# 〔パネルディスカッション〕イントラネットに明日はあるか

大野 浩之
東京工業大学大学院 情報理工学研究科

**概要**

分散システム運用技術シンポジウム'98 で行われたパネルディスカッション「Intranet の現状と将来」では，壇上の７名のパネラを含む会場の参加者は，イントラネットが抱える問題点を明らかにしていったが，時間制限のために，十分な議論がされたとは言いがたかった．しかし，今後も継続して議論する必要があるという認識が参加者間に芽生えたので，今回の研究会において再度パネルディスカッションを開催し，議論を続けることになった．本稿は，今回のパネルディスカッションの参考資料である．すなわち本稿では，著者が考えるモバイルコンピューティングとイントラネットとの関係，著者の研究室での実践例，今後の展望などが述べられているが，あくまで今回のパネルディスカッションの議論のきっかけを提供することを意図して執筆されている．実際のパネルディスカッションの内容は，本稿をきっかけにして著者の予想をこえた内容になることが期待されている．

# Managemnt and Operation of The Intranet and Its Future

Hiroyuki OHNO
Graduateschool of Information Science and Engineering, Tokyo Institute of Technology.

**abstract**

A panel discussion was held at the last session of the Distributed System Management Symposium '98. All attendees of the session had made discussion about how to manage their intranet better than now. However, the discussion ended without any conclusions because of the limitation of the discussion time. Therefore, we planed another discussion based session at this symposium. This paper has been prepared for the discussion. We introduced the relationship between mobile computing and the intranet, implementation at our laboratory, and future study. They are just introduced for the purpose of providing baseline of the discussion. The actual discussion at this symposium should be succeeded with new conclusion for all intranet system administrators.

## 1　はじめに

「分散システム運用技術シンポジウム'98（1998年２月に開催）」では,「イントラネットの現状と将来」というテーマでパネルディスカッションが行われた．壇上のパネリストは著者を入れて７名[1] で，それまでに積み重ねてきた経験と現在の立場から，それぞれのイントラネットが抱える問題を語った．限られた時間の中で，問題点を整理したり何らかの結論に到達することは当初から予想されたように困難であったが，このようなディスカッションの積み重ねが今後のイントラネットにとって重要であることは参加者が強く認識するところとなった．そこで，上記ディスカッションの続編を今回の研究会において行うことになった．タイトルは「イントラネットに明日はあるか」とし，イントラネット構築運用管理上の問題点を分散システム運用技術の視点からの検討する．パネルディスカッションであるから，壇上で展開される議論の内容は本稿執筆時点では性格には予測できない．したがって本稿の位置づけは，パネルディスカッションにおいて参照される資料であり，著者の研究室ネットワークの現状を提示することで討論のきっかけを提供する役割を担う．当日の討論の内容を詳細に論述した予稿を書くのは不可能であるので，このような執筆形態となった．

[1] パネリストの所属は，富士通，日本電気，ＮＴＴ，野村総研，トヨタ，インテック，東工大 (1 組織 1 名ずつ，順不同)

## 2　イントラネットが抱える問題点

分散システム運用技術シンポジウム'98 のパネルディスカッションでは，登壇者が自らが所属する組織のイントラネットを紹介したあと，会場の聴衆からの発言も交えながらの討論となった．その概要を当時のメモから書き下したのが以下である．書き下すにあたっては，発言のニュアンスを残すよう努力した．ただし記録が不明瞭で書き下すのが困難なものはやむを得ず割愛した．なお以下の記録では発言の順序は保存されている．

