UDC 681.3:654

エレクトロニクス·情報通信事業部における イントラネット利用と技術基盤

INTRANET Infrastructure and Applications of the Electronics & Information Systems Division

中口 功*(1) 澤谷元喜*(2) 谷口 修*(2) 宮辺 裕*(3)
Isao NAKAGUCHI *Motoki SAWATANI* *Osamu TANIGUCHI* *Yutaka MIYABE*

抄 録

1969年に米国で始まったARPANETを起源とするインターネットは，商用サービスの開始，安価な個人向けプロバイダの登場，WWWに代表される広域探索環境の開発などの相乗効果で1994～1995年にかけて爆発的に成長し，広く一般に浸透することとなった。更には，企業内システムの一部にインターネット技術を利用したいわゆるイントラネットの構築も広く行われるようになった。本稿では，イントラネット構築の例としてエレクトロニクス・情報通信事業部でのインターネットのビジネス利用とネットワーク基盤整備について紹介し，またインターネットの高度利用を目的とした企業内ネットワークの構造設計について提案した。

Abstract

INTERNET originated in ARPANET which was spread in the US in 1969 was developed explosively from 1994 into 1995 and had prevailed widely over the public through multiplier effects such as the introduction of commercial services, the advent of providers servicing for individual at a low price, the development of area search environments represented by World Wide Web (WWW) and so. Further, a network so-called INTRANET had been generally constructed in which the INTERNET technology was applied to a part of the local area network system. The present paper introduces a utilization of the INTERNET on business and a preparation of network infrastructure, as examples of the INTRANET construction, which have been accomplished in Nippon Steel's Electronics and Information Systems Division. Further, the paper proposes a structural design of the local area network system aiming at a high-degree utilization of the INTERNET.

1. 緒 言

今年に入ってから"インターネット(Internet)"という言葉が急速に一般生活の中ではんらんを始めた。また，本来は"ネットワークの間を結ぶ"技術としてネーミングされたこの技術を組織の内部(一つのネットワークの内部)で利用する形態を表現した"イントラネット(Intranet)"の導入を進める企業も急増している。

さまざまなビジネス，技術，製品，情報の宝庫であるインターネットは，もはや時代のちょう児の感があるが，その実態や現実，ユーザーに必要とされる素養・見識は，見かけほど安直なものではない。エレクトロニクス・情報通信事業部(以下EIと記す)では，1988年に国内におけるインターネットの前身であるJUNET(Japan UNIX/University NETwork)へ参加，電子メール，ネットワークニュース利用を開始以来，EI内情報システムへの適用を経て，技術と経験を蓄積した。

その成果は，現在のインターネットに関するソリューションビジネスの展開の見識や技術基盤として活用された。

本稿では，いわゆる情報系システムの基盤としてのEIのインターネット利用について紹介する。

2. EIにおけるインターネットのビジネス利用

EIは，顧客の企業内ネットワークとインターネットとの接続や，インターネット上で商用サービスを行うためのWWW(World Wide Web)を中心としたシステム構築，更に，インターネット上でのビジネス等，ソリューションビジネスの一環としてインターネットビジネスを展開している。

その一方で著者ら自身のビジネスツールとしてもインターネットは非常に有用である。EI全体でのPC(Personal Computer)の1人1台

*(1) エレクトロニクス・情報通信事業部 システム研究開発センター 主任研究員
*(2) エレクトロニクス・情報通信事業部 ITセンター 掛長
*(3) エレクトロニクス・情報通信事業部 ITセンター 部長代理

体制の推進，インターネットアクセスソフトの配布等により，今やインターネットはビジネスを行っていく上で不可欠なものになりつつある。

ここでは，EIにおけるビジネス用ツールとしてのインターネット利用の現状と，将来への展望，課題などについて述べる。

2.1 情報リソースとしての利用

インターネットといってまず頭に浮かぶのはWWWである。EIでもインターネット接続インフラが整って最も利用されるようになったのがこれであり，外部情報の入手のための"情報アンテナ"として利用されている。

その利用形態を見てみると，営業部門での利用で最も多いのが各メーカが公開している製品情報の入手である。カタログスペックや場合によってはまだ雑誌などでも紹介されていない新製品情報を知ることができるため，提案書作成時にも有効に利用されている。開発部門においても，開発環境にするハード・ソフト製品の情報をいち早く入手でき，購入後もその製品の不具合情報などが参照できることもあるので便利である。一部の取引先メーカでは，例えば製品在庫状況や仕切り価格等，従来であればVAN(Value Added Network)でのみ行われていた企業間情報提供サービスをインターネットで行おうとし始めているところもあり，後述のVPN(Virtual Private Network)の世界に近い形での情報提供も行われてくると予想される。

また，製品の配布媒体としてのインターネット利用も重要になってきている。従来であれば，自分たちで使用しているソフトウェアの不具合や納めた製品の不具合対応についてメーカに個別に問い合わせをし，その都度不具合対策版の入手やバージョンアップを郵送などで受けていたが，今はFTP(File Transfer Protocol)あるいは電子メールによって即時対応を受けることができ，業務効率が上がっている。メーカによってはソフトウェア製品の配布形態そのものをインターネット中心にシフトしてきているところもあり，今後ソフトウェアに関してインターネットによる配布は増加すると思われる。反面，心配になるのがウィルスに代表されるソフトウェア改ざんによるセキュリティ問題である。しかし，これらインターネット上での配布の問題についても，電子署名を施す等の対策が行われ始めており，将来ますます一般的になると予想される。

