平成 8 年度

イントラネットの現状と
構築上の課題

平成 9 年 3 月

インターネット・イントラネット研究部会

イントラネット研究グループ

【目　次】

研究グループメンバー

はじめに

第1部　イントラネットの現状と今後の動向

第1章　緒言

第2章　イントラネットの現状

2．1　アンケートの概要
2．2　集計結果
2．3　考察

第3章　現状の問題点と解決策

3．1　アンケートに見る問題点と解決策
3．2　考察

第4章　今後の利用分野

4．1　技術動向
4．2　運用動向
4．3　適用分野の動向

第5章　結言

第2部　イントラネット構築（設計）における手段と方法の課題

第1章　構築設計に関して

1．1　イントラネット化の対象範囲
1．2　機器・手段の選定基準
1．3　アクセス方式

第2章　イントラネットのセキュリティ

2．1　セキュリティポリシー
2．2　論理セキュリティ
2．3　物理セキュリティ

２．４　ファイアウォール
２．５　暗号化技術の要素
２．６　アクセス制限
２．７　セキュリティ教育

第3章　維持・運用

３．１　イントラネット運用コストの考え方
３．３　コンテンツの維持管理
３．４　操作教育
３．５　運用上の留意点

おわりに

はじめに

インターネットの世界的な発展に伴って、これらの情報技術を社内の情報システム構築のために利用したイントラネット構築が話題となっている。

インターネットが予想以上に普及するに伴ってイントラネットもブームのように騒がれているが、ややもすると、これまでの情報システム構築との比較において「何でもイントラネット」のごとく言われていることも注意が必要である。

情報技術の進歩は、我々ユーザーが何時のタイミングでその技術を採用すべきか混乱するほど激しく、イントラネットに関しても同様の傾向は否めない。

インターネット技術を社内の情報システム構築に利用することは確かに有用と思われるが、肝心なのは、これらの技術をどのようなアプリケーションに対して適用し、維持・運用までを考えた開発体制、運用体制を敷けるかが非常に重要である。

以上のような背景から、イントラネット研究部会ではユーザーの視点でイントラネットの現状と、構築する際の留意点に関して、以下の2つのグループで探ることとした。

イントラネット研究グループ構成メンバーは次ページのとおり（Aグループは本報告書第1部「イントラネットの現状と今後の課題」を、Bグループは第2部「イントラネット構築（設計）における手段と方法の課題」を担当）。

なお活動を始めるにあたって、下記各社のご協力によりイントラネット構築の事例紹介を受けた。

・横河電機㈱
・日本電信電話㈱
・日本サンマイクロシステムズ㈱
・㈱日立製作所
・日本ヒューレット・パッカード㈱

第1部　イントラネットの現状と今後の動向

第1章　緒言

近年、閲覧ソフトの出現によってインターネットが爆発的に広がるのに伴い、インターネット技術を閉じた 世界で適用したイントラネットが企業へ急速に普及していると見られている。このような事象は、情報システムを「ダウンサイジング」から「ネットワーク」パ ラダイムへシフトさせる原動力となると思われる。

「ダウンサイジング」パラダイムを定義すると、メインフレーム中心の情報処理（基幹業務系）をクライア ント／サーバー型へ移行しようとするパラダイムと言え、主体は情報処理と考えられる。それに対して「ネットワーク」パラダイムを定義すると、時間と空間を 超えたビジネスコミュニケーションを実現するパラダイムと言え、主体は情報処理から情報流通（情報発信・共有）へとシフトすると考えられる。
本格的な「ネットワーク」パラダイムにおいては、いわゆるサイバースペースによるバーチャルオフィス化が実現されると期待されている。

イントラネットを適用することでこのようなことが一気に可能になるのであろうか。我々は現状ではイントラネットはまだ揺籃期であり技術的にもまだまだ力不足であると考えているが、今後の進展によっては十分可能ではないかと考える。
また適用については、情報処理の面、情報流通の面、情報処理と情報流通の融合面の3つの面から考える必要があると思われる。

このような認識のもと、我々のグループはこの揺籃期にあるイントラネットの今後の適用可能性について考 えることにした。考察にあたっては、アンケートを実施することにより現在の日本の企業におけるイントラネットの普及と適用状況を正確に認識し、その中から 問題・課題を抽出し、技術動向を踏まえた上でのある種の仮説を立てようと試みた。
以下において、その報告を行う。

第2章　イントラネットの現状

2．1　アンケートの概要

（1）調査目的

インターネット・イントラネット研究部会ではインターネット・イントラネットに関して、さまざまな視点 から検討を行ってきた。この検討の中でイントラネットでサービスを提供していく場合の問題点と解決法について具体的に洗い出し、整理して実際の用に供する ことが必要となり、このためにできる限り具体的な工夫、問題点への対応事例を収集することが必要である。このためJUAS会員に対しアンケート調査を実施 し、多岐にわたる事例を収集し、この検討をより充実したものにしていく。

（2）イントラネットの定義

調査対象となるイントラネットについての当部会の定義を示し、その定義に沿って回答していただいた。
〔イントラネットの定義〕
「インターネットと同様の技術基盤を活用し、その企業内あるいはアクセスが許可された者だけで情報の共有化や交換を行い、業務遂行に活用するシステム」

（3）調査対象会社

JUAS会員会社から 500 社に調査を依頼した。

（4）調査内容

本調査は、JUASインターネット・イントラネット研究部会において定義した「イントラネット」に基づき、各社におけるイントラネットの構築状況、構築の理由、また何に利用されているか等の設問と、イントラネットを構築し実際に運用されている会社からはイ ントラネットに関する技術、運用上の問題点及びその解決策について記述していただいた。なおアンケートの設問等詳細については調査用紙を第1部巻末に掲載 する。

（5）調査回答会社集計

500 社中 110 社より回答をいただき回収率は 22%と予想を上回る結果であった。

（6）産業別会社内訳と従業員規模別内訳

回答をいただいた会社の産業別内訳を図2－1－1に示す。これより概ねまんべんなく各産業に渡って回答をいただいたと考えられる。

また回答していただいた会社の規模を従業員数から見た内訳を図2－1－2に示す。

図２－１－１　回答会社の業種別内訳

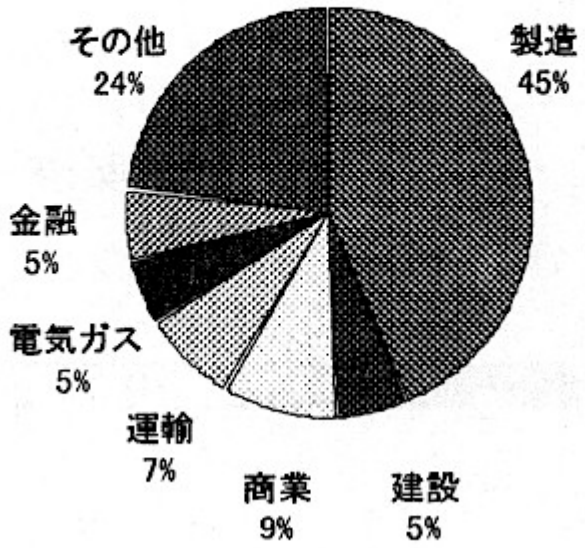


図2－1－1

図２－１－２　従業員規模別内訳

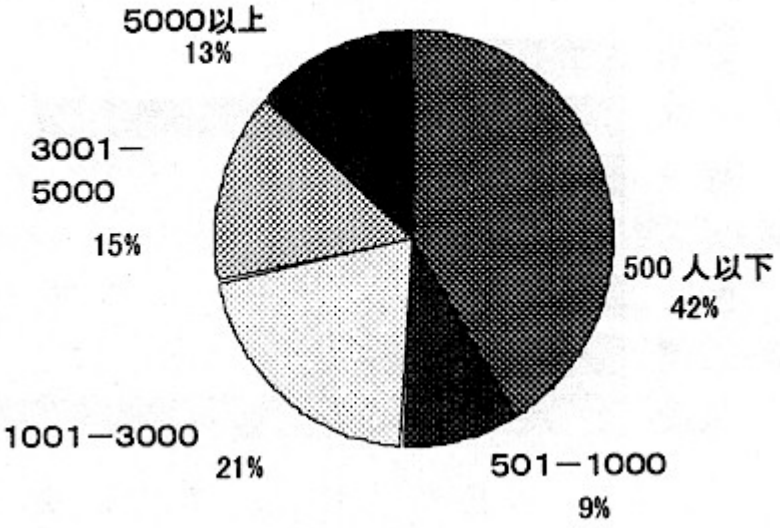


図2－1－2

2．2 集計結果

（1）イントラネットの構築状況

「社内にイントラネットを構築しているかどうか」という質問に対して、「構築している」が 28%、「構築を計画している」が 47%、「構築の予定はない」 が 25%であった。「構築の予定はない」を除くと 75%がイントラネットを社内のインフラとして考えており一般の同様の調査と比べると高い比率を示してい る。これは本調査がJUAS会員会社に対して行われたものであり、次項(2)に示すWAN化の実態からすると、社内におけるインフラ環境がある程度整備さ れ、イントラネットの構築がスムーズに行えたものと思われる。図2－2－1

（ファイルが見つからない）
図2－2－1

業種別に見ると、「予定なし」が 4/6 を占める金融の慎重な姿勢と、「構築済み」が 4/9 を占める商業の積極性が目立つ。

また従業員数で見た会社規模や、事務系／技術系／営業系などのユーザー構成別に構築状況を見たが、特に偏りは見られない。パソコン等の装備率は、回答いただいた各社は導入の有無に関わらず、ほぼ 1.5 人／台以上の装備率となっている。図2－2－2

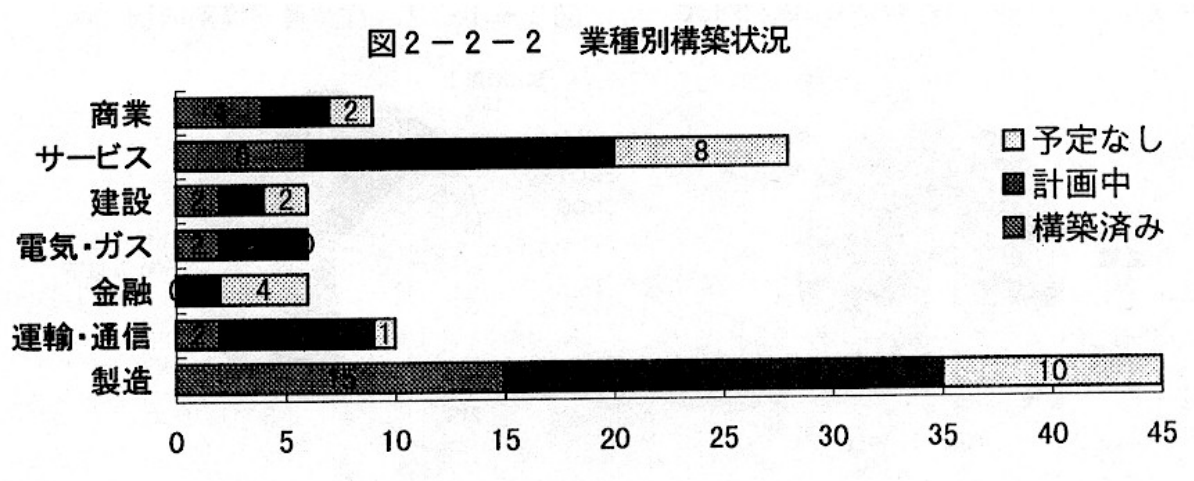


図2－2－2

（2）社内のWAN化の状況

「全社的にWAN化されている」が 61%、「部分的にされている」が 27%と、全体で 88%がWAN化されており、かなり高い割合でWANが整備されていることがわかった。

ただし、この設問ではあらかじめWANの定義をしていなかったので、その内容がルータ・ネットワークだけではなく、メインフレームや内線電話網用の専用線ネットワークまでをも含んでいる可能性がある。図2－2－3

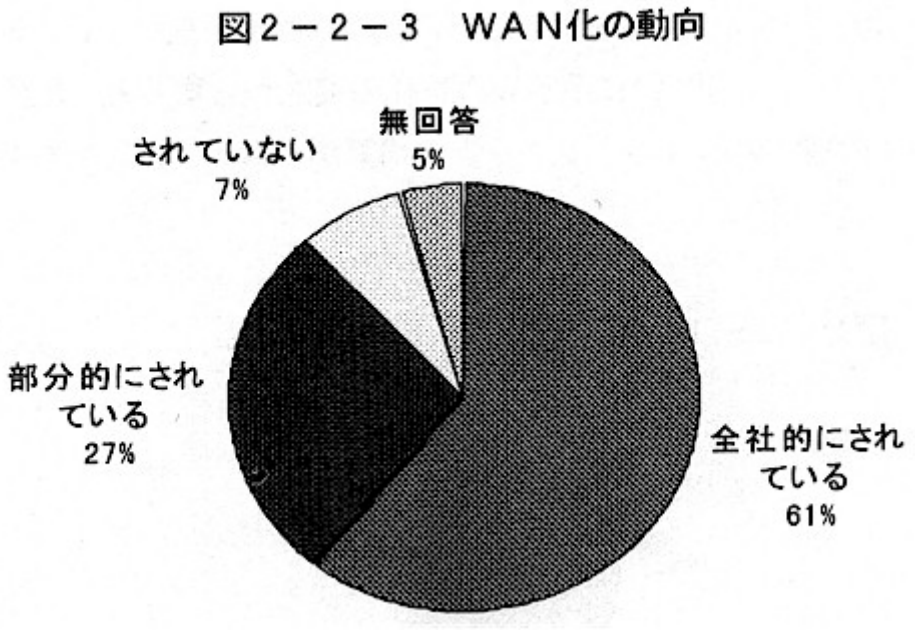


図2－2－3

（3）社内ネットワークのサーバーOS

「社内ネットワークを構築しているホスト・サーバーのOS」について質問したところ Windows NT が 73 社、UNIX が 58 社、NetWare が 43 社、メインフレームは 45 社であり、従来の UNIX、NetWare に対し WindowsNT の比 率が相当高くなっていることがわかった。図2－2－4

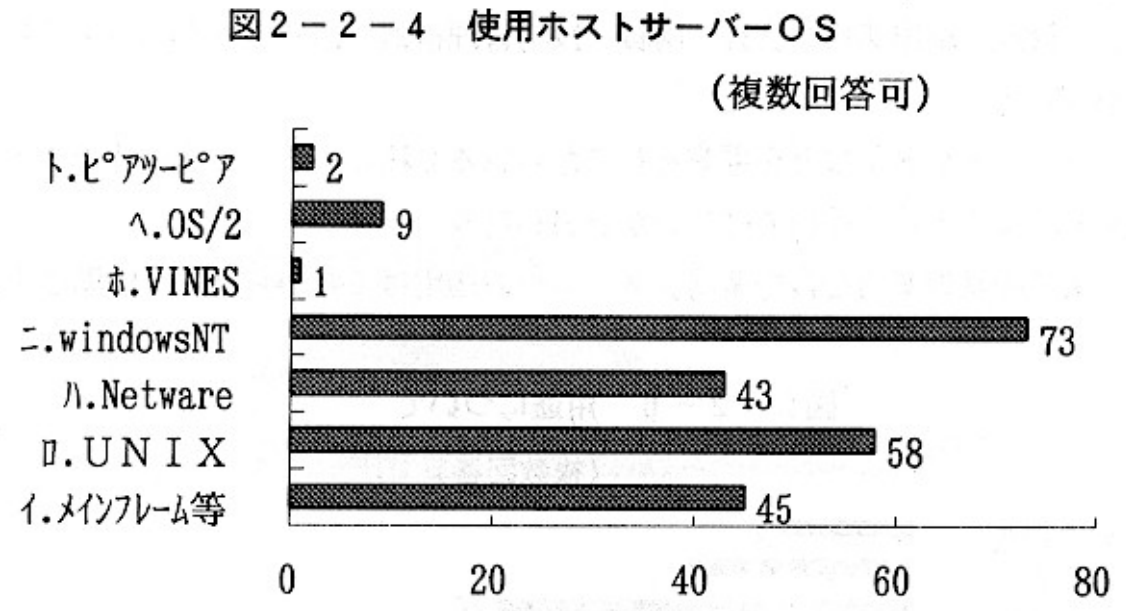


図2－2－4

(4)イントラネット構築を選択した理由

「イントラネット構築を選択した理由」については、「安価である」が 52%、「ユーザーインタフェース を統一できる」が 48%、「ユーザーの操作が単純」が 36%、「社外との接続が容易」が 31%の結果であり、一般的に言われているイントラネットのメリッ トを理由にする回答であった。図2－2－5

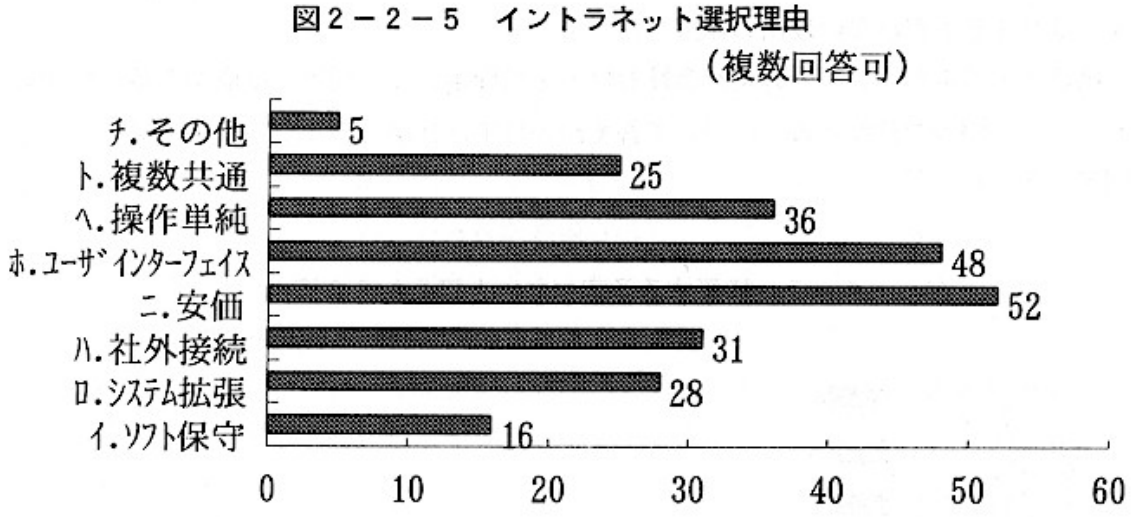


図2－2－5

(5)イントラネットを利用する主目的

「イントラネットをどのような用途に用いているか、または用いるか」という質問について主要な用途を掲 げ選択してもらった結果、すでにイントラネットを構築している会社及び構築予定の会社 82 社中「電子メール」が 54 社、「電子掲示板」が 53 社、「マニュ アル・技術資料等の文書管理」が 49 社であった。

