



飯塚キャンパス課外活動共用施設棟 LAN について - 学生の自治によるネットワークの運営 -

梅田 卓矢¹
岩男 皓一郎²

1 はじめに

九州工業大学飯塚キャンパスには課外活動共用施設 (通称サークル棟) があり, 施設内の各部室を多くのサークルが利用しています.



図 1: 飯塚キャンパス課外活動共用施設

私たち九州工業大学学生自治ネットワーク委員会は, サークル棟内の計算機ネットワーク (club.kyutech.ac.jp) を学生有志で管理する団体です.

サークル棟の各部室には, 自治ネットワーク委員会によって整備された 100Base-TX(一部 1000Base-T) の情報コンセントが導入されており, 各サークルは各部室のスイッチングハブに計算機を接続するだけで, ネットワーク資源にアクセスする事が可能です. また, メールサーバや www サーバ等の整備やサービスの提供, サークル棟内のネットワークポリシーの策定も委員会が行っています. 本稿では, 私たち委員会の活動内容や, サークル棟のネットワーク構成について紹介を行います.

¹九州工業大学学生自治ネットワーク委員会 運用部長 ume@club.kyutech.ac.jp

²九州工業大学学生自治ネットワーク委員会 運用委員 meta@club.kyutech.ac.jp

2 学生自治ネットワーク委員会

本章では、学生自治ネットワーク委員会が発足した経緯や、委員会組織の構成について紹介します。

2.1 委員会発足の経緯

飯塚キャンパスの課外活動共用施設は、情報工学部が飯塚キャンパスに設置された1987年に建設されました。建設当時から多くのサークルが部室を利用していましたが、サークル棟内のLANや、各種ネットワークサービスは導入されていませんでした。

1990年代になると、部室に計算機を持ち込むサークルが現れはじめました。次第に多くのサークルが計算機を持ち込むようになり、各計算機をネットワークに接続したい、共用のメールサーバやWWWサーバを導入して欲しいといった要望が、各サークルから出されました。

この要望に対し考えられた解決策が、「余った自治会予算をネットワークの管理費用に割り当て、自治による管理組織を作る」といったものでした。自治会執行部と各サークル部長により、学生の自治によるネットワーク管理を行うことが決定され、サークル棟から飯塚の幹線ネットワークに接続するための光ファイバも同時期に整備されました。

以上の経緯から、学生の自治によるサークル棟ネットワークの管理が可能となり、1996年に九州工業大学学生自治ネットワーク委員会が発足しました。自治ネットワーク委員会は、学生自治会を構成する専門委員会の一つです。従って、ネットワークの管理に関する高い自治権を持っています。発足以来、年間約50万円が自治会予算より割り振られ、ネットワークの自治管理を行っています。

2.2 委員会組織の構成について

今年度の学生自治ネットワーク委員会は、運用部員と運用部長で構成されます。運用部員は、サークル等のLANや各種共用サーバの維持管理を行います。運用部長は、運用部員の中から選出される、学生自治ネットワーク委員会の責任者です。サークル棟は独立したサブネットワークによるLANが構成されているため、私たちは飯塚キャンパスのサブネット管理委員会に参加しています。運用部長は、サブネット管理責任者となります。

運用部員の募集は随時行っていますが、特に年度の始めに1年生を対象とした募集を行っています。今年度は、新たに15名の1年生が運用部員に加わりました。もちろん、1年生の大半は、ネットワークの管理経験は有していません。このような管理経験のない部員を対象として、毎年四月から六月にかけて、週一回のネットワーク管理に関する勉強会を開いています。勉強会を終えると、余った部品を集めて計算機を組み立て、その計算機を用いてネットワークに関する実践的な勉強を行います。このような学習を経て2年生になる頃には、委員会が保有する主要な機器の管理を任されるようになります。

3 委員会が提供する各種サービス

学生自治ネットワーク委員会が提供する主要なサービスには、

- ネットワーク接続サービス (各部室の計算機を対象)
- 各種共用サービス (各ユーザが利用できるサービス)

があります。本章では、私たちが提供するこれらのサービスについて紹介します。

3.1 ネットワーク接続サービス

ネットワーク接続サービスは、サークル棟の各部室から学内ネットワークへ接続するための環境を提供するものです。各部室からネットワーク接続を行うためには、サークル棟 LAN の物理配線、サークル棟 LAN と学内ネットワークとの接続(ルータ、ファイアウォールの整備)、ネットワーク利用に必要なサーバ類(DNS、DHCPサーバ)に関する整備が必要となります。

