学内LAN管理・運用支援システムの構築と運用について

高比良 廣人、藤村 直美、堀 良彰、平山 善一
九州芸術工科大学

概要

インターネットの普及に伴い、九州芸術工科大学でも学内ネットワークに接続するホスト数は大幅に増加している。現在、約1800台のホストが学内ネットワークに接続されており、IPアドレスの割り当てやDNSの運用等の管理は情報処理センターが行っている。学内ネットワーク規模の拡大に伴い、情報処理センターの管理業務の負担も増大し、各種作業の効率と品質の向上は切実な問題である。本研究では、情報処理センターにおけるネットワーク関連業務を支援するシステムとして、端局設置申請のオンライン化、不正利用ホストの追跡特定、講義室のVLAN変更予約システムを構築した。

Implementation of LAN Management Support System in University

Hiroto Takahira, Naomi Fujimura, Yoshiaki Hori, Zen-ichi Hirayama
Kyushu Institute of Design

Abstract

The number of hosts connected to LAN has been increasing sharply. Now, about 1800 hosts are connected to our LAN, and the information processing center manage those hosts. The burden of the management in the information processing center has also been increasing with expansion of LAN scale. We have to improve the efficiency and the quality of network management. In this research, we implemented ths system of hosts registration in on-line, tracking wrong utilization hosts, and VLAN change reservation of lecture rooms.

1　はじめに

九州芸術工科大学 (以後本学と略す) では1990年2月に初めて学内LAN (イーサネット) を整備し、当時は約70台の計算機がこの学内LANに接続された。その後、基幹ネットワークを1994年3月にFDDIに更新し、2001年9月からは情報処理センター (以後センターと略す) に設置したギガスイッチを中心としたスター型のネットワークを導入して運用している。2002年6月現在で学内LANに接続されている計算機は約1800台であり、この10年間余、3名の技術系職員でセンターの計算機と学内LANの管理運用を一手に行ってきた。

具体的には、利用者管理や計算サービスなどの通常の情報処理センターとしての業務に加えて、学内LANに関しては、計算機の設置や廃止に伴うIPアドレスの割り付けと解除、DNSの運用、学内LANに関連した全教職員学生からのトラブル対応、各種の不正アクセス等に対する対応、ファイヤーウオールの設定と運用、監視などである。したがって、センターにおける職員の負担を軽減すると同時に、各種作業の効率と品質を向上することは切実な問題である。そこで、今回のネットワーク更新を機に、端局設置申請のオンライン化、不正利用ホストの追跡特定、講義室のVLAN変更予約システム等のネットワーク関連業務の支援システムを構築したので報告する。

2　端局設置申請のオンライン化

学内ネットワーク管理の一環として、端局の設置や廃止手続きはセンターが行っている。従来の紙の申請書を用いた端局設置申請では、事務処理

の手間やその後の端局情報の活用を考えると効率的ではない。本研究では、これらの申請をオンライン化することで、事務手続きの省力化と情報の有効活用を可能にする。

その結果、紙で管理されていた情報をオンラインで処理することが可能になり、端局設置状況の正確な把握が可能となる。さらに後述する不正利用ホスト追跡システムと連動することで、問題となっている端末を速やかに識別できる。

2.1 システム概要

システム全体構成を図 1 に示す。サーバでは、PHP4が組み込まれた WWW サーバ (Apache) とデータベースサーバ (PostgreSQL) が稼動している。申請者及びセンター職員は WWW ブラウザを介して、利用者認証、端局申請、登録確認作業を行う。WWW を用いることによって、入力データをそのままデータベースへ登録でき、端局情報の管理を効率的に行える。