その他，インターネットがまだ技術者の間だけの物であった時代からの活用法として，ホワイトペーパなどの公開技術情報や，それに付随するサンプルプログラムやデータの入手がある。これはWWWを始め，WAIS(Wide Area Information Services)，Gopher，archieなどの検索プロトコルを用いて行うが，検索対象の豊富さや入手したデジタル情報の再利用性など，場合によっては文献をあたるより効率的である。

インターネット接続が当たり前になってくると，営業や技術が外出先からオフィスにアクセスし，必要な情報を検索したり，必要なソフトウェアを取ったりすることも考えられる。ただし，この場合外部から内部情報へのアクセスが可能となるので，認証，アクセス管理などのセキュリティ対策が必要になる。

2.2 サービス窓口としての利用

EIでは，情報提供窓口としてもインターネットを利用している。

現在は，www.ei.nsc.co.jpとして外向けにWWWサーバを立ち上げており，EIの紹介，取り扱っている製品や技術の紹介，イベント情報，人材募集広告等を出している。その他，自社開発の全文検索エンジンNSEARCH*1を用いたインターネットニュースの検索サービスや，NSSUN*2(SunワークステーションのOEM販売)に関連したOSやソフトウェアのパッチデータの提供も行っている(図1参照)*3。

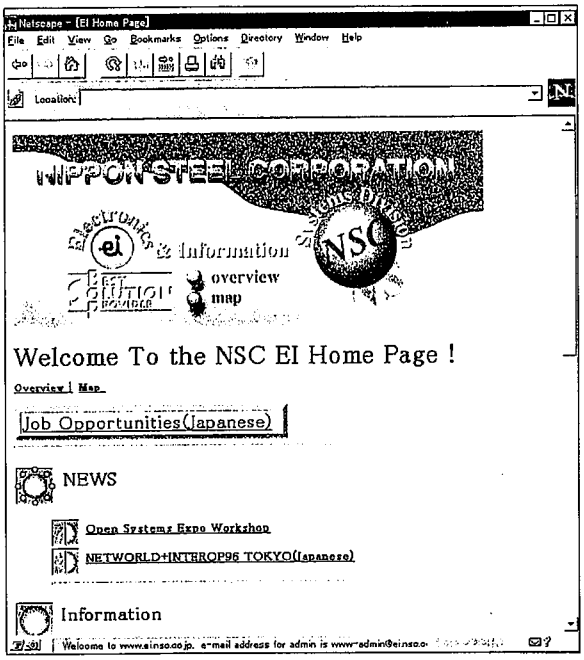

図1 エレクトロニクス・情報通信事業部(EI)のホームページ

また，システムソリューション導入先の顧客について，電子メールによる質疑対応や，Telnetによる遠隔システム障害対応も一部行い始めており，将来は顧客データベース，クレームデータベース等の社内システムと連携し，より迅速かつきめ細やかな対応を目指している。

2.3 企業間ネットワークとしての利用

EIではJUNETでのUUCP(UNIX to UNIX Copy)接続の時代から電子メールを利用してきた。電子メールは，相手の在不在に関わらず連絡ができる非同期性，デジタルメディアとして送受信されることによる記録性・再利用性，更にUUCPからIP(Internet Protocol)へと変わったことによる迅速性によって，電話，ファクスとともに必要不可欠な通信手段となっている。

EIで扱っている技術や製品は米国の企業のもの，あるいは共同で開発しているものも多く，従来は直接米国へ行って共同開発をするか，連絡を取り合って必要なものは郵送して受け渡すか等，費用や時間面で非常に負担が大きかった。現在でも，まとまった共同作業や，重要な会議は相手先へ出張しているが，ちょっとしたワークステーション上の作業や，開発中のソフトウェアコードの受け渡し，打ち合わせは，Telnet，FTP，電子メールを用いて行うようになっており，かなりの効率アップにつながっている。

*1 NSEARCHは新日本製鐵の商標です。
*2 NSSUNは新日本製鐵の商標です。
*3 EIのサーバ(http://www.ei.nsc.co.jp/)の他，新日本製鐵全体のサーバ(http://www.nsc.co.jp/)など，いくつかの社外向けサーバが運用されている。

今話題のVPNは，こうした業務形態の自然な拡張であり，インターネットを介した他企業とのより大規模な共同開発や情報共有の実現が期待できる。

その他，EC(Electronic Commerce)の進展により物品の調達がインターネット上で行えるようになる可能性がある。これに関しては，セキュリティ上の問題もあるが，現状の予算措置を含む調達業務フローとの兼ね合いを整理し，BPR(Business Process Re-engineering)を行うという問題が存在する。