サークル棟ネットワークの概要 サークル棟のネットワーク構成を図2に示します。サークル棟 2F の配管室には飯塚キャンパスの幹線ネットワークが引かれており、ここにルータ(ホスト名:gateway)を設置し、サークル棟 LAN(club.kyutech.ac.jp)と接続しています。サークル棟 LAN は 1F 部分と 2F 部分ごとにスター型のネットワークを構成しています。計算機室は 1F にあり、ここに DNS、DHCP 等の IP アドレスを管理するサーバ(ホスト名:ns)と、www サーバ(ホスト名:crystal)、メールサーバ(ホスト名:sapphire)、ユーザアカウントを管理する供用サーバ(ホスト名:ruby)があります。図2の通り、全ての部室が同一のネットワークに所属しており、所属する全ての計算機はグローバルネットワークに接続されます。

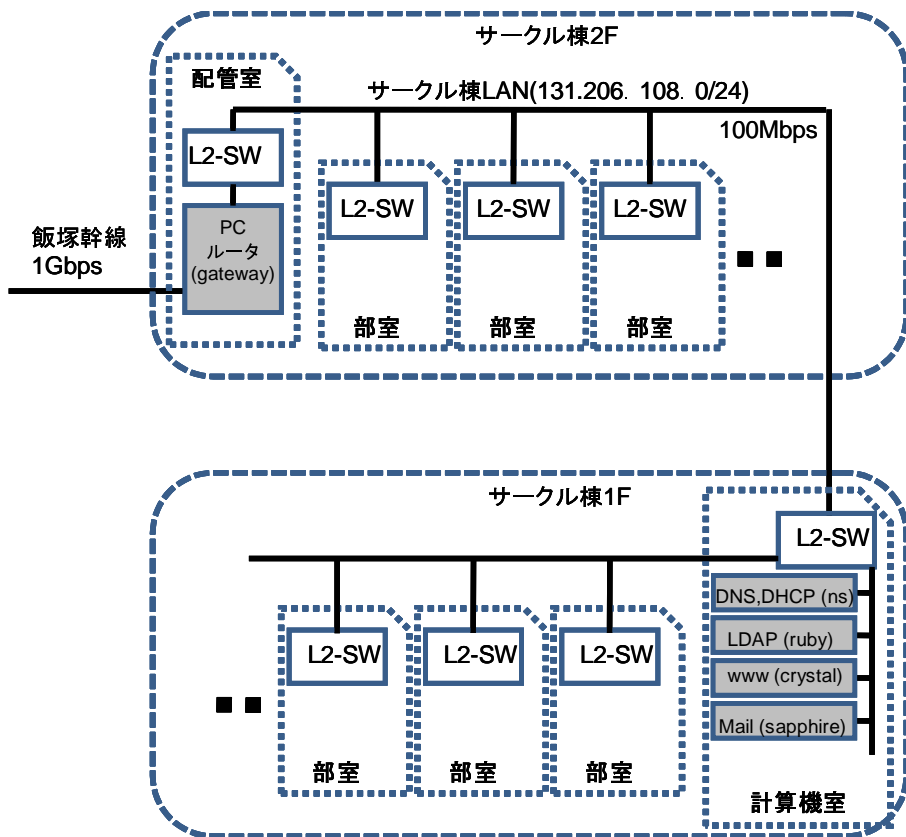


図 2: サークル棟ネットワーク構成図

ルータ サークル棟に整備しているルータの外観を 図3に示します。このルータによって、サークル棟 LAN と学内ネットワークを接続しています。図の通り、ルータは専用機ではなく、PC ベース (FreeBSD が稼動) によって構成しています。ルータを構成する PC の仕様は表 1 のとおりです。



図 3: PC ルータの外観

FreeBSD 上で経路制御プログラムである `routed` を動かし、ネットワークの経路制御を行っています。また、`ipfw` によるパケットフィルタを導入しており、簡易的なファイアウォールを実現しています。基本的には、対外ネットワークからのサークル内 LAN への接続は、`ssh` 以外許可を行っていません。特定のポート番号の解放を希望するサークルまたは個人に対しては、4 章にて述べる LAN 利用規則に基づき許可を行います。

