資料４－２

次世代ＩＰインフラ研究会
第一次報告書（案）

バックボーンの現状と課題

２００４年6月7日

目　次

凡例

◇　年次は原則として西暦を使用している。

◇　企業名については、「株式会社」の記述を省略している。

◇　補助単位については、以下の記号で記述している。

１，０００兆（10^{15}）倍	・・・Ｐ（ペタ）
１兆（10^{12}）倍	・・・Ｔ（テラ）
１０億（10^{9}）倍	・・・Ｇ（ギガ）
１００万（10^{6}）倍	・・・Ｍ（メガ）
１，０００（10^{3}）倍	・・・Ｋ（キロ）

◇　単位の繰上げは、四捨五入によっている。単位の繰上げにより、内訳の数値の合計と合計欄の数値が一致しないことがある。

◇　出典が明記されていない図表等は、総務省作成資料である。

序章　はじめに

電気通信事業者間の活発な競争とインフラ整備及び政府による環境整備により、現在、我が国は世界最安・世界最速のブロードバンド利用環境を実現している。

これを受け、２００３年７月に策定された「e-Japan 戦略Ⅱ」においても、我が国のＩＴ戦略の目標を、第１段階のインフラ整備及び競争政策から、第２段階のＩＴの利活用に移行させている。

具体的には、「医療」、「食」、「生活」、「中小企業金融」、「知」、「就労・労働」及び「行政サービス」という７つの先導的分野において、情報通信技術（ＩＴ）を利活用していくための施策を展開することとしている。

ブロードバンドの実利用が依然として少ない状況において、まず、先導的取組分野におけるブロードバンドの実利用率を高めることは、「２００５年までに世界最先端のＩＴ国家を実現する」という我が国のＩＴ戦略の目標を達成する上で極めて重要である。

他方で、先導的取組分野をはじめ、社会生活の様々な場面でＩＴを利活用することは、ネットワーク上に大容量の通信量（トラヒック）を発生させるものである。

そこで、当研究会では、次の３つの論点について検討を行った。

第１の論点は、現時点ではブロードバンド利用率が依然として低いことから処理できているものの、将来的に国民の大半がブロードバンドを利用した場合に、大量に発生するであろうトラヒックをネットワークは処理し切れるのか、今後ネットワークを増強すべきなのか、必要な技術開発は何か、という点である。

第２の論点は、大容量のトラヒックを発生させるＩＴの利活用の中には利用者から高い信頼性を期待されている分野もあることから、このような信頼性に関する利用者からの期待に応えられるだけの用意がネットワーク側にあるのか、という点である。

第３の論点は、多数のネットワークが多様に接続することによって成り立っているインターネットにおいては、１つのネットワークにおける通信障害が全体に波及するおそれがあり、インターネットの安定した運用を確保する観点から、障害連鎖を防止するためにどのような方策（事業者間の運用ルール、技術開発等）が必要かつ有効か、という点である。

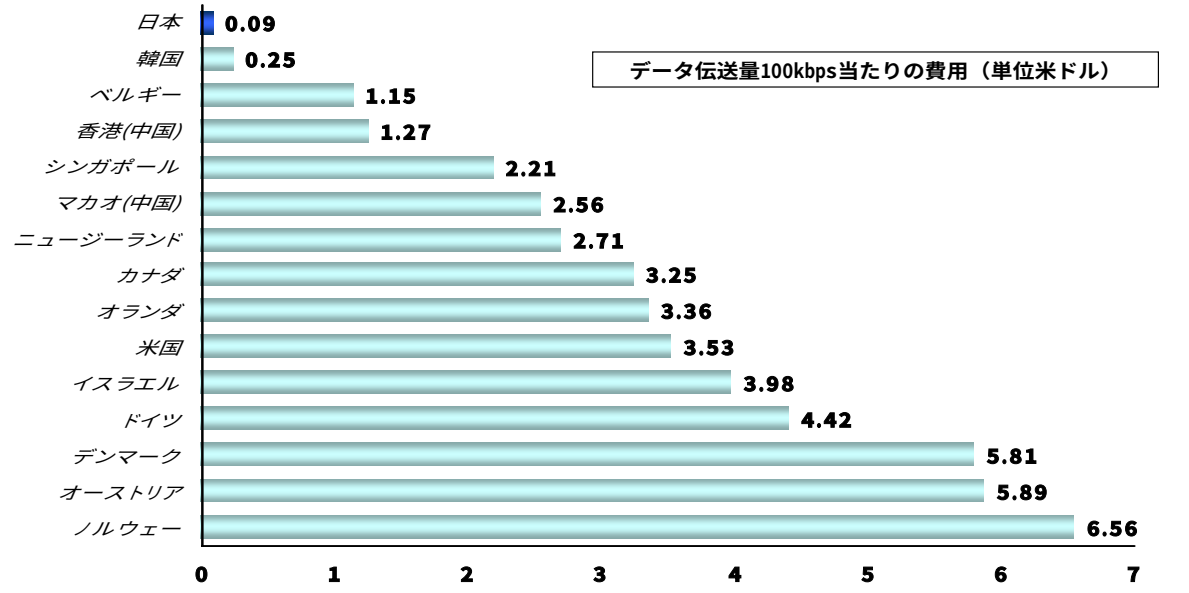
これら３つの論点については、研究会構成員間で、見解の一致している事項もあれば、一致していない事項もある。本資料は、見解の一致していない事項については異なる見解を併記し、これまでの議論を取りまとめたものである。

