ネットワーク管理運用支援データベースの構築と運用

大垣内 多徳 †　山下 芳範 †
福井医科大学 医療情報部 †

概 要

学内ネットワークの維持管理は，非常に重要な項目であるにも関わらず，そのために割くことのできる人的コストは限られているのが現状である．福井医科大学では，SQL データベースと WWW を用いた接続端末の増加に伴う登録管理業務やネットワーク管理を支援するためのデータベースを構築し運用を行った結果，センター職員の負担を減らすことに成功しているので報告する．

An Implementation of Network Management Database

Tatoku OGAITO†　Yoshinori YAMASHITA†
Fukui Medical University†

Abstract

Although management of LAN is very important item, the human resources we can assign to is limited. We have developed a system, which supports the registration of the terminal and LAN management, based on SQL database server and WWW. In the results, it releases members of information processing center from the simple but tedious work.

1　はじめに

福井医科大学 (以下，本学と略す) は職員数約 1200 名，学生数約 900 名の，単科医科大学である[1]．研究系，業務系のネットワークは分離されておらず，病院を含めた学内全体が一つのネットワークを構成している (以下，学内ネットワークと略す)．

学内ネットワークへの端末等の接続申請は年々増加し，2003 年 8 月現在で 4200 台を越えている．また，学内ネットワーク上では IPv4 だけではなく AppleTalk や IPX, LAT 等も利用されているため，利用者からの問い合わせやトラブル発生時には，複雑な対応が迫られる．

一方，すべての情報処理センターの職員は，医療情報部と兼任しているため，病院情報システムに関する業務や利用者からのトラブル対応に追われ，情報処理センターの業務に集中できる人員の確保が行われていないという点が永年の問題である．このため，ネットワーク全体を把握している職員も限られており，障害発生時に速やかに対応が取れない状況にあった．

我々は，このような状況を改善するために，情報処理センターの業務の一つであるネットワーク管理について品質を維持したまま省力化をはかれるよう，ネットワーク管理運用支援データベースを構築し，運用を行っているので報告する．

[1] 2003 年 10 月に福井大学と統合予定である．

2　運用支援データベース

2.1　設計方針

学内ネットワーク管理は大きく 2 つに分けて考えることができる．一つ目は，ネットワークの基本構成に関わるものであり，もう一つはそこに接続されている端末等の管理である．

本学の場合，一般利用者が学内ネットワークに接続するためには各部屋に設置されている情報端子を通して行うことになっているためネットワークの基本構成として管理するべきデータは表 1 にあげたものと，これらの物理的，論理的接続情報としてまとめることができる．これらの基本データは情報処理センターとして責任を持って管理すべきデータであるが，更新頻度はそれほど高くない．

ネットワーク機器	設置場所，機種，利用形態 Firmware version 等
情報端子	設置部屋名，所属部局

表 1: ネットワーク基本データ

一方，学内ネットワークに接続される機器管理は，更新頻度は高いものの基本データが適切に管理されていた上で，利用者が正確に必要なパラメータを提供すれば，センター職員が積極的に介入することなく行うことが可能である．しかしながら，従来は申請書ベースで接続申請が行われていたため職員がデータを入力した上で利用可能なネットワークパラメータを検索して割り当てを行っていた．これは単純ではあるが慎重さが要求される作業であり，センター職員に負担であると同時に手続きに時間がかかり，利用者にとっても不評であった．

我々は，この問題に対応するために，まず学内ネットワークに接続されている機器情報をデータベース化し，WWW によるオンライン申請を実現することにした．一方，ネットワーク基本データについては，一般利用者が更新する必要はないため WWW のインターフェースは用意しない．

2.2 データベース構造

構築するデータベース構造を決定する際にすでに登録されているホストデータを確認し，次のようなタイプの登録があることを確認した．

1. ネットワーク機器のように，複数の NIC を持ち，それぞれ異なる IP address を持っているものがある．

2. 負荷分散のために同一ホスト名が複数の IP address を持つものがある．

3. ノート型パソコンのように一台の計算機を複数の場所で使用している．(これらの計算機は接続される情報端子ごとに異なるネットワークパラメータを利用しなければならない．)

このような利用状況を記述するためには flat なデータベース構造では不適切であり，木構造もしくは複数のテーブルを用いた relational データベース構造を取ることが必要である．我々は次のようにテーブルを作成し，その間に相互関係を設定することにより現状を記述している．

