

学内ユビキタス環境を実現するための 情報コンセント及び無線LAN環境の構築と運用

菊地 裕明* 井関 文一**

大学構内において、安全で利便性の高いネットワークサービスの提供を行うため、PPTPを利用した全学的なネットワーク接続システムの構築を行った。システムは40台のPPTPサーバを利用した分散システムであり、ユーザは何処にいても、無線LANまたは有線の情報コンセントから同じ方法で安全に学内ネットワークに接続することが可能となった。また利用状況のログを収集を行い、利用率や負荷の解析を行った。これによりシステムの問題点を洗い出し、それに対する解決策の提示を行った。

キーワード : PPTP, WIFI, SNMP, CHAP, 暗号化

Construction and Management of Information Outlet and WIFI Network to realize Univ.ubiquitous

Hiroaki KIKUCHI and Fumikazu ISEKI

We constructed a network connection system using PPTP in university to provide the network service that it is secure and convenience. It is a distributed system using 40 PPTP servers. As a result, the user came to be able to connect the network safely from anywhere by the information wall socket or wireless LAN.

We collected logs of the use state, and analyzed availability and the load of the system. And we identified the problems of the system, and presented the solutions.

Keyword : PPTP, WIFI, SNMP, CHAP, encryption

*東京情報大学大学院総合情報学研究科
Tokyo University of Information Sciences, Graduate School of Informatics

2006年7月7日受理

**東京情報大学総合情報学部情報システム学科
Tokyo University of Information Sciences, Faculty of Informatics, Department of Information Systems

概要

大学構内においてノートパソコン等で、いつでも、どこにいても同じ環境でネットワークに接続できることは、学内のネットワーク利用者に対して高い利便性をもたらす。しかしながら、利便性のみを追求すると、大学という比較的オープンな環境においては、外部からの第三者によるネットワークの不正利用や無線LANの盗聴などのセキュリティの問題も発生する。

当大学ではこれらの問題を解決するために、平成16年4月より、PPTPサーバを利用した情報コンセント及び無線LAN環境の構築を行っており、最近では、17年度より必携となったノートパソコンによる利用者の増加に対応するための拡張も行った。現時点では40台のPPTPサーバを使用してシステムの運用を行なっている[1]。

PPTPによる無線LAN環境の暗号化についてはいくつか報告があるが[2][3][4]、本学のように全学で統一的に行われた例はほとんど無い。そこで本論文ではシステムの構築及び運用についての事例報告、システム利用の問題点及び解決案などを具体的に取り上げたい。

1. システム要件

大学等に於いて、持込のノートパソコンに対する学内ネットワークへの接続サービスは、学生・教員にとっては非常に利便性の高いサービスと言える。

しかしながら、便利さばかりに目を奪われると思わぬ落とし穴に陥る可能性もある。例えば本学でも初期のころは無線LANの暗号化にWEPのみを使用し、学生に対してSSID（セッションID）、WEPキー（暗号化キー）を通知していたが、このような場合、簡単に暗号を解読されてしまう可能性がある。

また接続時にユーザ認証を行わない場合、学外の第三者に無断でネットワークを利用される恐れもある。安全性を確保すると同時に利便性

を高めるためには以下の要件が必要かつ不可欠となる。

- (1) 無線LAN使用時の通信内容の安全な暗号化。
- (2) 接続時のユーザ認証。
- (3) 接続場所、方法に拘わらない、同じ接続方法の提供。
- (4) クライアントのマルチOS対応（Windows、Linux、MacOS）。

(1)の問題では暗号化にTKIP、AESを利用する方法も考えられるが、対応していないアクセスポイント（AP）の買い替えの必要性や、対応していてもAPの能力により同時接続数が大幅に制限される場合があるなどの問題が挙げられる。また(2)では、ユーザ認証機能を提供するスイッチも存在するが、該当する全てのスイッチをユーザ認証付きスイッチに買い替えなければならない、さらにユーザ認証の手間も煩雑である場合が多い。

これらの点を考慮し、当大学ではPPTP（Point-to-Point Tunneling Protocol）を採用することとした[1]。PPTPを採用することにより、上記の要件に対して以下のような機能を提供することが可能となる。

- (a) MPPEの128bitキーによる暗号化。
- (b) MS-CHAP v2+Radiusサーバによるユーザ認証。
- (c) 個別のDNSサーバによるPPTPサーバ名の同一化。
- (d) ベンダおよびフリーソフトによるクライアントソフトの提供。

(a)のMPPE（Microsoft Point-to-Point Encryption）ではRC4の128bit共通鍵暗号を使って、PPTPパケット内のPPPフレームのペイロードが暗号化される。

(b)のMS-CHAP v2（Microsoft Challenge Handshake Authentication Protocol Version 2）

もMicrosoftによる実装で、MD4のハッシュ関数を用いたCHAP認証が行われる。Radiusサーバは認証サーバであり、ユーザのIDとパスワードのチェックはRadiusサーバ上で行われる。