2.4 公衆情報回線としての利用

インターネットを電話などと同様の"個人ユースの情報インフラ"と考えた時出てくるのが，自宅や出張先からオフィスへのリモートアクセスである。

その中でも，特に要求が高いものとして，社外からの社内にある電子メールシステムの利用がある。現在では，まだ個人レベルでのインターネットアクセスインフラが整っていないため，利用者数を限定しつつ，直接公衆回線で接続する安全なアクセスポイントをオフィスに設置し，そこへ専用のPCメールソフト等で接続し利用できる環境を試験的に構築している。しかし，将来，どこからでもインターネットに接続できるようになれば，セキュリティ対策をしっかり行った上で，特にアクセスポイントを利用者数に応じて用意することなく，誰でもインターネット経由での社内電子メールシステムを利用できるようになる。

また，SOHO(Small Office, Home Office)の考え方からいくと，電子メールだけでなく，オフィスにあるサーバ上のファイルアクセスや，更には遠隔地からオフィスのマシン上での開発作業が行えると利便性が高まる。しかし，現状のシステム構成上の問題，セキュリティ技術上の問題，また，勤務体系の問題等，解決すべき点が多々ある。

3. EI事業部におけるイントラネット利用

3.1 イントラネットとは

イントラネットとは，インターネットの技術とアプリケーションによって社内情報系業務システムを構築するものである。通信プロトコルとしてはTCP/IPをベースに，インターネット・メールに利用されているSMTP(Simple Mail Transfer Protocol)，WWWに利用されているHTTP(HyperText Transfer Protocol)等のインターネット標準プロトコルを用いる。

イントラネットの導入メリットとして"低コスト"が一般的な認識である。これは，オープン系のインターネット技術を利用しているためであり，インターネットの安い，もしくは無料のソフトウェアで構築できるからである。また，WWWブラウザを利用することで，クライアント(端末)の機種を限定せず，なおかつGUI(Graphical User Interface)の統一が図れる。しかし，イントラネットは本当に導入コストが安いのであろうか，インターネット技術を転用するだけで良いのだろうか，といった点について，EIで進めてきた情報系業務システムの構築，イントラネットをもとに考察する。

3.2 EI事業部の取り組み

3.2.1 EI-OA

EIにおける情報系業務システム(EI-OA)の構築は事業開始当初より10年来，進められてきた。以下にEI-OAへの取り組みについて紹介する。

(1)電子メール

迅速な情報伝達手段として，1988年よりJUNETに参加し，電子メールの活用に早くから取り組んできた。当時はまだPCも高価で，導入メリットも利用率も不確定な状況であり，以前より使用していた業務用，開発用，設計用のPCの併用・流用も含めて，4～5名に1台の割合から始めた。この時点では一部の組織での利用に留まるが，これをEI全体へと発展させてきた。

電子メールは，ただ導入するだけで速やかに全員が活用する訳ではない。メール以前に，PCに不慣れな社員もいた。そこで，ワープロ専用機を廃止し，PC上のワープロソフトの利用から自然とPC操作に慣れ，電子メールにもなじんでもらった。

電子メールの利用率の向上に伴い，メールの利便性が浸透し，利用率は更に高まった。また，重要な会議連絡や，業務連絡も電子メールで送られてくるために，電子メールを利用せざるをえない状況になっていった。現在ではネットワークインフラが整備され，PCの1人1台体制にて運用されている。

また，メールの利用は情報伝達の手段としてだけではなく，メーリング・リストを用いた電子会議や共同作業等に活用している。

(2)業務システム

ワープロ専用機をPCに切り換えたことを前述したが，その他の業務もPCへと集約を行いつつある。PC上の会議室予約システムの導入，従来専用端末で行っていた保養所予約や，社内研修の申し込み，出張申請の経理や，勤務管理等もPC上から入力できるシステムを構築した。このように，様々な業務がクライアントにPCを用いたシステムへと移行中である。

(3)WWWサーバ

電子メールは単独の相手に送信するだけではなく，複数の相手に同一のメールを一斉に出すことができる同報性がある。特定メンバーに対して同一の情報を伝えるためには，非常に有効な手段である。しかし，何十人，何百人の相手に対して一斉にメールを出すことは，ネットワーク負荷も高く，あまり現実的な手段とはいえない。そのような場合，皆が見ることができる電子掲示板が有効である。電子メールの推進と並行して，EIの社員全員が見ることができる電子掲示板としてのWWWサーバを構築した(図2参照)。

EIにおいては，

(1)インターネット／イントラネット構築ビジネスを行っている，

(2)研究部門では1人1台のWWWサーバを持ち，自分のホームページを部内で公開している，

(3)多くの部が部内WWWサーバを用いてプロジェクト推進に役立てている，

等，WWWサーバに対する技術，ノウハウが蓄積されており，WWWサーバを利用した電子掲示板を作成した。

WWWサーバを利用した電子掲示板により，従来紙で配布されていた，社内報，規定類，セミナー案内等を発信し，円滑な情報提供を実現した。その結果，資料を机や棚にファイルすることなく，いつでも必要なときにWWWサーバを見れば良い。しかも，WWWサーバには常に最新の情報が登録されており，利用者個人が管理する必要がない。

なお，インターネットの初心者にもWWWサーバに慣れ親しんでもらうために，見やすさや使いやすさを考慮したのはもちろんのこと，電車・バスの時刻表や，社員食堂のメニューなどの親しみやすい情報を用意した。EI全社員の電子メールアドレスや電話番号が検索できるアドレス検索機能を持たせた。