電子メールについては、本アンケートのイントラネットの定義で想定しているのはSMTPベースの e-mail である。しかし、このアンケート結果に示される高い比率から、cc:Mail などのパソコンーLANベースの電子メールが含まれてしまっていることが推察できる。

また業務システムへの利用として「在庫照会」「オーダーエントリ」「出退勤管理」「その他」に分けて質問したが、回答はそれぞれ6社、5社、なし、11 社であった。さらに「その他」について具体的に利用している業務システムの内容を記述してもらった結果プ ロジェクト管理、輸出業務、会計、購買、技術管理検索、画像データベースを利用した検索等が挙げられた。

ただし、ほとんどがSIなどを事業としておられる会社である。まず自社で導入・運用経験を積んでみようという趣旨ではないかと思われる。一般の企業での基幹業務を含む業務システムへの適用はこれからという段階であろう。図2－2－6

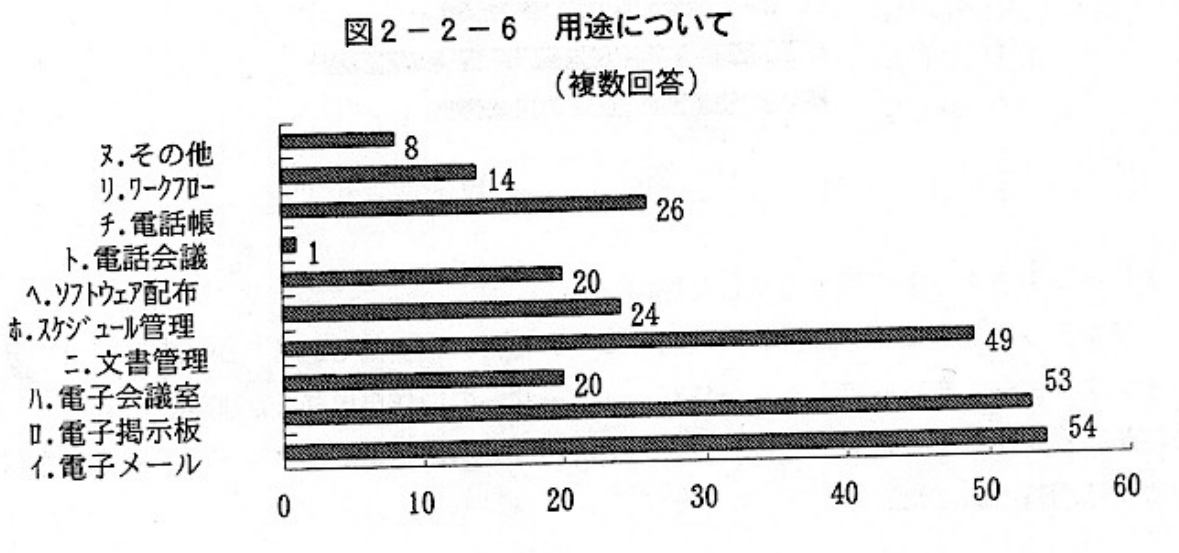


図2－2－6

(6)構築する予定がない理由の比率

「構築する予定がない」と答えた会社 27 社の主な理由は、「同等の機能がある」が 20 社であった。「同等の機能とは」について答えた 20 社中 16 社が「グループウエアツール」との回答であった。図2－2－7

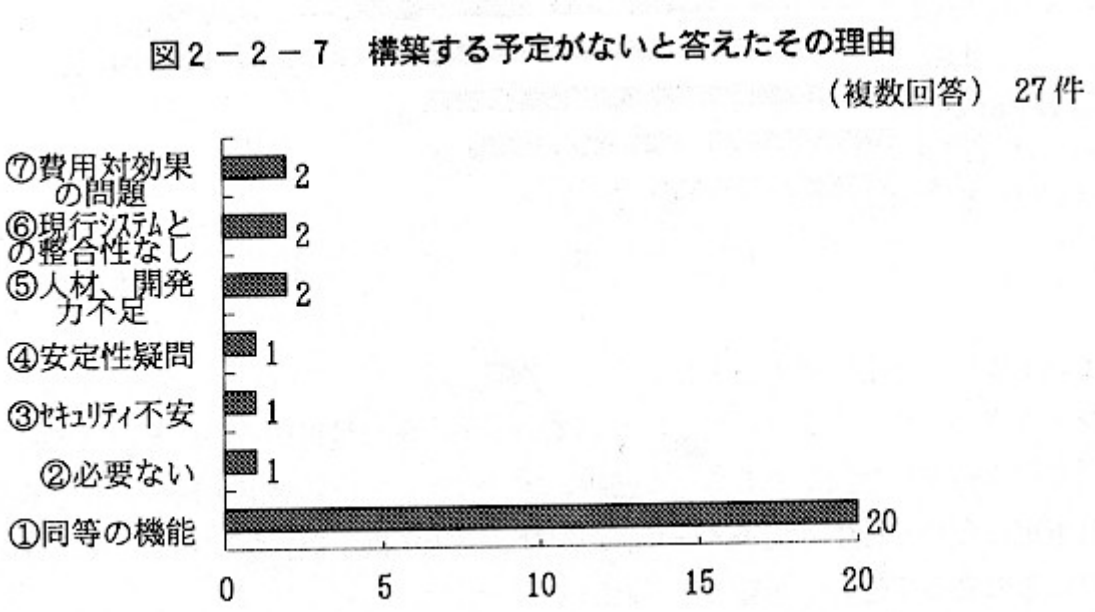


図2－2－7

（7）導入効果について

「効果があった」と回答した会社の効果の具体的内容は「業務効率向上」（17 社）、「運用コスト削減」(8 社）であり、6社は「効果なし」との回答であった。

実際にインフラの投資対効果を定量的に量ることは難しく、その定説もないことから「効果なしと」回答した会社ではユーザーの利用普及度、利用満足度等を勘案しての回答ではなかったと推測される。図2－2－8

ではなかったと推測される。

図２－２－８　導入効果

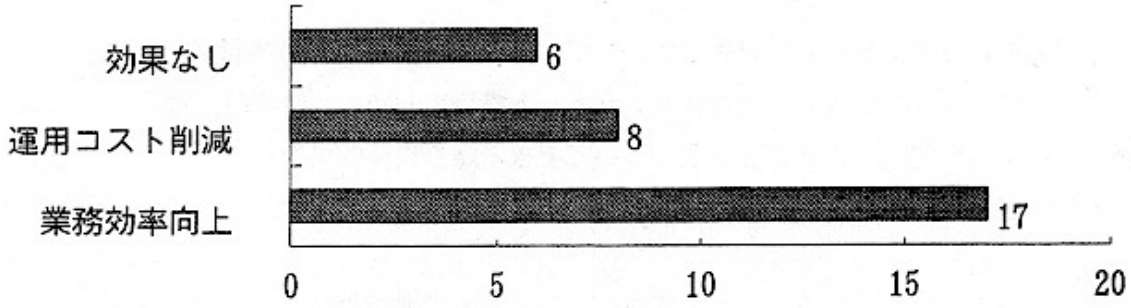


図2－2－8

2．3　考察

調査回答会社のうち2．2(1)に示したように約 75%が、すでにイントラネットを構築しているか計画 中である。会社規模や職種とは無関係に広く活用が試みられている状況がうかがえる。しかし業種で見た場合は幾分導入意欲に偏りが感じられる。これは「イン トラネットの特色を活かしやすい業種がある」という側面と、「インターネットの普及から受けるその業種への影響の感じ取り度合いの差を反映している」側面 とがあるのだろう

今回の調査では全社的規模で構築されているのか、部門単位で構築され全社的に展開していくかは明らかに されなかったが、すでに社内のWANが整備されている会社の比率が全体で 88%であったことから、WANが整備されている会社においてはイントラネットの システム構築が積極的に推進されていることがうかがえる。

一方、すでにWANが整備されている会社でもイントラネットに踏み切る段階にない会社も 27 社あった。そのほとんどがすでにグループウエアを導入しており、既存のグループウエアとイントラネットを比較しイントラネットを構築する投資対効果を見据えてのものと思われる。

またNetWare 環境を利用しながらTCP／IPに移行している会社が多いことがわかった。現状は両 者が併存している状況であろう。この併存は利用者に両ネットワーク環境に対応したソフトを別々に利用させるものであり、好ましい状態ではないはずである。 数年前まではTCP／IPプロトコルをパソコンで採用するにはメモリの制約やTCP／IPソフトが高価といった障害が多かったが、Windows95 以 降、パソコン用OSでのTCP／IPサポートが標準となってきたことと、Novell 社のTCP／IP対応で両者は融合していくのであろう。

第3章　現状の問題点と解決策

３．１　アンケートに見る問題点と解決策

今回実施したアンケートに記述していただいたイントラネットの問題点と解決策を表３－１－1(省略)に 示す。設問は「貴社のイントラネット構築において、計画時・導入当初には予想できなかった問題点、その解決法についてできる限り具体的に教えて下さい」で ある。具体的に記述いただいたのは、いずれもすでにイントラネットを構築されている企業である。

解決策については、明確に問題を解決できたとする記述が少なく、問題点として挙げられた事項の多くは現在も根本的な解決に到っていないケースが多いと見られる。

(1)サーバー／ネットワークの管理

情報システム部門の担当者がアンケートへ記入されるケースが多かったので、情報システム部門の立場からの開発・運用管理に関する問題の指摘が多かった。

①全般的な技術不足
②サーバー運用等の手間の増加
③WAN回線への負荷の増加
④セキュリティ、アクセス制御の難しさ
⑤データベース連携の難しさ

が挙げられている。

これらから、イントラネットの問題点として一般的に言われている事項が、このアンケートからも裏付けされたように思われる。

(2)コンテンツの管理・運用面の問題

①各情報発信部門でのHTML文書の作成、サーバーへの転送が面倒である
②これらの工数を公式な業務として認知する必要がある。

と指摘されている。

(3)その他

情報共有／情報発信を目指して構築したが、思ったように活用されない悩みが記述されている。

３．２　考察

(1)サーバー／ネットワークの管理

上記の①については、そもそもメインフレーム系やNetWareの経験が主体の技術者にはTCP／IP やUNIX系の知識（DNSサーバー、IPアドレスやドメイン名とその管理など）が要求されるインターネット／イントラネット技術は違和感が強いし経験も 不足している。WindowsNT がイントラネット用サーバーとしてもてはやされるのは、これらの層に表面的にはWindows パソコンと同様のユーザーインタフェース を提供している点に負うところが大きいと思われる。

また、TCP／IPやUNIXをすでに利用していても、イントラネットの回線への負荷は従来に増して大きく、これを現状把握・管理するネットワーク管理体制が後手に回っている様子が③からうかがえる。

②では、Web/ftp サーバーの立ちあげは容易だが、公式に稼動するとサーバーの管理体制が問題とし て浮上することが指摘されている。特に部門独自でWeb サーバを立ち上げた場合、その部門のサーバー管理要員のサーバー管理工数をその人の業務の中にどう 位置づけるべきかなど、UNIXの「ルート」（管理者特権を持つ人）と似たような問題を発生させているようである。

①もイントラネットの弱点として一般的に指摘されている点である。障害検知・性能監視・構成把握などの 個々のツールは多々あるが、統合化されたネットワーク管理ツールとしては決定打に欠ける感がある。また、各セグメントに専用の監視機器を配置せねばならな いなど、コスト的に全面的な導入は難しくなる。

従来は草の根的展開を進めてきた場合でも、今後は障害対策の面から、分散されたサーバの場所的集中や管理の集中が志向されるであろう。

④のセキュリティについては、社外からの不正アクセスはファイアウォールの普及で対策が確立されている ようである。アンケートからは、社内の特定の人にだけ見せたい情報に対するアクセス制御の方法についての問題の方が重視されていることがわかる。一般的に はディレクトリ・サービスに期待するところだろうが、現状ではLDAPなどのディレクトリ・サービスはいずれも十分実用化されているとは言えないし、アク セス制御としてのきめ細かい運用は難しい。グループウエアのアクセス制御の方が進んでおり、これを利用するのも当面の対応策であろう。

⑤のデータベース連携については、従来はCGIを使うのが普通で、性能面やセッション管理などを中心に問題が指摘されている。

（2）コンテンツの作成

1）インターネットに出す企業ホームページとは異なり、イントラネットの場合、HTML化を専門に行う部 署・人を置くというのは受け入れがたいことが多いであろう。これまでワープロで

作成し印刷し配布していた文書を、イントラネットを利用するためにHTML 文書へ変換するには、新たに覚えねばならない事項が多々あるのは確かである。また、作成したファイルをWeb サーバーへ送るには一般的には ftp を使うの であろうが、これも原稿を作る各担当者にはとっつきにくいかもしれない。Form を使ってコンテンツを記述しCGI経由でHTMLへ変換しサーバーに登録 する方法もあるが、今後はグループウエア・ソフトを使って登録し、ブラウザに送るときにサーバー側でHTML化するという方法が一層普及するであろう。

2）HTMLは本来ハイパーリンクが特色であるが、アンケートからはリンクの保守についての悩みが特に聞 かれない。恐らくこれは各部門ごとに管理される範囲内でしかリンクが張られていないケースが多いからではないかと想像される。全社的に文書の内容に踏みこ んでリンクを維持・管理しようという発想は、組織の規模が大きくなるにつれて困難となる。通常、リンクは階層化されたメニューとしてしか使われておらず、 文書内容での関連付けは文書データベースの全文検索機能などで補っているケースが多いように思われる。

（3）情報共有の中味・目的が再度問われる

いったんイントラネットを構築したところで、情報を発信し共有することについて改めて、何をどのような 目的でどのようなインセンティブで…といった問題が提起されてくるのだろう。電子掲示板などのように一方的に掲示する用途ですら、掲示すべき必要性を考え ないとコンテンツ保守にだけ手間取り、閲覧されることが少ないものまで掲示してしまう危険性がある。情報共有や「報連相」ツールとして全員参加型の会議室 や部門ごとの情報発信を計画すると、さらにこの問題をあらかじめ吟味する必要がある。グループウエア的な利用は、使う側にとってはサボることが可能なもの がほとんどのはずである。仕組みはできたが閑古鳥が鳴いている可能性もある。基本的なコンピュータリテラシーの水準向上から始まり、趣旨についての理解の 徹底と合意の形成、報奨制度など、周到な計画と地道な準備とが必要であろう。ただし、これはイントラネットの課題というよりも広く情報発信・共有を図ると きの課題である。特にグループウエアとしての活用を考えるときには正面から取り組むべき課題であろう。

アンケートを見ると、イントラネットで利用されているのは電子メール・掲示板、文書共有が主体である。既存のイントラネットは恐らく1年以上前の概念・技術をベースに構築されたものであろうから、内容的にはこれらが妥当な適用分野であろう。

言い換えれば、すでにイントラネットを構築した各社においても、一部では文書共用などでかなり業務レベ ルでの成果を挙げられているところもあるが、多くは「まず手を付けられるものでイントラネットを構築した」という段階であり、ここから次にどのように展開 すべきか思案されているという状況ではないだろうか？

そこで、今後の方向性について次に検討してみたい。

第4章　今後の利用分野

4．1　技術動向

（1）イントラネットの基本技術

現時点では Web に代わるものが見えていないため、イントラネットは、ここしばらくは Web（WWW）をベースとして構築されるであろう。ただし業務システムとしてトランザクション処理への適用を考えると、より性能・品質のよいサーバー環境が望まれる。

（2）サーバー

サーバーは、現在はハードがWS、OSがUNIXという組み合わせが主流であるが、ハードの高機能化が 進み、また Windows の普及が進むにつれて、ハードはパソコン、OSが Windows NT（95）という組み合わせが増加してくると思われる。ただし、ハードだけを見れば従来のWSとパソコンとの境界はほとんど消失してしまっているという のは周知の通りである。UNIXは一部支持者に根強い人気があり、またソフト開発環境としてはかなり使い勝手がよいため、すべてのUNIX環境が Window 環境に置き換わることはないと思える。その証拠というほどでもないが、最近、本屋でよく見かけるLINUX（パソコン上のUNIXもどき）な どは、UNIXのしぶとさを見せつけているものといってよいだろう。

（3）アプリケーションと Web の連携

今までは、アプリケーション（例えば業務プログラム）をイントラネット上でサービスする場合、CGIを 用いて Web とアプリケーションを強引に結合してきた。しかし、今後はアプリケーションを包含したようなサーバー（例えば、DOMINO など）が多用されるようになり、アプリケーションと WEB がシームレスに接続でき、使い勝手のよいものが提供されるようになるだろう。ただし、すべてのアプリケーションが これに置き換わるというのではなく、一部の限られたものとなるのは止むを得ないと思われる。例えば、DOMINO はワークフローに基づいたアプリケーショ ン向きではあるが、これ一つですべての業務が問題なく処理できるとは思えない

（4）ブラウザの高機能化

今でも、Netscape Navigator/Communicator や Internet Explorer などは、単なるブラウザとしての機能のほかに、メールの送受信や、FTPの実行など多機能化していて、ブラウザだけでかなりのことができ る。今後、サーバー側の高機能化（上記の DOMINO のような）とともにブラウザがさらに高機能化され、通常の業務はブラウザから離れずに行うことが可能 となるだろう。

（5）アプリケーション開発用言語

今まではアプリケーションの開発はCGIと従来言語で行われてきたが、今後は Java あるいは ActiveX で行われることが多くなるということは、周知のことである。

しかし、これらの言語で開発されたプログラムはサーバーから端末にダウンロードされる形式をとるため、 セキュリティの問題に必ずしも信頼がおけないと考えているユーザーは多い。ただし、Java によりソフトウエアの保守が軽減する（コピーがない）、デリバ リーが不要などの特性の他、開発用言語としては従来から注目されているOOPの流れを汲んでいるため、セキュリティに関する不安が解消されれば、その利用 は爆発的に増加することが予想される。

ただし、これらの言語で開発するためには、よい開発環境の提供が必須であり、現在行われているJDKの高度化（Java beans）などが待ち望まれる。

（6）マルチメディア化

マルチメディア化は言葉あるいは概念が先行して、実のところ何に使ったらよいのか模索している段階であろう。まずはDTC（Desk Top Conference）やインターネット／イントラネット画像電話などのような、音声＋動画像などから始まっていくと思われる。

また、CTI（Computer Telephony Integration）の展開にも注目したい。

現在のテキストベースの情報交換においても、gif などによる静止画像／擬似動画像が含まれているなど 情報量はかなりのものにのぼるため、早晩、現在の 10BASE－Tなどの回線では限界が見えてくると思われる。マルチメディア化が進展すれば、この速度で は到底間に合わない。今後のLANは 100BASE－TやFDDIなどの高速なものが必要となってくると考えられる。またWANではATMやフレームリ レー、セルリレーなどの高速の回線が利用されていくものと思われる。