(c) ではそれぞれのPPTPドメインで、ドメインごとに個別のDNSサーバ（今回はPPTPサーバマシンと兼用）を用意し、どのPPTPドメインから接続しても同じ名前（例：pptp.wl.tuis.ac.jp）でそれぞれのPPTPサーバに接続できるようにした。これにより学内では、無線・有線・接続場所を問わずに同一の設定ファイルでネットワークへの接続が可能となる。

(d) に関しては、MS Windows2000、MacOS X以降は、PPTPクライアントはOSに標準で搭載されており、簡単に設定することができる。また、Linuxに関してもpptp-linux[5]などのフリーウェアを使用することができる。Linuxに関しては設定・接続に若干の手順が必要のため、設定・接続用のスクリプトを用意した。

2. システムの概要

構築したシステムの概要を図2-1に示す。サーバはOSにVine3.1を使用し（途中増設したマシンはVine3.2）、PPTP、DHCP、DNSサーバも兼ねた構成となっている。サーバのOSにVine3.xを選択したのは、安定したカーネルとして定評のあるバージョン（2.4）を採用し、機能的にも実験的なものは排除しているため、

長期に渡ってトラブル無く動作することを期待した為である。

サーバにはネットワークカードを一枚追加し、オンボードと合わせて計2個のネットワークインターフェイス（共に100Mbps）を装備させる。この場合、学内LANに接続するインターフェイスを上位インターフェイスと呼び、PPTPドメイン（仮想ネットワーク）に接続するインターフェイスを下位インターフェイスと呼ぶ。

ユーザは無線LAN（WEPを使用）、または情報コンセント（有線での接続用コンセント）に接続することにより、DHCPサーバの下位インターフェイスからローカルなIPアドレスを割り振られる。接続した（物理的な）ドメインから学内ネットワークにアクセスするにはPPTPサーバの下位インターフェイスを経由するルートしか存在しないが、PPTPサーバはIP-FilterによりDHCPサーバが割り振るIPアドレスのパケットの中継を拒否する。したがってユーザマシンはDHCPサーバから振られたアドレスでは学内ネットワークにアクセスできないことになる。DHCPサーバから割り振られたアドレスはPPTPサーバとの通信にのみ使用される。

ユーザマシンで起動されたPPTPクライアントは、予め設定済みのPPTPサーバのドメイン名（FQDN：pptp.wl.tuis.ac.jp）をDNSサーバに問い合わせ、そのIPアドレスを得る。この時DNSサーバはPPTPサーバ名（FQDN：

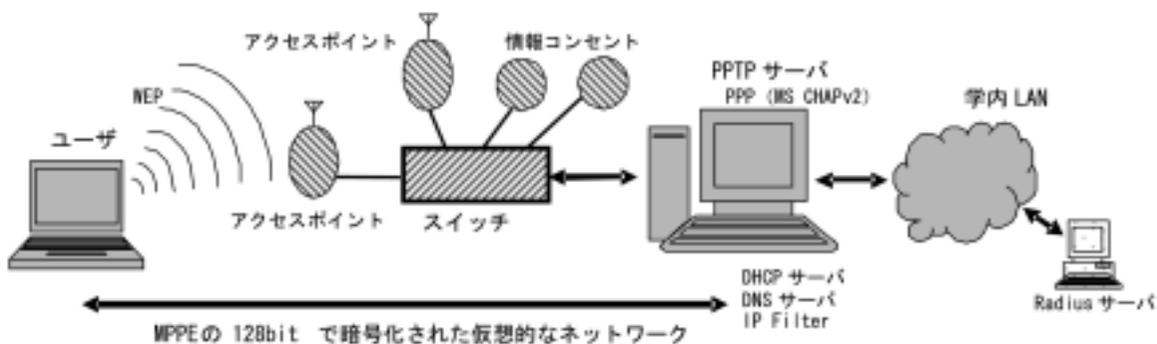


図2-1 無線LAN認証システムの基本構成

pptp.wl.tuis.ac.jp) に対して必ずその (物理的) ドメインのPPTPサーバの下位インターフェイスのIPアドレス (今回は自分自身のIPアドレス) を答えるように設定しておく。

PPTPサーバのIPアドレスを得たユーザマシンはPPTPサーバプロセスと通信を開始する。PPTPサーバはPPPデーモンを起動し、PPPフレームをカプセル化し仮想化する。次にユーザマシンはPPPデーモンとMS-CHAP v2を使用したCHAP認証を行う (認証自体は別に用意した2台のWindows2003 Server上のRadiusサーバが行う)。

認証が通過するとユーザマシンには新しい (仮想的な) PPP用のアドレス (PPTPリモートアドレス) が割り振られ、MPPEを使った暗号化通信が始まる。サーバの下位インターフェイスにも新しく (仮想的な) PPTPローカルアドレスが振られる。

このシステムではNAT (NAPT) は使用せず、PPTPサーバでPPTPドメインからのパケットのルーティングを行っている。NAT (NAPT) を利用しない理由としては、演習担当の教員からの「演習時に学生がどの教室から接続しているのか判別したい」との要望があっ

