

情報処理通信センター（聴覚部）における新サーバシステム

筑波技術短期大学 情報処理通信センター（聴覚部）¹⁾、情報処理通信センター長²⁾

浅草 肇¹⁾ 西岡知之¹⁾ 清水 豊²⁾

要旨： 本学聴覚部ネットワークにおける新サーバシステムの設計・開発指針を説明し、各サーバの設定運用状況を紹介する。

キーワード： ネットワーク サーバ 設計指針 設定 運用

1. はじめに

平成12年度教育改善推進経費、及び、平成12年度情報処理通信センター運営経費の一部を充当して、情報処理通信センター（聴覚部）ネットワークサービスの基盤設備である、サーバシステムを一新した。平成13年1月から順次、新システムへの移行作業を開始し、平成13年5月に切り替え作業が終了し、正式運用を開始したので報告する。

2. 新システムの設計

2. 1 旧システム

旧来のサーバシステムは、主に学外との通信を制御するサーバ（旧名：leo）と主に学内の通信を制御するサーバ（旧名：sirius）の2台体制であった。

このため、どちらのサーバが運用停止となっても、学内及び学外との通信が途絶する状態であった。実際、平成11年には、leoのハードディスクの不具合により自動起動が不可となり、約半日間学外との通信が途絶した。また、平成12年11月には、電源部の故障により33時間leoが停止し、学外への情報発信に支障を来した。

2. 2 設計指針

新システムの設計に際しては、サーバの停止に伴う学内外間の通信途絶が起こらないこと。また、折からの不正アクセス問題に対処できること。などを念頭に置き以下のような基本方針を策定した。

- (A) 安全性の向上
- (B) 安定性の向上
- (C) 保守性の向上

2. 3 機種選定

機種の選定にあたっては、保守性の向上を図るために、故障時に部品交換が短時間で、かつ、容易にできるようにハードウェア互換性の向上を最優先に考慮し、さらに、費用対効果を考慮して、PCサーバを採用した。さらに、OSの軽量化・高速化を考慮した結果、OSとしてはlinuxを採用した。

2. 4 安全性の向上

安全性の向上の観点からは、頑強なファイアーウォールを築くためと、さらに、『新高速ネットワーク』の導入を円滑に行うために、ファイアーウォールを構成するルータとサーバ機のためのセグメントを新たに設置した。これにより、学内向けのサービスを行うサーバ機群とファイアーウォールとを明確に分離できた。また、安全性の観点からのみではなく、保守性ならびに安全性も大きく向上した。

学内外間を接続するサービス（ファイアーウォール）は、表1に示すものだけを、proxyサーバによる接続とした。安全性に疑義のあるサービス、不要なサービスは停止した。特にtelnetサービスについては、学内から学外への一方のみとし、学外から学内へのtelnetサービスは禁止した。この他、利用者の端末機、サーバ機が直接学外と通信できないことを原則とした。

表1 学内外接続サービス一覧

学内外接続サービス	方向
http : 80	学内 ↔ 学外
ftp : 21	学内 ↔ 学外
telnet : 23	学内 → 学外
pop : 110	学内 ↔ 学外

このように、学外との通信はproxyサーバで一元管理するとともに、常時、これらの通信量の監視を行うサーバを設置し、異常事態の早期発見が可能となるように計画した。また、サーバ機に不正アクセスがあった場合に備えて、全サーバ機のアクセス記録の保存もこの監視用サーバ機で行うことにした。

2. 5 安定性の向上

故障を前提に、学内外接続用サーバ機、学内向けのサービスを行うサーバ機ともに、ハードウェアおよびソフトウェア両面からの二重化を図った。

安全性に問題がないサービスの場合は、常時、並列運用を行い、障害が発生した場合、自動的に障害のないサ

サーバ機だけの運用で対処できるように計画した。

並列運用を行ったときに安全性に問題があるサービスの場合については、障害発生時に、手動による切り替え作業が迅速に行えるように計画した。

これらのことから、学内外接続用サーバ機、学内向けサーバ機ともに、それぞれ、同じハードウェア仕様で、ソフトウェア設定を同じにしたサーバ機を2台ずつ合計4台用意することにした。

停電時対策として、これを検知し、自動的にかつ確実にサーバの運用を停止させることを目的として、必要最小容量のUPS（無停電装置）を各サーバに1台ずつ設置することにした。これまでの給電状況を分析した結果、数分以上の停電は先ずあり得ず、それ以上の停電は工事などの長時間に及ぶものであることから、10分以内の停電に対してはUPSによる運用を継続するが、10分を経過した後は速やかに運用を停止することを運用方針とした。これは、ハードディスクシステムの保護を最優先としたためであり、さらに、10分以上の停電状態では一般利用者もいないであろうと予測したからである。なお、雷雨時などの電圧変動時にも安定して給電できるように、常時インバータ給電方式のUPSとした。