- プロバイダを立ち上げた経験から以下を得た.
  - セキュリティの観点からの信頼性の問題や個人認証の問題がある.
  - 管理する側と使う側で利害が違うことがある.
  - どうやって運用管理していくかが明確でない.
- ネットワークを使って便利になる半面セキュリティの問題が解決できていない.
- 運用管理，性能管理の問題が未解決.
- もっと計算機資源を充実させるための資金が欲しい.
- 上の人達はシステムの管理をしたことがないので現場の苦労を理解できない.
- ファイアウォール作っていれば安全なのか.
  - ファイアウォールの外からの攻撃と内部からの攻撃がある.
  - ファイアウォール内からの攻撃事例もある.
  - イントラネットかインターネットかという問題ではなく，すべての他人は信用できないと考えるべきである.
- (組織内で) ネットワークやサービスを作っている (提供している) 人がめざしているイメージが見えない.
- そもそも誰が何を管理すべきなのか？
  - ユーザの意見を誰かがとりまとめる必要があるはず.
  - どの部署の仕事か？ システム部門？
  - ボトムアップ方式だと各部門ごと意見を取りまとめるのが大変．しかしトップダウン方式でうまくゆ保証もない.
- システム管理者は苦労している.
- 上司はシステム管理者が何をやっているのかを知らない.
- 周囲に仕事内容と量を正しく理解してもらう目的に使える数量的な指針が欲しい.

一見してわかるのは，議論にまとまりがないことと，セキュリティ関連の話題に関心が高いことと，当事者の仕事への周囲の無理解に対する「ぼやき」発言が繰り返されていることである.

議論にまとまりがないのは，司会を担当した著者の能力の問題もあるが，イントラネットの定義づけや要求されている仕事の内容，そしてそれに対処するための方法論などが明確になっていないことも影響している．これは好ましい状況ではない.

セキュリティ関連の話題に関心があつまるのは，本研究会の一般の研究発表からしても予想できることで，本研究会の現状をよく反映している．本研究会でのさまざまな研究発表やそれに伴う議論が活発に続けば，技術的問題に関しては事態を好転させることができるだろう．ただしセキュリティ問題は，技術だけでは解決できず，利用者の心構えやマナーなどの問題とも絡むので手放しには安心できない.

3つめの「周囲の無理解」問題は大きな問題である．この問題は，システム管理を副業としてこなしている人々の間でこの 10 数年間常に話題になっている．この間，計算機速度は飛躍的に向上して文字のみのコミュニケーションの時代から動画を自由に扱える時代になった．そしてインターネットは世界規模の情報通信基盤として認知されるに至った．今やネットワークや計算機システムの重要性は疑う余地はない．それにもかかわらず，統計的数値こそないがシステム管理者に対する無理解とそれに対する「ぼやき」が激減したという報告はない．このことはパネルディスカッション中に著者が壇上から聴衆の反応を観察したところ，周囲の無理解問題に共感していることを表情等で表現する者が少なからずいたことからもうかがえる.

周囲の無理解問題を少しでも軽減するには，システム構築と運用にかかる手間とそこで用いられている方法論を明確にするのがよい．ただしここで言う手間や用いられている方法論には線形性がないことを認識しなければならない．よく知られている事実だが，極めて優れた資質と経験をもつ一人のシステム管理者が 1 時間でこなす作業は，資質も経験もないエンジニアを何人投入しても置換できないことがある．なぜなら，現在のシステム構築や運用業務が工業製品の大量生産のような方法論では対処できず，担当者の洞察力と行動力が成果を大きく左右する研究開発業務にむしろ近いためである．したがってシステム構築と運用業務にかかる手間を工数といった線形空間における単一の数値で表現することは少なくとも現状では危険である．このことは現場にいるシステム構築運用担当者には理

解されているが，このことを周囲に伝える理解させる試みはあまり成功していない．この「説得工作」は従来は個人レベルで行われて来たが，この 10 数年間にさしたる進歩がないことから個人レベルでは解決が困難なのは明らかである．この問題については，たとえば本研究会がシステム構築および運用管理担当者に必要な資質と作業内容についての詳細な手順書を開発公表するといった組織だった対応が必要であろう．また後述する「標準ネットワーク」を定義して常に運用管理を行い，ネットワーク間の性能比較が随時可能な体制を作ることも重要である．

