

# ネットワークグループ活動報告2002

山本好弘 (工学部 技術部 第二系第四班)

## はじめに

事務部ネーム、メールサーバの管理から始まった工学部技術部ネットワークグループ(以下ネットワークグループと称す)の活動も4年目を迎えることとなった。代換、新規サーバの構築、就職情報室の立ち上げなど、この3年間で活動の範囲は拡大しつつある。また、これまでの活動内容については工学部技術発表会(2000、2001年度)にて行われているが、今回は過去1年間(2001年11月-2002年10月)に新たに行われた活動と通常行っている活動について報告を行う。

## ネットワークグループ設立の経緯

ネットワークグループは工学部から技術部に対し依頼のあった共通業務を行うため、平成11年8月に発足した。現在、技術部の有志5名により活動している。

## ネットワークグループの活動範囲

ネットワークグループの業務対象となる情報機器の設置場所は事務棟内の工学部事務部、サーバ管理室と講義棟内の就職情報室の3箇所となっている。

また、業務形態としてネットワークグループが運用・管理を直接行うものとその都度依頼を受けて間接的に行うものに分けることができる。直接行うものとしてはサーバ管理室、就職情報室のサーバ、クライアントPCの運用・管理などがあり、間接的に行うものとしては工学部事務部からの依頼(PC、プリンタ等のセットアップ、ウイルス対策など)などがある(これ以降事務部からの依頼業務をヘルプデスクと呼ぶ)。

ネットワークグループが直接または間接的に管理を行っている主な情報機器(サーバ、PC等)を図1に示す。なお、現在の情報機器の台数は以下に示す。

- ・工学部サーバ管理室(計6台)
  - 工学部 Web サーバ(1台)
  - 事務部メール、ネームサーバ(1台)
  - 技術部 Web サーバ(1台)

- バックアップ・リプレース機(2台)
- 作業用PC(1台)
- ・就職情報室(計10台)
  - ファイアーウォール(1台)
  - クライアントPC(8台)
  - バックアップ・リプレース機(1台)
- ・工学部事務部(多数)
  - クライアントPC(多数)
  - プリンタ等(複数台)

なお、今回新たにPC2台(サーバ管理室、就職情報室各1台)が追加された。

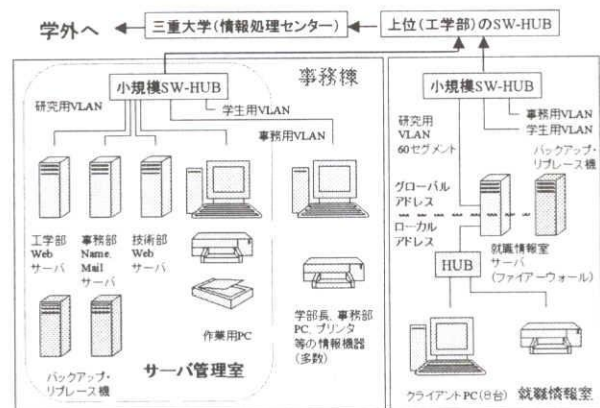


図1 主な管理対象機器の構成

## ネットワークグループの主な業務内容

主な管理対象機器に関する主な業務を表1に示すとともに、その内容を簡単に紹介する。

まず、直接管理下の機器に対する主な業務内容を示す。

### ○サーバの管理・運用

正常な常時稼動を行うためにセキュリティの確保やハードウェアの監視等を常時行っている。以下に主なものを示す。

- ・セキュリティホールへの対応
- ・ログ等の監視
- ・データ、ログのバックアップ

また、その他に各サーバが提供するサービスに関連する設定等の作業がある。これまではメールを受信する時のみ、大学のメールゲートウェイサーバを通過するように設定されていたが、今回

は送信する際にもメールゲートウェイを通過させるように大学のシステムが変更された。従ってメールサーバの設定をシステムに合わせて変更を行った。

#### ○クライアント PC の管理

クライアント PC についても正常な常時稼働を行うためにセキュリティの確保やハードウェアの監視等を常時行っている。以下に主なものを示す。

- ・セキュリティホールへの対応
- ・ウイルスへ対策

#### ○サーバのバックアップ、リプレース機の構築

常時稼働が必要なサーバが何らかの障害（故障、クラッキングなど）により運用が続けられない状況が発生した場合に対応するため、常にバックアップ機を用意している。

また、新しい技術の導入やベンダーのサポート停止への対応などのため、OS やアプリケーションのアップデートをある程度定期的（OS のメジャーバージョンアップ時を目安）に行うようにしている。その際予備の PC でサーバの構築を行い、安定動作が確認された時点で置き換えを行うようにしており、このような予備の PC をリプレース機と呼んでいる。

今回行った各サーバのリプレースは次の通りであり、変更を行った OS 及びアプリケーションも合わせて示す。

- ・工学部メール、ネームサーバ  
TurboLinux Server 2 → 6.5
- ・就職情報室ファイアーウォール（サーバ）  
RedHatLinux 6.1 → TurboLinux 7 Server  
DeleGate → Squid
- ・技術部 Web サーバ  
TurboLinux Server 6.5 → 7