利用者の利便性を高め，WWWサーバの知名度，利用率の向上を図るために，現状のイントラネットのメニュー項目のうち，およそ

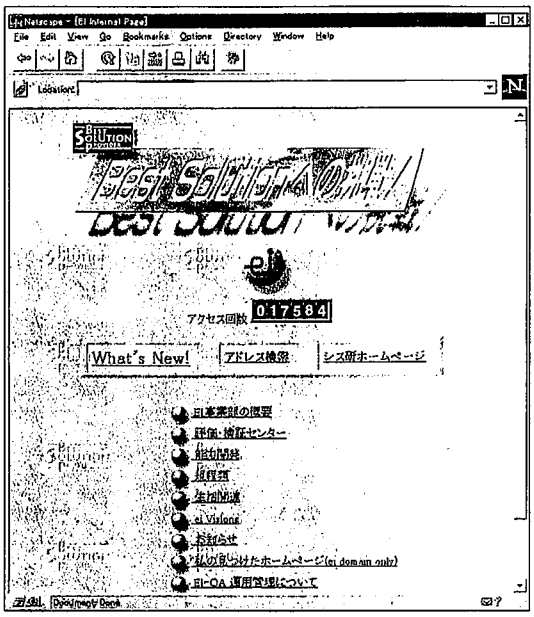

図 2　EIの情報系業務システムのホームページ

10%が"親しみやすさ，楽しさ"のために用意されている。

3.2.2　評価・検証センター

EIが推進しているソリューションビジネスにおいて，日々目まぐるしい革新を続けている情報技術(Information Technology)に対応し，最適なハード，ソフト，テクノロジーを組み合わせたシステム提案力の強化が不可欠である。マルチベンダーとして魅力的なソリューションの提案力向上のため，個人技術力依存を脱却し，組織としての技術情報の共有化を図る必要があった。

前述のWWWサーバの電子掲示板は，情報伝達の手段であり，情報が一方向でしかないのに対して，それを"情報の共有化"へと発展させるために，WWWサーバ上に"評価・検証センター"を構築した。つまり，社内報や規定類の情報は，利用者にとって収集するだけの情報であるのに対して，情報の共有化では，EIの一人一人の社員が持っている情報を共有化することが目的であり，収集だけではなく発信が可能な，個人やグループが持っている最新情報やノウハウを情報交換できるシステムの構築を行った。

したがって，"評価・検証センター"は，EIの社員全員が見て，参加し，情報を提供しあう場のシステムであり，なおかつ，互いの部の壁を越えたバーチャルな組織としての名称でもある。"評価・検証センター"は，役割に応じていくつかの異なるシステムにて構築した。それぞれについて以下に述べる。

(1)投稿技術情報掲示板

投稿技術情報掲示板とは，EIの各自が業務を通じて得た技術知見，あるいは社外から収集した情報等を自発的に投稿し，それらの情報をEIの各自が共有できるようにしたものである。

通常，WWWサーバは決められた管理者だけが情報を発信できる仕組みであり，不特定多数の人間が自由に情報を発信できるようにするためには，グループウェアを採用するか，システムの作り込みを行わなければならない。そこで，WWWサーバ上で誰でも簡単に自由に投稿ができるシステムを用意した。このシステムは，自由な入力画面テンプレートを作成でき，入力された情報の掲示期間などをきめ細かに管理できるデータベース機能を備えている。また，検索や表示も簡単にできるシステムである。このシステムは，ソリューション提供のためのSI(Systems Integration)の"部品"として顧客に提供している(図3参照)。

(2)技術情報掲示板

社員の持っている技術知見やノウハウだけではなく，定期的あるいは非定期的に社外のハード／ソフトベンダー，情報ベンダーや学協会から入手した技術情報を，許諾された範囲でEIの全員が必要なときに見ることができるようにした。更には，R&D成果の最新情報の紹介も行っている。このように最新の技術情報の公開を推進し，変化の激しい情報技術への対応力を図っている。

WWWサーバで公開しているこれらの情報の中には，管理職以上や特定者限り等の情報もある。そこで，これらの情報に対してアクセスコントロール機能を用いて，利用者の限定を行うことができるシステムとした。

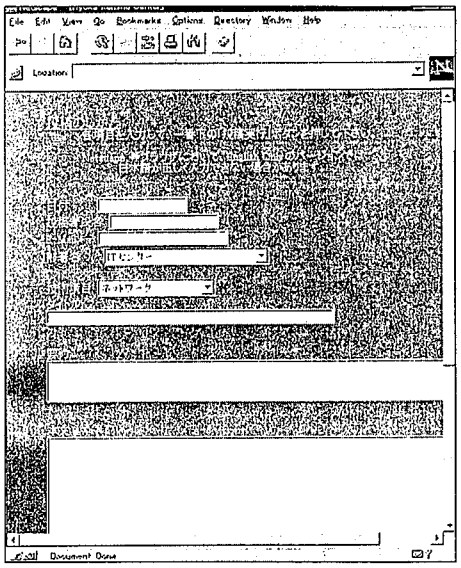

図 3　投稿技術情報掲示板の入力画面テンプレート

(3)技術情報Q&A

投稿技術情報掲示板は，各個人が持っている情報を発信する場であるが，掲示板に掲載されていない情報を必要とする場合も多い。特に，投稿情報では共有し難いノウハウなどがそうである。