## 3 イントラネットとモバイルコンピューティング

組織内のネットワークを構築運用に要する手間を減らしかつ安定に運用させるための方法のひとつに，標準化や規格化を進めそれに準拠したネットワークを構築する方法がある．ネットワークの標準的な運用形態を定義されていて，その形態を実装するための機材と運用に要する手間があらかじめ明確になっていれば，予算や人員の確保を含めたシステムの運用状況は好転する．どのようなネットワークを標準とするかは今後も本研究会で引き続き議論する必要があるが，著者はモバイルコンピューティングが目指す世界とそこで用いられている技法を正しく理解することが重要だと考えている．

残念ながら現在のモバイルコンピューティングに関する議論の大半は「総人数 $N$ 人 $(N > 1)$ の組織 $X$ からその組織に所属する一人 $(x_i, N \geq i \geq 1)$ が所属組織を離れて移動する場合」を想定している．同一組織から $n$ 人 (たとえば $x_1 ... x_n, N > n > 1$ ) が同時に移動した場合には移動者が行動を共にしていても「その組織に所属する一人が所属組織を離れて移動している」状態が独立に $n$ 組あるとみなしている．著者はこれを「狭義モバイルコンピューティング」と呼ぶ．現在のモバイルコンピューティングはこの発想に基づいているため，行動を共にしている同一組織の $n$ 人がそれぞれ独自に携帯電話を使って同一組織に電話をかけてネットワーク接続を行うという効率の悪い対応を強いられている．

もし「総人数 $N$ 人 $(N > 1)$ の組織 $X$ に所属する任意の二人以上が小集団を作り所属組織を離れて同一行動をとっている場合」および「そのような小集団が組織 $X$ 内に複数存在する場合」を前提にネットワークが設計できれば，そこで用いられた設計手法の応用範囲は大きく広がる．たとえばある部署の一部が物理的に離れたオフィスに移った場合などにも簡単に対応できる．加えて異なる組織に所属する小集団同士が連係してあらたな集団を構成する手法まで考慮されていれば，移動先の会合で暫定的な集団を作るといった対応に留まらず，組織の吸収や合併や分割にも柔軟に対応可能である．著者はこれを「本来のモバイルコンピューティング」だと考えている．狭義の (従来の) モバイルコンピューティングを個人のモバイルコンピューティングととらえ，本来のモバイルコンピューティングを組織のモバイルコンピューティングととらえることもできよう．これらの考え方の一部は，仮想ネットワークやアドホックネットワークとして知られており，すでに数多くの研究が進められ一部は商品化されているが，まだ特殊な事例として扱う傾向が残っている．しかし今後あるいは将来の組織のネットワークは，本来のモバイルコンピューティングを前提に設計/構築/運用/管理されなければならない．なお狭義のモバイルコンピューティングは，本来のモバイルコンピューティングの特殊形と位置付けられるので，本来のモバイルコンピューティングが実現すれば狭義のモバイルコンピューティングは問題なくこれに吸収される．

## 4 大野研究室の事例

前章で述べた本来のモバイルコンピューティングの実現方法を検討する目的で，著者の研究室では以前からさまざまな試みを続けている [1]．本稿では，このうち名前空間，セキュリティ，管理機構に焦点をあてる．著者はこれらの分野の研究は，本来のモバイルコンピューティング実現を支援するために必須の研究分野であると考えているが，イントラネット運用管理担当者も，自らの業務の関連分野であるととらえてしばしば興味を持つ分野でもあり，本稿で言及する意義がある．

もちろん著者の研究室で試みているさまざまな手法やそれに基づいて構築されたネットワークは，著者の研究室の事情を強く反映したものである．他組織においては，それぞれのさまざまな事情によって，本稿で述べる手法が容易に受け入れられるものばかりとは限らず，変更が必要であったり場合によっては受け入れがたいものもあろう．しかしすでに述べたように，明確な方針のもとに導入された運用管理手法とそれらを投入して実装したネットワークの実体を明らかにして

おくことは重要である．こうして作られたネットワークは，他のネットワークとの比較の際の基準となる．比較する側のネットワークでは，何をどう設定してどう運用しているのかを基準となるネットワークとの比較で表現できる．このような比較評価手法は，イントラネット同士の性能比較を容易にし今後のイントラネット運用管理にとって重要になると著者は考える．残念ながら現時点では，著者の研究室のネットワークを基準に比較評価せよ主張せざるを得ない．もちろんこれには無理があり暫定措置でなければならない．今後の議論をもとに標準となるネットワークを定義し，これを運用管理することでイントラネットの性能評価が随時可能な体制を作るのがよい．