（7）端末

パソコンは、Java などが普及すれば現在の重装備のパソコンは不要になってくると思われ、NC（Network Computer）などに取って代わられる可能性は高い。しかしユーザーの自分のローカルファイルは手元に置きたいという要求は強く、また本当に現在のパ ソコンに置き換えていいのかという検証がすんでいないため、当面、従来型のパソコンがオフィスから消えてなくなることはないと思われる。

（8）コンテンツ維持管理のためのツール、方法論の待望

現在提供されているツールは、イントラネットのメカニズムあるいはコンテンツを構築するということに主眼がおかれ、これらを維持管理するという視点は重要視されていない

しかし今後イントラネットへの依存度が高くなればなるほど、システム及びコンテンツの信頼性が要求されてくるため、維持管理という視点が重要になってくる。今後、このような視点に立った方法論やツールの出現が望まれる。

(9)セキュリティレベル

セキュリティ技術には暗号化や個人認証があり、これらは確立された技術である。これらはセキュリティの 対象に重みをつけることはない。しかし現実には部内と部外、社内と社外などセキュリティにはレベルが存在する。社内に対しては社外ほどセキュリティの強度 は強くなくてよい。つまりレベルごとのコストミニマムで、かつ利用性もそれに応じたものとなるような技術あるいは方法論の開発が望まれる。

(10)イントラネット／インターネットを介してのデータ交換

現在、イントラネットでのデータ交換は、HTML+アプリケーション固有のデータ構造を基本として行われている。これは、社内のシステムであり統一的な規則が適用できるイントラネットである限りは、あまり問題ない。ただしアプリケーションが社外で開発され たものである場合、そのアプリケーションの変更(バージョンアップ)に大きく依存してしまうという問題がある(これはイントラネットに限った問題ではな く、ソフトを利用する時のきわめて一般的な問題である)。このため、データ交換をHTMLに一本化できることが望ましいが、それには現在のHTMLでは機 能不足であり、高度化が必要である

一方、各社がインターネットで結ばれてきてCALSの利用が本格化してきた場合、このデータ交換形式が 大きな問題となる。社内と社外のデータ構造が一致している方が望ましいが、これは難しい問題を多く抱えており、解決は容易でない。CALSのデータ交換は SGMLで行うことが多いようである。HTMLはDTDが事前に定義されたSGMLと考えることができるが、それでもやはりSGMLとはたもとを分かった ものであり、データの交換となるとさまざまな障害が予想される。百歩譲って、HTMLは何とかなるとしても、各社内で利用しているアプリケーションのデー タの交換はどうすればよいのか。今後のイントラネット構築では、このあたりの技術的見通しを立ててから行わないと、あとで大きなツケを払わされることになりそうである。

4．2 運用動向

世の中に出ているさまざまな情報誌の報道を概観すると、今にもすべてのクライアント／サーバーシステムがイントラネットに置き換わりそうな気配である。

イントラネットは情報システムにとってバラ色の世界を約束してくれるのだろうか？

クライアント／サーバーシステム構築を行うときに直面するいろいろな問題が、イントラネットではすべて解決するのであろうか。

これまでに見てきたことから判断すると、必ずしもそうではないようである。
ここでは、ここまでにいろいろ議論してきたことを前提にして、イントラネットの運用管理について検討する。

(1)システムの運用管理動向

1)サーバー
前項の技術動向でもみたように現状、サーバーはUNIXが主流である。一方、Windows NTの台頭も無視できない。アンケート結果からもWindows NTが思った以上に浸透し始めている。

2)サーバー／ネットワークのシステム管理
現状のUNIXでは、サーバーのシステム管理には、UNIXの上級知識が必要であるかつUNIXのシステム管理は本来イントラネットで管理に必要とされることの一部であり、十分ではない。特にシステム運用管理の中でセキュリティや障害監視については問題が多い。

一方、Windows NTについては後発のOSでもあり、運用管理については考慮がなされている。しかし、これでも十分ではない。今後は、管理者にとってより簡便で、信頼性を 有し、堅牢なシステム管理ツールの出現が急務であろう。利用者にとって信頼性の高いイントラネットの構築には、より頑丈で安心なセキュリティ機能、障害発 生を素早く察知し、迅速な障害復旧を実現する障害監視回復システムなどが望まれる。

ネットワークの管理については、すべてのセグメントとクライアントを集中的に把握できる相対的に安価な仕組みが望まれるが、展望が開けていない。

構成管理や障害検知にはDMI(Desktop Management Interface)や各社独自の仕組みがあるが、網羅性が不十分である。SNMPも対応している機器しか管理できない。WBEM (Web Based Enterprise Management) などの目論見がどの程度の成果を出し普及し得るか注目したい。

3)アクセス制御
またアクセス制御についてはUNIXのセキュリティレベルでは不十分である。玄関のドアには鍵がついているが、一度入ってしまうと各部屋のプライバシー は大変心もとないそのためアプリケーションごとにACLの設定などが必要である。現実的にはNotesのようなきめ細かい設定が標準になるかどうかは、よくわからない。

(2)コンテンツの運用管理動向

1)現状の問題点及び課題
掲載する情報(コンテンツ)の鮮度と品質を保持したまま適宜更新することは、クライアント

にとって容易ではない。これまでは構築にのみ主眼が置かれてい たが、これからはこのようなコンテンツの鮮度、信頼度などの維持管理が問題である。これは技術的問題と人の意識や組織の問題に関係しており、簡単ではない。技術的問題はおそらく次々に解決されるであろう。一部ではLotus Notesなどの利用が進んでいる。またワープロソフトや表計算ソフトがHTML変換機能を備え始めている。すなわち、各人による情報の簡易更新ツール、 更新の履歴管理などが出てくるであろう。

2）関連機能、ツール

関連機能として、

- ディレクトリーサービス
- データベース連携
- データの更新ツール
- データそのものの管理ツール
- 個人情報管理とグループウエアとの連携処理

などがあり、これらに関してもいろいろなツールや考え方が出てくるものと思われる。

特にデータベースの機能については、CGI経由のアクセスが普通だったが、HTTP用APIや各データベース製品に対応したWebサーバーでデータベースとの間を取り持つオブジェクト・リクエスト・ブローカーなどが提供されつつある。

CGIは、起動したプログラムがWebサーバーと別のプロセスとして動くのでAPIを使うよりも安全で あるし多様なプログラミング言語が使えるが、性能面ではボトルネックとなりうるので、これらの新しい手段への期待は大きい。しかし全般的に各社各様で独自 色が強く、よりオープンな標準的な仕様の普及が望まれる。この分野は今後のイントラネット発展の本命であろうから、動向を注視する必要がある。

4．3 適用分野の動向

（1）はじめに

イントラネットの長所としては、構築する費用の安さ、1台当たりの安さ、柔軟な拡張性、インタフェース の均一性、インターネット／イントラネットの両方が使用できるなどがある。短所としては、双方向性に若干欠ける点がある。これらの長所・短所を踏まえて適 用分野については吟味する必要があるが、あまり分野を特定せずに広まる勢いである。これまでのところトランザクションの少ない基幹系に向いており、グループウエア（電子メールや掲示板）あたりからスタートしている。ダウン時のダメージの問題（サービス低下、回復時間短縮）などが課題である

主な適用分野の候補としては、以下のようなものがある。

（2）業務システム系

ホスト系・クライアント／サーバーシステムからの移行、業務システムのフロントエンド、受発注、販売、 購買、生産管理などがある。営業情報管理、顧客管理も大きく期待されている。ショールーム、カタログ／パンフレット・データベースなどの利用分野ではイン ターネットの方が先行しているが、ますます利用が進むであろう。

すなわち業務系についてはますます進み、自前システムから汎用 Web システムへ移行すると考えられる。

1）特にこれからの適用分野として、トランザクション処理が実用化すると考えられる。これまでは Web＋ミドルウエア＋ データベースエンジンで行われているデータベース連携が、分散オブジェクトなどの発達により、性能面でも信頼性でも業務に耐えるようになるであろう。

業務アプリケーションをイントラネットの環境下で実現することは、クライアント・マシンへソフトを配布するクライアント／サーバー方式よりも情報システム部門の保守・運用面で好ましいので、このようなプラットフォームで構築する事例が今後次々と出てくるであろう。

ただし、クラスタリングなどの障害対策と、複数の分散サーバーの保守・運用への対応が今後も課題であり、これが普及の障害としてしばらく残りそうである。

2）また「業務フローの各ステップを支援するアプリケーションをブラウザ上に作業手順書・ジョブディスク リプションのような形で個人やグループ別に整理しておき、新人でもすぐに仕事を覚えられるようにした」という事例が幾つか報告されている。このような使い 方はHTMLのハイパーリンクをうまく活用したものとして興味深い。イントラネットの特色とされているユーザーインタフェースの統一が活かされており、手 順やアプリケーションの変更にも簡単に対応できる業務密着型の使いこなしとなっている。ただし、これを実現するには基幹系業務も含めてあらゆる業務がブラ ウザ上からできる必要があり、既存システムの取り扱いが壁になる。

（3）情報システム系

アンケートからも、現状ではこの分野での利用が一番進んでいる。

- グループウエア（メール、スケジュール、報告書、掲示板、会議室、電話帳）
- 人事、庶務情報システム（個人情報、勤怠情報、給与、交通費清算、各種稟議）
- 技術情報の共有化（技術報告書管理、検索、製品情報）
- 図書館（文献情報、画像）
- データベース
- ソフトウエアの配信 など

またマルチメディア応用として、

・ DTC、画像電話

・ ヘルプデスクなどについては音声、画像の併用

が、技術的にも経済的にも見合って行くに従い、現在のメディアからのスムーズな移行が期待される。

そのためには、いろいろな意味でのブレークスルーが期待されるが、技術的にはそれほどの困難ではなく、 人の意識の問題であろう。また大きな組織になるほどアクセス制御及びセキュリティについての要求が複雑化するが、これにある程度応えることがイントラネッ ト普及の一つの壁かもしれない。

(4)その他

モバイル、SOHOなども見逃せない。社会的背景として、クイックレスポンスの要求成果主義の人事考課 や高齢化社会の進展といった不可避なトレンドがあるので、ますます普及する必然性がある。これらの環境では、集中管理するのが困難な電車・ホテル・車・家 庭など不特定の場所から、PDA・ケーブルモデムにつないだテレビなど不特定な機器からサーバーへアクセスされる。イントラネットにとって、ソフト配布・ バージョン管理・ライセンス管理を不要にし、ユーザーインタフェースを統一できるなどの特色を活かせる恰好の舞台である。これはNCの動向や通信コストの 推移などとも関係する。

また社外エクストラネットとのデータ交換の必要性が高まり、CALSやSGMLなどのデータ形式の標準化の流れもあるが、何が本命かは現時点ではよくわからない。

第5章　結言

イントラネットの現状の適用分野・問題点と解決策をアンケートによって把握した。
現状の適用分野は、①電子メール、②電子掲示板、③文書管理がメインである。
問題点として、①サーバー／ネットワークの運用管理、②コンテンツの管理、③その他が挙げられた。
これらを踏まえて、今後の技術動向を概観した上で、①システムとコンテンツの運用、②業務系・情報系の適用分野について、今後の方向を考察した。
以上の考察から企業としての適用を考えた場合、技術的側面にも増して情報の発信・共有と、それの整理・体系化・検索性の維持といった問題が、システムの有効性を決することがうかがえる。
最後に、以下の2点を指摘し、問題提起しておきたい。

（1）意識改革

イントラネットの場合、これまでのように中央が集中的にデータや情報を収集管理、更新するのではなく、 分散された環境で、かつ各部署ごとに情報の更新や公開を行う必要がある。また他人にとって有用な情報を積極的に出すか？、インセンティブは？、など、いろいろな課題がある。そのため人の意識や組織の問題を解決する必要がある。
意識改革に成功する者や組織のみが、イントラネットを本質的に活用できるのかもしれない。

（2）情報の取捨選択

イントラネット（あるいはインターネット）の出現によって、情報の発信は非常に容易になった。統制されたネットであるイントラネットでさえ、非常に多くの情報源が存在するようになるであろう。このとき情報の取捨選択ということが非常に重要になる。今まで情　報の選択は、個人のスキルに依存してきたようなところがあるが、今後は組織として情報の選択の方法論－例えば情報分類学など－を確立していく必要がある。

第2部　イントラネット構築（設計）における手段と方法の課題

第1章　構築設計に際して

情報共有による業務改善を達成するためのシステム構築ツールとして、電子メール、電子掲示板、DBMS、グループウエア等があり、新しいシステムの形態と してイントラネットがある（イントラネットはツールではないので、イントラネットを含めて以下これらを「ツール等」と表現する）。

これらのツール等の機能としては、情報の単一方向伝達、双方向伝達、蓄積等があり、プログラムを組むこ とによってこれらのツール等機能を活用して業務処理を伴ったシステムを構築することができる。ツール等によってそれぞれ持っている機能範囲が異なっている ため、業務改善の対象によってツール等の選択は一つだけではなく、どれを選択してもそれなりにユーザーの目的や要件を満たすシステムはでき上がる。さらに現在では、ツール等間でのデータのやり取りが可能になり、選択の幅が広がるに連れて、システム構築する際、どういう業務改善にどういうツール等を組み合わせたらよいのか、判断が難しくなってきた。

つまり、情報共有による業務改善は、その時代の情報技術、社の方針、対象とする業務利用環境等により、 いろいろな構築手段（ツール等）を選択することができるため、無秩序にツール等の選択を行うと、後に全社的に統一のとれた情報共有の仕組みを構築すること が、困難になってしまう。

そこで、そのようなことにならないように、全社的に効率よく、統一のとれた情報共有のシステム構築をするためには、ツール等の選択に何らかのルールなり基準なりが存在するものかどうか、先進企業はそれらをどう乗り越えてきたか、事例調査の結果も踏まえて検討する。

1．1　イントラネット化の対象範囲

どんなシステムについても言えることだが、対象化の範囲が明確でなければ業務改善にはつながらない。イ ントラネットについて考えてみると、イントラネットではある程度のネットワークインフラさえあれば、費用も大してかからず、それほど高度な知識がなくとも （難しいことをしなければ）構築が可能なため、草の根レベルで自然発生的に広まることが多い。

しかし情報発信は簡単だが、その情報が必要としているところに確実に伝わるかは別問題である。今まではコストや手間のため発信されなかった情報が広く共有 される環境ができてきたことは非常にありがたいことであるが、構築したシステムが業務改善にきちんと結びつくよう、インフラの整備状況等を把握し、対象範 囲を明確にしておくことが必要である。

以下に対象範囲を決める上で考慮すべき点を述べる。
基幹系はまだまだ少数で、かつ基幹系はトップダウンで進められるケースが多いので、ここでは主に情報提供型コンテンツについてのみ検討する。

（1）インフラ

インフラの整備状況がすべてを決定すると言ってよいだろう。対象者すべてがアクセスできる環境がなければ、広告のように見てもらえばラッキーといった情報しか流せない。イントラネットにアクセスできない人のために別の手段を用意することは業務改善に反し かねない。製造業の工場のようにスペース的にも利用頻度からみてもPC1人1台体制が難しい場合は、特に注意が必要である。

ネットワークコンピュータのような安価な機器が普及するまでは、紙情報の置き換えのため新たにインフラを整備するのはどうかと思われるため、電子メールを含め新たなコミュニケーションツールとして考えれば別だが、現状の整備状況は重要である。

（2）スキル

ここでいうスキルとはサーバーを構築・運用する能力ではなく、コンテンツ作成能力である。サーバーの構築・運用は情報システム部門が行えばよく、ここでコストが問題になるなら初めから不必要なシステムであり、構築するに当たらない。

多くの部署より業務として情報提供を続けていくには、情報発信者自らがコンテンツを作成する必要がある。簡単なツールや環境が用意されているか、教育体制が整備されているかが問題になる。この点は第3章・維持運用で触れる。

（3）コンテンツ内容

自分たちが行っている業務内容の説明等の広報のように、ただ単になるべく多くの人に見てほしい内容なら特に注意する必要はない。
しかし、保養所の申し込みを早いもの順で受けるような内容では、対象者全員が平等にアクセスできる環境か注意すべきである。例えば製造業や流通企業では本 社の社員はPC1人1台、工場や店舗といった現場は数人で1台といった環境では、とても平等とはいえない。事前に受付をして抽選にする等の配慮が必要であ る。

またインフラの項で述べたことに反するが、イントラネットと現行同様の紙での情報発信といったような二度手間になる内容でも紙の量を減らすことでコスト削減につながればそれはそれで業務改善になるので、最善ではないがイントラネット化の対象になろう。 さらに、社外秘や人事情報といった特定の人にのみアクセスが許された情報の扱いも注意すべきである。

紙でもコピーされてしまえば同じことだが、ネットワークはより広範囲に広がる可能性があるので注意したい。

アクセス権の制御については今後の技術の発展いかんであるが、現時点ではイントラネットよりグループウエアの方が勝っていると思われる。そのような情報についてはグループウエアとの使い分けなどを検討する必要がある。

（4）グループ会社の扱い

社員だけを対象にしても、出向者を考えればグループ会社との接続も必要になる。この場合、グループ会 社の規模にもよるが、すでに別々にインフラが構築されている場合は簡単にシステムを結合できない場合もある。特にIPアドレスにプライベートアドレスを利 用している場合は、アドレスの重複が懸念される。早めにグループ会社を含めたインフラ整備を検討する必要がある。

コンテンツの項でも述べたが、ここでも情報へのアクセス制御がポイントになる。
対象範囲について、イントラネットだからといって特別なことはそれほど多くないと思われる。ただし現状では情報提供型のコンテンツが多いこと、情報発信は簡単だが受信側のインフラが必ずしも同じでない点を考慮し、不平等が生まれないような配慮をすることが大事である。

以下、機種やOSなどの選定、セキュリティ、そして維持・運用に関して調査結果などを含めて報告する。

１．２ 機器・手段の選定基準

（1）手段（イントラネットやグループウエア等のツール）の選択基準

1）ツール等の選択基準は存在するか

情報共有による業務改善のシステムを構築する上でのツール等の選択基準の例として、非常に大まかな例であるが、

1)『どういう対象業務は、どのツール等で構築する』という基準
例：社内規程等の表示系は、グループウエアを使用して構築する
あるいは、イントラネットの環境で構築する
例：営業系のシステムは、グループウエアを使用して構築する

2)グループウエアとイントラネットを使い分ける基準

例:『セキュリティ確保が必要な場合は、グループウエアを使用する』

等がある。

このような基準が成立し、有効であれば、今後、システム開発をする上で大いに参考になる。しかし多くの企業のシステム構築の経緯から見て、どの企業にもそのような基準は存在しないようだ。