接続機器に関するテーブル群は次の通りである．

Machine : 上記の 1 および 3 に対応するために導入した接続機器の筐体を管理するテーブルである．ネットワーク管理上は必要ないが，申請者や機器名等の管理を行う上では自然な発想と考えられる．

NIC : MAC address と属する筐体名データを持つ

IP : MAC address と接続端子，逆引きの際に返すホスト名等のデータを持つ

Hostname : hostname とそのホストに対する CNAME, MX 等のデータを持つ

IP assign : 上記の 2 に対応するために導入した IP address と hostname の対応を保持するテーブルである．

一方，ネットワーク基本データに関するテーブルとしては，

Socket : 各情報端子の設置場所，利用可能なネットワークパラメータ群，接続元のネットワーク機器およびポート等のデータを持つ

を導入した[2]．

これらのテーブル間の関係を図 1 に示す．

3 接続機器管理システム概要

システム構成を図 2 に示す．一般ユーザは WWW サーバ (Apache) に接続し，perl で記述された CGI を通して，データベースサーバ (PostgreSQL) を利用する．

センター職員は，各自の端末から直接データベースサーバに接続し，認証を行ったあと操作が可能である．インタラクティブにデータベースを操作す

[2]実際には利用可能なネットワークパラメータ群を管理するテーブルや他の情報を管理するテーブルも存在するが，煩雑となるため割愛する．

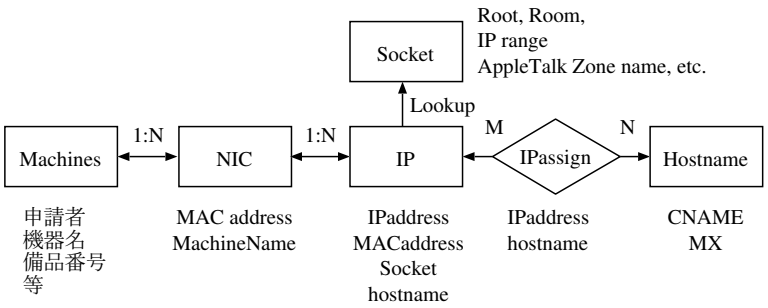

図 1: テーブル間の関係

る際のフロントエンドとしては，PostgreSQL，MicroSoft Access 等を利用している．

また，誤った操作に起因するデータの消去等の事故に備えるため，一日一度データベース内の各テーブルを checkout し，CVS による履歴管理も行っている．

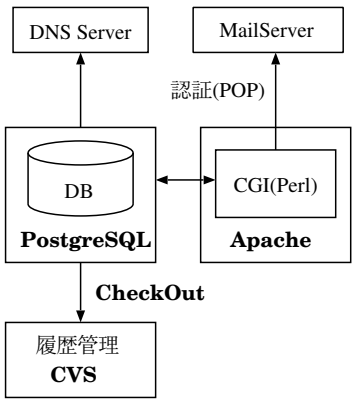

図 2: システム構成

3.1 申請の流れ

利用者が学内ネットワーク接続に関する申請を行う際の流れは次のようになる．

1. 認証および利用資格の確認
2. 申請手続きの種類の選択
   新規設置，変更，廃止，検索と申請書再取得
3. 申請内容の入力
4. 与えられたパラメータのチェック
5. データベースへの反映
6. ネットワークパラメータの発行
7. 利用者から情報処理センターへの申請書の提出
8. DNS 等への反映

このうち，認証からネットワークパラメータの発行までは，利用者自身が都合の良い時間帯を選択して行うことが可能であり，接続申請から利用可能なネットワークパラメータの取得までの時間が大幅に短縮された．

認証および利用資格の確認には情報処理センターのメールサーバを用いる．これは，本学では大多数の利用者が情報処理センターのメールサーバを利用しており，学部学生を除くメールアカウント保持者すべてが利用資格を有しているためである．

パラメータのチェックの段階では，与えられた端子情報や MAC address，ホスト名などを，30 項目以上に渡り確認し，不適切なデータの入力を防いでいる．特に RFC で定められている要件に違反しているものや，Microsoft Windows で利用されているワークグループ名やドメイン名との衝突が起きていない事の確認等，ネットワーク利用上問題となる可能性のあるものは過去の事例に基づいて全てエラーとして処理するように配慮した．