なお、ルータを通過するトラフィック量については、学生自治ネットワークの `www` ページで閲覧することができます。利用の多い時間帯は昼休みや 16 時台で、平均で 500kbps 程度と、決して少なくない通信量を示しています。このような通信量を PC ルータで支えています。現状ではトラブルは僅かであり、安定したネットワーク接続を維持できています。

DNS, DHCP IP アドレスの管理を行うための DNS サーバと DHCP サーバを設置しています (図 4, 表 2) これらのサーバもルータと同様に、PC-UNIX(NetBSD) 上で動作しています。DNS は `bind9`, `dhcp` は `isc-dhcpd` を導入しており、利用者が決定したホスト名が自動的にネームサーバに登録されるダイナミック DNS を実現しています。



図 4: DNS, DHCP サーバの外観

表 2: DNS, DHCP サーバ (ns) の仕様

model	Sun Blade100
CPU	UltraSPARC-IIe 500MHz
RAM	640GByte
HDD	40GByte
OS	Solaris9
DNS サーバ	BIND 9.4
DHCP サーバ	ISC DHCP 3.1

各部室の計算機には、DHCP による動的な IP アドレスの割当を基本としています。固定の IP アドレスを希望するサークルまたは個人に対しては、後述する LAN 利用規則に基づき割当を行います。

LAN 配線 ネットワーク構成の紹介で触れましたが、サークル棟 LAN は 1F 部分と 2F 部分ごとにスター型のネットワークを構成しています。各階に 24 ポート級の部室収容スイッチングハブ (図 5)(100Base-T × 24) を整備しています。各部室にはにメタル配線が伸びており、各部室ごとに 1 台のスイッチングハブ (図 6) を整備してい

ます．このように，各部室の末端部分の情報コンセント(スイッチングハブ)を含めたネットワークの整備を行っているため，ネットワークにあまり詳しくないサークルも，手軽にネットワーク資源を利用することが可能です．



図 5: サークル棟部室収容スイッチ



図 6: サークル棟各部室スイッチ

3.2 各種共用サービス

共用サービスは，サークルに所属する各部員が，電子メールの利用や www による情報の公開等を行うためのものです．現在，各ユーザ向けに，www，電子メール，IRC の各サービスを提供しています．

アカウント管理 アカウント管理サービスは，直接的なサービスを提供するものではありませんが，www や電子メールを利用するためのユーザ情報を蓄積，管理を行います．

アカウント管理サービスは，LDAP サーバによって構築されています(表 3)．www や電子メールサービスの利用を希望するユーザ情報は，共用サーバ上で動作する LDAP サーバ (OpenLDAP) で管理しています．現在，600 人のユーザが共用サーバに登録されています．なお，LDAP は管理データベースの多重化を行える仕組みが備わっているため，将来的に管理サーバを増強する事が容易に可能です．(増強が必要な程のユーザ数の増加はありませんが，管理情報のバックアップ用途としての必要性を感じています)．



図 7: 共用サーバの外観

表 3: 共用サーバ (ruby) の仕様

model	Dell PowerEdge 1600SC
CPU	Xeon 2.4 GHz
RAM	256MByte
HDD	36GByte
OS	Solaris9 x86
アカウント管理データベース	OpenLDAP 2.3

www サービス www サービスは，各サークルやユーザによる www ページの公開や，後述する web メールや www-IRC クライアントの提供を行います．www サービスは，www サーバとデータベースサーバによって構築されています(表 4)．管理サーバに登録されたユーザは，www コンテンツを公開する事が可能になります．html を用いた一般的な www ページだけでなく，perl や ruby を用いた CGI，PHP を用いた動的な www ページが

構築できます(図8)。また、jsp/servlet/strutus等のjavaを用いた高度なwebサイトや、MySQLを用いたデータベースによるデータ管理も可能です。