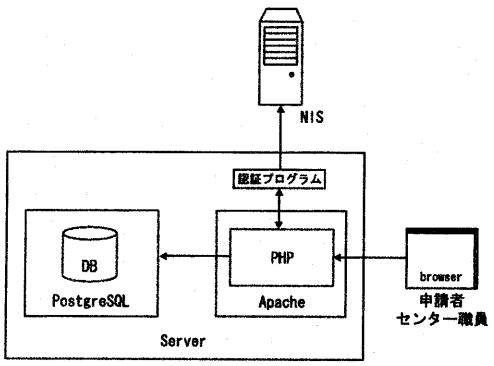

図 1: システム構成

2.2 申請手順

端局設置申請手順を図 2 に示す。記入者は端局設置申請フォーム (図 3 参照) に必要事項を入力する。入力されたデータは仮データベースに登録する。仮データベース登録後、記入者が学生の場合は申請者の欄で入力した教官のメールアドレスに登録確認のメールが届く。教官は申請内容の確認を行い、問題があれば修正し、なければ承認する。記入者が教官の場合は、教官による確認は省略する。いずれにしても教官が確認した時点で、センター職員に登録依頼のメールが届く。

教官からセンター職員に登録依頼のメールが届くと、センターで登録内容を確認し、アドレス情報を追加する。問題がなければ、担当者が DNS にデータを追加し、本データベースへ端末のデータを登録する。本データベースの登録と連動して、申請者に登録完了のメールを送信する。

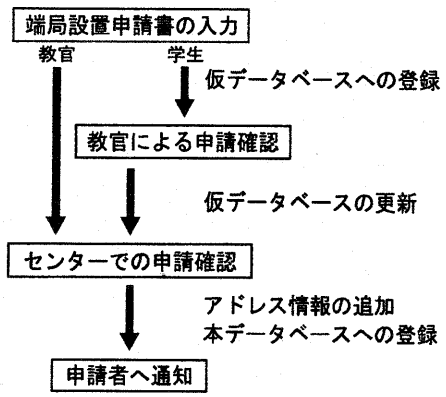

図 2: 申請手順

2.3 認証

本システムは、学内からのみの利用を考え、セキュリティ確保のために学外からのアクセスを拒否している。また、個人の認証にはセンターが発行しているアカウントを用いて認証を行う。

本システムでは、認証を行う際に作業内容によって利用者の身分を区別する必要がある。センターでは、UID には教官、学生等の身分によって異なる範囲の値を割り当てているので、UID の値を調べればユーザの身分を特定することができる。

認証の仕組みとしては、色々と検討した結果、ユーザ名とパスワードを使って、NIS を使用しているサーバにログインして確認している。その後に、UID を調べて身分を識別し、身分に応じた処理を行う。

2.4 端局廃止申請

端局廃止申請の申請手順は基本的に端局設置申請と同じ手順である。端局設置申請と異なるところは、端局廃止申請は申請者である教官のみが端局廃止申請を行うことである。教官は図 4 のフォー

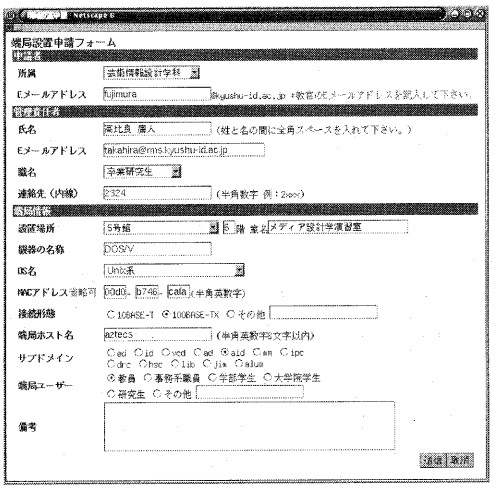

図 3: 端局設置申請フォーム

ムで、現在自分が登録しているホストの一覧を表示することができ、その一覧から廃止したいホストを選択する。これまで、使われなくなった計算機の IP アドレスを返却する手続きが充分に行われていなかったが、これによって、割り当てられているが使われていない IP アドレスの解消を目指している。

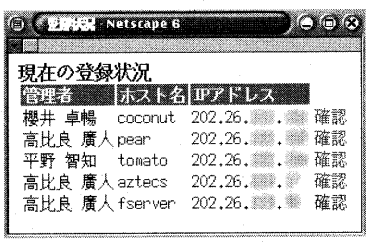

図 4: 申請ホストの一覧

3 不正利用ホストの特定

ネットワークに接続されたあるホストが設定の不注意あるいはソフトウェアの不具合等により、不要なパケットを送出し、別のホストの通信を妨害してしまうことがある。このような場合は、不要なパケットを送出しているホストを特定し、場合によってはネットワークから切り離す措置が必要となる。例を挙げると、同じ IP アドレスを複数のホストに設定した場合や、不要なブロードキャストパケットを送出している場合などがこれにあたる。

