

名古屋大学情報メディア教育センターにおける 情報コンセント / 無線 LAN を用いた個人端末利用システム

岡田 啓, 山里 敬也

名古屋大学 情報メディア教育センター

概要

名古屋大学情報メディア教育センターは、本学の情報教育を飛躍的に発展させることを目的に設立された。本センターではコンピュータ、ネットワーク、マルチメディア技術を駆使した総合的な情報基盤としての情報処理教育システムを「授業メディア空間」と見なし、運用を行なっている。現在は、約 800 台の端末を提供しているが、将来的には学生自身が所有するコンピュータをこの「授業メディア空間」に接続し、講義を受けるといったスタイルが当たり前になるのではないかと予測している。そこで、このようなシステムの実現をめざし、情報コンセント及び無線 LAN を用いた個人端末利用システムの実験的運用を 2000 年 5 月より始めた。本稿ではこの個人端末利用システムの概要について述べるとともに、運用状況、今後の課題について報告する。

A Connection Service for Personal Terminals via LAN Sockets/Wireless LAN at CIMS, Nagoya University

Hiraku OKADA, Takaya YAMAZATO

Center for Information Media Studies, Nagoya University

Abstract

Center for Information Media Studies (CIMS) in Nagoya University was established with the aim of development of information education systems. We aim not only at the fulfillment of the computer literacy education, but also at the educational breakthrough by utilizing the multi-media technologies. More than 800 terminals are located campus wide in Nagoya University. In the future, it is expected that many students take their own computer to the campus, connect it to the information education network, and take lessons. To realize this plan, a connection service for personal terminals via LAN sockets/wireless LAN has been in experimental operation since May 2000. In this report, we describe a brief summary about this system, and discuss the issue of the system.

1 はじめに

名古屋大学情報メディア教育センターは、本学の情報教育を飛躍的に発展させることを目的に設立された [1]。本センターではコンピュータ、ネットワーク、マルチメディア技術を駆使した総合的な情報基盤としての情報処理教育システムを「授業メディア空間」と見なし、運用を行なっている。

このシステムを利用するためには、主センターと各部局に分散配置したサテライトラボがある。現在は、主センター、サテライトラボを合わせて約 800 台の端末を提供しているが、学内で個人のパソコンで利用するための設備は十分では無いのが現状である。さらに、将来的には学生自身が所有するコンピュータを情報メディア教育ネットワークに接続し、講義を受けるといったスタイルが当たり前になるのではないかと予測している。

そこで、学生自身が所有するパソコンから情報メディア教育ネットワークへの接続の実現をめざし、情報コンセント及び無線 LAN を用いた個人端末利用システムの実験的運用を 2000 年 5 月より始めた。本システムでは、情報コンセントおよび無線 LAN を用いることで、個人端末に対するネットワークの口を用意している。本稿では名古屋大学情報メディア教育センターにおける個人端末利用システムの概要について述べるとともに、運用状況、今後の課題について報告する。

2 要求事項

本システムを構築するにあたり、以下の要求事項が挙げられた。

- 認証されたユーザからのみ情報メディア教育ネットワークへ接続できること。
- 通信内容が他のユーザに傍受されないこと。
- 認証されたユーザからの接続でも、不必要なサービスは提供しないこと。
- 地理的に分散している場所に設置可能なこと。
- システム設計の自由度を増すため、情報メディア教育ネットワークに接続するまでの経路において複数のネットワークをまたがった構築が可能であること。
- 本センターでは、既に ISDN 回線や、PHS 無線 LAN によるリモートアクセスサービスを提供しており、このシステムと同じアカウント管理システムを使うこと。