2. 6 保守性の向上

新サーバシステムでは、サーバ機数が増加したため、ホスト名もその役割に応じて機械的に割り付けた名前と呼称することに改めた。

さらに、各サーバで実行される一般利用者へ供する各種サービスについては、可能な限り、「機能名」として別名を割り付けた。一般利用者が、各種サービスを利用するときには、ホスト名ではなく、「機能名」を指定することになる。

この「機能名」の採用により、将来、各種サービスを実行するサーバ機を変更するなどのシステム変更を行った場合でも、情報処理通信センターのDNSサービスのデータ変更を行うだけで、一般利用者のパソコン設定を変更する必要はない。また、この「機能名」を別のサーバ機に変更する手法は、各サーバの障害時に、当該サービスを別のサーバに移し替える際にも利用でき、保守性の向上にも寄与する。

さらに、情報処理通信センターにおいてDHCP（Dynamic Host Configuration Protocol）サービスを開始し、一般ユーザがこのDHCPを利用するようにパソコンの設定を行えば、情報処理通信センター側のシステム構成の変更にも自動的に追従するようになり、情報処理通信センターにとっては保守性の向上に、一般ユーザにとっては利便性の向上になる。

3. サーバ機一覧

情報処理通信センター（聴覚部）が、管理するサーバ機は、学内外接続用サーバ（ホスト名：ns系）として2台、学内向けサーバ（ホスト名：mail系）として2台、監視用サーバとして1台、以上5台が新設機である。この他に、旧システムで運用していたサーバ機（旧名：leo, sirius）を広報委員会運営の本学ホームページ運用機（ホスト名：web系）として再構築した。総計7台体制でネットワークサービスを提供している。写真1にこの7台を示す。上段が再構築した本学ホームページ運用機（2台）、下段が新設機（5台）である。

以下に、各サーバの仕様とサービス内容（平成13年5月末現在の状況。その後、新高速ネットワークの導入により若干の変更が加えられた。）を示す。監視用サーバについては省略する。

3. 1 学内外接続用サーバ（ns系）

仕様： Pentium III 700 MHz×2, RAM 1GB, HDD 36GB

ns系は、学内と学外との通信を中継する唯一のサーバ機であるため、高速な処理が要求される。このためdual CPU構成とし、さらに、メインメモリーも1Gbytesとし、高速処理が可能になるようにした。運用実績を解析すると、メインメモリーには若干の未使用領域が残っており、ハードディスクのキャッシュメモリーはほとんど使用されていないことから、学内外接続サービスはメインメモリー上で高速に処理されていると推測され、CPU及びメインメモリーを補強した効果は十分に発揮されている。

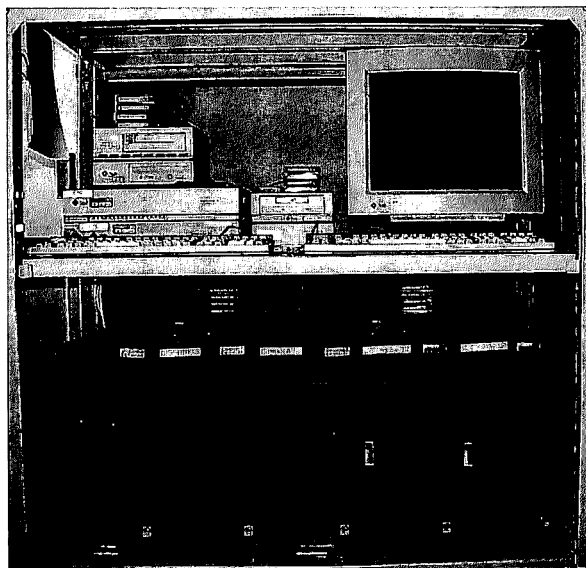


写真1 全サーバ機

- (a) 学内外接続用サーバ A : ホスト名 ns1
- ・学外向けDNSサービス (主)
 - ・学内外間電子メール中継サービス (主)
 - ・フォワードプロキシサービス (副)
 - ・リバースプロキシサービス (hot standby)
 - ・学内外接続サービス (hot standby)
- (b) 学内外接続用サーバ B : ホスト名 ns2
- ・学外向けDNSサービス (副)
 - ・学内外間電子メール中継サービス(副)
 - ・フォワードプロキシサービス (主)
 - ・リバースプロキシサービス
- 機能名 : www.tsukuba-tech.ac.jp
- ・学内外接続サービス
- 機能名 : gw.a.tsukuba-tech.ac.jp