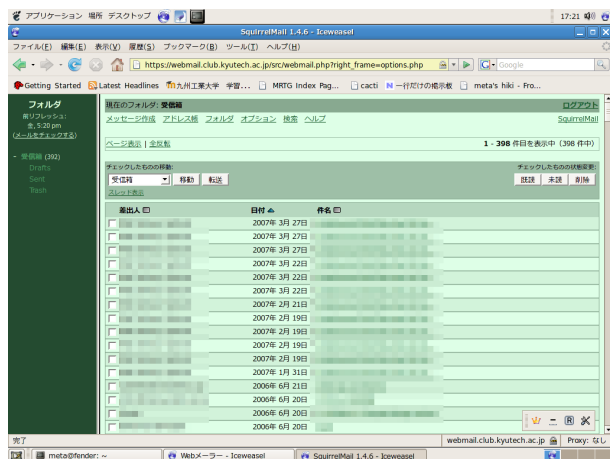


図 8: PHP/MySQL を利用した www ページ (webmail クライアント)

表 4: www サーバ (crystal) の仕様

model	Dell PowerEdge 400SC
CPU	Pentium4 2.4 GHz
RAM	256MByte
HDD	40GByte
OS	NetBSD-3.1
www サーバ	Apache 2.2.4
SQL サーバ	MySQL 5.0
利用可能なスクリプト	perl, ruby, PHP
JAVA ベースのシステム	jsp, servlet, strutus

電子メールサービス 電子メールサービスは、サークル内からの電子メールの送受信および対外からのサークル向けの電子メールの受信を提供しています。電子メールサービスは、SMTP, IMAP/POP の各サーバ、および SPAM/Virus 対策ソフト、メールフィルタソフト(表5)によって構築されています。

アカウント管理サーバに登録されたユーザは、サークル棟内からの smtp サーバの利用、サークル棟内からの pop/imap サーバの利用が可能になり、自由に電子メールの送受信が可能です。なお、www サービスと同様に、メールボックスの容量制限はありません。

メール受信時のサービスとして、procmail によるメールの振り分け、Clam AntiVirus を用いたウィルスメールやスパムメールの検出等を提供しています。申請を行えばメーリングリストを設置する事も可能です。

また、サークル棟外からの電子メールの送受信を行えるよう、www ブラウザによるメールの送受信が可能な web メールシステムを導入しました。

http 上で web メールを利用する場合、サークル棟までの通信は暗号化されていません。従って、第三者からメールの内容を盗聴される可能性があります。この事態を防ぐために、http を ssl を用いて暗号化する必要があります。暗号化を行うためには、暗号化鍵と、その鍵に関する第三者機関からの証明書が必要になります。小規模なネットワークでは、自分の組織で作った ssl の鍵を自分の組織で証明し、そのまま用いる事例が多く見受けられます。当然、暗号化はできるのですが、自分の組織で自分の暗号化鍵を証明していることになり、悪意のあるグループからのなりすまし等が可能です。したがって、正しい使用例とはいえません(オレオレ証明書、などと呼ばれたりします)。私たちは、ssl の暗号化鍵に対して、証明期間であるジオトラストからのからの証明を受けました。証明を受け、証明書を発行してもらうためには、手数料(6万円程度でした)が必要ですが、割り当てられた予算で賄うことができました(より手数料が安価な証明機関も存在しますが、そのような証明機関は信用度が低いので、証明書を取得する意味が薄れてしまいます。)

このような証明書を取得することにより、信頼性の高い(なりすましの出来ない)web メールサービスを提供しています(図9)。なお、対外でのメールの送受信が可能にする方法として、smtp や imap を ssl によって暗号化



図 9: 署名を受けた SSL 証明書

表 5: 電子メールサーバ (sapphire) の仕様

model	自作 PC
CPU	Pentium4 2.8 GHz
RAM	1GByte
HDD	40GByte
OS	FreeBSD 4.9R
SMTP サーバ	Postfix 2.4
POP/IMAP サーバ	Dovecot 1.0
web メールシステム	SquirrelMail 1.4
SPAM/Virus 対策	Clam AntiVirus 0.91
メールフィルタ	procmail 3.15

する方法も検討しましたが、メールサーバの設定（メールの中継や外部ネットワークからの受信を許すための項目など）の手間を省くため、web メールサービスの提供を選択しました。

IRC サービス IRC (Internet Relay Chat) は、専用サーバーに接続することによってチャットを行うことができるシステムです。IRC サーバは、DNS サーバ (ns) 上で稼働しています。

チャットを利用することにより、オンライン上で複数の人が情報の交換を行うことができます。各サークルの部員は、サークル棟に集まれない場合等はチャットを利用して情報を共有する事が多いため、IRC サーバを整備しています。