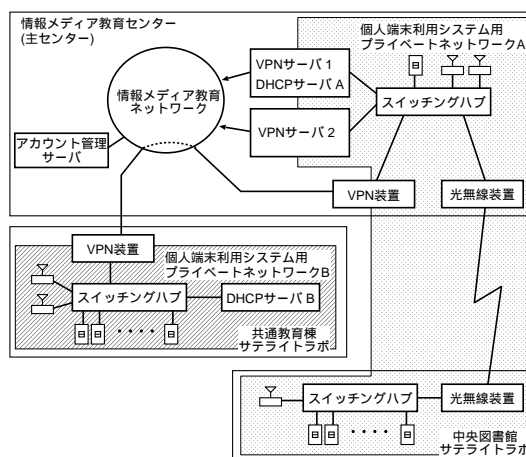


図 1: システム構成

- 既存の技術をできるかぎり利用し、システムの構築をアウトソーシングしやすくすること。

これらの要求事項に基づいて、システムの構築を行った。次節において、本センターが構築した個人端末利用システムの概要について述べる。

3 システム構成

情報コンセントや無線 LAN を用意し、学生個人が所有するパソコンを学内のネットワークへ接続するという同様の試みも既に幾つかの大学においてなされてきた [2] ~ [6]。これらの試みにおいて幾つかの方式が検討されてきたが、名古屋大学における個人端末利用システムでは VPN を用いることで、個人端末から情報メディア教育用ネットワークへの接続を可能にしている。そのシステム構成を図 1 に示す。

本システムは、VPN サーバ、アカウント管理サーバ、および個人端末利用システム用プライベートネットワークから構成されている。また、情報コンセントおよび無線 LAN は情報メディア教育センター (主センター)、中央図書館サテライトラボ、共通教育棟サテライトラボの 3 箇所に点在している。

3.1 VPN サーバ

VPN サーバとして、汎用パソコンで構成された PC サーバと VPN 専用機を用いている。図 1 において、VPN サーバ 1 が PC サーバ、VPN サーバ 2 が VPN 専用機である。VPN 専用機は Nortel Network 社製 Contivity Extranet Switch 1510 を用いている。VPN サーバの基本的なスペックは表 1 の通りである。これら 2 つの VPN サーバを用いて、PPTP (Point-toPoint Tunneling Protocol) [7]、IPSec (IP

表 1: VPN サーバのスペック

	サーバ 1 (PC サーバ)	サーバ 2 (VPN 専用機)
CPU	Pentium III 500MHz	Celeron 400MHz
Memory	128MB	64MB
NIC	Intel EtherExpress Pro/100+ 3Com Fast Etherlink XL	10/100 Ethernet LAN x2
OS	linux 2.2.16	

Security Protocol) [7], PPPoE (PPP over Ethernet) [8] による接続を可能としている。以下において、これら 3 つの VPN プロトコルの実装方法について述べる。

PPTP

PPTP による接続は VPN サーバ 1 (PC サーバ) 上で実現している¹。PPTP サーバ用ソフトは、poptop-1.0.0 [9] を用いている。また、通信路を暗号化するために、MS-CHAPv2 (Microsoft PPP CHAP Extensions version 2) および MPPE (Microsoft Point-To-Point Encryption Protocol) を利用している。このため、ppp-2.3.10 に ppp-2.3.10-openssl-norc4-mppe パッチをあてたものを PPP サーバとして用いている。

PPTP のクライアントは、Microsoft Windows に標準でサポートされている「仮想プライベートネットワーク」を用いている。このため、ユーザは特別にクライアント用ソフトを用意する必要がないといった利点がある²。

IPSec

IPSec による接続は VPN サーバ 2 (VPN 専用機) 上で実現している。この専用機は最大で 100 の VPN 接続をサポートしている。

クライアントソフトは同製品に付属の Contivity Extranet IPSec Client を使用している。このクライアントソフトは無制限配布ライセンス付であり、また比較的簡単にインストール可能である。ユーザはこのクライアントソフトを個人端末にインストールし、ユーザ ID、パスワード、VPN サーバの IP アドレスの設定を行うことになる。

¹PPTP サーバとして VPN 専用機を用いることも可能であるが、本システムでは認証サーバとして外部 RADIUS サーバを利用しており、この RADIUS サーバが MS-CHAPv2 をサポートしておらず、通信路の暗号化が行えないため、使用していない。

²バージョンによっては OS のアップグレードが必要だったり、コンポーネントの追加といった作業が必要である。

PPPoE

ADSL サービスの開始に伴い、PPPoE を一般的なユーザレベルで利用する機会が増えていることもあり、ユーザにとっては導入しやすいと思われる。この点を踏まえ、PPPoE サーバの実験的導入を行った。