なお、現時点ではバックアップ、リプレース機を各サーバ毎に用意できるだけの台数が不足しているため兼用にて対応している。

#### ○ホームページの管理

工学部 Web サーバにて公開している工学部ホームページの記載内容の更新・追加等の作業を行っている。これまで、記載内容の更新については（工学部広報委員会の合意の下に）、可能な範囲で自主的に行っていたが、今年度からは工学部広報委員会との話し合いにより、手続きが定められた（工学部ホームページにて公開）。

また、工学部ホームページの他に技術部のホームページ技術部 Web サーバ上で公開しており、この記載内容の更新・追加等も行っている。

#### ○メール、ネームサービスに関連

メール、ネームサーバが提供しているサービスに関連する業務内容について示す。

- ・メールアカウントの管理
- ・メーリングリストの管理
- ・ドメイン名の管理

最後に間接的に行っているヘルプデスクに関するおもな業務内容を紹介する。事務部からの業務依頼や相談等に対する対応を行っている。主な依頼内容等を下記に示す。

- ・情報機器（PC、プリンタ等）のセットアップ
  - ・ウイルス等に関する依頼、相談
  - ・ソフトウェアの操作、動作に関する相談
- また、依頼等に対する対応だけでなく、提案等も行っている。

表 1 主な業務内容と対象機器

主な対象機器	主な業務内容		
工学部Webサーバ	サーバ管理	工学部ホームページのコンテンツ管理	サーバの更新 予備機の準備
工学部事務部 Name, Mailサーバ	サーバ管理	メールアカウントの発行 IPアドレスの登録	サーバの更新 予備機の準備
作業用PC	PC管理		
技術部Webサーバ	サーバ管理	技術部ホームページの コンテンツ管理	
就職情報室サーバ	サーバ管理		サーバの更新 予備機の準備
クライアントPC	PC管理		
工学部事務部 情報機器	ヘルプデスク (PC、プリンタ等のセットアップ、ウイルス対策、相談など)		

### ネットワークグループ独自の活動

ネットワークグループでは、依頼業務の他にグループ独自の活動も行っている。

新たなサービスやアプリケーションの導入に向けての試験的運用やアプリケーションの改良・開発等を行っている。また、これらの成果や依頼業務を行って行く上で蓄積された成果の還元として、技術講習会の開催、技術研究会等への報告（発表）などを行っている。以下に今回の新たに行った講習会、報告等の活動を示す。

- ・技術講習会の開催  
「グループウェア — 機能、運用事例の紹介と導入の提案 —」、2002年9月27日（金）、13時～15時
- ・技術研究会への参加

「Web データアプリケーションによるグループウェアの開発」、平成 13 年度核融合科学研究所技術研究会、2002 年 3 月 14 日・15 日

- ・産学官研究交流フォーラムへの参加  
「グループウェアの構築・運用紹介」、産学官研究交流フォーラム・オン・キャンパス 2002、平成 14 年 3 月 9 日
- ・広報誌への投稿  
「グループウェアの構築・運用紹介」、三重大学情報処理センター広報 Vol. 12 (2002. 3)

表 2 役割分担

担当者	主な役割	
中村(勝)	工学部 Web サーバ	広報委員会(オブザーバ)
伊藤	事務部 Name、Mail サーバ	環境委員会のネットワーク WG
山本(好)	作業用 PC	報告・研修
	技術部 Web サーバ	
平山	就職情報室全般	広報
新美	工学部 事務部 全般	予算管理

### 業務の役割分担

以前からもある程度の担当範囲を決めて活動を行って来たが、今回からはある程度分担と責任を明確に行うようにした。ただし、担当者が技術的な問題や作業量の増大などにより対応できない場合は、これまで通り全員で協力して行っている。

表 2 に主な役割分担を示す。役割は依頼業務の他にネットワークグループ独自の活動に対しても役割を分担している。主な役割として、委員会や委員会のワーキンググループへの参加、成果報告の取りまとめや予算管理などがある。

また、就職情報誌室のクライアント PC に関しては、ネットワークグループ全員で管理を分担しており、対応が行えない場合は就職情報室の担当者が対応することとしている。

なお、各サーバが提供しているサービスに係わる業務はそのサーバの担当者が行う。例として Web サーバに対するホームページコンテンツ管理やメールサーバに対するアカウント管理がこれにあたる。

### サーバの管理・運用業務についての実際

現在、日常の業務でインターネットサーバが提供するサービス（特にメールサービス）を当たり前のよう利用している。また、これらのサービ

スが利用できなければ業務に支障が生じるまでになってきており、各サーバの常時稼働が求められる。従ってネットワークグループの依頼業務の中で各サーバの管理・運用は重要な位置を占めている。