## 4.1 名前空間の維持

著者の研究室のネットワークは，東京工業大学大学院情報理工学研究科数理・計算科学専攻が運用管理するネットワークの下流に位置するが，研究室の計算機資源だけで独立したネットワークを構成している．およその構成を図1に示す．ファイオウォールとバリアセグメントを有し，10BASE-T と 100BASE-T ネットワークを使った典型的な小規模組織型ネットワークである．

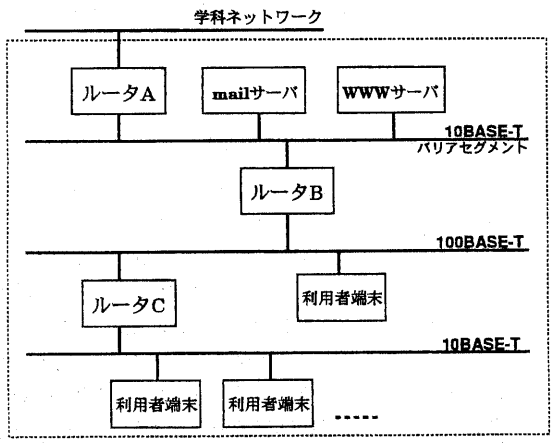


図 1: 著者の研究室のネットワーク構成の概略

著者らはここに専攻が提供する計算機資源に依存しない独立したネットワークを構築するにあたり必要となる事項を洗い出した．ハードウェア資源の面では独立は比較的容易であった．専攻が提供するファイルサーバにあった研究室構成員のホームディレクトリの内容を研究室内のファイルサーバに移し，専攻が提供するファイルシステムに一切依存しないようにするだけで完了した．

問題は名前空間であった．著者の研究室が所属する専攻のドメイン名 is.titech.ac.jp を使用する限り，ホスト名やメールアドレスなど，名前空間にドメイン名が含まれるケースにおいて専攻内の他者と名前の衝突が生じる可能性が常にあり，専攻ないでの調整が必要となる．これでは独立したネットワークとは言えない．また将来著者の研究室は，学内の他専攻や他大学あるいは国内の民間企業や国外に移動(異動)する可能性がある．その際ドメイン名の変更が生じると，移動のたびに全計算機の設定変更や関係者へのアドレス変更通知を行わなくてはならない．現状では移動は多くても年に数回であるが，今後は頻繁に生じる可能性が大きい．そこで著者の研究室用の独立したドメイン名を確保することにし，InterNIC から ohnolab.org ドメインを取得した．gTLD (Generic Top Level Domain) である org ドメインの下に ohnolab.org を設定したのは活動拠点が将来海外に移る可能性を考慮したためである．なお gTLD に関しては，多くの問題が露呈しており，現在多くの議論がなされている最中である．今後の動向に注目したい．

ohnolab.org の取得により，ホスト名，メールアドレスなどにおいて専攻の名前空間とは別の名前空間が確保できたので，名前の衝突はなくなり自由な命名が可能になった．しかし IP アドレス自体は，学内ネットワーク運用部門が著者が所属する専攻に割り当てたサブネット群のいくつかを利用している．したがって，たとえば，www.ohnolab.org を DNS で検索すると，東工大に割り当てられたアドレス空間内の 131.112.40.70 が得られる．このアドレスを正引きしても www.ohnolab.org は得られず，著者が所属する専攻のサブドメイン is.titech.ac.jp を含むホスト名が返ってしまう．また学内のネットワーク管理部門からは，学内のサブネットが titech.ac.jp 以外を名乗ることについて学内のネットワーク運用規則上の制限はないが，学内にどのようなドメインが存在するのかは把握しておきたいので協力するようにという指示が非公式ながら送られてきている．