ns1は主として、DNSサービスと学内外間の電子メールの送受信中継サービスを行う。

ns2は主として、プロキシサービスと学内外接続サービスを行う。

フォワードプロキシサービスは学内から学外へのhttp接続要求を中継するサービスであり、学内利用者には、自動設定により、このサービスを利用することを推奨している。

リバースプロキシサービスは、学外からのhttp://www.tsukuba-tech.ac.jp/ に対する接続要求を学内の各webサーバに中継するサービスであり、最も不正アクセスの危険性が高いサービスである。したがって、学外から不正アクセスがあった際に発見・対策が容易になるようにns1/ns2の並列運用とはせず、正常運用時にはサービスをns2で一元管理し、ns1をhot standby状態に設定している。ns2不具合時には手動操作でns1に切り替える。

学内外接続サービスは、表1のftp, telnet, pop の各接続要求を処理する。このサービスも不正アクセスを考慮してns1/ns2の並列運用とはせず、ns1をhot standby状態に設定し、ns2不具合時には手動操作でns1に切り替える。

学外向けDNSサービスとしては、学外と通信を行う必要のあるホストの情報と電子メールの受信に必要な情報だけを送出しており、学内の情報はできる限り学外に出さない方針である。

3. 2 学内向けサーバ (mail系)

仕様 : Pentium III 700MHz, RAM 512MB, HDD 36GB

mail系は、ns系に比較して、高速のリアルタイム処理能力は要求されないが、学内ネットワークサービスの中核をなす重要なサーバ機である。このため、並列運用を

行い、障害発生時にも、一般利用者には障害が検知されないようなシステム設計とした。

- (c) 学内向けサーバ A : ホスト名 mailA
- ・学内向けDNSサービス (主)
 - ・学内メール配送サービス (主) smtp受付
 - ・ntpサービス
- 機能名 : ntp.a.tsukuba-tech.ac.jp
- ・情報処理通信センターwebサービス
- 機能名 : wwwi.a.tsukuba-tech.ac.jp
- ・自動proxy 設定配布
- http://wwwi.a.tsukuba-tech.ac.jp/proxy.pac
- (d) 学内向けサーバ B : ホスト名 mailB
- ・学内向けDNSサービス (副)
 - ・学内メール配送サービス (副) smtp受付
 - ・ntpサービス
- 機能名 : ntp.a.tsukuba-tech.ac.jp
- ・net news サービス
- 機能名 : news.a.tsukuba-tech.ac.jp : 119

mailAは主として、DNSサービスとメール配送サービスを行う。また、情報処理通信センターの全学情報と聴覚部向け情報のwebサービスを行う。なお、当webサービス内でwebブラウザに対する自動proxy 設定情報を配布している。この利用方法の詳細も当webサービスで提供・配布されている。

mailBは主として、internet newsサービスを行っている。しかし、DNSサービスとメール配送サービスについては、補機の役割を常時果たしており、mailAに障害が発生したときには自動的にこれらのサービスを代行するように設定されている。

ntp (Network Time Protocol) サービスは、mailA、mailB双方が同期して動作するように設定され、どちらを参照しても同程度の無視できる程度の誤差になっている。なお、平成13年度の新高速ネットワーク導入後、この機能名は別のntpサーバに移されたが、ntpサービス自体は継続している。

3. 3 webサーバ (web系)

web系は、広報委員会がホームページを運用するサーバ機として、旧システムのサーバ機を再構築し、新設サーバ機と同程度の安全性と安定性を確保した。

- (e) 学外向けWebサーバ : ホスト名 web1
- RAM 352MB, HDD 9GB
- 機能名 : www.tsukuba-tech.ac.jp

(f) 学内向けWebサーバ：ホスト名 webA
RAM 224MB, HDD 2+2+4GB
機能名：web1.a.tsukuba-tech.ac.jp

web1は、学外から閲覧できるホームページの運用が

できる設定になっている。
webAは、学内からは自由に閲覧できるが、学外からは一切閲覧できない設定となっている。
安全性を確保するために、webAはもちろんweb1も、学外とは直接通信できない設定になっている。