3.1 本学のネットワーク構成

本学のネットワーク構成を図 5 に示す。本学では、現在主要な建物内にワークグループスイッチ (catalyst4003) を 1 ～ 2 台配置し、建物内の各室へ 100base-TX のケーブルを付設している。各建物のワークグループスイッチは 1000base-SX でセンターに設置された基幹スイッチ (catalyst6509) へ接続されている。基幹スイッチはレイヤ 3 スイッチとして、ワークグループスイッチはレイヤ 2 スイッチとして機能している。またこれらのスイッチは VLAN 設定機能および管理機能を有している [1][2]。

レイヤ 2 ネットワークを構築する場合は、ホストの識別は MAC アドレスでのみ行われる。スイッチにおける転送表はホストから送出される始点 MAC アドレスを認識して自動構築される。ネットワーク管理を行うためにはどのホストが、スイッチのどのポートに接続されているかを知ることが重要である。このような観点から本学におけるネットワーク構築にあたっては管理機能を有する基幹スイッチおよびワークグループスイッチを導入している。

3.2 不正ホストを発見した場合の対処

同じ IP アドレスを複数のホストに設定し使用した場合等、不正なパケットを送出しているホストを発見した場合、管理者は次の手順で問題となるホストの場所を特定し適切な対処を行う必要がある。

1. 不要なパケットを送出しているホストの MAC アドレスを調査する。
2. 基幹スイッチの転送表を参照し、不要なパケットを送出しているワークグループスイッチを特定する。
3. 当該ワークグループスイッチの転送表を参照し、不要なパケットが送られてくるポートを特定する。
4. ワークグループスイッチのポートを特定することで、不要なパケットを送出している機器の部屋を特定する。

5. 部屋の管理者に連絡をとり障害を解決する。もし他のホスト影響が大きい場合はワークグループスイッチの当該ポートの通信を遮断する。

このような作業は、システムに精通したネットワーク管理者でも、ある程度手間がかかる。さらに、ネットワークに詳しい管理者が不在の場合を考えると、通常のセンター職員でもこのような作業を行えるようにすることが望まれる。そこで、これらの作業をWWWブラウザから行えるようにし、さらに、前述の端局設置申請のデータベースを利用し、不正ホストに関連した情報を的確に表示する仕組みを実現した。