パラメータチェックで問題なく，データベース上に登録が終了した段階で割り当てられたネットワークパラメータは，WWW 上の画面に表示されるとともに申請者，各部局の運用責任者にメールにより通知される．同時に必要なパラメータが記入された申請書の発行が行われ，申請者，運用責任者が捺印

した上で，情報処理センターに提出し，申請が終了することになる．

発行する申請書には，申請番号をバーコードで埋め込むことにより，申請書受付，承認書発行までの手続きも半自動化されている．

4　ネットワーク管理への利用

4.1　DNS 管理

PostgreSQL データベースには参照整合性規約が設定できるため，あらかじめ各テーブルに適切な参照整合性を設定しておくだけで，登録データに矛盾がないことが保証される．

そのため，登録データベースから DNS データを作成するのは，非常に単純な作業であり，さらにプログラムを用意したことで，DNS データ形式に不馴れな職員であっても，DNS の設定ミスや運用ミス [6] をおこさずにデータ更新を行うことが可能である．

4.2　ネットワーク機器管理

本学のネットワークは 20 台程度の L2/L3 スイッチと 100 台以上の L2 スイッチ等から構成されている．このうち，IP が利用できるものについては機種，設置場所が判るようなホスト名をつけて登録している．その結果，データベースから正規表現を用いたホスト名を検索することにより現在稼働中の機器一覧を目的にあわせてもれなく抽出することができる．この出力を SNMP コマンドに渡すことにより，firmware が更新されていない機器の検出，更新作業等を効率的に行うことが可能となっている．

また，SNMP で参照できる変数に管理番号等の個体識別を行う値を設定してこの値と MAC address を用いて，登録データベースと照合するプログラムを定期的に実行することによりネットワーク機器の登録データが正確であることを確認している．さらに論理ネットワークの分岐点である機器を抽出し，その設定内容を履歴管理することにより，誤ったパラメータを設定してネットワーク障害が発生した場合等に以前の内容が参照できるよう備えている．これらのプログラムはネットワーク機器が正常に動作しているかどうかのチェックも兼ねており，障害発生から短時間で異常を検出することが可能である．

4.3　不正利用端末の検出

誤った設定が行われた機器をネットワークに接続した際には，他の接続機器のネットワーク利用を侵害する等の障害が発生する．このような不正利用に備えるために，我々は定期的にネットワーク機器の FDB や ARP テーブルを query し，登録データとの整合性をチェックしている[3]．

利用者からの障害報告が行われた場合の手順は次の通りである．

1. 障害内容の聞き取り．
2. 該当 MAC address の決定．IP address で報告が行われた際には，ARP table の検索を行い MAC address を決定する．
3. 該当 MAC address がデータベースに登録されているかの検索．見つかった場合，登録されている申請者に通知し対応を行うように求める．
4. 見つからなかった場合，データベースに登録されている学内の全ての L2 スイッチの FDB を query し，出現ポートを決定する．判明した出現ポートは，データベースを用いて部屋名に変換することが可能であるので電話もしくは現場調査により対応を行う．連絡が取れない等，時間がかかる場合は該当ポートを不活性にすることにより対応する．

この手順は，単純ではあるが面倒な操作であるため，IP address, hostname, もしくは MAC address を引数にとり，一連の操作を行った上でその時点での出現ポートもしくは端子番号や部屋名を表示するようなプログラムを用意している．これにより，ネットワーク構成等を把握していない職員であっても，問題となっている端末の設置場所が特定でき，対応が可能となった．

[3] 現在は，不整合が発見された段階での利用者への通知は行っていない．

4.4 端末管理への利用

情報処理センターが学生を含む学内利用者に解放している端末や，医療情報部が管理している病院端末は台数も多く，設置場所が分散している．特に病院端末については，故障が発生した際にセンター職員以外による端末交換等が行われるため，備品管理は非常に困難である．

我々は，備品番号と MAC address の対応をあらかじめ調べておき，前述の不正利用端末を検出する方法を用いて，ネットワーク上から該当の物品の設置場所を割り出す方法を取っている．なお，必要時に電源が切られていた場合であっても，記録されている MAC address を用いて，WOL パケットを送付することにより，設置場所を問わずネットワークに接続されていれば電源を入れることが可能である．

