機動性に配慮した小規模ネットワークの構築経験 −(3) 設計と実装−[1]

4S−7

本庄 利守† 大野 浩之†
† 東京工業大学大学院 情報理工学研究科

1 はじめに

コンピュータネットワークの普及は、小規模な組織でも独自のコンピュータネットワークを構築し運用する傾向を助長した。

小規模な組織のネットワークでは、大規模な組織のネットワークと異なり例えば以下のようなことが望まれる。その小規模な組織が、接続している組織とは異なった運営ポリシーでネットワークを運用したい場合にその組織の運営ポリシーをネットワークに反映させることができるネットワークであることが望まれる。また、組織の構成変更などに伴ってその組織の場所やネットワークの接続先が変更されることがある。このような場合に備えてネットワークの独立性を配慮したネットワークであることが望まれる。さらにそのような組織に所属する人は、外部からそのネットワークを利用することがある。このためモバイル環境からの利用を配慮したネットワークにすることも望まれる。

そこで、筆者らは大学の研究室を対象にして、上記のような要求を満たす小規模ネットワークの設計と実装を行った。本論文ではこの小規模ネットワークの設計と実装について述べる。

2 小規模ネットワークの設計方針

筆者らは、大学の研究室を対象とした小規模ネットワーク(以下 研究室ネットワーク)を設計するに当たって、まず以下のような設計方針を立てた。

- 運用のポリシーを容易に反映できること

  ネットワークの運営ポリシーを反映させやすいネットワークにする必要がある。特にセキュリティーに関する運営ポリシーをいつでも直ちに反映できるネットワークにする必要がある。

- ネットワークの接続先を容易に変更できること

  可能な限り接続先の組織に依存しないネットワークにすることを目指した。このようにすることによりネットワーク自体の独立性を高めることが可能になる。

- 外部からも研究室ネットワークを利用できること

  ラップトップコンピュータなどを利用して外出先から研究室ネットワークにアクセスしたり、自宅から研究室ネットワークにアクセスしたいという要求がある。このため外部から研究室ネットワークを利用することも考慮する必要がある。

- 現行の機器を引続き利用可能にすること

  ネットワークを新しく構築するに当たって、現行の機器を引続き利用可能にすることは重要である。例えば、10BaseT によるネットワークが中心のネットワークに 100BaseT によるネットワークを導入することを考える。この場合には、100BaseT と 10BaseT によるネットワークの双方を利用可能にすることが必要である。

- 安価に作成できること

  ネットワークを新しく構築するに当たって、コストの面を考慮することは重要である。筆者らは、コストの面を考慮してパーソナルコンピュータ(以下 PC) と PC-UNIX を利用したネットワークを作成することにした。

以下では、上記の設計方針に基づいて設計および実装を行ったネットワークの構成、セキュリティ、ネットワークのパフォーマンスについてそれぞれ詳しく述べる。

3 ネットワークの構成

ネットワークの構成を考える上で、特に以下の2点を考慮した。

- 運営のポリシーの1つであるセキュリティを実現しやすい構成にすること
- 100BaseT と 10BaseT によるネットワークの双方を利用できる構成にすること

筆者らは、ネットワークの構成として外部からのアクセスを受けるバリアセグメントとそれ以外である内部ネットワークの2つから構成した。内部ネットワークはさらに 100BaseT と 10BaseT による2つのサブネットから構成した。ネットワークの構成を図1に示す。このような構成にすることにより、上記の2点を満たすことが可能である。

[1] Networks with Mobility for SOHOs - Part.3 Design and Implementation -
Toshimori HONJO, Hiroyuki OHNO. Graduateschool of Information Science and Engineering, Tokyo Institute of Technology.

セキュリティに関する運営ポリシーは、ルータAおよびルータBを利用して反映させる。また、外部からのアクセスがあるDNS, WWW, Mail, Real Audioなどの各種サーバは、バリアセグメント上に配置した。さらに外部から利用するためのログインポート,PPP,ISDNルータなどもバリアセグメント上に配置した。

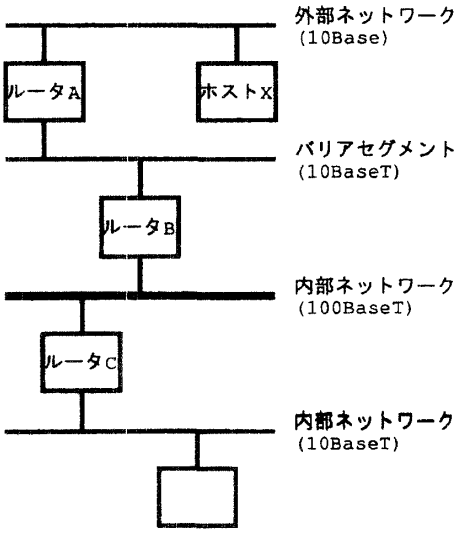

図 1: 研究室内ネットワークの構成

4　セキュリティ

セキュリティを厳重するとネットワークを利用する上で不便な点が多くなる。しかし、セキュリティを考慮していないネットワークでは、危険である。セキュリティに関しては、このような矛盾があり、いかにして運用するかは難しい問題である [1]。筆者らの研究室ではセキュリティレベルを導入して、これらの対処をすることにした。各セキュリティレベルは以下の通りである。

レベル１　スクリーニングおよび監視
レベル２　スクリーニングの強化
レベル３　アプリケーションゲートウェイの利用
レベル４　外部との接続を切り離す

普段はできるだけネットワークを自由に使いたいという要求があるのでレベル１で運用を行い、内部からの利用に関してはできるだけ自由に使えるようにした。監視によって危険だと判断された場合にはレベル２、３、４と順にセキュリティレベルを上げて対処することにした。各セキュリティレベルを即座に実現可能にするために、あらかじめ全ての準備が行なった。

上記のようなセキュリティレベルを実現するために以下のツールを使用した。

パケットフィルタリング	screend v2.5
アプリケーションゲートウェイ	fw-tk v1.3
ファイルの監視	tripwire v1.2
メールサーバ	qmail v1.00
ワンタイムパスワード	logdaemon v5.3
サービスの制限	TCP wrapper v7.4

5　パフォーマンス

PCを中心としたネットワークを構築するに当たって事前にどの程度のパフォーマンスが得られるかを測定した。測定に用いたマシンのスペックはCPUがPentium133MHz Memoryが32MBである。10BaseTのNICには3COM 3C590, 100BaseTのNICにはDEC DE500を使用した。OSには、BSDI Internet Server 2.1を使用した。測定にはttcpを使用した。測定結果は表1である。表中のA,B,C,Xはそれぞれ図1中のルータA, ルータB, ルータC, ホストXを表す。

表 1: パフォーマンス測定結果

X → A	1030 KByte/s
X → A → B	809 KByte/s
X → A → B → C	795 KByte/s
A → B	949 KByte/s
B → C	6380 KByte/s
A → B → C	962 KByte/s

表1から分かるように、現状のネットワークとしては十分なパフォーマンスが得られていることが分かる。

6　おわりに

本論文では、機動性に配慮した小規模ネットワークの構築例として大学の研究室におけるネットワークを構築について述べた。PCとPC-UNIXを用いたネットワークでも小規模な組織におけるネットワークとしては十分なパフォーマンスが得られることが分かった。今後は、さらにネットワークの強化方法や管理方法についてまとめていく予定である。

参考文献

[1] William R. Cheswick and Steven M. Bellovin. *Firewalls and Internet Security*. Addison-Wesley, 1995.