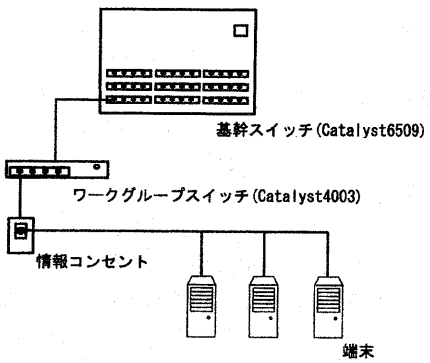

図 5: ネットワーク構成図

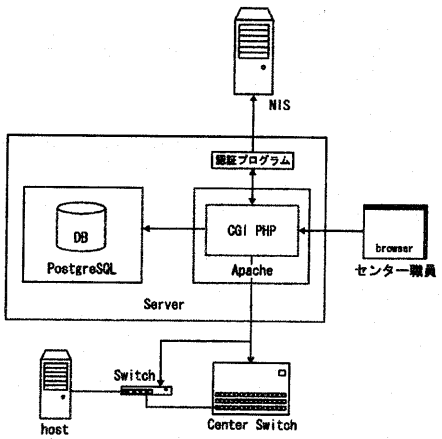

図 6: システム構成

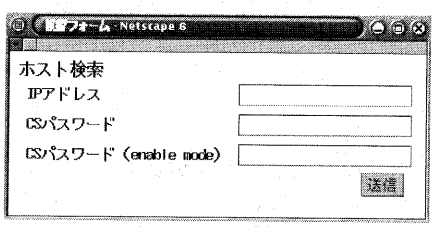

図 7: ホスト検索入力画面

3.3 システム概要

システムの全体構成を図6に示す。サーバ側の構成は端局設置申請と同様である。センター職員は認証後、検索したいホストのIPアドレスと基幹スイッチのパスワードを入力する(図7参照)。CGIプログラムは、先に述べた手順を自動実行する。基幹スイッチにログインし、arpテーブルを参照し、入力されたIPアドレスから検索したいホストがどこのワークグループスイッチに繋がっているかを調べる。次にワークグループスイッチにログインして、検索するホストが接続されているポートを調べる。結果を表示する際に、前述の端局設置申請で使用しているデータベースからホストの詳細情報を取得し、表示する(図8参照)。また、場合によっては、スイッチのポートを閉じて、外部と通信できなくすることもできる。

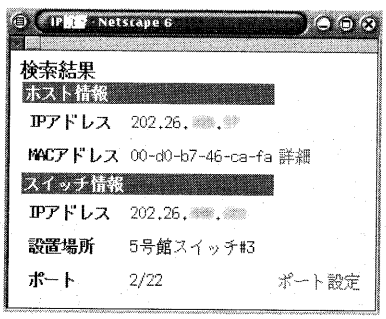

図 8: 検索結果の表示画面

4 講義室のVLAN変更予約システム

従来のFDDIとイーサネットによるネットワークでは建物単位でしかネットワークの管理ができなかったが、新しいネットワークでは、ポート単位で任意のVLANを構成することができる。そこで、新しいネットワークの導入にあわせて学科単位でVLANを構成した。講義室の情報コンセントは「講義室」という分類のVLANに割り当てている。講義等の際に、教官が講義室の情報コンセントからネットワークを利用するには2通りの方法がある。1つは、利用したい講義室の情報コンセントに割り当てられているVLANに対応したIPアドレスを一時的に割り当てる方法である。もうひとつは、情報コンセントが繋がっているポートを所属学科のVLANに変更する方法である。どちらも、センターに事前に連絡をとり、管理者に設定してもらう必要があり、管理者に連絡がつかない場合には、利用者は講義室でネットワークを利用することができない。

そこで、教官が時間を指定して、講義室からネットワークを利用できるように、講義室の情報コンセントのVLAN設定を利用者が所属する学科のVLANに変更する仕組みを実現した。この方法では、研究室等で使用している自分のパソコンを何の設定も変更せずにそのまま講義室で学内ネットワークに接続して使用することができる。こうすることで、授業の準備を行っていたノートパソコンを電源を切らずにそのまま講義室に持参し、続けて作業、授業を行うことができる。

4.1 システム概要

システムの全体構成を図9に示す。サーバ側ではWWWサーバ(Apache)と時刻を指定してコマンドを実行するatdデーモンが稼動している。利用者は、認証の後に、登録画面に移る。登録画面では、利用時間帯、教室名、希望するVLANを選択する。CGIプログラムは、atコマンドによって、指定された開始時刻と終了時刻にVLAN変更プログラムを実行するように設定する。VLAN変更プログラムは、指定された時刻になると、スイッチにログインし、指定された講義室の情報コンセントに繋がっているポートのVLAN設定を変更するコマンドを実行する。元に戻す時も同様である。