一般に、システム開発は、新規であれ再構築であれ、その時代の新しい情報技術やツール等、またはデファ クトスタンダードな情報技術やツール等が採用され構築されてきた。したがって企業の情報資産である既存システムには、過去から現在にかけての情報技術やツール等が混在している。そのような中で、すべての既存システムを対象にして、うまく治まるような基準を作成するのは容易ではない。基準を作成し、全社的 に統一のとれた情報共有のシステム構築を目指すことが望ましいが、常に新しい情報技術やツール等がどのようなシステムに利用できるかを考えて積極的に取り 込んでいるのが現実のようだ。イントラネットを早くから始めた先進企業においては、イントラネットの技術はこれまで構築したシステムのどの部分に活用できるかを検討し、有効な部分を再構築する。例えば、クライアント側のソフトは、Excel が適当か、Access が適当か、ブラウザが適当か、を検討する。 ブラウザに決定すれば、新規システムであれば「イントラネットの環境で新規開発」したことになり、既存システムであれば「イントラネットの環境で再構築」 したことになる。

今日のような情報技術の進歩が激しい時代にツール等の基準を定めていては、かえってそれがシステム構築の足かせにもなりかねない。基準を定めて固定化するよりも、常に新しい情報技術やツール等を取り込める柔軟さ、スピードが重要と考える。

つまり企業に求められるものは、決して基準ではなくて、常に新しい情報技術やツール等を取り込める柔軟さ、スピードとその実行力にあると思われる。

2)ツール等の統一

価格の低下とEUCの普及に伴い新規のツール等が出始める頃は、どこの企業においても社内的に無秩序に種々のツール等が導入され、徐々に普及してしまうのが通常である。全社的に管理側が社内統一しようとする時点では、製品まで統一するのはすでに手後れというのが多くの企業の実状であろうと思われる。全社的 にツール等の統一を考えるとき、部門等で導入された種々のツール等を捨てきれれば別であるが、既存の資源を有効活用するとなると、ツール等の統一はなかなか容易ではない。

そうした中でも製品の統一をしている企業もある。例えばブラウザはホームページからダウンロードして使用する。古いバージョンを使用していてアプリケー ションが使用できないユーザーは、ダウンロードしていないユーザーの責任となる。また一方で、製品の選択はまったくユーザーの自由という企業もある。ユーザーが技術者中心の企業は特にそうである(そ

のような企業の各部署は技術レベルも高く、自ら利用環境を構築することができるので、無理に拘束する必要がない)。

一般的に言えば、製造業と非製造業とでは若干違いはあるが、情報システム部が支援をする必要のある部署は、技術者のあまり多くない管理部門、営業部門、事 務部門、製造部門の一部であり、これらを統一することは比較的容易と言えるだろう。企業の規模、社員数、業種等により異なるが、特定したツール等の統一は 可能であり、最終的にはそれぞれの企業のポリシーによるところが大きい。

3)製品側からの解決

インターネットは世界的なネットワークで、かつコストが安いことから、今後はどの企業においてもインターネットを無視した情報化は考えられない。社内の情 報化といえどもユーザーの利用環境は、社内、社外共通した利用環境の方が使い勝手がよく、ユーザーニーズは自然とその方向に高められる。したがってイント ラネットの普及と共に、各製品は生き残るためにインターネットのサービスを意識し、インターネットとの共存を目指し、インタフェースを求めている。

グループウエアは、インターネットのブラウザからも利用できるように歩み寄った。このようにグループウエアがインターネットのWWW技術を取り込むことに よって、徐々にグループウエアとイントラネットの利用上の垣根が低くなっている。厳密にツールの統一さえ考えなければ、以前ほどツールの選択に悩むことは なくなってきたとも言える。ツール等を統一できるのが一番よいが、無理してツール等の統一を図るよりも、これまで導入したツール等のインタフェースを利用 して有効活用する方が現実的な解決かもしれない。ツール等の出発点がグループウエアであれイントラネットであれ、完全に利用者のツール等が統一されていな くても、ある程度、情報共有環境が共存できるようになってきた。グループウエアとイントラネットの融合はすでに始まっている。

今後ますます製品間の歩み寄りが考えられるが、ユーザーはオープンな規約を前提としたものを強く望んでいる。

4)イントラネットに有効な対象業務

基準とまではいかないにしても、イントラネットの入門として最も一般的で取り組みやすく有効なものに「表示系」がある。イントラネットを活用している多く の企業は、その対象業務の傾向を見ると、各種お知らせ、各種印刷物(定型文書、社内規程等)、各種有効情報等をホームページ化している。イントラネットで 情報公開の仕組みを作り、情報伝達の迅速化、ペーパーレス化等を図り、生産性向上を図っている。

電子掲示板、グループウエア等で構築されてきた既存の「表示系」は、イントラネットの環境で組み替えられている。ユーザーの利用環境（ツール）は、ソフト ウエアとしてブラウザがあればよいという手軽さが受けている。例えば Notes の Domino 環境がそうであるように、「表示系」の場合、グループウエア はイントラネットと組み合わせて使用するのが経済的でよい。イントラネットが弱いとされるセキュリティも確保できる。

さらに発展させた段階として「処理系」のレベルがある。表面的にはイントラネットであるが、背景では ユーザー主体のワークフロー的な業務処理の流れに沿って、グループウエア、DBMS等と連携して処理をしている。情報発信側が主体となって進めてきた「表 示系」は、いずれ有効な対象業務は網羅されてしまう。それ以上の「表示系」の対象業務は、苦労して作る割にユーザニーズが低い。そのことに早く気づき「表 示系」の限界点を見極めた企業は、業務処理の対象を情報発信側主体からユーザー主体の「処理系」に切り替えた。しかし処理の内容が複雑になるにつれて技術 的にも高度になり、イントラネットだけでなく、既存の資源をうまく活用した総合力が求められるため、それなりの技術レベルや経験と情報投資が必要だ。

（2）電子メールの統一

イントラネットをすでに活用し始めている企業に共通していることは、 イントラネットを活用していく前に電子メールが業務の中で相当使用されている文化がある。したがってここではイントラネットのメールと既存の電子メールの 整理などが1つの課題となるため少し触れておくこととした。

1）背景

前にも述べたように、インターネットは世界的なネットワークで、かつコストが安いことから、どの企業においてもインターネットを無視した情報化は考えられ ない。その利点を生かし社内に活用したのがイントラネットであるから、インターネットの主なサービスである電子メール、NEWS、WEBは自然と社内に取り込まれてくる。

また、イントラネットの活用をWEB（ホームページ）に求めている企業は多く、ホームページをうまく活用しようとすると、問い合わせ、返信等で電子メールが必要になり、既存の電子メールを使用していても、インターネットの電子メールは自然に社内に広がる。

最初から社内用電子メールを活用してきた企業は、イントラネットの活用が広がるに連れて、社内用とインターネットの2系統の電子メールが存在することになる。さらにグループウエア等の電子メールが加わり、一層複雑化している。このように、どの企業も電子メールの統一に問題が生じてきている。またイントラ ネット利用上の電子メールとしてもいくつかの課題を持っている。

2)電子メールの統一

例えば人事、総務等から社員に電子メールで連絡したい場合、社員の電子メールの製品が統一されていた方がよいに決まっている。添付ファイルの取り扱い形式 が異なるメーラ間で使用される場合は、ゲートウエイでコード変換されるときに添付ファイルの内容が文字化けすることもあり、注意を要する。将来的には、添 付ファイルの取り扱い形式が異なる製品でもゲートウエイ機能が充実し、製品間のインタフェースがとれるようになり、ユーザーの心配は不必要になるだろう。 またそういうメーラでないと生き残れないであろう。

現在では、単独機能の電子メール、インターネットの電子メール、グループウエアの電子メール、これらの各電子メールの位置づけ、棲み分けは、各企業共すっ きりとした整理はできていないのが現状である。ユーザーが多少不便でも、それぞれの電子メール文化で使い分けて使用しているのが実状のようである。現状の 電子メールの利用は、どの企業も統一が難しく混沌とした状況にあると言えよう。

メーラが統一されているに越したことはないが、イントラネット(インターネット)の世界だけを考えれば、電子メールは標準プロトコル(SMTP)の下で送 受信されているため、メーラまで統一する企業はまだ少ない。ただしメーラの不統一が添付ファイルの文字化けなど若干の課題を残している。

3)イントラネットの電子メールの課題

①日本語名表示
社内で利用する場合は、社員名は日本語名表示の方がわかりやすい。

例えば、標準的なエイリアス(アドレス)ではないかもしれないが、
田中　一太郎　総務部長　のアドレス　:　taro@aaa.co.jp
鈴木　　花雄　経理部長　のアドレス　:　hana@aaa.co.jp
とする。

FROM 表示は、taro@aaa.co.jp　(Ichitaro Tanaka)より
taro@aaa.co.jp（田中　一太郎）　の方がわかりやすい。

しかし日本語名表示は、すべてのメーラ、ゲートウエイサーバーが日本語名表示を保証しているわけではないので、文字化け等のリスクを伴う。FROM表示で は、社内間では日本語名表示の方がよいにしても、インターネットへ出た瞬間から正しく配信されるか保証がないので、海外に送信する場合は日本語名表示では 困るときがある。日本語名、英文名が自由に扱えるようになると便利であるが、現在は、英文名で慣れるしかない。

CC（写し）の表示は、taro＠aaa.co.jp,hana＠aaa.co.jp となり、受信者側は、tarohana を見ただけでは、送信者が CC（写し）を誰に出しているのか判別できない場合がある。人数が多くなると全員調べる気にもならない。そのような場合、紙文書と同様に本文にCC（写 し）の送信者を記載してカバーしている企業も見受けられる。

写し： 田中 一太郎 総務部長、鈴木 花雄 経理部長
以下本文が始まる。

これらの日本語名、CC（写し）等について、インターネット世界から入った企業は、インターネットの文化に慣れ、あまり問題視していない企業もある。企業文化の違いや慣れの問題かもしれない。

②アドレス帳の管理

アドレス帳の管理は、管理側が作成している企業と、ユーザー任せの企業と2系統あるようだ。全社共通的なアドレス（部長、課長一覧）は管理側が作成しておくべきであろうそれによって便利さは非常に違ってくる。アドレス帳をホームページに載せている企業もある。

③アドレスの統一

インターネットを早くから個人的に使用していた人は、Eメールエイリアスをそのまま社内のイントラネットで使用している。taro、hana 等ニック ネーム的に付けている場合は社内では適さないことがある。社内業務として電子メールを使用する場合、社内統一されたルールがあった方がよい。taro、 hana が新入社員なら誰だかわからない。エイリアスには姓を入れた方がわかりやすい。

田中 一太郎 の場合、フルネーム ichitaro.tanaka＠aaa.co.jp が長ければ姓を入れ i-tanaka＠aaa.co.jp とするなど工夫する。社員数が多ければエイリアスはバッティングするが、それはまたルールを作ればよい。

もう一つ問題になることにサブドメインがある。人事異動があったときに特に問題になる。
サブドメイン bbb : taro.tanaka＠bbb.aaa.co.jp

ネットワークの管理から言えば、サブドメインを付けて、余計なトラフィックを出さないことである。しかし人事異動があると、異動した先のサーバーにアドレスを移すかどうかが問題になり、その手間は大変である。名刺等のアドレス表示も変えなければならない

人事異動等の影響をなくすためには、サブドメインを付けない企業もある。そうすると国際的な企業は日本 国内に送信するにも関わらず、ネットワーク的には非常に無駄なことであるが、いったんアメリカのサーバーまで行ってから日本に戻って来るような使い方をし ているケースもある。うまい解決策がなく、今後のディレクトリサービスが技術的解決をしてくれるものと期待する。

(3)OSやハードウエア等の選択(判断)の基準

1)サーバー選択(判断)の基準

サーバーとして主要な選択(判断)の基準をあげ、PCベースのOSとWSベースのUNIXでの比較を行い、どのような特徴があるのかを述べる
(表1－2－1)。

表1－2－1

表1－2－1　サーバー（OS、ハードウエア）選択規準

OS / 項目	PCベースのOS (Windows NT server / NetWare 等)	WSベースのUNIX	要約
機種	・本体が一般的に低価格である。 ・アップグレード用のパーツの増設・交換が可能である機種選択が望まれる。	・本体が一般的に高価格である。 ・アップグレードは本体交換。	
UPS (無停電電源装置)	・管理アプリケーションが標準サポート。	・UPSに管理ツールがある。	・電源に関わるトラブルからデータを守る。 ・瞬時電圧低下影響防止策としても必要。 ・価格も低下している。
バックアップ	・OSにバックアップツールがバンドルされている場合が多い。 ・DAT、DLTなど本体に組み込みが一般的。	・基本的に管理者がコマンドベースで設定/スケジュール。 ・外付け装置が一般的。 ・多種多様な装置がある。	・人為的、機械的ミスからデータを守る。 ・バックアップスケジュールは、平日は差分バックアップ、休日はフルバックアップが望まれる。 ・ユーザーデータのみを対象とすることで、バックアップ時間を短縮できる。
設定・管理	・全てGUIで可能。 ・ヘルプ機能、書籍が充実。 ・市販アプリケーション・ソフトウェアが豊富であり、低価格である。	・UNIX技術者が必要。 ・一部GUIで可能。(基本はコマンドベース) ・ヘルプ機能はあるが、UNIX専門知識が必要。 ・より高度で柔軟な設定・管理が可能。 ・市販アプリケーション・ソフトが少なく、しかも高価格である。フリーウェアソフトが充実している。	・GUI、ヘルプ機能が充実している設定・管理が望まれる。
トラブル対応(ソフトウェア)	・システムトラブル対応は、保守契約あるいは有償である。	・システムトラブル対応は、保守契約あるいは有償である。	・保守サービスを契約する方法がある。
トラブル対応(ハードウェア)	・パーツが低価格であるため、予備品を確保して置きやすい。 ・耐久性の面で信頼性に　欠ける。	・パーツが高価であり、交換時には専門知識が必要。 ・耐久性があり信頼性がある。	・保守サービスを契約する方法がある。

2)クライアント選択(判断)の基準

ブラウザが最適に動作するために必要なクライアントの選択基準として主要な項目をあげ、基準となるべき内容を述べる(表1－2－2)。

表1－2－2

表１－２－２　クライアント（ＯＳ、ハードウエア）選択規準

	基準
機動性	営業マンなどは、席にいることがないためノート型 PC が良い。さらに、外出先からのアクセスのためにモデムが必要。
OS	操作性、機能面で最新版が望ましいが、業務アプリケーションの動作確認が必要。
ハードディスク容量	OS とアプリケーションのみの容量。ユーザーデータは、サーバで一括管理。メンテナンスやバックアップの面でメリットがある。
CPU とメモリ容量	使用OSおよびアプリケーションの推奨動作環境を基準とする。一般的には16MB以上。
モニター	画面が小さ過ぎては見づらく、大きすぎては場所をとるため、15～17インチ程度を基準とする。

今後はNC（Network Computer）などの動向にも注意が必要である。またWWWサーバーそのもののパフォーマンスはさほど問題ではなく、むしろネットワークやファイル及びDBアクセスを行うアプリケーションのパフォーマンスに注意が必要である。

（4）ネットワーク機器及び環境整備

イントラネットは、ネットワークへの負荷がかけやすい傾向にある。イントラネットを構築するソフトウエ アが、アクセス手段として Web ブラウザを前提にしている場合が多くいとも簡単にリンク先の画像（静止画／動画）、音声等の大量なデータをネットワークに 流れてしまう。したがって、エンドユーザーの視覚的・操作性には有効であるが、ネットワーク構築には注意が必要である。

そこで、ネットワークを構築・拡張する場合の構成を述べ、それぞれのネットワークの概要を説明する。

1）ハブ（集線装置）による基本ネットワーク

クライアントとサーバーをハブへ接続する最も基本的なネットワーク構成である。ハブと端末間は 10BASE-T 規格のケーブルを使用する。（図1－2－1）

図１－２－１　ハブによるネットワーク構成図

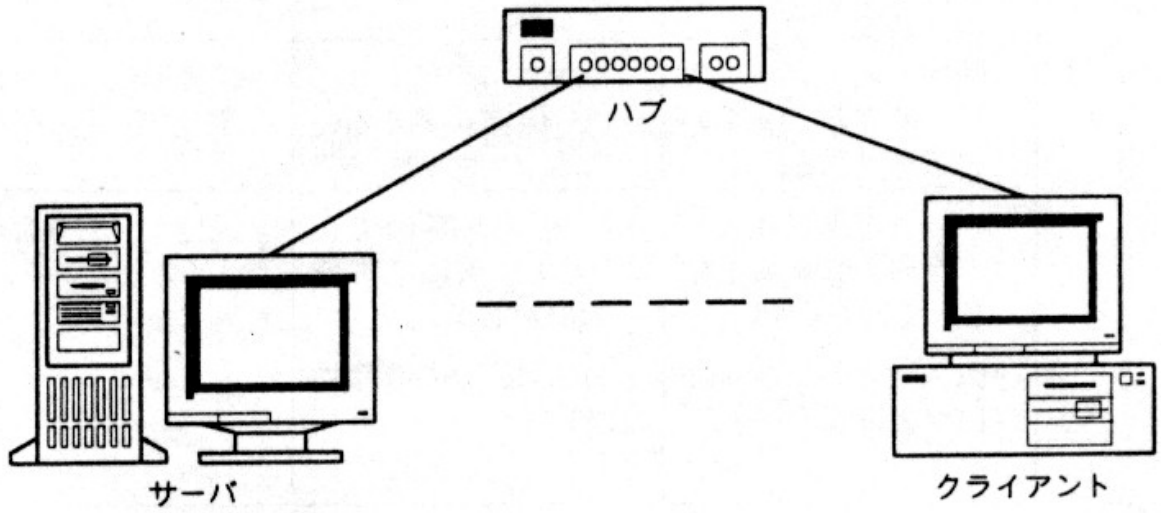


図1－2－1

2)マルチポートトランシーバによる基本ネットワーク

クライアントとサーバーをマルチポートトランシーバへ接続する、最も基本的なネットワーク構成である。マルチポートトランシーバと端末はトランシーバケーブルを使用する（図1－2－2）