## 4.2 セキュリティの維持

イントラネットを考える時，セキュリティの維持に関する議論は不可避である．かつてはインターネット

接続を全く行わなければ安全であるとか，電子メールなど限られた通信だけを透過させれば安全であるとか言われた時代もあった．たとえば社内ネットワークに繋がるマシンは一切対外接続させず，社内ネットワークにIP接続しないマシンを1台だけ用意してこのマシンのみインターネット接続性を与えて対外メールの送受を担当させ，社内ネットワークに繋がる社内向けメールサーバはこの対外メールサーバとUUCP接続してメールをやりとりするという実装すら存在した．これは，メールのやりとりは安全だがTCP/IP接続では何がおきるかわからないと考えたからだと思われる．今はこのような極端な例は姿を消したが，ファイアウォールとバリアセグメントで対外接続を制限し，さらにNAT技術を併用するといった手法はしばしば見られる．著者の研究室のネットワークもこのスタイルである．

しかしこの方法は，ないよりはましという程度であることを利用者に意識させる必要がある．ファイアウォールがあっても絶対に侵入不可であると宣言しているわけではない．またいわゆるマクロウィルスの類は，メールが到達できる環境にターゲットとするOSとアプリケーションソフトウェアが動いていればそれだけで問題を起こせる．また組織の規模が大きくなるにつれ，ファイアウォールの内部にいるマシンから侵入などの攻撃を受けることもある．また1年に何度かは必ずインターネット上で話題になるように，デマの類を巧みに使って人心を撹乱させる心理的攻撃が行われると，それが巧みであればあるほど防ぐのは難しい．

よってセキュリティを確保するためには，ファイアウォール構築だけでなく利用者教育が必要である．しかし的確な利用者教育を短期間に達成するカリキュラムを作る研究はほとんどなされていない．至急対処すべき問題の一つである．

### 4.3 システム管理機構の充実

ネットワーク管理をネットワーク上で行うのではネットワークが深刻な障害にみまわれたときに満足な対等ができない，というのが著者らの一環した主張である[2]．しかしシステムが順調に動いている間はネットワーク上でネットワークを管理する機構も順調に稼働するのでこの問題はなかなか真剣に検討されず，障害発生時になると管理者が飛び回る結果となる．システム管理機構に関する研究は，は本研究会でも多数発表されており，それらを整理分類して日常業務に投入可能な状態にまで実装水準を引き上げだれでも利用可能な状態にすれば，それだけでイントラネットの運用管理は大きく進歩すると思われる．しかしそのような活動はなされていない．本研究会で発表された研究およびその関連研究だけでも確実にサーベイすればかなり有用だと思うがそれすら行われていないのが現実である．今後の早急なる検討を要する事項である．

さて著者の研究室では，上記の主張のもとさまざまなネットワーク管理機構を試作運用してきたが，それらの中で最近実装されたのがNIISシステム[3](図2)である．NIISはファイアウォールやルータの設定変更を効率よく実施する機構であり以下の特徴を有する．

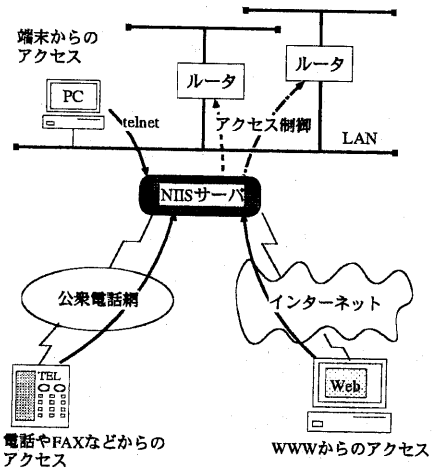


図2: NIISによるルータの一元管理

1. ポリシと呼ばれるルールから，各ファイアウォールやルータの設定変更操作をexpectスクリプト形式で自動生成する．
2. ポリシ作成のためのユーザインタフェースが多種ある．
   - WWW上で使うGCIベースのインタフェース
   - 低速回線でログインした場合でも実行可能な文字端末用のインタフェース
   - WIDE/PhoneShell技術を用いたテレホンサービス型インタフェース(図3)
   - OCR/OMR技術を用いたFAXを利用したインタフェース