たためである。

この時、PPTPサーバでは特にRIP等のルーティングデーモンは起動せず、学内ネットワークの基幹L3スイッチでスタティックルーティング (PPTPリモートアドレス<-->PPTP上位インターフェイスアドレス<-->学内LAN) を行っている。

PPTPサーバの構築では、雛形のサーバマシンを作成し、ハードディスクのイメージコピーツールを使用して他のハードディスクへのコピーを行った。コピー後はハードディスクをパソコンに戻し、予め用意した設定シートに従ってマシンの設定を行った。

PPTPサーバシステム構築で使用したソフトウェアは以下の通りである。

- PPTPサーバ** : pptpd-1.2.3 (Poptop) [6]
- PPP** : ppp-2.4.3 [7]
- MRTG** : mrtg-2.12.2 [8]
- DHCPサーバ** : dhcp-3.0pl2 (Vine3.x付属)
- DNSサーバ** : bind-9.2.4-0vl1 (Vine3.x付属)
- IP-Filter** : iptables-1.2.10-0vl2 (Vine3.x付属)
- SNMP** : net-snmp-5.1.1-0vl1 (Vine3.x付属)
- PPTPクライアント (Linux用)** : pptp-linux-

表3-1 無線LAN提供エリア

△は主たる使用方法が無線LANでないエリア

建屋	エリア	エリア名	PPTPサーバ名
1号館 (本館)	北側 (F1~F5)	無線LAN 1	PPTP-GW5
	南側 (F1~F5)	無線LAN 2	PPTP-GW37
	各階ホールなど	無線LAN 3	PPTP-GW38
	203教室周辺 (コンセントと共用) △	203教室	PPTP-GW2
3号館 (体育館)	体育館周辺 (部室内コンセントと共用)	体育館	PPTP-GW3
4号館 (総合情報センター棟)	全館 (MSHなどのコンセントと共用)	総合情報センター	PPTP-GW0
2号館 (食堂)	全館	学生会館	PPTP-GW4
6号館 (学生会館)	全館 (フロア, 部室内コンセントと共用)		
7号館 (新研究棟)	全館 (会議室などのコンセントと共用)	新研究棟	PPTP-GW7

1.4.0[5]

HDバックアップ：Norton Ghost 9.0 (Windows用)[9]

また、サーバに使用したマシンのスペックは以下の通りである。

[従来マシン]

CPU：Intel Pentium4 2.8GHz、メモリ：512MB

[増設マシン]

CPU：Intel Pentium4 3.0GHz、メモリ：512MB

3. エリア構成と利用状況

当大学では現在、学内無線LAN及び情報コンセント用として各エリア・教室ごとにPPTPサーバが稼動し、全体で40台のPPTPサーバが分散稼動している。教室などで情報コンセント数が100個を超える場合はPPTPサーバを冗長構成としてDNSラウンドロビンで負荷分散を行っている。

当初は、能力の高いPPTPサーバ1台で全システムを構築するという案も存在したが、1台で全てのエリア・教室をサポートした場合、接続位置を特定することが難しく、「演習時に学生がどの教室から接続しているのか判別した

表3-2 情報コンセント提供エリア

建屋	エリア	教室・ホール	PPTPサーバ名
1号館 (本館)	1 F	101	PPTP-GW9、11
		102	PPTP-GW10、12
	2 F	201	PPTP-GW15、16
		202	PPTP-GW14
		203	PPTP-GW2
		204	PPTP-GW13
		221	PPTP-GW6
	3 F	301	PPTP-GW17、18
		302	PPTP-GW19、20
		303	PPTP-GW21、22
		323	PPTP-GW8
	4 F	401	PPTP-GW23、24
		402	PPTP-GW25、26
		403	PPTP-GW27
		404	PPTP-GW28、29
		421	PPTP-GW30、31
		422	PPTP-GW32、33
	423	PPTP-GW34	
	424	PPTP-GW39	
	5 F	526、527	PPTP-GW1
3号館 (体育館)	2 F	部室内	PPTP-GW3
4号館 (総合情報センター棟)	1 F	メディアホール (MH)	PPTP-35、36
		メディアサブホール (MSH)	
	2 F	ワーク・スペース	PPTP-GW0
6号館 (学生会館)	1 F	ホールカウンター	PPTP-GW4
	2 F	部室内	
7号館 (新研究棟)	1 F～4 F	会議室	PPTP-GW7

い」という演習担当教員の要望を満たすことができなかつた。そのため、現在のような各エリア・教室ごとの分散方式を採用している。

無線LANの提供エリアは表3-1、情報コンセントの提供エリアは表3-2のようになっている。利用者となる学生及び教職員は、この提供エリア内からPPTPクライアントを用いることで学内ネットワークに接続することが出来る。その際にそのエリア内で、どのサーバを利用してネットワークに接続するかなどということは、全く意識する必要はない。