図１－２－２　マルチポートトランシーバによるネットワーク構成図

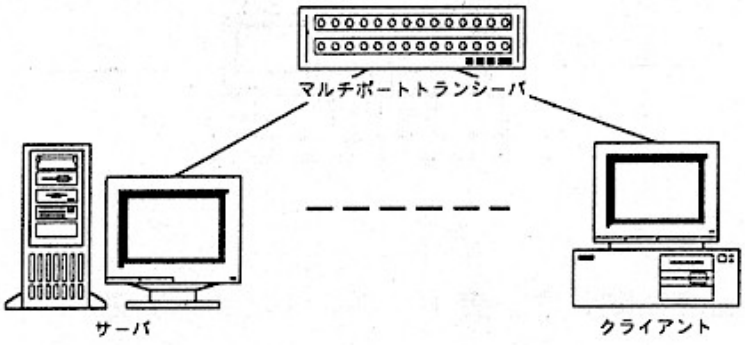


図1－2－2

3)ブリッジによるネットワーク拡張ネットワーク

ハブ(集線装置)による基本ネットワークあるいは、マルチポートトランシーバによる基本ネットワークを拡張するネットワーク構成である。ブリッジ接続は 10BASE-5 規格のケーブルを使用する。(図1－2－3)

図1－2－3　ブリッジによるネットワーク構成図

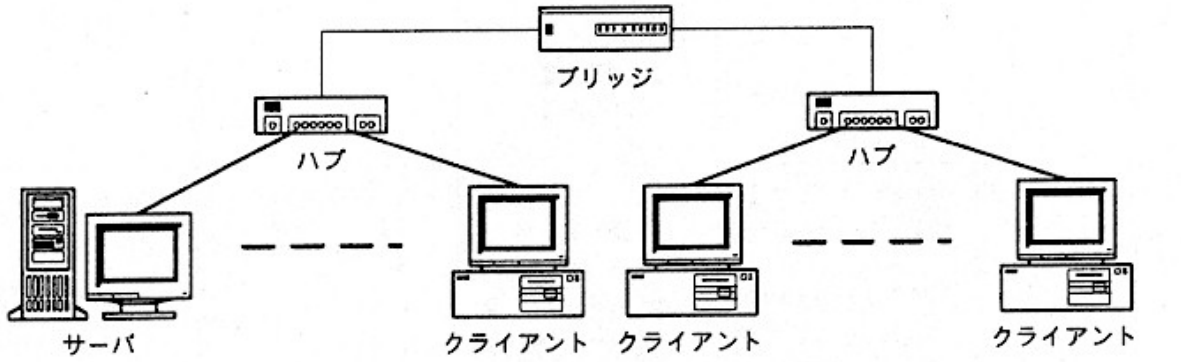


図1－2－3

4)ルータによるネットワーク拡張ネットワーク

ハブ(集線装置)による基本ネットワーク、あるいはマルチポートトランシーバによる基本ネットワークを拡張するネットワーク構成である。ルータ接続は 10BASE-5 規格のケーブルを使用する。

各ネットワーク構成に関して、(表1－2－3) にまとめる。

表1－2－3

各ネットワーク構成に関して、表1－2－3にまとめる

表1－2－3　ネットワーク構成概要

	特徴	留意点	拡張目安	価格
ハブ	・接続口の増設は、カスケード接続(ハブの下にハブを接続)。段数制限がある。 ・ネットワークは同一。 ・電気的ノイズ／エラーが全体に影響する。	・通常は10Mbpsであるが、100Mbpsもある。しかし、クライアント側で100MLANボード必要。 ・機器との接続は、扱いやすい10BASE-Tを使用。 ・接続距離(10BASE-T)は100M。	・接続端末数がハブの口を超える時。 ・ネットワークレスポンスが遅い時。 ・端末が分散され始めた時。	・10Mbpsは安価。 ・100Mpbsは高価。
マルチポートトランシーバ	・接続口の増設は、カスケード接続(マルチポートトランシーバの下にマルチポートトランシーバを接続)。段数制限がある。 ・ネットワークは同一。 ・電気的ノイズ／エラーが全体に影響する。	・機器との接続は、10BASE-5を使用。 ・接続距離(10BASE-5)は約50M。	・接続端末数がハブの口を超える時。 ・ネットワークレスポンスが遅い時。 ・端末が分散され始めた時。	・安価
ブリッジ	・ネットワークは同一。 ・電気的ノイズ／エラーをブリッジがおさえる。	・機器との接続は、10BASE-5を使用。 ・接続距離(10BASE-5)は約50M。	・ネットワーク管理を本格的に考慮した場合。	・高価
ルータ	・ネットワークは複数。 ・ネットワーク単位で管理可能。 ・ブロードキャストが全体に流れるのをおさえる。	・TCP/IP以外(Windows NT,NetWare等)はマルチプロトコル対応が必要。 ・ルータ動作設定が必要。	・ネットワークを更に分けたい時。	・高価

1．3　アクセス方式

(1)組織ネットワークへの接続

ここでは外部から組織(社内)のネットワークに接続されるケースについて、簡単な構成と、主な特徴を述べる。

1)専用線での接続

セキュリティ上は一番安全であるが、通信費が高価である。(図1－3－1)

図１－３－１

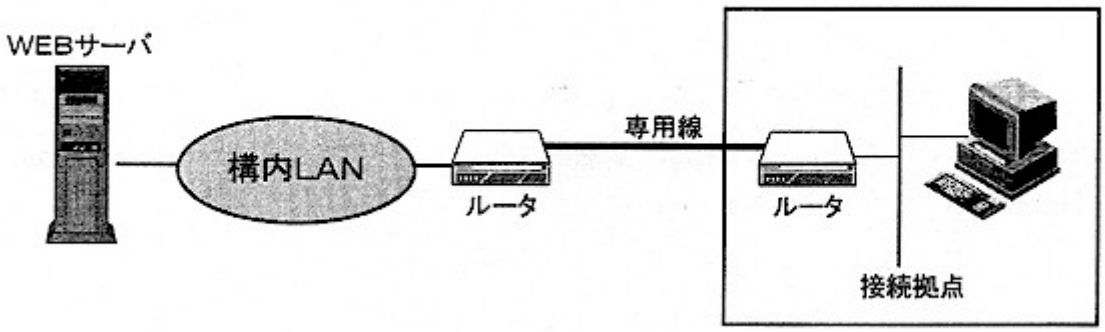


図1－3－1

2)アナログ公衆網での接続

接続方式としては最も容易であるが、パフォーマンスと距離によっては通信費も不利になるケースもある。(図1－3－2)

図１－３－２

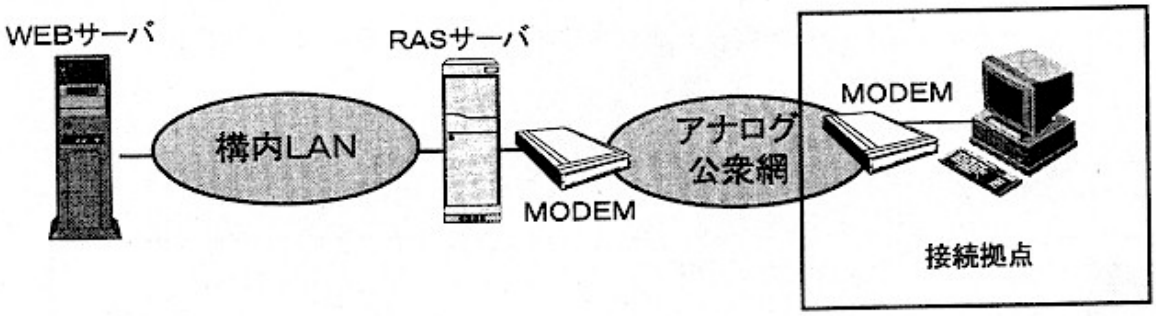


図1－3－2

3)ISDNでの接続

アナログ公衆網に比較してパフォーマンスは有利であるが、基本的には2)項と同じである。接続拠点にISDN接続口が必要。(図1－3－3)

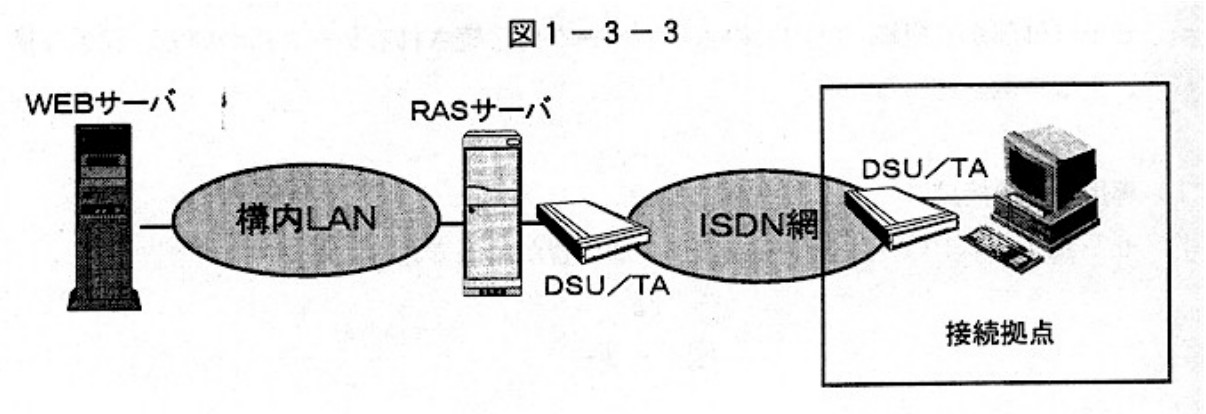


図1－3－3

4）ネットワークプロバイダのAP（Access Point）からの接続

最も近いAPを利用することにより、通信コストは有利であるが、ネットワーク使用料金を別途支払う必要がある。（図1－3－4）

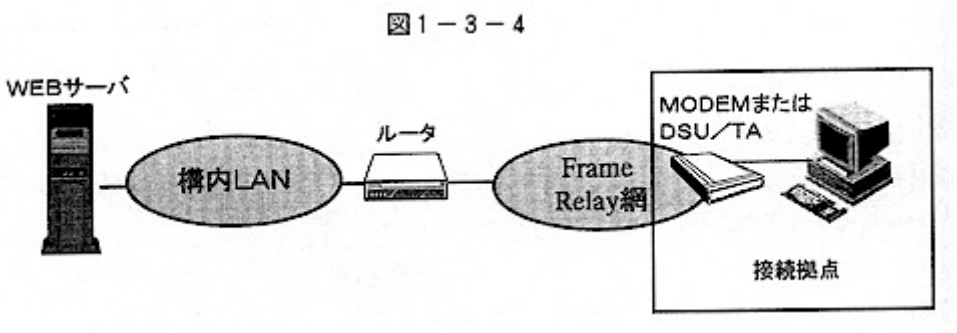


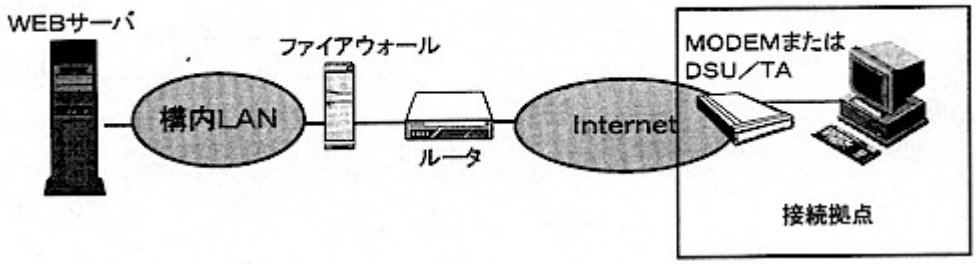
図1－3－4

5）インターネット経由での接続

インターネットプロバイダのAPを利用するが、ファイアウォールでIDを個別に認識するなどの技術が必要とされる。

表1－3－1にそれぞれの主な特徴を記載する。（図1－3－5）

図１－３－５



実際の商業活動がインターネットで行われるようになってくるなど、経済的にも重要な価値を持つ情報が取り扱われるようになってきており、一段とセキュリティ問題がクローズアップされてきた。

同時に、セキュリティに関する技術情報も数多く流れており、問題が発見されても迅速な対応が可能になってきたとは言え、未だにセキュリティ問題はなくならず、増えてきているのが現状である。

イントラネットのセキュリティは基本的にはインターネットのセキュリティと同一レベル、あるいは利用業務によっては、より以上のレベルで論じられるべきであろう。

2．1　セキュリティポリシー

（1）セキュリティの対象

対象（守るべきもの）としては、以下があげられよう。

- システムの安全かつ安定した稼働
- システムが保存している情報
- システムが処理する情報

（2）具体的対策

セキュリテイ対策の基本は、個々のシステムにおけるセキュリテイであり、カテゴリーとしては、下記があげられよう。

- アカウント管理：システムの入口になるログインを守る基本的な対策
- ファイル管理：必要な情報は関係者のみとし、他人に見せないことを徹底させる対策
- 通信管理：通信機器、マシンの接続が必要か否かを判断する対策
- ログ管理：システムにおけるアクティビティを監視する機構を導入し、ログを厳重に管理する対策

（3）ネットワーク環境でのセキュリティポリシー

ネッ トワーク環境では、自らのサイトのことだけではなく、ネットワークに接続された他のサイトに対する影響も考えなければならない。例えば、インターネットに 自由にアクセスできるモデムがあれば、それは侵入者の入口にされるし、セキュリティ対策をしていないサイトがあれば、それにまず侵入し、他のシステムに侵 入を試みる、いわゆる「踏台」にされる可能性

もある。ネットワーク環境におけるセキュリティポリシーで最も重要と思われるポイントは、「侵入されない／侵入されにくい環境を作る」ことである。

基本的には、以下のような方法がある。

- 不必要なネットワークサービスの停止
- セキュリティホールが報告されているツールは、即刻停止し、必要な対策を施す
- ファイアウォールを仕掛ける
- 裏口を作らない
- 認証なしのアクセスを可能とする機構は利用しない
- ネットワーク経由のモニタアクセスは、必ずパスワードを付け、不正アクセス排除する
- 不正アクセスが発生していないかどうかを常にチェックできる体制を整える
- ネットワーク管理外の機器が接続されることを防ぐ

インターネットに接続されている組織では、ネットワーク・セキュリティ対策を施すことは必須の作業であり、それを怠ることは、インターネットの他のサイト に対して迷惑をかけることがあることを充分認識すべきである。これらはセキュリティ教育をしっかり行うことも重要であり、2.7項にて、より詳細に触れ る。

2．2 論理セキュリティ

イントラネット構築において外部ネットワーク（インターネット）と内部ネットワーク（イントラネット）を明確にし、その上でシステムの技術導入を行うこと が重要であると考えられる。すなわち、イントラネットのセキュリティでは、外部と内部の間に構築するファイアウォール（防火壁）をいかに効率よく構築する かが重要となる。

（1）不正侵入に対する対策

不 正侵入に対しては「内部ネットワークの隠蔽、外部からのアクセスを制限に基づくパケットフィルタリング」により対処し、ネットワークの構成によりその構築 方法は異なるが、ルータやファイアウォールを使用したパケットフィルタリングにより、外部からのIPパケットに対してアクセスの許可・禁止を行う。また、 ネットワークサービスを提供するサーバーはアクセスの監視を行いログやレポートを残すようにする。

さらに、外部から内部へのアクセスを行う場合には認証技術や暗号化技術を導入することが必要不可欠となる。

- パケットフィルタリング :ルータ、ファイアウォール
- 認証技術及び暗号化技術

（2）システム上のセキュリティホール

不 必要なネットワークサービスは行わないようにし、セキュリティホールの確認されているツールやシステムの使用は避け、セキュリティホール情報を入手する努 力をすると共に、ベンダーから提供されるパッチは必ずあてるようにする。また認証なしのアクセスを可能とする機構（例えばUNIXのリモートコマンド）は 利用しないようにする。

プライベートなIP接続やダイアルアップIP接続はネットワークの裏口となりうるネットワークサービスなので、このサービスを行う際には認証やアクセスに 対して細心の注意が必要であり、認証・暗号化・データのカプセル化等の技術を実装したファイアウォール間の通信技術VPN（Virtual Private Network)の導入をすべきであろう。具体的にはセキュリティ・チェック・ツールを導入し下記を実行する必要がある。

- 不必要なネットワークサービスの排除
  RPC（Remote Procedure Call)、TFTP、NIS、NFS
- OS及びアプリケーション、ツールへのパッチあて
- イントラネットへのアクセスには必ず認証を設ける
- 内部監査 :システム設定ファイルなどのチェックセキュリティポリシー
  COPS（Computed Oracle and Password System)
- 外部監査 :外部ネットワークからイントラネットを攻撃してチェック
  ISS（Internet Security System） 、SATAN（Security Administrator Tool and Analyzing Networks ）

（3）コンピュータウイルス／ワーム

コンピュータウイルスやワームに対しては、これまでネットワーク上の各クライアントごとで対策をとるしか方法がなかったが、1996 年秋から外部からのウイルスの侵入を監視できるサーバーアプリケーションがいくつか登場し（CheckPoint 社 FireWall-1 Ver.3、TrendMicro 社 InterScan Virus Wall 等）、ファイアウォール上でウィルス侵入を監視できるようになった。

インターネットの急速な普及の要因となったWWWサーバーやインターネットを利用する上で欠くことのできないDNSサーバー、メールサーバーなどについても言及すべきであるがここでは省略し、最後にネットワークセキュリティの重要項目をあげておく。

- パケットフィルタリング
- アクセス監視
- ファイアウォールサーバー
- 認証技術
- 暗号化技術
- VPN（Virtual Private Network)
- WWWサーバー
- proxy サーバー

・ DNSサーバー、メールサーバー（攻撃の対象となる代表的なサーバー）
・ ウィルス監視サーバー

その他、管理面で気をつけることとして、

個人使用のPCの管理
PCの個人使用者がかなり増えてきている現状より、PCがらみのトラブルも増えている。各個人で良識と責任をもって、管理してもらう教育が必要。

パスワードの管理
定期的に変更する。一般的な単語は使用しない。特殊文字との組み合わせ。手帳、メモなどにパスワードを記入しない。

対策の明確化
システム構築に際して、システムを明確化し、具体的にどのような
・ サービスを実現するのか（Web、E－Mail、電子掲示板等）
・ 不正アクセスから何を守るのか
・ フィルタリングを行うのか
・ 運用をするか（運用上のルールの設定）
・ 管理者、ユーザーの教育を行うのか
等を明確にしておく必要がある。

2．3 物理セキュリティ

サーバー／クライアント、PC、ルータ、ケーブルなどの機材を不正使用や外部からの衝撃などから保護するのが物理セキュリティであり、以下の方策があげられる

（1）第3者使用禁止

・ 担当者以外の人間にはマシンを使用させない
・ 席を離れる場合はロックスクリーン、ログオフをする
・ ID、パスワードによる保護、スクリーンセイバーもパスワードを必ずつける