サーバの常時稼働を妨げる要因として、

- ・ハードウェア故障・誤動作、ソフトウェアの不具合
  - ・クラッキング等による不正アクセス、コンピュータウイルスの感染による動作不良
- などが考えられる。特にクラッキング行為はサーバの常時稼働の妨げになる他に、
- ・他のサーバ等への攻撃の中継に利用
  - ・ホームページの書き換えなどによる非社会的メッセージの発信
  - ・サーバ内の情報の流出

などの重大な損失を招く恐れがある。

従って日常のサーバの管理・運用に関して以下の様な対応を行っている。

#### ○セキュリティホールへの対応

クラッキングの対象となりやすいのが、ソフトウェアのセキュリティホールである。セキュリティホールが発見されると対応策のアナウンスや対策済みのソフトウェアの提供が行われるので、常に関連するサイト(OSベンダーや情報の提供を行っているサイト)を常時監視し、アナウンスがあったなら直ちにソフトウェアのアップデートを行うなどの対応を行うようにしている。

技術部 Web サーバにおけるセキュリティ関連のアップデートの件数は以下の通りである。

システム：TurboLinux 7 Server

期間：2001 年 12 月 7 日(OS リリース) ～ 2002 年 10 月 31 日

セキュリティアナウンス：66 件

アップデート対象のセキュリティ：48 件

なお、セキュリティアナウンスの件数とアップデート対象件数に差があるのはサービス提供する際に使用するアプリケーションの有無によるものである。

#### ○ログの監視

OS や各サービスからのメッセージ(ログ)を常時監視することにより、サーバの動作状況やクラッキング情報を得ることができ、これらの得られた情報を元に素早い対応をとることができる。

通常のログ収集デーモン syslog 以外にもネッ

トワークのポートを監視しログとして記録できるツール(iplog などの導入を行っている。また、ログの内容を1時間毎にメールで配信するスクリプトを cron デーモンを用いて実現している。これによりその都度サーバにアクセスしてログの内容を見ることなく、メールを読むことにより各サーバの状況を監視することができる。

これまでログに記録された主なサービスへの不正アクセスを以下に示す。なお、今回のデータは工学部 Web サーバのものであり、2001年11月1日から2002年10月31日に記録されたものである。アクセス数の内訳をみると公開されているサービスの多さとサービスアプリケーションの機能上の攻撃への脆弱性に比例しているように感じられる。セキュリティの問題が重要視されるようになって、telnet から SSH への切替が行われつつあり、両者のアクセス数に実状が反映されている。

表2 各サービスへの不正アクセス数

サービス名	ftp	SSH	telnet	SSL	その他	合計
ポート番号	21	22	23	443		
アクセス数	240	73	11	38	69	431

なお、三重大学では学外へサービスを公開するサーバは情報処理センターへ登録することとなっている。これにより学外からの不正アクセスの対象となるサーバに限られる(登録したサーバのみ)。

#### ○データ、ログ等のバックアップ

サーバ停止状態からの速やかな復旧を行うためにもホームページのコンテンツやメールボックスの内容等のデータを常時バックアップを行う必要がある。自動バックアップを定期的に行うために、バックアップスクリプトを作製し cron を用いて行っている。また、スクリプト処理ができないデータについては、定期的に手動でバックアップを行っている。

#### まとめ

今回(1年間)も特に大きな障害も無く依頼業務を行うことが出来た。

なお、通常の依頼業務の対応やネットワークグループの活動に他に、今回新たに行われたことを以下に示す。

- ・サーバ管理室、就職情報室に各1台、計2台のPCを新規に導入
- ・学内のメール配信システムの変更に伴うメールサーバの設定変更
- ・ホームページコンテンツの変更・追加等に関する依頼方法の確立
- ・技術講習会の開催(工学部技術部)
- ・技術研究会への参加(核融合科学研究所)
- ・産学官研究交流フォーラムへの参加(三重大学)
- ・広報誌への投稿(三重大学情報処理センター)

#### 今後の予定

現在進行中の作業や新たに計画したものを以下に示す。

#### ○バックアップ・リプレース機の構築

工学部 Web サーバのリプレース機の構築を行っている。次期サーバの OS として TurboLinux 8 server を導入(現行機は TurboLinux Server 6.1)した。

#### ○バックアップシステムの検証

各サーバのデータ(ホームページやメールボックス等)やログ等の喪失(ハードディスクのクラッシュ等による)を防ぐために、ハードウェアミラーリング(RAID 1)ユニットの導入を行い、動作検証等を行っている。導入は事務部メール、ネームサーバから順次行っていく予定である。

#### ○技術研究会への参加

「Web 技術を用いた技術部業務運用・管理システムの紹介」のタイトルで、平成 14 年度東京大学総合技術研究会(平成 15 年 3 月 6, 7 日開催)への参加(口頭発表、ポスター発表各 1 件)を準備している。

#### ○新たな管理体制の再構築

ネットワークに接続された情報機器に関する様々な規程を定めた「三重大学情報セキュリティポリシー」が来年度から実施予定となっており、ネットワークグループとしてもこれに則した情報機器やコンテンツの管理体制の再構築が必要となってくる。なお、現在対応を検討中である。