そのような中で，本論文誌で提供された最新の技術及び実際のシステム導入に関わるノウハウを役立てて頂ければ幸いです．本誌が情報系センターのみなさま，ひいては各大学の発展に寄与するための有益な情報源になることを願って，編集後記とさせて頂きます。

「学術情報処理研究」
編集委員会主査　河原英紀

「学術情報処理研究」編集委員会

学術情報処理研究 No.15　2011
Journal for Academic Computing Networking
2011 年 8 月編集
2011 年 9 月 14 日発行

編集　「学術情報処理研究」編集委員会
主査　河原　英紀

発行　三重大学総合情報処理センター
〒514-8507　三重県津市栗真町屋町 1577
TEL 059-231-9772
MAIL support@cc.mie-u.ac.jp

URL　http://www.cc.mie-u.ac.jp/cc/ipc2011/

ISSN　1343-2915

Journal for Academic Computing and Networking

学術情報処理研究

No.15　2011

学術情報処理研究編集委員会