（2）サーバー、重要なデータの保護

・ 入口に鍵のかかる部屋の中に置く
・ ICカード暗証番号などで入室時に入力させる
・ 入退室のログを取る
・ バックアップデータは別の場所で保管する

(3)ケーブル等の周辺機器の保護

ケーブル、プリンタ、ルータなどの周辺機器にはメールや重要なデータが流れているので、これらも保護の必要がある(スニフッィングの防止)。

(4)社内側からの不正アクセス

・ 部署やグループごとにルータやファイアウォールなどで保護する
・ ユーザーID パスワードによるユーザー単位で保護する

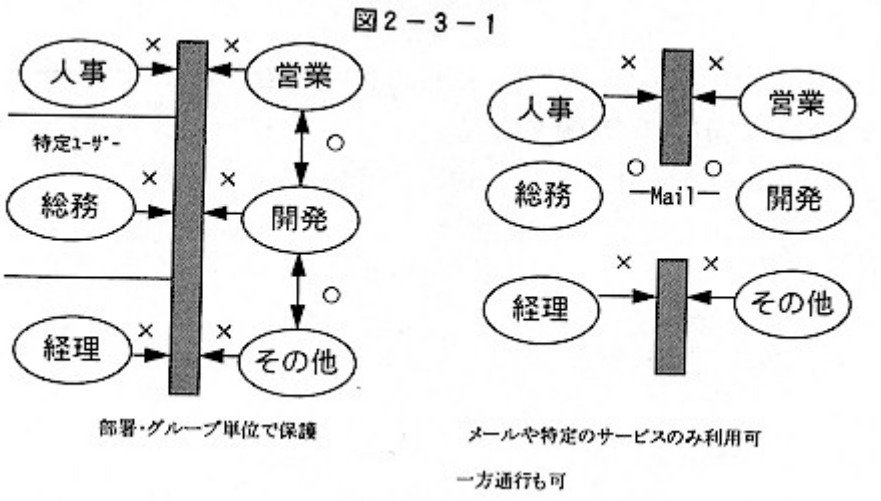


図2－3－1

(5)社外からの不正アクセス

・ ルータやファイアウォールなどでポート単位に保護する
・ マシン上でユーザー認証、ウィルスチェック、ルータ・ファイアウォールにてフィルタリングを行う
・ Proxy サーバー経由でのアクセスも、マシン上でユーザー認証を行う。Anonymous FTP も同じ方法
・ ルータの位置、台数、ファイアウォールの位置／組み合わせ、公開サーバー、非公開サーバーの区分にも充分留意する。

図2－3－2、図2－3－3、図2－3－4 を参照。

2．4 ファイアウォール

(1)ファイアウォールとは？

1)インターネットの危険性

インターネットに接続すると膨大な情報に簡単にアクセスできるようになる。しかし裏を返すと、外部からも自分の領域に簡単にアクセスできてしまうことを意味している。そのため悪意の第三者による脅威から、

- データ:コンピュータ上の情報
- 資源:コンピュータそれ自身
- 信用

といったものを保護することが必要になる。

データについては言うまでもないが、機密情報の盗用をはじめデータの破壊や改ざんから守る必要がある。

資源としては、CPUタイムやディスク領域をはじめシステムそのものも守る必要がある。

また侵入者が内部ユーザーを偽って他の組織に侵入したり、他社との取り引きのための重要なデータなどが破壊されれば、信用の回復は非常に困難なものとなる。

2)基本機能

このようなインターネットの危険性と利点とのバランスを取る手法の一つがファイアウォールである。

ファイアウォール(防火壁)は本来、隣家の出火が自宅に燃え移らないためのものであるが、インターネットファイアウォールは、インターネット上の脅威が内部のネットワークに及ばないようにすることが主な目的であり、以下のような基本的な機能を持っている。

- 内部に攻撃者が入り込むのを禁止する
- 外部の攻撃から内部を保護する
- 内部から人が出ていくことを監視する

(2)実現方式

このようなファイアウォールの基本的な機能は、隘路(Choke Point)によって実現する。隘路とは、狭い道という意味の言葉である。インターネットと内部との間を行き来する際に、必ずそこを通過するためチェックや規制を容易に行うことができる。

この隘路においてチェックや規制を実現する方式は次の3つに分けることができる。

- パケットフィルタリング
- アプリケーションレベルゲートウェイ
- その他

1)パケットフィルタリング

パケットフィルタリング方式とは、インターネットの通信プロトコルであるIPのパケットの内容によって 規制を行う方式である。送信元や送信先のIPアドレスや、TCP／UDPのポート番号に応じて通信を許可したり禁止したりできる。柔軟性が高く多くのイン ターネットアプリケーションで使用できる反面、設定に注意しないと穴を生じやすい。またIPパケットレベルでのフィルタリングであるため、アプリケーショ ンの特性に応じた高レベルでのセキュリティ設定はできないが、一般に処理が高速だといわれている。最も基本的なパケットフィルタリング方式のファイア ウォールはルータでも構築できる。

2）アプリケーションレベルゲートウェイ

アプリケーションレベルゲートウェイは、一般に Proxy とも呼ばれるもので、HTTPやFTPといっ た特定アプリケーションのゲートウェイでインターネットと内部を接続する方式である。ゲートウェイがあるアプリケーション以外の通信は完全に禁止され、さ らにインターネットとの通信はすべてゲートウェイプログラムが行うので、内部に侵入することはかなり困難になる。ただし、最新のアプリケーションや独自の アプリケーション、マイナーなアプリケーションなどでは、ゲートウェイプログラムが入手できないか、入手までに時間を要する場合がある。

3）その他の方式

最近では、パケットフィルタリングをベースとしながら、アプリケーションレベルゲートウェイと同等のセ キュリティレベルを実現する方式も現れている。この方式では、パケットの内容をアプリケーションのレベルまで解析し、かつ前後に通過するパケットの内容も 照合することで実現している。

（3）ファイアウォールのテスト

ファイアウォールを設置し、設定を行った後、設定が正しく動作しているかを検証するために、テストを行 うことが必要である。テストには、Telnet やFTPといった実際のアプリケーションで行うことができるが、その場合、すべてのアプリケーションについ てテストすることは現実には困難である。

より確実に設定を確認するためには、ファイアウォールを検査するためのツールを利用する。このような ツールは、一般にセキュリティスキャナと呼ばれ、フリーウェアや市販製品が存在する。セキュリティスキャナは、TCP／IPのポートをしらみつぶしに チェックしたりOS等の既知のセキュリティホールを利用して侵入を試み、結果をレポートとして出力する。このようなツールでテストすることにより、ファイ アウォールの設定の誤りだけでなく、ファイアウォールソフトウエア自身の不具合等によるセキュリティホールや、ファイアウォールが動作しているOS等の問 題に起因するセキュリティホールまで検出することが可能になる。

主なセキュリティスキャナは、以下のとおりである。

フリーウェア

- SATAN
- ISS フリーウェア版

製品

- ISS Security Suite（米国ISS社）
- PINGWARE（米国 BELLCORE 社）

(4)ファイアウォール製品の概要

ファイアウォールは、当初は製品がなく、ルータのコンフィグレーションでフィルタリングを行ったり、フリーウェアを利用して構築されていたが、現在では多くの製品が発売され、より簡単に高度なファイアウォールを構築することが可能になっている。

発売された当初は、単純なパケットフィルタリングや基本的なゲートウェイで構成されていたが、イントラネットの拡大に伴い、イントラネット間をインターネットを使って接続するエクストラネット構築のためのVPN（Virtual Private Network）機能、リモート端末をインターネット経由でイントラネットに接続する機能などを持つ製品も次第に増えている。また、イントラネット内の機密情報を扱う部門を保護するためのファイアウォールなども一般的になりつつある。

1)製品形態

製品の形態は、次の3種類に分けられる。

- ・一般OSソフトウエアパッケージ
- ・独自OS付きソフトウエアパッケージ
- ・独自ハードウエア

一般OS用ソフトウエアパッケージは最も一般的な形態で、ハードウエアメーカーが自社マシン用に出荷している通常のUNIXや Windows NT といった汎用のOS上で動作する製品である。

独自OS付きソフトウエアパッケージは、ファイアウォール用に不要な機能を削ったりOSのセキュリティ ホールを塞いだりするなど、独自の改良を行った専用のOSと組み合わせて販売されている製品である。セキュリティ上は汎用のOSに比べて有利である反面動 作するハードウエアが限られる。最近では、通常の一般OS用ソフトウエアパッケージであってもOSの一部を独自に置き換えたり不要な部分を停止するなどし て、セキュリティを向上させる製品もあり、独自OS付きソフトウエアパッケージのセキュリティ面での優位性は薄れつつある。

独自ハードウエア製品は、ハードウエアに組み込まれた形で販売されている製品で、高度なセキュリティを 実現するために専用のハードウエアと組み合わせて販売されているものと、

ルータをはじめとする各種の機能と組み合わせてハードウエアに組み込まれた簡易で 安価なファイアウォールなどがある。

2)プラットフォームOS

ファイアウォールが動作するプラットフォームとなるOSとしては、UNIXもしくは Windows NT がほとんどである。Windows NT で動作するファイアウォール製品は 1996 年中頃から増え始め、従来、UNIXで開発されてきた製品もNT版を入手できるようになっている。また、最初からNT のみを対象として開発されている製品も出てきている。当初 NT 版の製品はUNIX版に比べて機能が劣っていたり安定性に欠けたりするものが多 かったが、その差は次第になくなりつつある。

3)ハードウエア

UNIXをプラットフォームとする製品のほとんどは、特定ハードウエアメーカーのマシン用のものである。あまり数は多くないが、PC上のUNIXをサポートしているものもある。Windows NT をプラットフォームとする製品のほとんどはPC上で動作する。

(5)ファイアウォール製品に必要な機能

1)アクセスの制限

ファイアウォールの最も基本的な機能は、内部のネットワークを外部から自由にアクセスさせないためにア クセスを制限する機能である。より高度なセキュリティが要求されるケースでは、内部から外部へのアクセスも制限することが必要になることもある。ファイア ウォールには、必要とされるセキュリティポリシーを確実に実現する機能が要求される

2)内部ネットワークの隠蔽

外部からの侵入を防ぐためには、内部のネットワークの構成や、ユーザー情報、ホスト名、ホストのIPア ドレス等の内部情報を公開しないことが重要である。ファイアウォールは、これらの情報にアクセスできないように構成する必要がある。例えば、パケットフィ ルタリング型の製品では、内部IPアドレスを隠蔽するためのNAT機能は必須であろう。

3)侵入時の被害の低減

ファイアウォールは、侵入を困難にして侵入までの時間を稼ぎ、侵入の検出の機会を増やす。また侵入に必要な労力を増大させることによって、侵入によって得られるものに対して侵入を割の合わないものにできれば、侵入の可能性をかなり低くすることができる。

4)アタックの監視と警告

通常、外部からのアクセスはすべてファイアウォールを通過するため、外部からの侵入を検出するのに最も適している。外部からの侵入の試みを検出し管理者へ迅速に通報できる機能が望まれる。

5)ログとレポート

内部と外部との間の通信状況をログとして記録しレポートとして出力することは、危険性を事前に把握したり、侵入が発生したときの経路や手段を特定するためにも重要な機能である。

(6)ファイアウォールに今後必要とされる機能

1)暗号化

インターネットによるイントラネットの拡張であるエクストラネットを実現するために最新のファイア ウォール製品では暗号化をサポートするようになってきている。本来別々のネットワークを、インターネットを経由してファイアウォール間を暗号化された安全 なコネクションで接続することにより、1つのネットワークとして利用できる、いわゆるVPN(Virtual Private Network)の機能である。

また、他のファイアウォールとの間だけでなく、リモートクライアントとの間をインターネット経由で接続し、安全に内部ネットワークを利用するといった機能も一部の製品では実現されている。

2)各種認証方式への対応

ファイアウォールを通過する際に利用者を特定し、許可された利用者のみが通過可能とするようなセキュリ ティポリシーを設定する際、ユーザー名やパスワード等によるユーザーの認証に各種の外部システムが利用可能になってきている。トークンカードや同等のソフ トウエアを利用したワンタイムパスワードによる認証システムや、リモートアクセスサーバー用の認証情報を利用したりすることが可能となってきており、セ キュリティの向上や管理性の容易化が図れるようになってきている。

3)ウイルス検出

インターネットの普及に伴ってウイルスの被害も急増している。そのようなウイルスの侵入を水際で食い止 めるために、ファイアウォール上でウイルスを検出し侵入を防ぐことが必要になってきた。一部のファイアウォール製品では、ファイアウォール上を通過する電 子メールや各種のファイル等のデータをスキャンしてウイルスを検出し侵入を阻止する機能を持つようになってきており、今後は必須の機能になってくると思わ れる。

4)内部ファイアウォールと集中管理

人事部門や研究開発部門といった、より機密性の高い情報を扱う部署をイントラネットに接続する際に、他 の部門との間にファイアウォールを導入するなどの措置が必要になるこのような内部的な利用のためにも、通常のファイアウォールを利用することも可能である が、内部利用に目的を絞ることでより安価で、かつ複数のファイアウォールを集中的に管理できるような機能を持つ製品が増えてきている。

(7)主要製品

表2－3－1(主要製品)参照。

表2－3－1

7
(8) 主要製品

製品名 / 開発元	連絡先	OS/ハードウェアプラットフォーム
BlackHole Milkyway Networks	Info@milkyway.com	UNIX (独自カーネル) Sun / PC
BorderWare Secure Computing	sales@border.com	UNIX (独自カーネル) PC
Centri Firewall Global Internet	info@gi.net	NT PC
CyberGuard CyberGuard Corporation	info@mail.cybg.com	UNIX 独自、PC
AltaVista Digital Equipment Corporation	altavista-sales@altavista.digital.com	UNIX,NT WS, PC
Eagle Raptor Systems	info@raptor.com	UNIX,NT WS,PC
Firewall-1 Checkpoint Software Technologies	sales@CheckPoint.com	UNIX,NT WS,PC
Gauntlet Trusted Information Systems	tis@tis.com(us) info@eu.tis.com(non-us)	UNIX WS
GFX Internet Firewall System GNAT Box Global Technology Associates	gfx-sales@gta.com gb-sales@gta.com	独自ハードウェア
Guardian Firewall NetGuard Ltd.	info@netguard.com	NT,OS2 PC
Secure Network Gateway IBM	peter_crotty@vnet.ibm.com	AIX WS
PrivateNet NEC Technologies	info@privatenet.nec.com	BSD UNIX PC
Sidewinder Secure Computing	challenge.sidewinder.com	BSD UNIX / NT PC
SunScreen SPF-100 Sun MicroSystems	sunscreen@incog.com	専用ハードウェア

[出典先]
Web サイト

・National Computer Security Association
http://www.ncsa.com/

・Firewall Product Overview
http://www.waterw.com/~manowar/vendor.html

・Find the Right Firewall
--ZD Magazine, Janualy 27, 1997
http://www.zdimag.com/content/anchors/970127/1.html

・Behind the Line of Fire
--PC Magazine, December 17, 1996
http://www.pcmag.com/issues/1522/pcmg0058.htm

・Search For Intruders Fuels New Firewalls
--PC Week Online, December 16, 1996
http://www.pcweek.com/news/1216/16sea.html

・Firewall Comparision
--LAN TIMES、June 17, 1996 -- Vol. 13, Issue 13
http://www.lantimes.com/lantimes/toc/toc06s.html

・Internet Firewalls: Keeping Data Out Of Danger
--Inter@ctive Week, August 15, 1995
http://www.zdnet.com/intweek/print/950814/digitdev/doc2.html

書籍

- インターネットファイアウォール、アスキー
- ファイアウォール、ソフトバンク
- ファイアウォールを知る、トッパン
- ファイアウォール構築、オライリー・ジャパン
- イントラ＆インターネットセキュリティ、オーム社

２．５ 暗号化技術の要素

データの改竄や破壊、なりすまし、否認等の不正な利用が行われないようにするための技術として、データの暗号化技術がある。この暗号化技術はイントラネットだけではなく電子商取引などにも応用されている。

（1）公開方式と非公開方式

暗号化方式には、そのアルゴリズムが公開されているものと非公開のものがある。一見鍵とアルゴリズムの 両方によって秘匿が守られている「非公開方式」の方が信頼性が高いように思われるが、自分自身も知らないアルゴリズムなので、簡単に解読されるものかもし れない。逆に「公開方式」はアルゴリズムが公開されているにも関わらず十分暗号化方式として成り立っているということは、そのパラメータ解読の難しさによ る信頼性が十分にあるということが一般に認められていることを意味している。一般に用いられる暗号化方式は「公開方式」である。

（2）共有（秘密）鍵暗号方式

暗号化と復号化（暗号化されたデータを元に戻す）に共有（秘密）鍵を使用する方式である。この方式では通信する当事者間で同じ共有鍵を共有する必要がある。また、

・鍵を配布していない相手とは通信できない

・通信の当事者が多数存在する場合に、任意の2者間でも通信できるようにするには膨大な数の鍵が必要になる

などの問題点などがある。

（3）公開鍵暗号方式

共有（秘密）鍵暗号方式の問題点を解決するために考え出されたのが公開鍵方式である暗号化に公開鍵、復号化に共有（秘密）鍵を使用する方式である。公開鍵は誰の手に渡っても問題がないので鍵配布局に預けるなどして必要な人には自由に配布する。また、

・暗号処理に非常に長い時間を要するので、長いメッセージ（データ）全体を暗号化すると膨大な時間がかかる

などの問題点がある。

（4）共有（秘密）鍵暗号方式と公開鍵暗号方式の組み合わせ

公開鍵暗号方式の問題点を解決する方式として、共有鍵方式と公開鍵暗号方式を組み合わせた方式もある。公開鍵方式を利用する場合は、この方式を採用するのが一般的である

表2－3－2(一般ユーザーに対して必要な教育)

（1）一般ユーザーに対して必要な教育

対象項目	教育内容
パスワード及びユーザーＩＤ管理	ユーザーＩＤは、パスワードを必ず設定し、複数のユーザーで利用しない。また、利用しなくなったユーザーＩＤは、速やかにシステム管理者に届け出ること。 パスワードはユーザーＩＤ毎に設定し、随時変更する。また、紙媒体等に記述しておかない。
情報管理	重要な情報を送信する場合は相手先を限定し、宛先を充分に確認すること。 重要な情報は、盗用、改ざん、削除等されないように厳重に管理すること
コンピュータ管理	コンピュータを入力待ち状態状態で放置しない。また、持ち運び可能な携帯型コンピュータを使用する場合は、その管理に充分気をつける。
事後対応	不正アクセス等を発見した場合は、速やかにシステム管理者に連絡し、指示にしたがう。
情報収集	セキュリティ対策に関する情報を入手した場合は、システム管理者に随時提供する。

表2－3－3(部門管理者に対する教育)