5 運用上の問題

本学で，本システムの運用を開始してからすでに 2 年が経過しており，この間に行われた申請は 2000 件を数えているが大きなトラブルは発生していない．しかしながら，いくつか問題点が確認されているのでそれぞれについて議論を行う．

5.1 Virutal host に対応していないブラウザによる申請

ユーザに対するインタフェースである WWW サーバは負荷分散や保守作業等による停止時間を短縮するために，2 台のマシンを利用しそれぞれのホストで apache の機能である virtual host を用いて実現している．

運用を開始した直後，非常に古いブラウザを利用しているユーザから該当 URL が見当たらないという報告があった．調査の結果，HTTP リクエストに hostname が含まれておらず，virtual host を用いた運用が原因であることが判明した．これには，該当ホストの本来のトップページに virtual host で参照できる領域をしめす link を付け加えることにより対応を行った．

また，このようなブラウザの利用者であっても問題なく申請が行えるように CGI から出力する HTML は HTML 2.0 しか理解しないようなブラウザやでも問題なく処理できるようなタグのみを用いるようにしている [7].

5.2 離学した申請者

利用者の多くは，接続時には必要に迫られて申請を行うが，退職，転勤等により本学を去る際には廃止もしくは変更申請を行わないことが多い．このような機器は必要な際に連絡する担当者が存在しないこととなり支障をきたす．この問題に対応するために我々は各部局に全端末の接続に対して責任を負う運用責任者を設置することとした．設置した運用責任者からなるメーリングリストも設置し，ネットワーク運用上の連絡等を行うとともに定期的に連絡が取れることも確認している．

5.3 日々増加する不整合

従来，情報処理センターはユーザは自主的に必要な申請は行うものと期待していたが，整合性チェックの結果を見る限り，多くの利用者は申請を行う事なく端末の移動や機器交換を行うことが明らかとなった．その数は徐々に増え続け，2 年間で登録台数の 10%を越えるまでになった．このうち，他の機器のネットワーク利用に対して障害を引き起こした不正利用については個別に対応を行ったが，機器 (NIC) 交換に起因すると考えられる不整合についてはセンター職員の負担増となるため行っていない．

そのため，利用者からの問い合わせや障害発生時にデータベースを参照するだけでなく，現状の利用状況の調査を行う必要が発生している．

これに対応するために，利用者に対して登録データを正確に維持することがネットワーク管理上重要である事を周知/教育した上で，不整合が発生した段階で通知する機能を追加することを検討中である．

5.4 プログラムの更新・保守

始めに述べたように，情報処理センター職員の負担は大きく新たに作成した当システムの更新保守作業を行える人的資源は非常に限られている．このため，バグが発見されたときや，利用規程の変更に伴う改変，負担軽減のための機能追加等を行う際に，開発・テスト作業がなかなか進まず，本来の目的を達成できていない面も存在する．

5.5 古いネットワーク機器の管理

IP に対応しているネットワーク機器については 4.2 で述べたように管理が行われているが，学内ネットワーク上にはまだ IP に対応していない管理ハブが存在している．これらについてはヘルスチェックも行えず，また障害発生時の切り分けも困難となっている．これらについては IP に対応している intelligent ハブの価格が下がっていることもあるので，順次置き換えていく予定である．

6 今後の課題

現在，我々は有線系の学内ネットワークに加えて，無線接続の提供の準備を進めている．有線接続と異なり，無線接続の場合は端子情報が存在しないため申請や，不正利用端末の探索機能等への修正が必要であると考えられ，現在運用方法の検討およびプログラムの作成中である．

また，現在運用中の学内ネットワーク監視システム [8] との連携を行うことにより，障害発生時の状況確認や対応等に利用できるよう拡張を行っていきたいと考えている．

参考文献

[1] RFC 1033: DOMAIN ADMINISTRATORS OPERATION GUIDE

[2] RFC 1034: DOMAIN NAMES - CONCEPTS AND FACILITIES

[3] RFC 1035: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION

[4] RFC 1123: Requirements for Internet Hosts -- Application and Support

[5] RFC 1178: Choosing a Name for Your Computer

[6] RFC 1912: Common DNS Operational and Configuration Errors

[7] http://www.w3.org/MarkUp/html-spec/

[8] 大垣内 多徳，山下 芳範，高岡 宏光「マイクロサーバを利用した学内ネットワーク監視システムの構築」，情報処理学会研究会報告 2002-DSM-28 pp43-48 (2002).