IRC サーバにログインしているユーザ数は、学生自治ネットワークの www ページで閲覧することができます。利用者がゼロになる時間帯はほぼ存在せず、多い時間帯には 30 人程が利用しています。サークル棟には必要不可欠なサービスであると言えます。

4 管理方針

本章では、サークル棟ネットワークの管理方針について紹介します。ここでは、サービスを利用するサークルやユーザに守ってもらうべき規則に関して、日常の管理業務に関して、各サークルとの情報交換の必要性に関して述べたいと思います。

前章で述べた各種のサービスを各サークルおよび所属部員が利用する際には、利用規約を遵守する必要があります。現在は、以下に示す 4 つの規約を設けています。

1. 共用計算機利用規約 (アカウントの利用に関する規約)

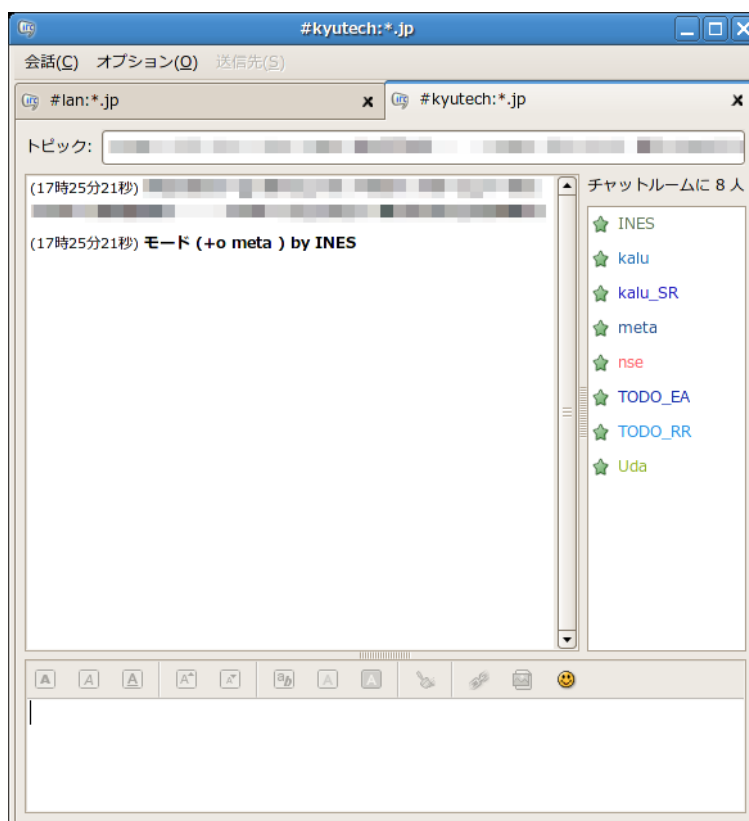


図 10: サークル棟 IRC サーバを用いたチャット

2. 共用計算機 WWW 利用規約 (WWW サーバの利用に関する規約)
3. 共用計算機メーリングリスト (ML) 利用規約 (メーリングリストの利用に関する規約)
4. 課外活動共用施設内 LAN 利用規約 (固定 IP アドレスの取得等に関する規約)

電子メール等の利用アカウントの発行，www サービスの利用，メーリングリストの開設，固定 IP アドレスの取得や外部からの接続を行う場合は，各種の利用申請が必要です．必要なサービスを得る際に各サークルは，サービスに応じた利用申請書を提出します．提出された申請書に対し，自治ネットワーク委員会で審査を行った後，サービスの割当を行っています．割り当てられたサービスの利用に対し，ユーザおよびサークルは利用規則を遵守しなければなりません．また，サービスの利用状況や，利用規則を遵守しているかの調査を行うために，定期的に各サークル部長とのミーティングを行っています．

多くの利用規則や面倒な申請手法を採っているように思えますが，管理側 (自治ネットワーク委員会) と利用側 (各サークル) の双方が学生であるため，明確な管理方針がなければ，管理体制がいい加減なものになってしまうと考えています．幸い近年では見受けられませんが，利用規則に違反したユーザ・サークルに対しては，アカウントのロックやネットワーク接続の物理的切断を行い，当分の間はネットワーク接続の申請を受け付けず罰則を設けています．このように厳しい管理方針を採る事により，学生の自治によるネットワーク管理は成立すると考えています．