PPPoE による接続は、VPN サーバ 1 (PC サーバ) 上で実現している。PPPoE サーバ用のソフトとして、rp-pppoe-3.0 [10] を用いている。rp-pppoe の実装方法として、user モードと kernel モードの 2 種類があるが、PC サーバの環境を大幅に変更するのを避けるため、user モードでインストールした。クライアントソフトとして、RASPPPOE [11] を使用している。

上記の VPN 接続を用いて情報メディア教育ネットワークに接続する。認証されたユーザのみの接続を許可するため、VPN 接続のみを許可し、個人端末利用システム用プライベートネットワークからの接続は禁止している。また、VPN 接続自体にもフィルタリングを行うことで、情報メディア教育ネットワークに対するセキュリティをある程度確保している。

3.2 アカウント管理サーバ

本センターに既に導入されているリモートアクセスシステムでは、WEB によるユーザ登録をしている。ユーザ情報は WEB サーバ上に保存されるとともに、RADIUS サーバ [12] にも送られる。そして、ISDN 回線や PHS 無線 LAN のリモートアクセスサーバでは、RADIUS サーバによる認証、アカウントリングを行っている。

本システムも同じ RADIUS サーバによる認証、アカウントリングを用いることで、管理を一元化することが好ましく、VPN サーバ 2 ではこれを実現している。しかし、VPN サーバ 1 では通信路の暗号化を行うために MS-CHAPv2 による認証を行っているのだが、RADIUS サーバを用いて MS-CHAPv2 による認証を行うのに失敗したため、WEB サーバ上のユーザ情報を直接 VPN サーバ 1 に送ることで

表 2: 設置状況 (2001 年 9 月現在)

	中央図書館	共通教育棟	主センター	SCS*1
無線アクセスポイント (無線 LAN カード)	1 (20)	5 (50)	2 (16)	1 (30)
情報コンセント	14	58	0	2

*1) スペース・コラボレーション・システム 名古屋 1 局

ユーザ情報を統一している。

3.3 主センター、サテライトラボ間の接続

主センターと中央図書館サテライトラボ間はキャノン社製 CANOBEAM DT-50 [13] を用いた光無線により接続されている。伝送速度は 25Mbps ~ 156Mbps である。これは、ブリッジとして機能するため、主センターと中央図書館サテライトラボは同じネットワークに属することになる。

また、主センターと共通教育棟サテライトラボ間は Cisco 社製 Cisco2621 を用いて、情報メディア教育ネットワーク上で VPN 接続している。これはルータとして働き、主センターと共通教育棟サテライトラボは異なるネットワークに属している。なお、プライベートネットワークと情報メディア教育ネットワークは論理的には分離されており、ここでの VPN 接続からは相互に接続できない。

上記のような 2 種類の方法で、地理的に離れた場所の接続を行っている。このため、図 1 に示されているように個人端末利用システム用プライベートネットワークは、主センターおよび中央図書館ではネットワーク A、共通教育棟ではネットワーク B といったように、異なるネットワークで構成されている。

3.4 DHCP サーバ

プライベートネットワーク A, B それぞれに DHCP サーバを設けている。プライベートネットワーク A では、VPN サーバ 1 である、PC サーバ上に ISC DHCP [14] をインストールしている。プライベートネットワーク B では、DHCP サーバとして Cobalt Qube2 を用意した。どちらの DHCP サーバも、利用状況を把握するために、無線 LAN カードには予め決められた IP アドレスを固定して割り当てるようにしている。

3.5 情報コンセント、無線アクセスポイント

個人端末を接続するための口として、情報コンセントおよび無線アクセスポイント (AP) を提供している。設置状況を表 2 に示す。

情報コンセントは中央図書館の閲覧室の一角、共通教育棟コミュニティホールおよび教室に設置されている。情報コンセントは VLAN を用いて異なる教室間の情報コンセント同士の接続はできないようにしてある [2]。

無線アクセスポイント (AP) として、メルコ社製 WLA-T1-L11 および WLA-L11 を用いている。無線 LAN カードは主センター、各サテライトラボの事務室において貸出を行っている。無線 AP で MAC アドレススペースのフィルタリングを行うことで、貸出用の無線 LAN カードのみ接続可能なように設定がされている。