（2）部門管理者に対する教育

教育対象	教育内容
管理体制の整備する教育内容	システム部門からのセキュリティー方針を周知・徹底すること
一般ユーザー管理	ユーザーＩＤの登録は、必要な機器に限定し、ユーザーの権限を必要最小限に設定すること。また、外部からアクセスできるユーザーＩＤは、必要最小限に設定する。 パスワード設定規則等を確立し、一般ユーザーに対し周知・徹底させる。
情報管理	重要な情報およびコンピュータ及び通信機器を維持、保守するために必要なファイルは、盗用、改ざん、削除等されないように厳重に管理すること。また、ファイルのバックアップを随時行ない、安全な方法で保管すること。
設備管理	重要な処理を行なう機器や移動可能な機器は、厳重に管理する。機器及びソフトウェアの導入・変更を行なう場合は、セ
	キュリティ方針に適合していることをあらかじめ確認してからおこなう。
履歴管理	システムの動作履歴、使用記録等を記録し、不正アクセスがないか随時確認する
事後対策	不正アクセスがあることが判明した場合は、速やかに原因を追求し、関係者と強調して被害の状況を把握し、さらに防止のするための処置をおこなうこと
情報収集及び教育	セキュリティ対策に関する情報を随時収集する。また、一般ユーザーにセキュリティを随時実施する。

２．６ アクセス制限

イントラネットをインターネットと接続したことによって、外部から組織ネットワークへの不正侵入が生じる可能性がある。また、社員など内部からの不正侵入により社内データの盗み見や改竄が考えられる。 これらの不正侵入を防ぐために、ネットワーク、ホストアプリケーション等にアクセス制限を設ける必要がある。

（1）オープンな接続

ホストと組織ネットワークの間では、何も制限せずに接続する。
セキュリティは組織内の各部門、各ホストの運用管理にまかされる。

運用管理事項
- ホストと組織のネットワークの間の回線の管理
- 組織のドメインのサーバーの運用管理

（2）ファイアウォールホストによる接続

ホストと組織ネットワークの間にファイアウォールホストを介して接続する。
アクセス制御がホストに集中している。

運用管理事項
- ファイアウォールホストの経路制御の管理
- ファイアウォールホストのDNSの設定
- ネットワークアプリケーションの設定
- ファイアウォールホストのセキュリティ対策

（3）アクセス制限を加えた接続

ゲートウェイのIPパケットフィルタリング機能を用いて、組織ネットワーク内の特定のマシンのみ通信を許可する。

運用管理事項
- 経路制御とDNSの設定
- 組織ネットワーク内の特定のマシンのセキュリティ
- フィルタリング機能の設定

（4）通信量抑制によるアクセス制限

1）スイッチを利用したバーチャルLANによるアクセス制限

スイッチを利用し、サーバーや端末を仮想的なグループにまとめる。グループ内のトラフィックはネットワーク全体には送出されず、グループ内部に閉じ込める。組織ネットワーク全体としてのネットワーク負荷が減り、セキュリティも高まる。

2）プロキシ・サーバーの設置

アクセスが集中し混雑しそうな部分や、回線速度の低い部分への接続部分に設置する

3)ミラーサーバーの設置

プログラムやデータを蓄えたFTPサーバーへのトラフィックを緩和するのに有効である。

(5)認証サーバーの設置

組織ネットワーク外部からの不正侵入に対するセキュリティ対策としてファイアウォールが普及している が、いったんファイアウォール内部に入れば、あらゆるリソースにアクセスができるようになる。ファイアウォールで防ぎきれない侵入や内部の不正アクセスを 防ぐために、認証サーバーを設置する。

1)ディレクトリ・サーバー

ユーザーの属性情報やリソース情報を複数のサーバーやドメインに渡って一元管理することが可能である。 システムを利用する権利のある正当なユーザーにはデータやプログラムの存在場所を教える「案内係」であり、権利のないユーザーにとっては不正利用を阻止する「警備員」になる。

2)認証サーバー

認証サーバーは、ユーザーに対して「本人に間違いない」という電子証明書を発行するユーザーは、この電子証明書とユーザーIDをディレクトリ・サーバーに提出し、アプリケーション・サーバーの利用許可を得る。

2.7 セキュリティ教育

従来の情報システムなら、システムに蓄積した情報の管理はシステム部門に任せておくことができた。しか しイントラネットでは違う。システムを利用するものすべてが責任を負わなければならない。企業の外部または内部からの不正侵入や個人のモラルにより、デー タの改竄や破壊、なりすまし、否認等の不正な利用が行われないように、キュリティ教育をしなければならない。ここでは一般ユーザーと部門管理者に対してど のようなセキュリティ教育が必要かを述べる。

(1)一般ユーザーに対して必要な教育

(2)部門管理者に対する教育

第3章　維持・運用

３．１ イントラネット運用コストの考え方

現在のように「イントラネット」が大きな注目を集めるようになったのは、費用が安いことが最大の原因だろう。事実、すでに社内LANを構築しPCを多数購入している企業であれば、WWWサーバーを構築するのにかかる経費は事実上0であるといえる。

しかし新しい投資が0であっても運用コストが0であるとは限らない。また、たとえコストが安価でも効果 があがらなくては意味がない。このことを誤解し、話題になっているという理由のみで「イントラネット」構築を行うのは無益であり、社内の情報化をかえって 阻害することになりかねない。このことをよく理解し、コストを正しく評価して効果と対比する目を持つことが効果的な運営に必要である。

（1）イントラネット≠安価

「イントラネット」の特徴として安価であることがよく強調されるが、これは必ずしも正しくない。確かに 新規機器の購入は通常は不要であるし、サーバー類も多くの場合はフリーウェアで十分賄える。このため立ち上げ時のイニシャルコストは劇的に安価にすませる ことができる。しかし保守・管理・情報作成のコストは通常のシステムとさして変わらないし、場合によっては通常のシステムよりコストがかかる場合もある。 また「イントラネット」といえども、業務に使用するのであれば盗聴や運用停止、データの紛失などへの対処を怠ることはできないはずである。

多くの場合、「安価にイントラネットを構築できた」事例では、社内や各事業部の「パワーユーザー」たちのボランティアによって運営され、構築されていることが多い。すなわち、費用が安くすんだのではなく、隠されているだけなのである。

例えば「イントラネット」で情報共有を行う際に最もよく使われるのはWWWシステムである。通常はこの システムで公開するデータは、HTMLと呼ばれるフォーマットで書かれている必要がある。しかしこのフォーマットは、すでに導入されているワードプロセッ サで編集・作成可能であるとは限らない。また既存のドキュメントをHTML形式に変換するのは、たとえ専用のツールを用いたとしても多くの時間を必要とす る。多くの場合は完全な変換を行えるわけではなく、いくらかの手作業が発生してしまう。またインターネット用サーバーの導入と運営は、ある程度の知識と基 盤がある人にとっては確かに簡単ではあるが、本当に誰にでもできるほど簡単なわけではない。

このように、「イントラネット」の優越点は安価であること自体にあるのではない。イニシャルコストが安価であることから、ボトムアップかつボランティアとして構築していくことが可能である点こそが重要である。

（2）ボランティアでのスタートから、基盤としての整備へ

社内コミュニケーション基盤が十分に機能しており、必要な情報が必要な部局・個人にスムーズに伝達され ていれば、イントラネットもグループウエアもまったく不要だと言ってよい。しかし現実には、市場の変化に迅速に対応できる柔軟な組織と柔軟な情報伝達を実 現できている企業は、いまだに少数にとどまっている。この原因をコミュニケーションの質、量、スピードの不足にあると考え、その変革を指向するのが社内情 報システム・イントラネットの真の狙いであろう。

そのとき、アクセスを義務化したり情報の提供を強制することでは、決して良質のコミュニケーションは生 まれ得ない。情報を持っている人が積極的に提供するような雰囲気が醸成されること、そして相互に自発的に協力し合うような文化を生み出すことが必要であ る。そして、この独特の雰囲気はボトムアップの動きによる方が生み出されやすい。

このため「イントラネット」も発足当初はボランティアベースで運営されることが予想されるし、またその方が自発的情報発信を促す効果を期待できる。しかし、すでに述べたように、「イントラネット」が安価であるのはあくまでイニシャルコストであって、運用コストはかえって高価になることもある。い ずれは業務として認定し、専従スタッフを設けることが継続的な社内コミュニケーション基盤の維持に必要である。もちろん専従スタッフといってもすべてをシ ステム部門が行うのではなく、利用者側に立った人間がシステム部門によるアドバイスを受けて調整・運用を行うようにすべきだろう。

（3）課金・情報流通促進のための対価の支払い

情報の流通を促進するために、「神の見えざる手」を利用する、すなわち情報に対する課金によって、いわば「情報の市場」を作り出し、流通を促進するという手法も存在する

一般にほとんどのサーバーソフトには、利用者のアクセスをカウントし、記録する機能が必ず存在する。これを利用すれば、例えばメールを送信した数や受信した数、WWWを見た回数などから課金することは、非常に簡単である。しかし、これはごまかしの入りやす い数字であり、妥当性の検証が難しい。無理にこの数字から課金するのは、不信感を無意味に煽る可能性がある。

また一つの会社の中という狭く閉じた世界のなかでは、通常は「神の見えざる手」は有効に働かないことが 多い。むしろ個人や社内組織が外部の情報を利用しなくなり、内部に自ら

の情報を溜め込む傾向を助長してしまう可能性が高い。このため課金という考え方は社 内ネットワーク運営においてはあまり推奨はできないと言える。

むしろ情報公開そのものは、インターネットにおける情報発信と同じように、ある種の広報活動であると考 えるべきだろう。個人や部門の実績を積極的に公表することにより、社内での評価やその次のビジネスへの足がかりとするという考え方である。このためには人 事評価などに個人の情報発信貢献度を取り入れるなどの方が、課金などの手段よりも役立つだろう。また、本社や総務部門などによる報奨金制度なども有効であ る。

3．2 イントラネット活用のルール

(1)ドキュメント内容のチェック

企業において扱われる情報は、そのほとんどが守秘の必要がある。単一サーバーへのアクセスであれば、そ こでのみ社員情報とセキュリティ情報を管理すればよいが、全社的なイントラネットの上では単一サーバーという運用形態は無理がある。このため複数の Web サーバーにわたって統一的・一元的にセキュリティ情報を管理する必要がある。また、それらセキュリティ情報は人事異動などに伴って迅速に更新されなくては ならない。WWWシステムは最近セキュリティを担保するための仕組みを実装しつつあるが、いまだに複数のサーバーに渡って一元的にセキュリティを保証する ための仕組みは一般的になっていない。

このため、厳密なセキュリティ管理が必要な場合には、現段階ではWWWシステムを利用するのは困難であると言える。そのような目的には、今のところ専用のグループウエアや暗号化されたメールを利用する方が安価で効果的だろう。

またWWWシステムはその特性上、誰もが自由に情報を発信できる。そのため守秘の必要がある情報が不用 意に漏らされてしまうことも少なくない。しかし、それを恐れるあまりに上司による査読や許可を何重にも必要とするシステムを構築していたのでは情報発信が 円滑に進まず、結果的に役に立たないシステムができあがってしまう。

これらの問題に対してコストと効果の兼ね合いから考えると、情報作成者・発信者の署名と、直属上司の許可及び署名を義務づける程度が妥当だと考えられる。直属上司の許可であればそれほど時間的なコストはかからないし、自分及び上司の2人によるチェックがあれば、十分効果的にチェックすることができるだろう。

どのような制限をかけるとしても、また情報共有システムがあろうとなかろうと、情報の流通／開示／守秘 に関してはなんらかの社内ルールが必ず必要である。おそらく、すでに多くの企業では社内的にそのようなルールを設定ずみであったり、社員規則の援用で補っ て

いたりすることと思われる。しかし、いまだに明確なルール化がなされていない企業では、明示的な「情報管理規則」のようなものを定めておくことが望ましい。

（2）著作権の啓蒙と教育

企業内のネットワークも、多数の人間に対して公開された場であるから、著作権については十分に留意する必要がある。特に社外ネットワークや一般図書からの記事や写真の取り込みは安易に転載されることが多い。これは特にそれら著作物に転載可能であるとか著作権フリーであるとかという断りがない限り、明白な著作権法違反である。著作権意識はネットワークに限らずコンピュータ時代の大きな問題であり、十分な教育・啓蒙活動を継続的に行わなくてはならない。また、そのようなトラブルを未然に防ぐためのルールも必要である。

（3）ドキュメント規格の必要性

インターネットの世界では、今もWWWシステムは進化を続けている。特に最近では Java や ActiveX といった新世代のテクノロジーも進境が著しい。しかし全社的な情報共有にスコープを絞ったシステム構築は、そのような要素はなくても充分可 能である。むしろそのような過渡期のテクノロジーの採用はWWWシステムのオープン性を削ぐ場合があるこのため、情報共有までをスコープと置くようなシステムではより一般的な、HTMLドキュメントの共有にとどめる方がよいだろう。またHTMLの規格もあまり新しいものを採用する必要はなく、HTML2.0 規格などで充分である。

また情報の個人による発信が活性化したとき、多種多様な情報は無秩序に発信され、巨大な迷路を構成する 可能性が高い。多様な情報が無秩序に蓄積されただけでは、必要な情報を必要なときに探し出し、利用することは不可能である。このため各社の次世代の Web サーバーは検索機能を備えることを宣言している。またドキュメントに標準や規格を設定することで再利用性を上げられる。

（4）「ネチケット」

ネットワーク上でのコミュニケーションは基本的には文字のみにて行われ、互いの表情や細かな感情を読み 取ることは難しい。このため些細な行き違いが大きなトラブルにつながることも珍しくない。このようなことを避けるため、社内ネットワークによる情報流通促 進を図るときには事前になんらかの指針や指導書などで教育や啓蒙を行うことが望ましい。

インターネット上でもこれらの要因から、よく感情的な問題が起こっている。そのなかから生まれてきた暗 黙のエチケット集的なものとして、RFC 1855 に「ネチケットガイドライン」というものが規定されている。これは全く強制力を持たない文書であり、従う必要性もなければ強制力もない、そして書いてある ことは当たり前のことばかりである。しかしネットワーク上では、

対面での会話では起こり得ないようなことがしばしば発生する。事前に読み、留意しておく価値のある文書といえるだろう。

3．3 コンテンツの維持管理

ここでは、WWWのコンテンツの維持管理に関して述べてみたい。
まずWWWサイトの運用管理における本コンテンツ維持管理作業の位置づけを整理してみる。

(1)コンテンツの維持管理の位置づけ

図3－3－1に 示すように、コンテンツの維持管理はWWWサイトで保管管理される情報の管理を示す。つまり、WWWサーバー、ネットワーク、各クライアント等、システム を運用するためのシステム運用／保守管理がどちらかと言えばWWWのインフラ面の管理項目であるのに対して、コンテンツ維持管理はその中の“情報”そのも ののの運用管理である。

図３－３－１　WWWサイトの運用管理

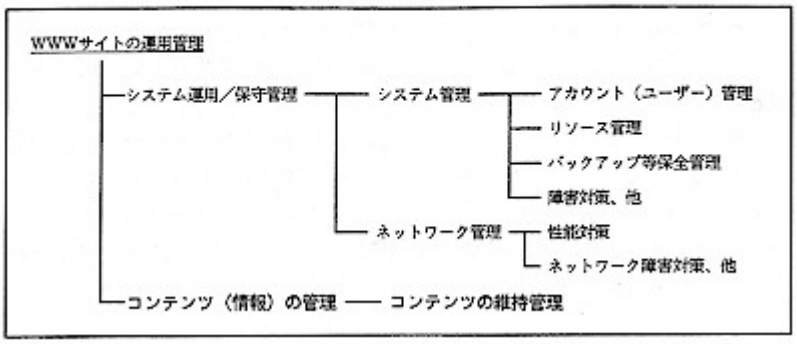


図3－3－1

(2)コンテンツ維持管理作業

次にコンテンツの維持管理における具体的な作業項目を考えてみたい。
一般的なWWWサイトで必要なコンテンツ維持管理作業と、その課題／問題点等について以下に列記する。

1)コンテンツ製作作業

主にエンドユーザーによるコンテンツの作成／編集作業を示す。ここでの課題としては最終的なHTMLを意識せずに文書を作成／編集するツールの選定等がある。

コンテンツの作成方法は、WWW普及以前からのエディタ等によるHTMLファイルの編集作業から昨今の ワープロソフト等が提供する便利なHTML文書生成機能の利用と、さまざまな手段が選定可能であるが、ホームページ作成の専門業者等を除き、一般企業のエ ンドユーザーを想定した場合には、ユーザーに極力HTML等を意識させないツールの選定が妥当であり、すでにその商品が存在する。また、社内のツールの標 準化等も考慮したツールの選定が必要と思われる。

2)コンテンツの更新作業

コンテンツの更新作業も、1)コンテンツ製作作業同様に、編集作業が容易なツールの選定等に関わる問題 が大きいと思われる。特にニュースソース等、日々更新されるホームページを管理する新聞社、出版社においては、情報の更新管理を容易にする独自の文書管理 環境を構築し、WWW環境との連携を実施している事例もある。

3)コンテンツ製作／更新の承認管理作業

エンドユーザーが作成したコンテンツをそのままサーバーに登録・公開してよいか、あるいは定められた承 認部門の了解後に登録・公開すべきかの問題は、コンテンツ情報の内容及び公開するWWWの役割等によるものであろう。しかし承認管理が必要な運用においては、ワークフロー的に作成したコンテンツが制作部門承認部門登録・公開へと流れる情報システム自体の仕掛けづくりが必要となる。

4)コンテンツのステータス管理

ここで言うステータス管理とは、個々のコンテンツが広く公開されている“生”の状態であるのか、または古い情報で廃棄されるべき“死”の状態であるのかを管理することを示す。

事例として、某出版社ではWWWで公開するさまざまな雑誌の記事トピックスやニュース情報等に対し「公 開前」「公開（中）」「廃棄」といったステータス管理を効率化させるため、コンテンツ作成時にそのコンテンツの公開日、廃棄日等を登録する文書管理システ ムをWWWサーバー内に構築し、CGI等のインタフェースを利用して指定日に該当情報がWWWサーバーに登録できる環境を構築している。もちろんコンテン ツは上記以外に更新されるため、これらの改廃管理も場合によっては必要となるケースもあり、この場合にはデータベースでの文書の改廃管理との連携機能等が WWWシステムに必要になる。

5)コンテンツのアクセス管理（鮮度管理）

ここで言うアクセス管理とは、コンテンツ自体がどれだけのユーザーに検索されているか、また、そのアクセス数が日々どのように推移しているかといった、各コンテンツの鮮度を管理することを示す。

前述の出版社の事例では、アクセス数の多い記事等をカテゴリーごとに分類・集計する機能をシステム化し、WWWホームページへのアクセス情報から現在の読者の興味分野や人気商品等の情報入手に役立てている。