各サークルとの情報交換 前節に記述した通り，自治ネットワーク委員会と各サークルの間では，年に数回の定期ミーティングを行っています，このミーティングでは，各サークルが必要としているサービスのヒアリング

解説

を行います。多くのサークルが必要としているサービスがあれば運営委員で協議を行い、サービスの実現に向けて動き出します。近年では、サークル棟外からのメールの送受信を行うための web メールサービスや、通信効率を向上するためのスイッチングハブ交換、IRC サーバの立ち上げ等を行いました。これらのサービスは、各サークルとのミーティングによって出された要望に応える形で実現したものです。

日常の管理 各サービスへの利用申請に対する対応や、新たなサービス実現のためのシステム構築以外に、日常のトラフィック監視も重要な管理業務です。サークル棟と学内ネットワークを中継するルータ上では SNMP サービスが稼働しています。中継したパケットの流量を監視する事ができるため、サークル等外からの不正なアタックや、サークル内の計算機からの異常なトラフィックを検知できます。ルータの通信断は運用部員宅から検知できるため、ダウンタイムの減少にも貢献しています。また、ルータ上で動作しているファイアウォールのアクセスログに関する監視も行っており、不正な通信が起きている場合はすぐに検知する仕組みを導入しています。

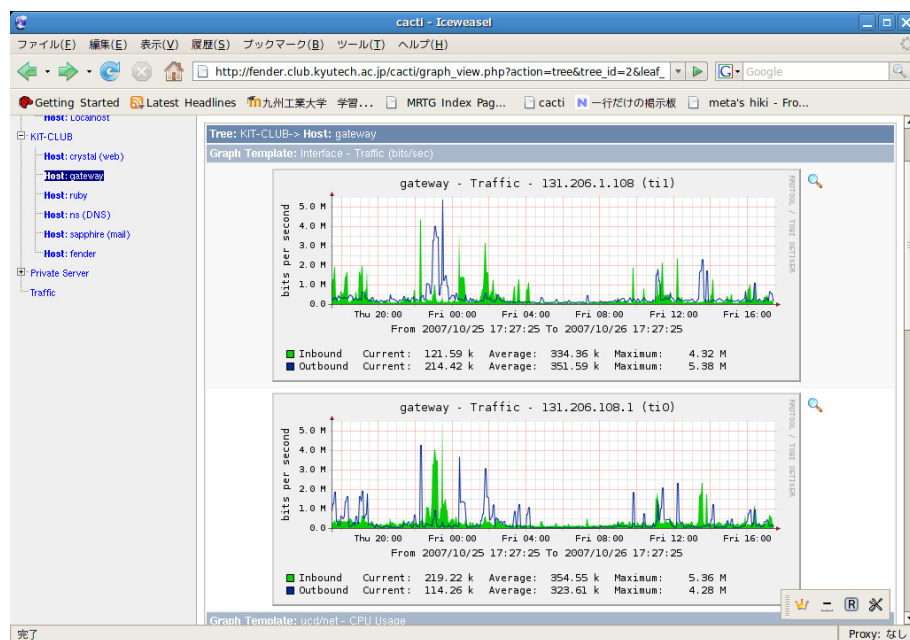


図 11: SNMP 監視例 (ルータのトラフィック量)

5 将来の構想

本章では、サークル棟 LAN の将来構想について述べたいと思います。

まず、サークル棟内に無線 LAN を整備したいと考えています。最近のノートパソコンは無線 LAN が標準で装備されており、サークル棟内でも利用できれば便利です。従って早い段階で導入したいと考えていますが、サークル棟全域で利用可能にするためのアクセスポイントの設置計画や、利用可能なユーザの認証方法を考慮して、導入を検討する必要があります。

加えて、RAID5 により冗長化されたファイルサーバを整備したいと考えています。近年、www を用いて公開するコンテンツの大容量化、メールに添付されるファイルのサイズも増大しています。これらの大容量のデータ

を安定して扱えるよう、RAID5による冗長化、ホットスワップへ対応したファイルサーバが必要であると考えています。

以下は、更に将来的な構想です。一つ目は、学内の幹線ネットワークと接続しているルータの、サークル棟内の計算機室への移設です。現在ルータをサークル棟内の配管室に置いています。この部屋には空調がありません。夏期にルータが停止した事はありませんが、かなりの高温下で動かしているため、あまり好ましい状態とはいえません。また、ルータ以外の計算機は全て計算機室に設置しています。ルータも同じ部屋に移設できれば、管理効率が向上するため、この点からも移動を行いたいと考えています。