従来ならば，知っている人間を探して，電話をかけたり，訪ねたりして，質問を行っていた。しかし，グループや部が違ったり，東京，大阪など何か所にも分散していると，情報を持っている人間を探し出すのが困難であったり，たずねることに戸惑いを感じたりした。そこで，教えてもらいたい情報があったときに，気楽にQ&Aを行えるシステムを構築した。

このような双方向の情報交換のシステムを，インターネットのNetNewsの仕組みを利用して構築を行った。NetNewsの採用理由は次の通りである。WWWと同じくオープンな技術であり，クライアントを限定せず，様々なPCやワークステーションから参加できる。過去のやり取りを残すことができ，質問者以外の人も見ることができるため，Q&Aの情報を共有化が図れる。NetNewsの利用に対して，EIの一部では10年近い歴史があり，ノウハウや技術が蓄積されていた。WWWブラウザがニュース・リーダーを兼ね備え，

NetNewsの初心者に対して，ニュース・リーダーとWWWが連携した操作性が良くなじみやすいシステムを構築できる。

(4)検索機能

評価・検証センターに蓄積された様々な大量な情報の"森"の中から"木"(目的のもの)を探し出す手助けのために検索機能を設けた。

EIが開発，外販している"超高速全文検索ソフトウェア(NSEARCH)"を社内利用し，超高速に全文検索できるシステムを構築した。これによって，大量な情報の中から目的とする技術情報が容易に探し出せる。この際，NetNewsやWWWなどの様々なシステムに蓄積された技術情報を同一画面で検索し，同一画面に表示させることや，複数の検索したいキーワードをAndやOrで自由に組み合わせられること，検索対象となるページを(例えば，技術情報Q&Aだけに)限定できることなど，"木"を探すための工夫も施している(図4参照)。

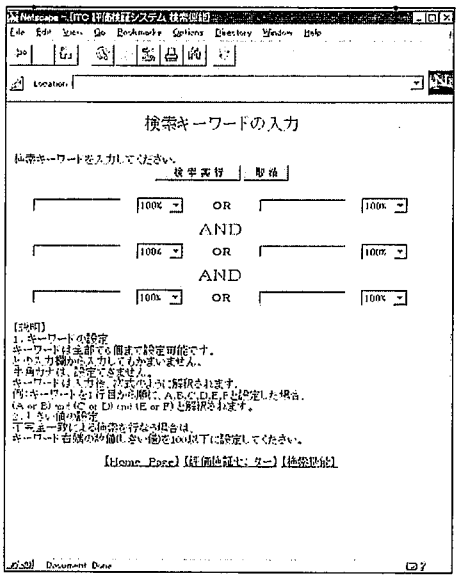

図 4　検索機能

4.　ネットワーク構造設計

ここでは，企業の内部に異なったネットワーク運用方針をもつ複数の組織が存在する場合の，安全性と利便性を両立させる社内ネットワーク構造の設計について述べる。ここでの実証ネットワークは前述したEIのイントラネット構築のネットワークインフラストラクチャとして利用している。

4.1　背　　景

社内ネットワークとインターネットとの相互接続において，低コストで内部ネットワークの安全を守りつつ，内部ユーザーに対しインターネットへのアクセスを提供するため，ファイアウォールを利用する例が広く見られる。一般的には，相互接続点を一つに限定し，その接続点にも設けられたファイアウォールで組織全体を守る構造にすることが多い。

ファイアウォールは

・内部のネットワーク運用・管理・利用に関する方針(以下，ポリシと記す)が単一であること，
・内部は安全であること，ユーザーが信用できること，
・ユーザーが要求するサービスはゲートウェイによる中継で提供可能なこと，

を前提として構築されてきた。

しかし，ネットワークの利用が進むにつれ，以下の4点の問題が顕在化しつつある。

(1)内部のポリシは単一ではない。

一つの会社の中に，単にユーザーとしてインターネットを利用しているだけの組織と，インターネットそのものをビジネスあるいは研究の対象としている組織とが混在している場合がある。前者に対してはインターネット上の限定されたサービス(例えばWWW)へのアクセスを提供すればほぼ要求を満たすことができるが，後者は例えば外部からの(ログインを含めた)アクセスを必要とすることがある。

また，ある組織が社外から共同開発者を受け入れ，彼らに社員と同等のアクセス権を与えることは，他の組織にとってはセキュリティ上の脅威になる可能性もある。

(2)内部は必ずしも安全ではない。

外出先からアクセスしてくるユーザーに対応するため，着信可能モデムを設置している社内組織が存在することがある。そこが足掛かりとなり内部ネットワーク経由で他の組織に侵入される可能性がある。

個人向けプロバイダが出現し，誰でも簡単な設定・手続きでインターネットに接続できるようになった。知識のない管理者，ユーザーが行う不用意な設定は，外部から内部ネットワークへの裏口を作ることになる。