このような、PPTPによる無線LAN環境の暗号化については今までもいくつか報告があるが[2][3][4]、本学のように情報コンセントも含めて、全学で統一的に行われた例はほとんど報告されていない。

3.1 ログの収集

各エリアとそこに配置されているPPTPサーバの動作状態については、SNMP+ MRTG[8]を用いて監視を行っている。各サーバではcronにより5分間隔で状態を記録しており、そのデータを元にMRTGでグラフの作成を行うと共に、同時に保存用のログファイルにも記録を残している。

ログファイルへの出力は独自に作成したスクリプトによって行われる。このスクリプトはSNMPのsnmpwalkコマンドを用いて、PPTPサーバで利用されている2つのネットワークインターフェイス（上位および下位インターフェイス）のトラフィック、利用者の数（動作中のpppプロセス数）、CPUロードアベレージ、メモリの使用量（空きメモリの変化、スワップの利用状態）の状態を取得し記録している。

利用者の数については、動作中のpppプロセス数を元に算出しているため、pppのプロセスが正常終了しない場合などに若干の誤差が生じる場合がある（通常は0～2個程度/日）。

なお今回分析に用いたデータは平成17年度後期の授業期間（2005年9月24日～2006年1月23

日）、及び18年度前期の現時点（2006年4月1日～2006年6月18日）までの201日間であり、2006年1月25日から3月31日までの休み期間中は、利用形態が大きく異なるため除いてある。

3.2 利用状況

利用状況を確認するため、201日間の1時間ごとの総利用者延べ人数を図3-1に示す。総じて無線LANエリアの利用者数が、教室などの情報コンセント利用者数を大きく上回っていることが分かる。特に無線LAN1の利用者数は顕著である。

次に曜日別利用者の延べ人数のグラフを作成した。図3-2は無線LAN提供エリアの延べ利用者数のグラフである。このグラフからも無線LAN1のエリアの利用率が他の無線LANエリアに比べて、非常に高いことが分かる。

情報コンセント提供エリアについては利用者数にバラツキが大きいと、図3-3に総利用者数が2,000人を超えるエリア、図3-4に総利用者数が500人～2,000人のエリア、図3-5に総利用者数が500人に満たないエリアのグラフを示す。これらのグラフに関しては、縦軸の目盛りに注意して頂きたい。

無線LANでは、ほぼ曜日に拘らず一定の利用者が存在するが、情報コンセントでは先に述べたようにエリア（教室）・曜日ごとに非常にバラツキがある。

102教室のように高い利用率の教室もある一方、今年度の4月より新しく設置された423教室では、まだ一人の利用者もいないといった状況である。これは主に情報コンセントが授業で使われるためであり、授業によって情報コンセントの使用・不使用の差が大きいためであると考えられる。

また曜日に関しても、木曜日に集中して使用されていることが分かる（図3-6）。これは木曜日にノートブックを使用する授業が集中的に配置されているためであると思われる。時間割の問題でもあるが、システム的には均等に配置