今後は，このようなさまざまなインタフェースを要

して，ネットワーク管理を容易にかつネットワークに依存しなくても確実に実施できる体制が必要になる．

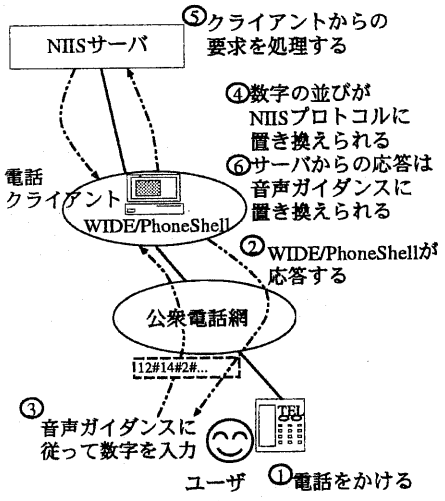


図 3: NIIS によるルータの一元管理

また見落とされがちだが，ネットワーク管理者の端末環境の整備も進める必要がある．多くの専用ルータやワークステーションではシリアルコンソールが用意されており，通信機器室に設置されたルータやワークステーションのシリアルコンソールは，多数のシリアルポートを擁するターミナルサーバに収容され，管理者はターミナルサーバに経由で，任意の機器のコンソールを操作できる．しかしＰＣが安価になり，業務用であってもＰＣベースのサーバやルータが使われるようになってきた．現在のＰＣ互換機には，システム管理に耐えるシリアルコンソール機能は搭載されていない．ひとたびＯＳが起動してしまえばシリアルコンソールが利用可能になったり，GUI 画面をそのまま他のマシンに転送して遠隔操作を可能にするサービスが存在する．しかし BIOS 設定の段階からシリアルコンソールが使える機種はほとんど皆無である．USB (Universal Serial Bus) 対応ＰＣが普及すればキーボードやマウスはある程度離れた地点からも利用できるが，モニタ画像は USB では電送できないし，電送できたとしても通信量の問題があって低速シリアル回線経由の遠隔操作には適さない．つまり例外的に存在するシリアルコンソール対応 BIOS が普及しないかぎり，ＰＣサーバやＰＣルータの障害対応は現場に駆けつけるしかない．この問題はもっと真剣に検討されるべきである．

## 5 まとめ

本稿では，本来のモバイルコンピューティングの目指す方向がイントラネットの構築運用管理に役立つことを指摘し，標準ネットワークを構築し，ネットワークの性能比較の基準とすることを提案した．また著者の研究室でつづけられている試みをいくつか紹介し，標準ネットワークのありかたを検討するための叩き台を提供した．本来のモバイルコンピューティング実現にはまだ解決しなければならない問題が多数あり実現は容易ではない．今後もひきつづき議論する必要がある．一方，標準ネットワークは，慎重な議論を長期間続けるよりは本研究会のような場で集中的に議論した後，初版の実装に着手するのがよい．本稿がきっかけになり有意義な議論と実践的な活動が始まることを期待したい．

## 謝辞

本文冒頭で述べたように，本稿は分散システム運用技術シンポジウム'98 におけるパネルディスカッションが発端となって執筆された．著者に本稿執筆のきっかけを与えてくれた同シンポジウムの全参加者，特にパネルディスカッションの際に議論に参加した人々に感謝したい．また大野研ネットワークの構築に携わった大野研ネットワーク構築グループ，特に本稿執筆に際して有用な参考資料を提示してくれた上田仁君に感謝する．

## 参考文献

[1] 大野浩之. システム管理者が離散した状況下におけるシステム管理手法. pp. 13–18. 情報処理学会分散システム運用技術研究会, 7 1997.

[2] Hiroyuki Ohno. Improved Network Management using WIDE/PhoneShell. In *Proc. INET93*. Internet Soceity, August 1993.

[3] 辻元孝博, 大野浩之. さまざまなアクセス手段を備えたルータ運用支援機構. 情報処理学会分散システム運用技術研究会, 5 1998.