(3)外部との固有の接続が要求されている。

例えば共同開発先との密な連携のために対外接続点インターネット経由ではなく固有の接続(例：共同開発先との専用線)を必要としている組織が存在する。

(4)ゲートウェイで中継できないサービスが存在する。

ファイアウォールは，TCP/IPの"ネットワーク上の任意の二つの計算機が通信可能"の原則を崩す構造であり，内部計算機と外部計算機の通信を可能にするためにはゲートウェイによりパケットの中継を行う必要がある。

ゲートウェイとしてはSOCKS(TCPの中継)，udprelay(UDPの中継)などのトランスポートゲートウェイ，CERN httpdなどの代理サーバが用いられることが多い。前者を用いるとTCP，UDP(User Datagram Protocol)に関してははん用的な中継サービスを提供することができるが，クライアント(一般に内部計算機)がゲートウェイに対応することが必要(connect()，bind()などの置き換え)であり，すべてのクライアント側アプリケーションで利用できるわけではない。後者ではクライアント側の対応に加え，利用できるサービスがゲートウェイ管理者により提供されたもの(例えばWWW，FTP，Gopherなど)に限定される。

単一のファイアウォール，単一のポリシでは多様化するユーザーの要求に対応できない。また，セキュリティの弱い組織，あるいは最もセキュリティを確保しなければならない組織を基本に全体のセキュリティ方針を決めなければならない。これらのことがユーザーの勝手な設定を誘発する結果となる。特に社内組織が広域にわたり分布している場合，全社管理機構の目が届かず内部からネットワークが破たんするケースが今後増えてくると思われる。

これらの問題を解決するため，

・内部ネットワークを運用方針ごとにサブネットワークに局所化する。

・各サブネットワークにファイアウォールを設ける。
・サブネットワークを相互に接続する。

の方針で社内ネットワークの階層的な構造を考え，実証ネットワークとしてnetsys/IXA(netsys-proj Internet Exchange Architecture, netsys-projは研究開発チーム内での略称)と呼ばれる構造を実装した。netsys/IXAは次の方針で設計した。

・交換機能を有する社内バックボーンを構築する。
・接続組織のポリシを尊重する。
・バックボーンと接続組織との管理境界を明確にする。
・接続組織は"自分の身を自分で守る"方針でバックボーンに接続する。
・接続組織固有の接続を許容する。
・複数地点でのインターネット接続に対応できる。
・必要に応じ，インターネットと接続組織との直接の接続性を確保できる。

4.2 構 造

図5はnetsys/IXA設計の概念を表した図である。

図6はnetsys/IXAの現在の構造である。

netsys/IXA－相模原，netsys/IXA－大分，netsys/IXA－新宿と呼ぶネットワークオペレーションセンターを設け，それらの間を専用線あるいはフレームリレーで接続しバックボーンを構成した。netsys/IXA－相模原には筆者の所属するEIシステム研究開発センター，EI事業部相模原，WIDE(Wide area Integrated Distributed Enviroment)

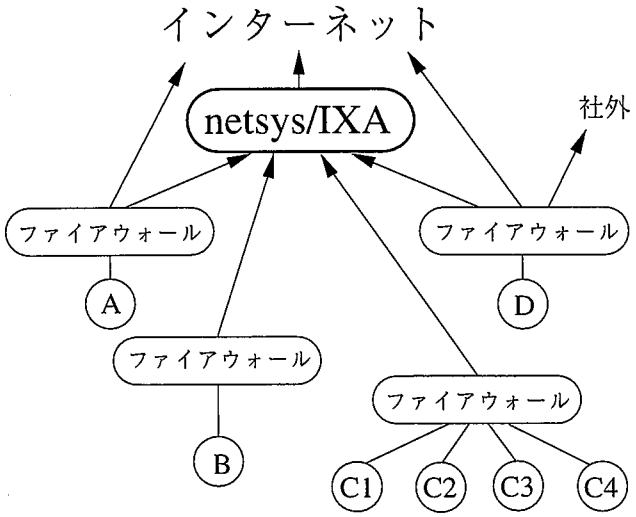

図5 netsys/IXA設計の概念図

Project共同研究環境が接続されている。netsys/IXA－大分には大分製鐵所，八幡製鐵所(の一部)が，またnetsys/IXA－新宿にはEI事業部新宿，本社がそれぞれ接続されている。なお，大分，八幡以外の製鐵所へは本社経由で到達可能である。

各組織は"自分の身を自分で守る"方針を実現するために，ファイアウォールを構築しnetsys/IXAバックボーンに接続している。

4.3 アドレスと経路制御

インターネットと各接続組織との間の直接の接続性を確保するため，各接続組織のファイアウォールにはグローバルアドレス(プライベートアドレスではないアドレス)を割り当てた。IPアドレスの有効利用の立場から，アドレスを"必要な場所に必要な分だけ"割り