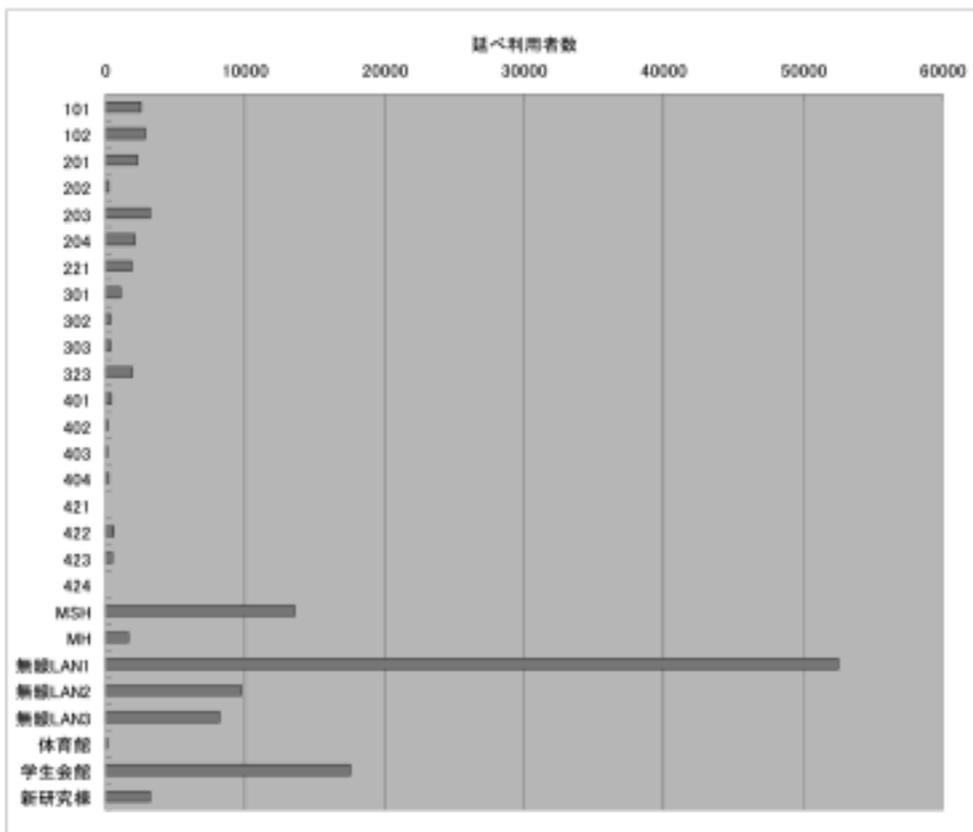


図3-1 各エリア毎の201日間の総利用者延べ人数

する方が望ましいであろう。

利用者数の時間的推移については、代表的な2つのエリアのデータを図3-7に示す。無線LAN1では授業等に関係なく山型を示す（中央の窪みは昼食のためと思われる）が、102教室は午前の授業時間帯以外では利用率が下がることが分かる（102教室の授業は午前中が多い）。102教室などの演習室では、授業時間以外はオープン実習室として利用可能だが、その場合でも、PPTPシステムの利用者は少ないようである。