6)コンテンツへの検索等ツールの提供

最後に検索等ツールの提供とは、さまざまの情報を持ったWWWサーバーが立ち上がった状況下での必要情 報の検索ツールを示す。つまりWWWで一般的な外部の検索サーバー相当の機能はもとより、イントラネットの対象となるすべてのWWWサーバーコンテンツの情報を、できれば統合的に検索できる検索ツール及び検索環境の提供を、構築の際に一考する必要がある。しかし現状では統合的なWWWの検索システムを安価 に入手できず、したがって基本的なアプローチとしては、RDBMS等により検索情報を管理し、実情報は各WWWサーバー内で管理するシステム形態がある が、コンテンツの更新と本RDBMS情報の同期等を考慮したシステム構築が必要である。

以上、コンテンツ維持管理について簡単な事例を交え論じたが、実際の適用に際してはユーザー個々の運用規模、必要機能、開発／管理リソース(人、物、金)に合ったシステム整備のための計画が必要であり、応分の投資を覚悟する必要がある。
オープンシステムの拡張性を生かし、維持管理項目をプライオリティを元に順次実行することが現実的な回答であると思われる。

3．4 操作教育

(1)管理部門での教育(情報システム部門)

会社方針に沿ってイントラネット技術をどのように進めていくかを決め、必要技術を習得し、各部門でのホームページ作成時協力して作成し、同時に各部門で維持ができるように教育を行う。
また利用部門に対しては正しい利用方法の教育を実施する。

＊管理部門で作成する教育マニアル
・利用部門教育マニアル
・維持管理部門への運用基準教育

(2)ホームページ維持部門での教育

1)ホームページ維持部門は、初めはホームページを作った経験のある部署と協力してベースとなるものを作り、それをもとに自部門でバリエーションをつける改善を行う。習うより実施してみることが必要である。

2)コンテンツの維持ルールと担当者を決め、マニアルの作成を行い、後任者への教育を行う。
・情報収集方法
・コンテンツ作成方法

(3)利用部門への教育

1)イントラネットのための端末操作に関しての教育は不要と考える。
〔理由〕インターネット、イントラネットは不特定多数の利用を前提にしており操作教育が必要なホームページは利用されなくなる。

2)端末を利用するにあたりモラル教育が必要である。
・端末から離れるときは必ず処理を終了させる
・端末利用については会社の利益にならないことには使用しない
・社会ルールは守る(著作権、個人中傷)
・フロッピーの保管は確実に(机に放置しない)
・パスワードの変更を随時行う
・帰社時、端末の電源を切る
・端末の清掃を行う

3)利用部門に推進担当を決める(運用になるかもしれない?)
・多く利用している部署については推進担当を任命してもらい教育の窓口を作る(改善情報、新技術提供等)

3.5 運用上の留意点

ここでは運用上の留意点について述べる。せっかく安価に、しかも短期間で構築したイントラネットも、障 害対策が不十分でダウンしたり、陳腐化の早い情報の鮮度管理を怠ったりすると、情報系の場合使われなくなるケースも出てくる。また外部との接点にファイア ウォールで関所的にセキュリティを強化しておかないと、ハッカーの不正侵入によるパスワードの入手やクラッカーによる妨害を受けることになる。またイン ターネットからのウイルス感染も脅威になってきている。

(1)バージョン管理について

クライアント端末におけるバージョン管理は、基本的にはブラウザソフトのバージョン管理である。しかしブラウザ機能の競争によりバージョンアップが激しいが、実務から冷静に判断し、常に最新のバージョンでしか見られないようなコンテンツは作成すべきでない。

（2）性能トラブル未然防止について

イントラネットは知らず知らずのうちに大量データの通信を行うことになるので、ゲートウェイやルータな どの通信機器の通信を監視し通信量をチェックすることは、日々の運用上より重要なことである。これらの作業は、ネットワークの性能見積もりや通信量の多い ノードの負荷分散の検討を行う上で重要な資料となり、性能トラブルの未然防止に役立つはずである。例えばトラフック測定の結果が基準値前後になったら次の 手を打つことを考え始めた方がよい。測定から将来を予測し、予測に対する検討・対策を早期から始めるのである。これらの検討は日々上長へ報告し、月例会議 などの場で関連部門への報告をしておくべきである。

このようなアナウンスにより次期回線増強などの設備予算申請のネゴにもつながり、あとあと何かと都合がよい面がある。

（3）ファイアウォール運用上のポイントについて

ファイアウォールの内容設定については、社内のセキュリティルールに基づいた設定ができることが望ましい（図3－5－1）。

図３－５－１　プロトコルの制限

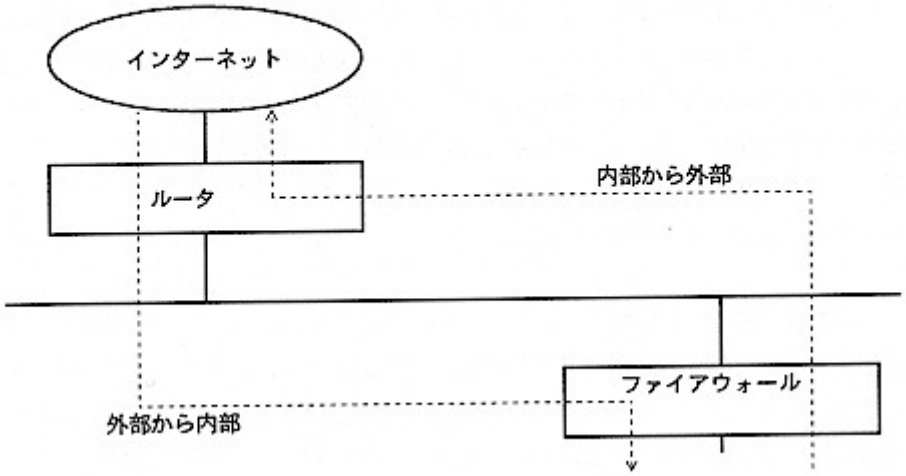


図3－5－1

図3－5－1の例で利用者に対し、外部から内部への場合はSMTP（Simple Mail Transfer Protocol）・NNTP（Network News Transfer Protocol）、内部から外部に対してはSMTP・NNTP・HTTPなどのように通過できるプロトコルを自社にてルール化しておくとよい。

FTPの使用はやめとくのが無難かもしれない。例えばFTPの場合は相手サイトに入り getコマンドでファイルを簡単にダウンロードできる。ファイル内にウイルスが潜んでいた場合、社内への感染の危険を作りかねない。

電子メールでも添付ファイルには注意が必要で、クラッカーなどによるパスワード取得検索プログラムが あった場合、そのプログラムがパスワードを検索し電子メールで自動返送する機能を有するとき、パスワードが盗まれる危険性があるからである。またファイア ウォールのアクセスログは膨大な量になるので、人間の目によるチェックは不可能に近いよってアクセス状況をWWWブラウザ画面からビジュアルに監視する ツールを使用することにより、迅速な対応がとれるはずである。

万が一、不正アクセス等の警告すべき内容が発生した場合は、管理者へ対し電子メールにて通知する。この 際、社内での不正アクセス等による連絡体制を確立しておくことが前提である。不正アクセス以外でも恐ろしいのは、電子メールの添付ファイルにウイルスが潜 伏しているケースである。これについてはファイアウォールだけではチェックが難しい面もあるので、適切なウイルスチェックルールに基づいた運用が必要であ る。最近ではファイアウォールの機能の1つにウイルスチェッカーのあるものが発売され始めている。

ファイアウォールは、グローバルに考えると、インターネットに接続している企業すべてが適切なセキュリティルールの基に運営していなければ意味をもたないのかもしれない。
ハッカーの侵入の手口として、自分の所在をかくすために複数のサイトを経由してターゲット企業にアタックをかけるのが一般的である(図3－5－2)。

図３－５－２　ハッカーの侵入手口

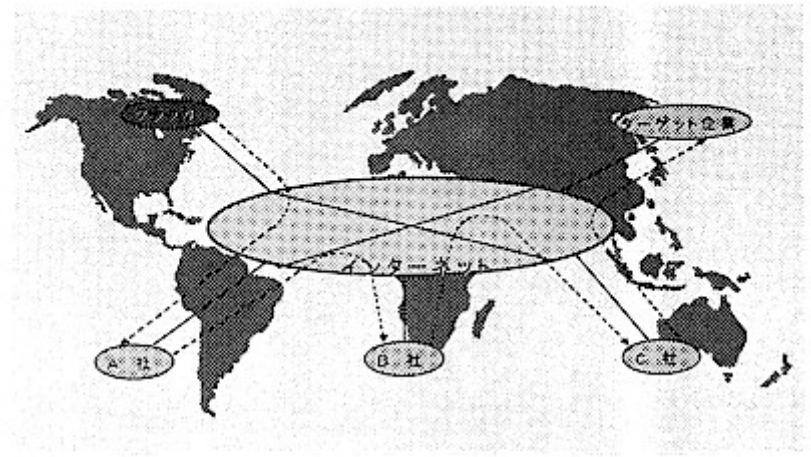


図3－5－2

例えばA社、B社、C社のセキュリティが弱い場合、ハッカーによってターゲット企業までの踏み台にさ れ、ターゲット企業への侵入の手助けを知らないうちにしてしまっていることになる。またターゲット企業におけるファイアウォールアクセスログがC社からの 情報しか残らない場合、ターゲットにされた企業はC社に対しクレームをいうことにもなりかねない。
結果としてC社が不本意な責任を負うことになるので注意がいる。

(4)ウィルス対策について

通産省の調べによると、96 年に届け出があったコンピュータウィルスの被害数は 755 件と前年に比べ 13%増えている。特にマイクロソフト社製のワープロソフトに感染する“マクロウィルス”と呼ばれるコンピュータウイルスの被害が増えたのが特徴である。

これまではフロッピーディスクなどからの感染が主だったが、インターネットの普及により電子メールによる感染が増えつつある。コンピュータウイルス対策に関しては、次のようなことを留意した方がよいと思われる。

1)ユーザー側の管理について

インターネット経由で外部より入手したソフトウエア及びデータについては、一度、FD等にダウンロード し、ウイルス検査後、利用する方が望ましい。また圧縮ファイルについては解凍後にウィルス検査する。ネットワークに載せるデータについても事前にチェック する必要がある。極端なことを言えば個人の持ち込みソフトウエアは禁止した方がよい

しかしインターネットの発達が目覚しい今日、フリーソフトウエアの利用によるホームページの作成やシス テム構築のための一部部品としての利用価値もあるため、まったく禁止にするのではなく、外部からの入手に関しては出所不明のソフトウエアは避ける、そして 一度ウイルス検査をしてから使用することが必要である。とにかくウイルス感染を未然に防止するため、ユーザーは「ウィルスを持ち込まない、自分のPCから 感染させない」を意識として持ち、定期的なウィルス検査を実施することが重要である。

2)システム管理者側について

システム管理者は、ウィルス対策のガイドラインを作成し、ガイドラインに基づいた運用を徹底する必要が ある。最低限やらなければならないことは、利用者PCに対してウイルスパターンの最新情報を更新する。方法はネットワーク配信でもFD配布でもかまわない が、必ずすべての利用者が更新したことを確認しなければならない。最新情報で利用者PCをウイルス検査してもらい、報告を受ける。

このようなことを最新情報で更新するたびに実施する。またウイルス被害に備えるため運用システムのバックアップを定期的に保存し、緊急時の連絡体制を定め、周知徹底する必要がある。万が一、ウイルスが発生した場合は必要な情報を利用者に対し通知する。例えば図3－5－3のようなフォーマットをあらかじめ決めておき、通知するとよい。

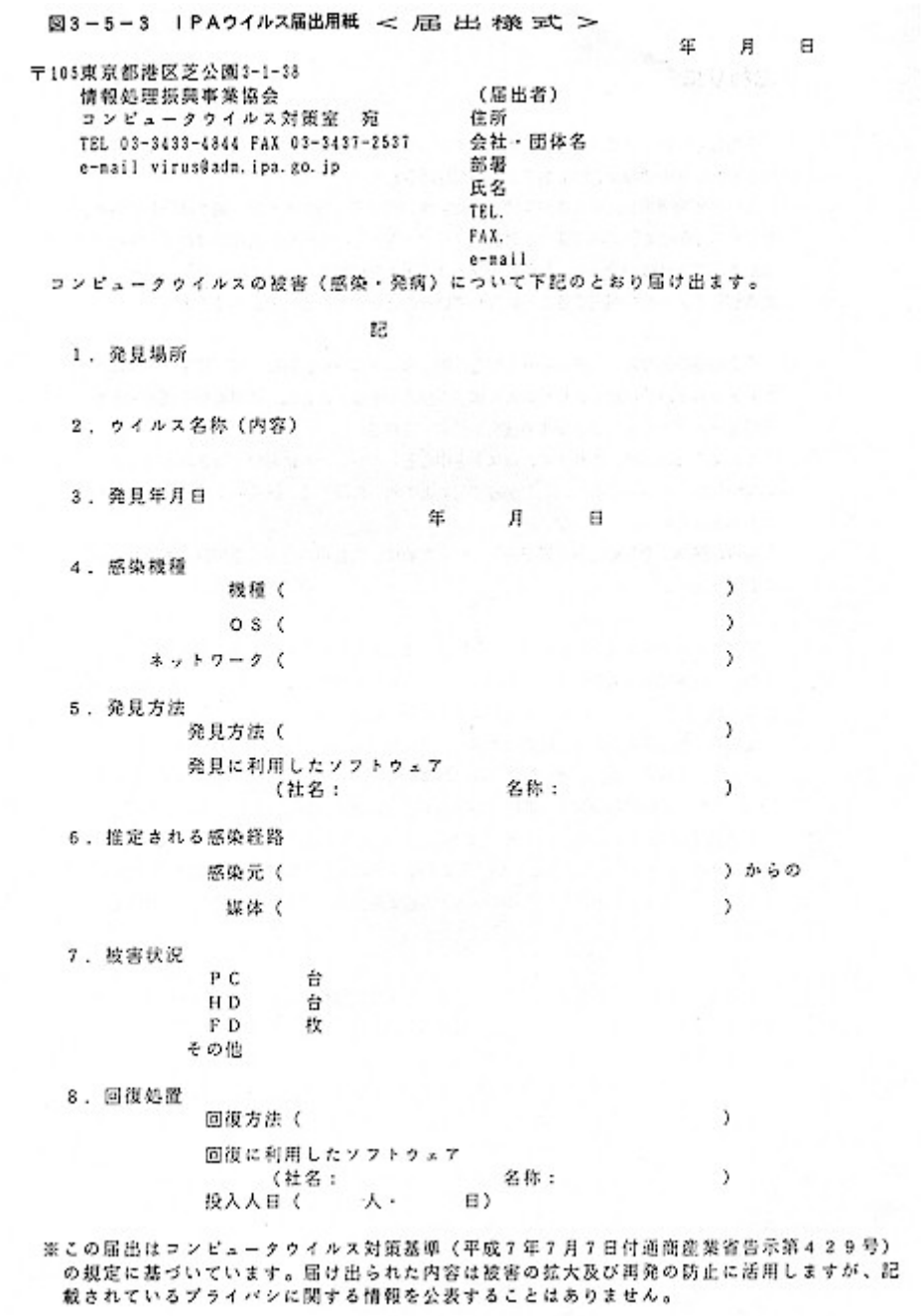


図3－5－3 IPAウイルス届出用紙 ＜届出様式＞

年　月　日

〒105東京都港区芝公園3-1-38
情報処理振興事業協会
コンピュータウイルス対策室　宛
TEL 03-3433-4844 FAX 03-3437-2537
e-mail virus@adm.ipa.go.jp

（届出者）
住所
会社・団体名
部署
氏名
TEL.
FAX.
e-mail

コンピュータウイルスの被害（感染・発病）について下記のとおり届け出ます。

記

1．発見場所

2．ウイルス名称（内容）

3．発見年月日
年　月　日

4．感染機種
機種（　）
ＯＳ（　）
ネットワーク（　）

5．発見方法
発見方法（　）
発見に利用したソフトウェア
（社名：　名称：　）

6．推定される感染経路
感染元（　）からの
媒体（　）

7．被害状況
ＰＣ　台
ＨＤ　台
ＦＤ　枚
その他

8．回復処置
回復方法（　）
回復に利用したソフトウェア
（社名：　名称：　）
投入人日（　人・　日）

※この届出はコンピュータウイルス対策基準（平成７年７月７日付通商産業省告示第４２９号）の規定に基づいています。届け出られた内容は被害の拡大及び再発の防止に活用しますが、記載されているプライバシに関する情報を公表することはありません。

図3－5－3

システム管理者は感染源を徹底的に調査し、感染範囲を明らかにすることが重要であり場合によっては発生部署のシステム利用を一時停止し、感染範囲が判明するまで利用はさせない方がよい。

おわりに

予想していたことではあるが、実際にイントラネットを本格的に構築するとなると、やはりそれなりの準備が必要であることが再認識された。

これまでの情報システム構築手法とは相当趣が異なるものであるが、基本は同じであるただその広がりや、開発期間など対象アプリケーションの選択を間違えな ければ、格段の差があることは確かである。しかしイントラネットを採用するためには、対象となる「利用者が電子メールを利用することになれていることがま ず必要」のようである。

実際の構築となると、そのキーとなる技術はネットワーク、特に「TCP/IP をベースにしたLANおよび公衆網を介したWAN構築の技術が必要」とされ、利用者が不特定・多数となるため「セキュリティ関連の技術が要求」される。

このような技術は、これまでのホストを中心としたシステムにおいてはさほど気にする必要がなかったものであり、したがって自ずとこれらに関しての技術の蓄積がなく、技術者もあまり多くは育っていない。

今後は構築、そして維持・運用をしていくために、これらの技術者を早急に養成していく必要がある。

アプリケーション（コンテンツ）の実際は、まだまだ基幹業務への適用事例は少ない。また、これまでのシステムで特に不都合がないものまで無理にイントラ ネット化をする必要もない。しかしイントラネットは利用者の範囲を格段に広げることができるし、簡単な「情報系・照会系であれば短時間に実務に十分供する ものの作成が可能」である。

しかし、それらの維持・運用はそれなりの体制を必要とする。特にコンテンツの企画部門は、これまでの情報システム部門への一括お任せスタイルから、かなり自分たちでそれらの維持を覚悟する必要がありそうである。このことはむしろ、EUC（End User Computing ）と叫ばれてから久しいが、正に利用部門がシステム構築に主体的に参画せざるを得ないもので、「利用部門主体のシステム構築を推進」するものと考えるべきかもしれない。

本研究グループでは、構築にあたって基本的な事項に関して、その留意点をハンドブック的に示すことはできたと考えている。実際の構築の際、チェックリスト的に利用いただけるものと思う。

インターネット・イントラネット研究部会　部会長　金　修