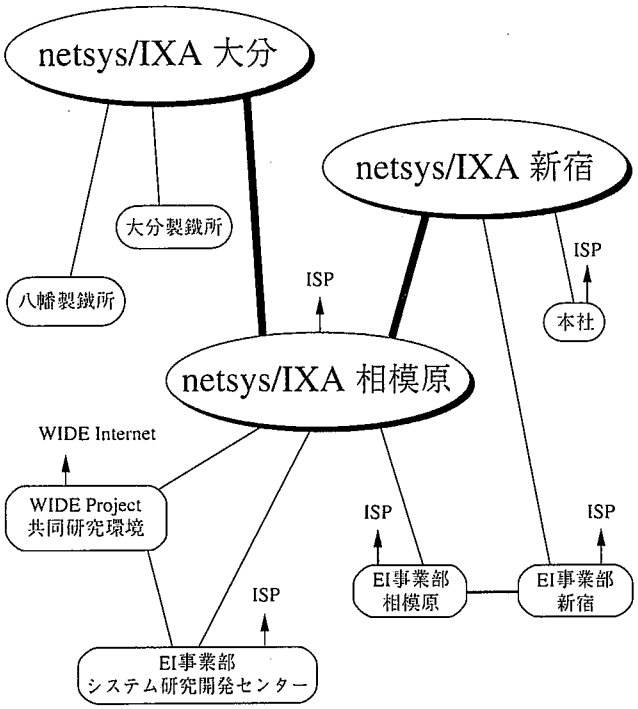

図6 netsys/IXAの現在の構造

当てるために，各組織のマスクを27ビットから29ビット(point-to-point部分はunnumberedあるいは30ビットマスク)の可変長とし，経路制御プロトコルとしてOSPF(Open Shortest Path First)を採用した。

表1はWIDE Internet上の計算機から八幡製鐵所CSセンター(csc.nsc.co.jp)へのtracerouteの結果である。プロバイダとの接続点(9行目)から更に内部にまでインターネットからの到達性を確保している。

netsys/IXAに複数地点で接続している組織，例えばEIは内部にnetsys/IXAバックボーンのバックアップ経路となり得るリンクを持っている。

netsys/IXAバックボーンがダウンしている場合，この内部リンクを他組織がバックアップ経路として使用してよいかはEIにより判断される。ある組織は通過を許可され，別の組織は拒否されるかもし

表1 tracerouteの例

```
nakaguch@sh.wide.ad.jp% traceroute csc-gw.csc.nsc.co.jp
traceroute to csc-gw.csc.nsc.co.jp(202.230.50.147), 30 hops max, 40 byte packets
 1 sun1.tokyo.wide.ad.jp(133.4.2.2)8 ms 8 ms 8 ms
 2 cisco9.tokyo.wide.ad.jp(133.4.3.27)11 ms 11 ms 9 ms
 3 tokyonet.nspixp.wide.ad.jp(202.249.3.38)9 ms 9 ms 9 ms
 4 harajuku-bb.TokyoNet.AD.JP(202.239.61.2)144 ms 146 ms 142 ms
 5 otemachi-bb6.TokyoNet.AD.JP(202.239.61.6)206 ms 207 ms *
 6 router00-Fddi2-0.tokyo1.TokyoNet.AD.JP(202.230.255.162) 281 ms * 220 ms
 7 router01-Serial1-3.yokohama.TokyoNet.AD.JP(202.239.61.250)231 ms 235 ms 208 ms
 8 router04-Ethernet0.yokohama.TokyoNet.AD.JP(202.239.62.5)271 ms 252 ms *
 9 tokyonet-cisco.netsys-ixa.nsc.co.jp(202.230.50.1)252 ms 247 ms *
10 sagamihara-cisco-1.netsys-ixa.nsc.co.jp(202.230.50.2)205 ms 183 ms 215 ms
11 oita-cisco-0.netsys-ixa.nsc.co.jp(202.230.50.49)253 ms * 287 ms
12 oita-cisco-1.netsys-ixa.nsc.co.jp(202.230.50.52)248 ms 257 ms 252 ms
13 yawata-ixa-cisco.csc.nsc.co.jp (202.230.50.145)277 ms 300 ms *
14 csc-gw.csc.nsc.co.jp (202.230.50.147)293 ms 228 ms *
```

れない。このようなポリシを反映した経路制御を実現するために，各接続組織をAS(Autonomous System)とし，AS間の経路をBGP(Border Gateway Protocol)で交換する解が考えられる。プロバイダ間の相互接続で一般的に使われている方法であるが，管理負荷やルータの制約(BGP非対応ルータの存在，ルータのメモリ容量など)の点で社内で適用することを今回は見送った。現在はnetsys/IXAバックボーン内で各接続組織のポリシに合致した経路を計算し，それをバックボーンと各組織との境界ルータでそれぞれの組織の希望する経路制御プロトコル(RIP(Routing Information Protocol)あるいはOSPF)に変換し組織内に送出することで解決している。

4.4 共同利用セグメント

異なったポリシを持つ組織Aと組織Bの間で共同利用できる計算機を用意することを考える。組織Aが組織Bを信用し，組織A内に置かれた共同利用計算機に組織Bからアクセスできるようにするためファイアウォールの制限を緩めたとする。組織Bに外部から侵入があった場合，組織Aにまで被害が及ぶことが考えられる。