なおこのグラフでは102教室の目盛りレンジは、無線LAN1の目盛りレンジの十分の一になっているので、注意してほしい。

以上のデータより、学生は授業以外で自分のノートブックを使用する場合、主に無線LAN

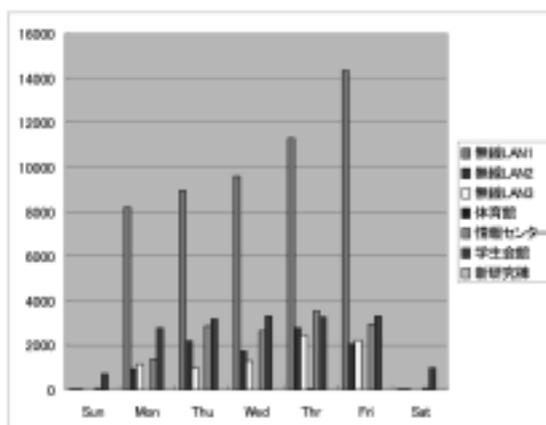


図3-2 無線LANエリアの曜日別の延べ利用者数

を好んで使用する傾向にあると考えられる。また、本学のPPTPシステムには以下のような問題があることも分かる。

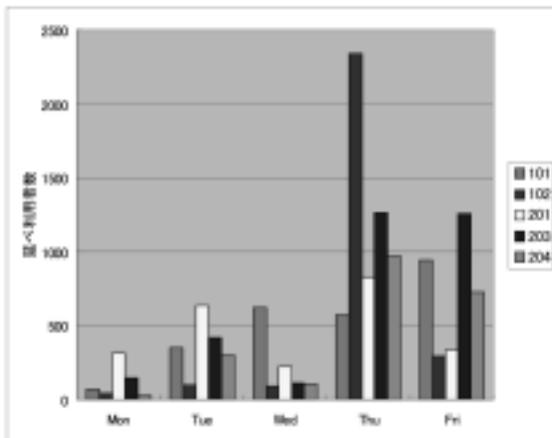


図3-3 情報コンセント提供エリアの曜日別の延べ利用者数（総延べ人数が2000人を超えるエリア）

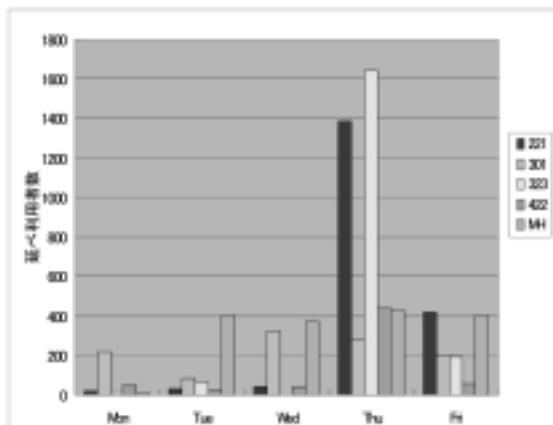


図3-4 情報コンセント提供エリアの曜日別の延べ利用者数（総延べ人数が500~2000人のエリア）

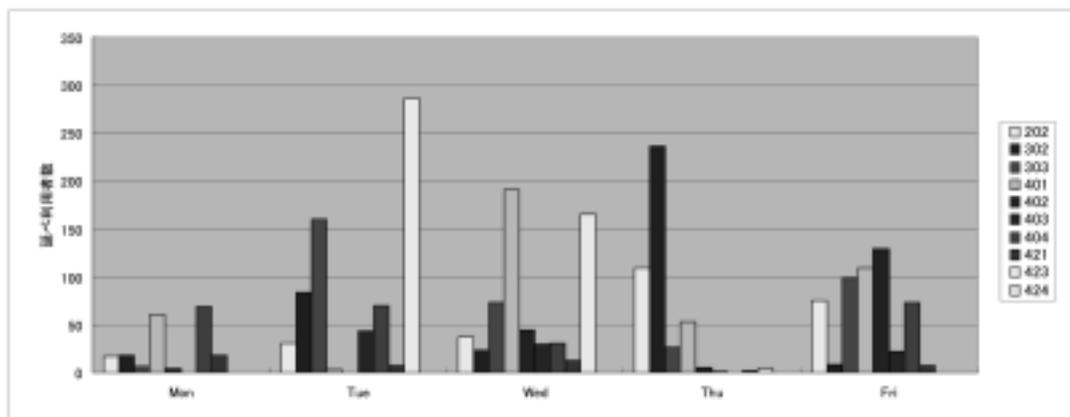


図3-5 情報コンセント提供エリアの曜日別の延べ利用者数（総延べ人数が500人に満たないエリア）

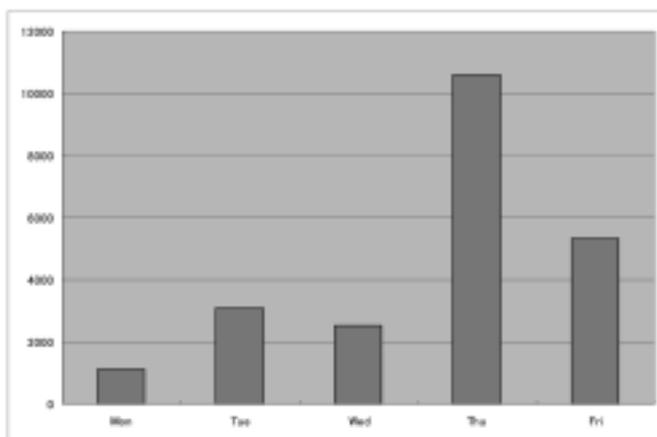


図3-6 情報コンセントの曜日別の総利用者数

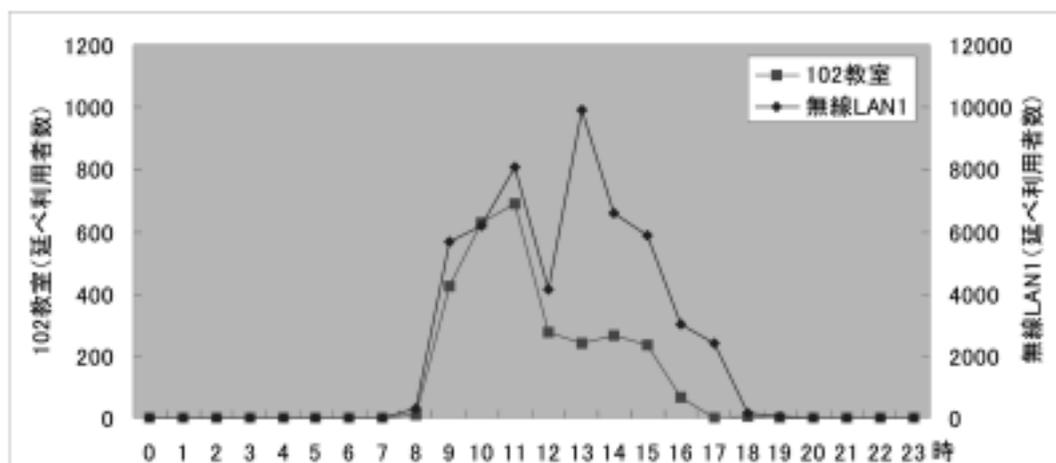


図3-7 102教室と無線LAN1利用者の時間推移

(1) 教室情報コンセントの利用率のバラツキ (教室・曜日)

(2) 無線LAN、特に無線LAN1への負荷集中。

(1) については、現在はノートブック主体の授業への過渡期であり、曜日の偏りも教務上の問題であるため、ある程度は仕方の無いことかもしれない。少なくとも1～3年生がノートブックを必携する、19年度まではデータを取り続け、分析する必要があるだろう。(2)の問題に関しては、次章で詳しく議論する。

3.3 DNSラウンドロビンの効果

システムの冗長構成をとる手法としてDNSラウンドロビン方式が挙げられる。これはDNSにサーバ名の名前解決の問い合わせがあったときに、順に複数のサーバの中から一台のIPアドレスを返すことにより、実際にアクセスを処理するサーバを分散させるものである。この方法を利用すると、特別なハードやソフトウェアを使用すること無しに、1つのエリアにサーバを複数台用意できるため、容易にシステムの冗長構成をとることができる。

DNSラウンドロビンによる負荷分散の際に注意すべき点は、クライアントに於けるDNSのキャッシュの問題である。クライアントは

DNS問い合わせによる無駄な通信を避ける為、前回に得た応答を保存し再利用することがあり、その場合、意図したようにうまく分散されない可能性がある。

ただし、この問題の影響を顕著に受けるのは、短時間に頻繁にDNSを利用する場合である。今回のシステムのように、一度DNSを利用してPPTPサーバのアドレスを検出した後は、再接続するまではPPTPサーバの名前をDNSに問い合わせに行くことのない場合では、余り影響はないと思われる。一度接続した後、一旦切断し、さらに再接続を行なう場合の時間は、十分長いことが期待できるからである。