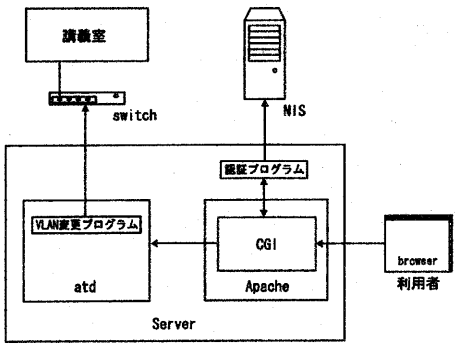

図9: システム構成

4.2 登録内容

VLANの変更予約の登録は、図10のフォームで、利用時間帯、教室名、変更VLANを選択し、登録する。

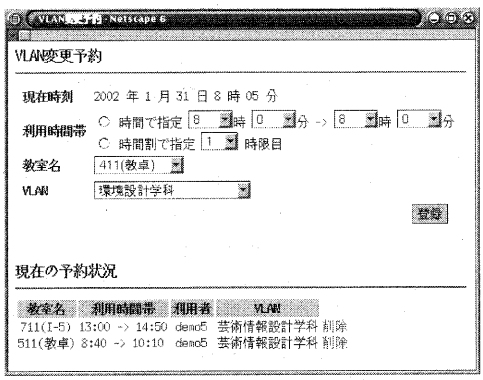

図10: 設定画面

現在時刻 正確な時刻を取得するために、サーバ側でntpd(タイムサーバ)を起動し、本学のNTPサーバと時刻同期を行っている。

利用時間帯の指定 本システムは、通常の授業や臨時の講義や研究会等で、講義室の情報コンセントから学内ネットワークに接続することを想定している。そこで、時間帯の指定方法には、授業の時間割による指定と時間帯による指定の2通りから選択する方法をとった。登録はその日のみとし、時間割での指定の場合は、授業開始後にも変更できる。時間帯での指定は、10分単位での指定としている。

教室名 VLANを変更したい教室名を選択する。教室名のリストを外部の設定ファイルから読み込み表示している。教室名の変更等の場合は設定ファイルを修正することで、容易に選択内容を変更することができる。

VLANの指定 希望するVLANを指定する。通常は利用者の所属する学科のVLANを指定する。VLANのリストも設定ファイルを変更することで、容易に変更できる。

現在の予約状況の表示 すでに登録されているジョブと現在実行中のジョブの一覧を表示する。時間帯、利用者、教室名、変更VLANを確認できるようになっている。

登録の削除 予約したジョブを削除する。実行中のジョブは削除することができず、登録を削除できるのは、登録した本人と管理者のみである。

4.3 スイッチのパスワードの暗号化

スイッチにログインする際に、パスワードが必要であり、このパスワードはネットワークの管理者しか知らない。本システムでは、管理者以外にパスワードを教えない方針で、スイッチのパスワードを暗号化し、ファイルに保存する方法をとった。ファイルからパスワードを読み込むことで、利用者にパスワードを教える必要がなくなり、管理者でない者も本システムを利用できる。

スイッチのパスワードは基本的にはスイッチ毎に異なる。したがってスイッチ毎にパスワードを準備する必要がある。管理者はスイッチのパスワード登録フォームから、個々のスイッチのIPアドレスと、パスワードを入力し、登録する。プログラムは入力されたIPアドレスと暗号化したパスワードをファイルに書き込み、VLAN変更プログラムでは、このファイルを読み込み暗号化されたパスワードを復号化し、スイッチにログインしている。暗号化アルゴリズムにはBlowfishを使用している。

5 おわりに

本研究では、ネットワーク規模の拡大に伴い増加する一方のセンターの管理業務を支援する3つのWWWベースの管理運用支援システムを構築した。

端局設置申請のオンライン化では、端局の申請手続きを省力化し、データベースを利用して、効率的に端局情報を管理できる仕組みを実現した。不正利用ホストの特定と講義室のVLAN変更予約システムでは、通常、管理者がスイッチにログインして行う作業を自動化した。これらのシステムは、ユーザインターフェースにWWWブラウザを用いることによって、システムに詳しくないセンター職員でも、容易に作業を行うことができ，管理者の負担を軽減できる。また、端局設置申請のオンライン化やVLAN変更予約システムでは、利用者側にも、利用上の自由度が増すなどのメリットがある。

今後の課題として、プログラムの汎用化による本システムの本学以外での利用と、認証の際にSSLを用いて通信を暗号化するなどのセキュリティの強化があげられる。

参考文献

[1] Catalyst 6000 ファミリー IOS ソフトウェア・コンフィギュレーション・ガイド

[2] Catalyst 5000/4000 ファミリー ソフトウェア・コンフィギュレーション・ガイド