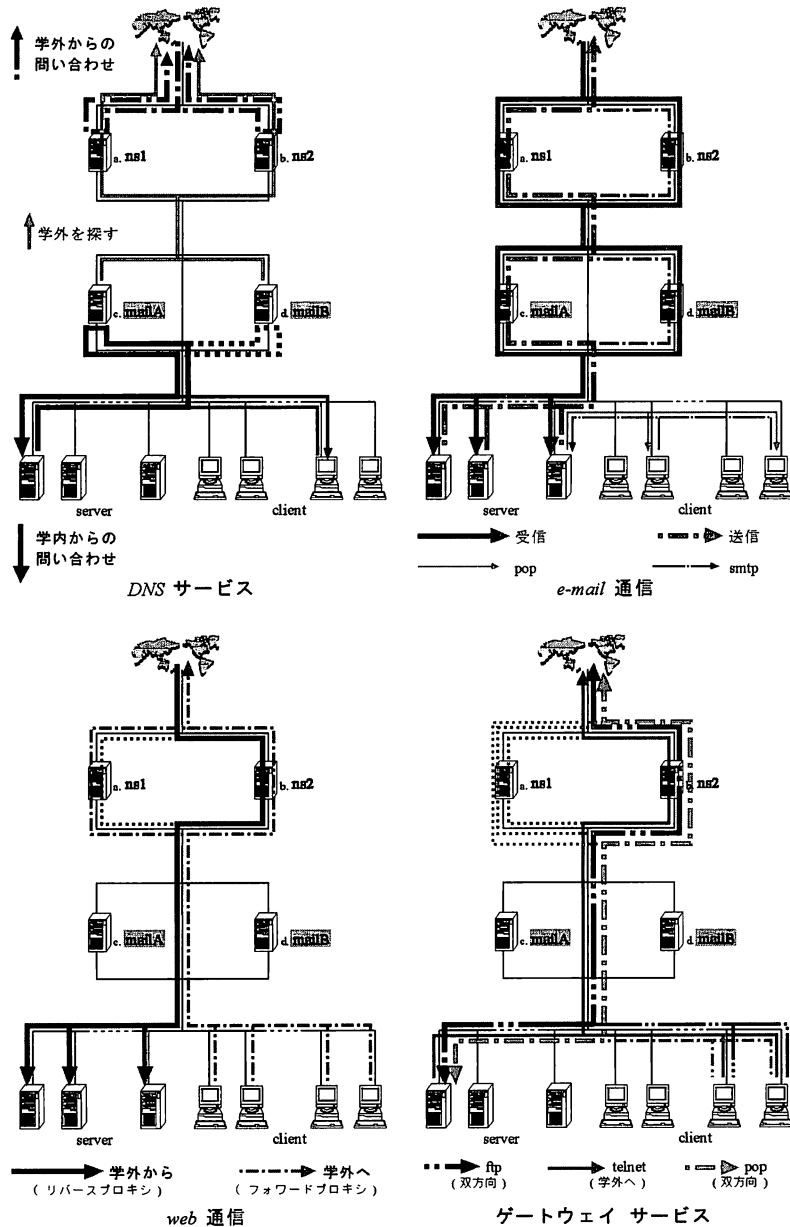


図1 通信データの流れ

4. 通信データの流れ

通信データの流れ方の概略を図1に示す。学内外間の通信は必ずns1/ns2を経由する。

DNSでは、学外からの問い合わせには、ns1/ns2が応答し、学内の端末機及び学科サーバからの問い合わせには、mailA/mailBが応答するが、学外の情報について

は、ns1/ns2を経由して問い合わせることになる。つまり、mailA/mailBは全世界のDNS情報を回答できるのに対して、ns1/ns2は全世界の情報から学内の情報が抜け落ちた情報しか回答できない。

電子メールの配送は全てのメールが一度mail系に集められ、ここから、学外向けメールはns系に送られ、発送

される。学内向けメールは各学科サーバに送られる。学外からのメールもns系で受信された後、mail系に集められ同様の処理がなされる。

このような意味において、mail系のサーバ機は高速処理の必要はないけれども重要な役割を果たしており、並列運用を行い、機能停止が起こらないようにする必要がある。

5. おわりに

新サーバシステムの構築により、旧サーバに比較して、安定・安全な運用ができるようになった。今後も、安全確保のために制限する必要のあるところ以外は、より一層自由に使用できる、安定した、ネットワークサービスを提供したい。

New Network Server System at the Division for the Hearing Impaired

ASAKUSA Hajime ¹⁾, NISHIOKA Tomoyuki ¹⁾ and SHIMIZU Yutaka ²⁾

¹⁾ Center for Computers and Communication at the Division for the Hearing Impaired

²⁾ Director of Center for Computers and Communication

Abstract : A New network server system at the Division for the Hearing Impaired, Tsukuba College of Technology, was designed and created. This system was constructed from several computers, which are operated by the Linux OS. The assigned functions were the network server as the DNS, the proxy service for the LAN, the mail service, and the news service. A firewall function was also mounted in the system. In addition, the Web service is still working for the Internet and for the LAN at the two workstations.

The constructed system seems to have improved the stability and the maintainability.

Key Words : Network, Server, System, Design, Construct, Function, Service