現在の本学のシステムでも、情報コンセント数が100個を超える教室に於いてはPPTPサーバを2台用意し、DNSのラウンドロビンにより冗長構成をとっている。冗長構成は最大でPPTPサーバ2台となっているため、理論上は接続要求を1/2に分散することが期待できる。

ここで、システムが本当に期待通りに作動しているかを検証するために、PPTPサーバの冗長構成をとっている教室に関して、2台のPPTPサーバの同時刻の利用者の差(の絶対値)の総数の割合(不均等率)の計算を行なった。計算式は以下の通りである。

不均等率＝

$$\frac{(\sum | \text{同時刻利用者の差} |)}{(\text{総利用者数}) * 100}$$

各教室での不均等率の分布図を図3-8に示す。

分布図で示すのは、総利用者数によりデータの正確さが異なると考えられるためである（利用者数が少ない場合は不正確）。グラフより、DNSのラウンドロビンを使用することにより、利用者数が十分多ければ、40～60%程の効率で、負荷分散が可能なことが分かる。

なお、102教室では、1台のPPTPサーバが不調であることが報告されており（その後の調査によりハードウェア故障と判明）、不均等率も95%になったため、計算結果からは外してある。

4. 問題点と解決方法

4.1 無線への負荷集中

現在、5号館（フロンティア研究棟）を除く全ての建物でIEEE802.11bによる無線LANが利用可能である。利用の多い1号館（本館棟）では建物内でもエリアが区切られており、北側の

各教室をカバーするエリア、南側の各教室をサポートするエリア、各階ホールをサポートするエリアなど大小含め4つのエリアが存在する。

これらのエリアの中でも、1号館北側の無線LAN1エリアの利用頻度が高い。このエリアには情報コンセントを備えた教室が多く配置されているが、無線LANへの利用の偏りが存在する。

無線LAN1エリアを管轄するPPTP-GW5については今後更に利用者が増える可能性があり、実際に接続者数の上限に達しそうな日も数日あった事から負荷の分散は急務である。また、利用者が常に一定数存在することから、安定したサービス提供も行なわなければならない。そのためには無線LAN1エリアの分割、DNSラウンドロビンによる冗長構成をとる必要がある。体育館エリアのサーバについても、無線LAN1～LAN3と同じ情報センターのサーバ室内にサーバがあるため、これらのサーバの統廃合も検討すべきであろう。

一方、教室のPPTPサーバについては、複数教室のサーバの統合や無線LANと情報コンセントの統合による負荷の平滑化も考えられる

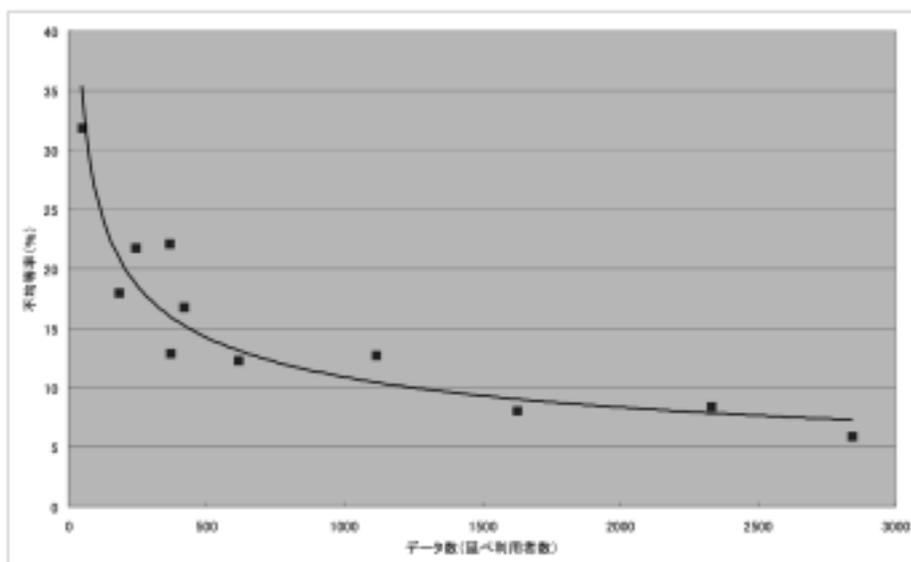


図3-8 冗長構成をとっている教室の不均等率
(曲線は累乗近似曲線)

が、そもそも分散管理体制をとった理由である、演習担当の教員からの「演習時に学生がどの教室から接続しているのか判別したい」という要望を考慮すれば、このような処置は難しいと言える。