二つ目は、各部室へのネットワークをプライベートネットワークに置き換えるという事です。現在は全ての部屋がグローバルネットワークに所属しており、DHCPでグローバルIPアドレスを取得する事ができます。近年はNATを用いればプライベートネットワークでも不自由のない利用が可能ですし、セキュリティの観点からも好ましいと言えます。このような理由より、計算機室と申請を行ったサークル以外はプライベートネットワークに所属できれば、と考えています。上記の二つの構想を実現するためには、配管室と計算機室の二箇所に、VLANの設定が可能なスイッチングハブを導入する必要があります。このようなスイッチを予算内で買う事ができれば、導入したいと考えています。図12に将来のネットワーク構想を示します。

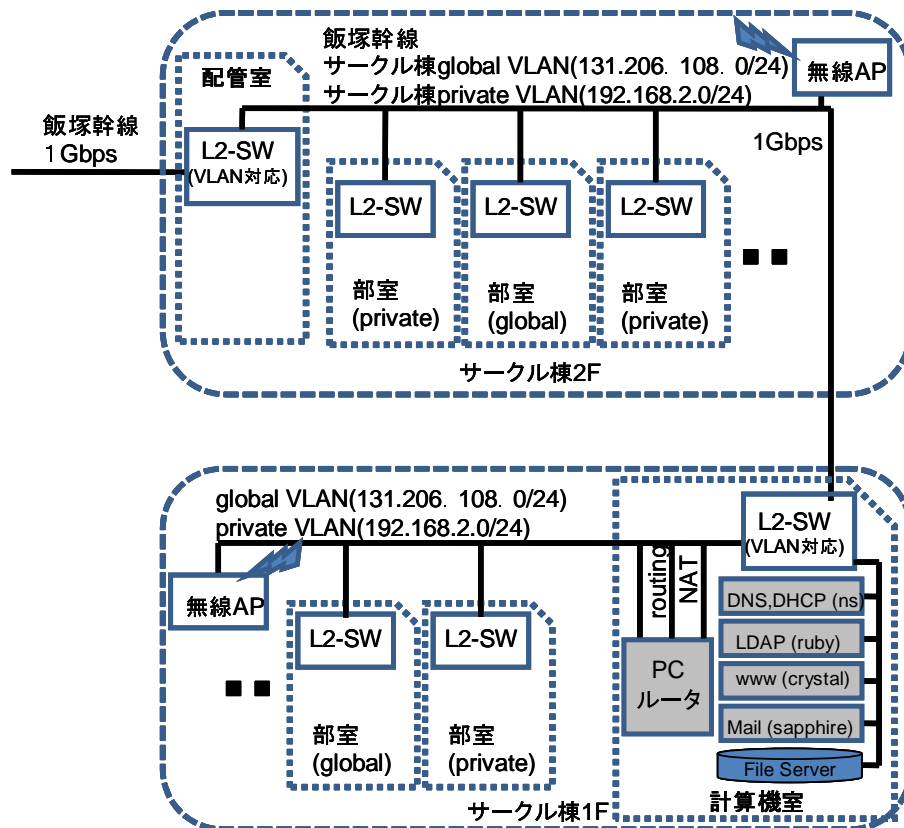


図 12: サークル棟ネットワーク将来構想

6 まとめ

本稿では、九州工業大学学生自治ネットワーク委員会の活動内容に関して説明を行いました。

解説

私たちは学生の自治により、サークル棟内のネットワークの整備や、各種サービスの提供を行っています。管理者と利用者の双方が学生であるため、ネットワークの秩序を保つためには、各サークルとの情報交換や利用規程の厳格な適用が不可欠です。現状では、利用者の満足度の高い、秩序あるネットワークが提供できているのではないかと考えています。

2章に示した通り、本委員会では管理スタッフを随時募集しています。管理経験は全く問いません。計算機やネットワーク構築への興味とやる気があれば、どんな方でもネットワークの管理を行う事ができます。多くの方の活動への参加をお待ちしています。今後も、学生自治ネットワーク管理委員会へのご理解とご期待をお願い致します。