3.6 個人端末の接続手順

以上のように本システムは構成されている。本節ではこのシステムを使用するにあたり、個人端末における情報メディア教育ネットワークへの接続手順について述べる。

1. 主センター、サテライトラボに設置されている情報コンセント、無線アクセスポイントに接続。このとき、各端末は DHCP サーバ、VPN サーバのみに接続可能である (ただし、プライベートネットワーク B からプライベートネットワーク A へのルーティング情報は個人端末は知らない状態である)。
2. DHCP により、IP アドレスを取得。プライベートネットワーク B に接続した端末は、VPN サーバへのルーティング情報も取得することになる。
3. 個人端末利用システム用プライベートネットワークを経由して VPN サーバに接続。
4. ユーザ認証を行う。
5. 認証に成功すれば、VPN 経由で情報メディア教育ネットワークへの接続を許可する。

4 設置の経過

本システムは、以下のように 3 回に分けて導入された。その経過を簡単に述べる。

第1期(1999年12月～2000年5月)

主センター、中央図書館サテライトラボに情報コンセントおよび無線LANを設置した。主センターと中央図書館サテライトラボ間には光無線装置とVPN装置の両方が導入された。VPNサーバとして、PCサーバを導入し、個人端末からの接続方法はPPTPを使用している。2000年5月より運用開始した。

第2期(2000年6月～2001年1月)

共通教育棟サテライトラボに無線APおよび情報コンセントを設置した。主センターと共通教育サテライトラボ間の接続は、中央図書館に用いられていたVPN装置を使用している。VPNサーバとして、VPN専用機を導入し、セキュリティ強化の意味もあり、接続方法はIPSecに変更した。2001年1月より運用開始。

第3期(2001年3月～2001年6月)

スペース・コラボレーション・システム(SCS)名古屋1局に個人端末利用システムを設置した。また、PCサーバにPPPoEサーバを導入することで、共通教育棟サテライトラボ以外ではPPPoEによる接続が可能となった。

5 利用状況

2000年5月より本システムは実験的運用を開始した。図2に運用開始後の利用状況を示す。

2000年5月～12月までは、主センターおよび中央図書館サテライトラボのみで運用していた。2001年1月以降は、共通教育棟サテライトラボでも利用可能になった。さらに、2001年4月には、新入生を対象に全員に案内書を配る等して広報活動を行った。こういった背景を踏まえて利用状況をみると、運用開始後7月までは徐々に増加してきているが、それ以降はほぼ横ばい状態であった。しかし、2001年4月以降、急激な増加がみられ、広報活動による効果が大きかったといえる。なお、8月は夏休みに入ったこともあり、利用数は減っている。

情報コンセントと無線LANの種類別の利用数をみると、初めはほぼ半々であったが、2001年4月以降、情報コンセントによる利用数の方が多くなっていることがわかる。現状では、情報コンセントと無線APは基本的に同じ場所に設置されており、無線LANカードのみ貸出をおこなっている。このた

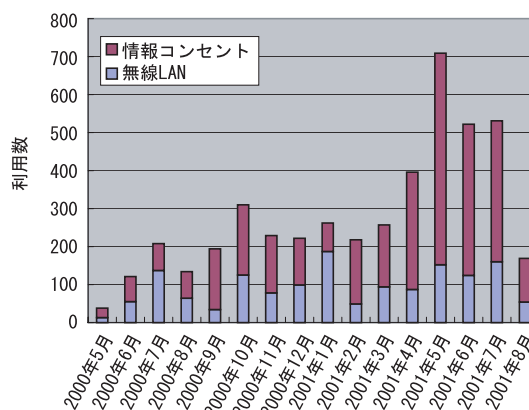


図2: 利用状況

め、自分で有線LANカードを持っていたり、ノートパソコンに予め付いている場合は、伝送速度が速いうえ無線LANカードを借りる手間が省けるために情報コンセントを利用している。個人端末利用システムの運用開始後、有線LANカードを個人で購入したり、予め有線LANポートが付いているノートパソコンを購入したユーザが多いのではないかと予測される。