具体案としては、無線LAN1エリアを3つに分割し、その内の一つと体育館エリアを統合する。また、これらのエリアについては、DNSラウンドロビンによる冗長構成をとることが考えられる。今後、この具体案については、至急検討して行きたいと考えている。

4.2 ログの項目

現在記録しているログの形式では、サーバがシャットダウンされた場合などを検出することが出来ない。そのためトラフィックの値を計算する際に正確な値が算出できない可能性がある。

トラフィックの計算はネットワークインターフェイスを通過する通信データ量を元に算出するが、直接インターフェイスから得られる値は「その時点でインターフェイスを通過した通信データ量の総和」である。現行のシステムでは5分間隔でトラフィックデータを取得しているが、これは直前での通信データ総量と現在の通信データ総量との差を計算することで、その時刻でのトラフィックを算出しているのである。

そのため、もしサーバがシャットダウンされた場合、通信データ量のカウンタは0からの再計算となるため、保存してある直前の値との差をとっても正確なトラフィックを得ることができない。

通信データ量が0になることは、通信データ量が格納メモリ内でオーバーフローした場合も起こりうるので、これらの区別を通信データ量だけから判断することは難しい。

現在SNMPで取得している監視項目は、PPTPサーバで利用されている2つのネットワークインターフェイスのトラフィック（通信データ量）、利用者の数（動作中のpppプロセス

数）、CPUロードアベレージ、メモリの使用量（空きメモリの変化、スワップの利用状態）である。先にも述べたように、これらの項目だけでは、サーバがシャットダウンされた場合などを検出することが難しいので、新しい項目を監視対象とする必要がある。

即ちsysUpTimeという項目で、最後に初期化されてからの経過時間を表すものである。この値は100分の1秒の単位でカウンターとしてカウントアップされ、シーケンシャルに加算され続ける。つまりシャットダウンや再起動が起こらない限り減ることはない。この値を指標として再起動の検出を行えば、トラフィック計算時の誤りを訂正することが可能となる。

4.3 収集方法

現在、各サーバのログはcronにより自動的に収集されローカルホストに保存される。ローカルホストにデータを保存するのは、ネットワーク上に障害が発生した場合でも状態を記録できるように考慮したものだが、保存したログを参照するためには各サーバを直接参照しなければならない。現行では、サーバ上ログの選択・圧縮（自作スクリプトによる）およびデータ転送は全て手動で行なっている。

利用するPPTPサーバの台数が少なければ、各サーバからログを収集する作業も特には問題にはならないが、管理する対象が多い場合は、省力化・自動化を進める必要がある。PPTPサーバが40台もあればなお更である。

取得したサーバのログを手動で回収してることが非効率的であるという問題に対しては、回収作業を自動で行わせることで解決を図りたい。そのための方法として検討しているのが、SSHのサブシステムであるscpである。

SSHでは公開鍵を利用した自動運転で指定のコマンドのみを実行することが出来る。つまり、各サーバでのSSHの鍵ペアauthorized_keysにcommandオプションを登録しておくことにより、指定コマンドのみを実行させることができ

るのである。これに加えてfromオプションを併用してアクセス制御を行うことにより、安全にデータ転送を行うことが可能となる。この仕組みを利用することで、自動的にサーバからログを転送してこることが可能となる。

- [6] <http://www.poptop.org/>
- [7] <http://www.samba.org/ppp/>
- [8] <http://www.mrtg.jp/doc/>
- [9] <http://www.symantec.com/region/jp/>

5. まとめ

本学の無線LANおよび情報コンセントの環境については、これまで利用動向などの調査は積極的に行なわれて来なかった。今回、PPTPサーバの利用状況を調査することにより、実際にどのように利用されているのか把握することができた。その上で、現状のシステムが持ついくつかの問題点とその解決策についても検討を行なった。

今後は、課題として取り上げた「負荷の平滑・分散化」「より正確なログデータの収集」「ログデータの自動転送」などの問題について解決を図ると共に、今回のような調査を今後も継続し、より安全で利便性の高いネットワークを提供できるよう更なる検討を進めたいと考えている。

参考文献

- [1] 菊地裕明、井関文一、「学内ユビキタスを実現するための情報コンセント及び無線LAN環境の構築」、情報処理教育研究者集会講演論文集、pp. 117-120, Nov., 2006, 九州大学
- [2] 藤川賢治、古村隆明、岡部寿男、「京都無線インターネットプロジェクトみあこネットの設計と運用」、情報処理学会研究報告 2002-CSEC-20, pp.1-4, 2002
- [3] 榊田秀夫、大角祐介、鈴木未央、中西通雄、「生協食堂における無線LANサービス実証実験」、2002 PCカンファレンス、pp. 348-349, Aug., 2002, 早稲田大学
- [4] 榊田秀夫、竹村亮介、大角祐介、中西通雄、「生協食堂における無線LANサービス実証実験(続編)」、2003 PCカンファレンス、pp. 383-384, Aug., 2003, 鹿児島大学

参照

- [5] <http://pptpclient.sourceforge.net/>