これを防ぐために，共同利用セグメントを設け，ルータで以下のパケットフィルタを設定した。

・組織A，組織Bからは共同利用セグメントへのアクセスは可。
・共同利用セグメントから組織A，組織Bへのアクセスは不可。

組織Bに侵入があった場合，共同利用セグメントまで被害が及ぶ可能性があるが，その先，組織Aにまで侵入することは極めて困難である(図7参照)。

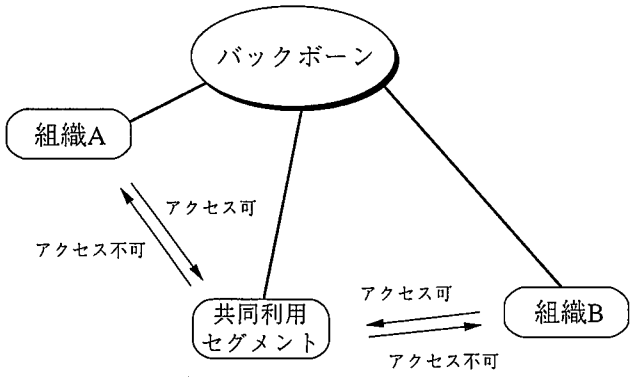

図 7　共同利用セグメント

4.5 EI-OAでの適用

歴史的経緯から,EIシステム研究開発センター(elelab.nsc.co.jp)とそれ以外のEI(ei.nsc.co.jp)とは異なったポリシで運用されている。

互いのポリシを尊重した相互接続を実現するため，それぞれがファイアウォールを構築し，netsys/IXAバックボーンに接続した。いくつかの共同利用計算機(例えばEI共通のWWWサーバ)は共同利用セグメントに置かれている。

インターネットから参照される必要がないため，共同利用セグメントにはプライベートアドレスを割り当てている。

なお，プライベートアドレスの逆引き，インターネットから見える必要がない内部名はnetsys/IXA rootネームサーバにより管理されている。netsys/IXA接続組織は，インターネット上のrootネームサーバ(A.ROOT-SERVERS.NETなど)の代わりに，このnetsys/IXA rootネームサーバを使用することで，インターネット上のアドレス・名前とプライベートアドレス，内部名の両方を参照することができる。

5. 結　　言

本稿では，EIでのインターネットに関するビジネス利用，事業部内利用，及びその基盤となるネットワークトポロジー技術に関して概説した。

EIのイントラネットとして，WWW，電子メール，Net News，データベース，グループウェア等の組み合わせによる事業部内技術情報インフラは，事業部長から新人に至る全構成員に普及しつつある。この情報インフラは，部，室，掛といった新日本製鐵の組織階層構造を流通する情報とは異なり，水平な(異なる組織の同じ立場の)情報の流通・共有化を実現するため，特に技術情報にとって新しい価値を持つシステムである。また，こうした情報流通の結果は，決して組織構造に妨げとなる結果をもたらすのではなく，構成員の自由かったつな発言を許しつつも結果として組織の力を向上させている。今後，利用の高度化対応や基幹業務サポートの充実のため，現在では各部の個別運用となっているグループウェアの事業部レベル導入による業務フロー全体のシステム化が必要となる。

また，イントラネット構築のためのネットワークインフラストラクチャとして，複数の運用方針が存在する場合の社内ネットワーク構造の実装例netsys/IXAを紹介した。各組織が"自分の身は自分で守る"方針で接続することで，他組織の運用方針の違いによる自らの自由度を阻害されることなくネットワークを運用できる。netsys/IXAにより，各組織の運用方針を尊重し，かつ安全な社内ネットワークが実現され，1994年から研究開発を実施，1995年からはEI及び鉄事業の一部のネットワークインフラ全体として利用されている。

今後の技術課題として，利便性と安全性のより高いレベルでの両立が挙げられる。イントラネット構築の際には，個人への情報サービスレベルの確保と，同一運用ポリシ(組織)内の共同作業を支援する環境を実現した。組織を越えた共同作業に対する，利便性の確保については，現在のところ共同利用セグメントで解決している。将来的にはIPトンネリングと暗号・認証技術の組み合わせによりファイアウォールを越えた相互接続の実装が必要であり，実験，準備を進めている。この際，どの情報を共同利用できるようにするか，誰からのアクセスを許可するか，その相手をどの程度信用するか，などの点を設計の際に整理する必要がある。このことはセキュリティ確保の第一歩である"何のために(目的)，何を(対象)，何から(脅威)守るのか"を再確認するために意義のあることであり，"何でも守る"という発想によるセキュリティ確保の過大な投資を抑制する効用もある。

参照文献

1) 田坂　広志：イントラネット経営，生産性出版，1996
2) 黒田　豊：西海岸メディア通信，東京万華鏡，
http://www.smn.co.jp/JPN/features/mr/index.html
3) ExecutiveのためのINTRANET，NTT America, Inc.，http://www.nttca.com/library/NowInternet/3/
4) William R. Cheswich and Steven M. Bellovin.
5) Firewalls and Internet Security -- Repelling the Wily Hacker, Addison-Wesley, 1994.
6) 1993年度WIDEプロジェクト研究報告書.
7) Moy, J.: "OSPF Version 2", RFC1583, March 1994.
8) Rekhter, Y., Li,T.: "A Border Gateway Protocol 4 (BGP-4)", RFC1654, July 1994.