また、本サービス運用開始後、ユーザからの質問が多数発生した。2000年12月までは、無線LANカードの設定、ネットワークの設定、VPN接続の設定等一般的に質問があったが、2001年1月のIPSec接続に移行後は、無線LANカードの設定方法に関する質問が大部分を占めるようになってきた。これは、IPSec接続はクライアントソフトを個人端末にインストールする形態をとっており、個人端末のOSのバージョンや設定に影響を受けにくくなったためと思われる。

6 むすび

本稿では、名古屋大学情報メディア教育センターにおける、情報コンセント/無線LANを用いた個人端末利用システムのシステム構成および運用開始後の利用状況について報告した。

実験的運用開始から1年以上が経過したが、この間に明らかになった課題点について紹介する。

- 情報コンセントと無線LANについて、それぞれの特徴を生かした形で設置してはどうか。具体的には情報コンセントではマルチメディアコースコンテンツをストレスなく閲覧することが可能なため、端末の無い端末室といった落ち着いた環境を提供する。また、無線LANは伝送速

度は限られるもののいつでもどこでもを可能にするため、教育活動や研究活動に必要な情報・サービスを提供するキャンパスポータルに利用してはどうか。

- 人によって環境が異なる個人端末を利用するため、サポート体制の充実が必要である。
- 文房具として学生が個人レベルで購入できる携帯型端末を提供してはどうか。
- 個人端末を使うため、人によって端末にインストールされているソフトウェアが異なることがある。このため、学生であれば誰でも使えるソフトウェアの提供をしたり、WEB ベースで授業が行えるようにする。

謝辞

本システムの構築にあたり、貴重なご意見を頂いた本学工学研究科情報工学専攻結縁祥治助教授および情報メディア教育センター梶田将司助手に深く感謝致します。また、本研究の一部は、日本学術振興会科学研究費補助金の助成をうけて行われたものであります。記して謝意を表します。

参考文献

- [1] 山里敬也, 梶田将司, 濱口毅, 結縁祥治, “名古屋大学情報メディア教育システムの現状と課題,” 情報処理学会分散システム/インターネット運用技術研究会, pp.55-60, 1999 年 11 月.
- [2] 丸山伸, 浅野善男, 辻斉, 藤井康雄, 中村順一, “既存の DHCP 端末で利用できる利用者にも管理者にも安全な情報コンセントシステム,” 情報処理学会分散システム/インターネット運用技術研究会, pp.131-136, 1999 年 7 月.
- [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, vol.42, no.1, pp.79-88, 2001 年 1 月.
- [4] 石橋勇人, 山井成良, 森下英夫, 森俊明, 安倍広多, 松浦敏雄, “無線 LAN における利用者認証機構,” 情報処理学会分散システム/インターネット運用技術研究会, pp.13-18, 2001 年 5 月.
- [5] 篠宮俊輔, 萩原洋一, “大学キャンパス無線アクセスシステムの構築,” 情報処理学会分散システム/インターネット運用技術研究会, pp.7-12, 2001 年 5 月.
- [6] 梶田秀夫, 鈴木未央, 中西通雄, “PPPoE を利用した認証付き情報コンセントの実装と評価,” 情報処理学会分散システム/インターネット運用技術研究会, pp.19-24, 2001 年 5 月.
- [7] 是友春樹, *VPN/VLAN 教科書*, アスキー出版社, 1999 年.
- [8] L. Mamakos, K. Lidl, J. Evarts, D. Carrel, D. Simone, R. Wheeler, *A Method for Transmitting PPP Over Ethernet (PPPoE)*, RFC2516, 1999.
- [9] PoPToP - The PPTP Server for Linux, <http://poptop.lineo.com/pptp.html>
- [10] Roaring Penguin Software (PPPoE), <http://www.roaringpenguin.com/pppoe/>
- [11] RASPPPOE Home Page, <http://www.user.cs.tu-berlin.de/~normanb/>
- [12] C. Rigney, S. Willens, A. Rubens, W. Simpson, *Remote Authentication Dial In User Service (RADIUS)*, RFC2865, 2000.
- [13] キヤノン CANOBEAM DT-50, <http://www.canon-sales.co.jp/canobeam/dt50/index-j.html>
- [14] Internet Software Consortium - DHCP, <http://www.isc.org/products/DHCP/>