第１章　我が国におけるブロードバンドの普及状況

１．ブロードバンド通信の「安さ」と「速さ」

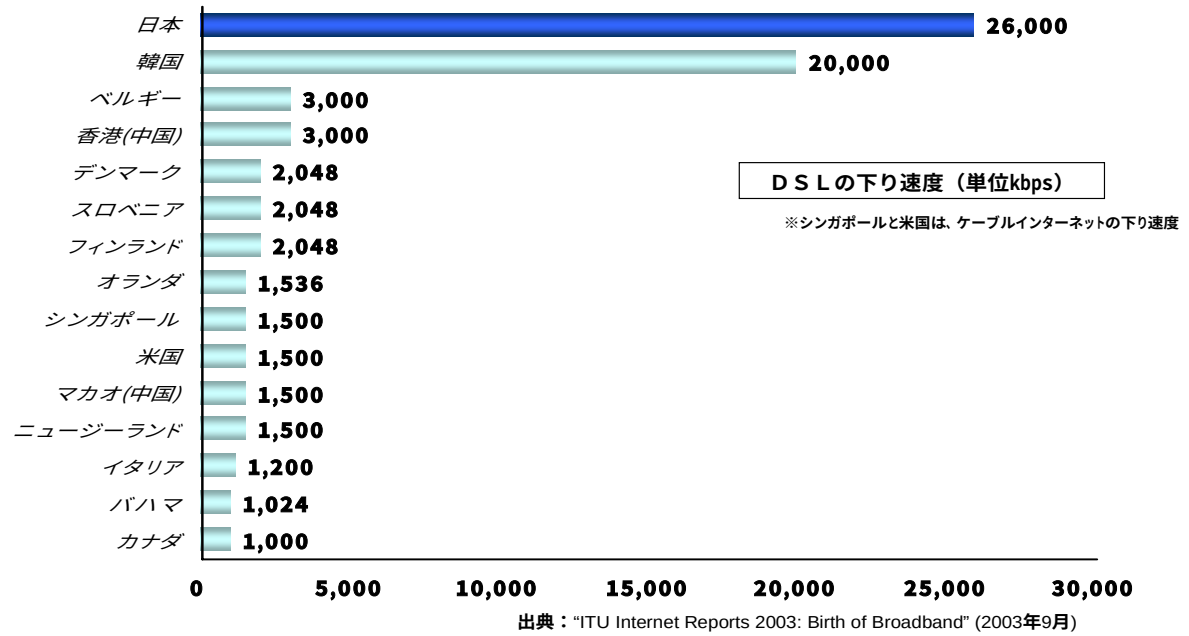
電気通信事業者間の活発な競争と政府による公正競争促進のための環境整備等により、我が国のブロードバンド料金は、世界的に最も低廉な水準を実現するに至っており、２００３年の国際電気通信連合（ＩＴＵ）の調査によれば、ブロードバンド通信の「安さ」と「速さ」の総合評価において、我が国は世界一という評価を受けているところである（「ITU Strategic Planning Workshop on Promoting Broadband Background Paper」）。

通信速度当たりのブロードバンド料金



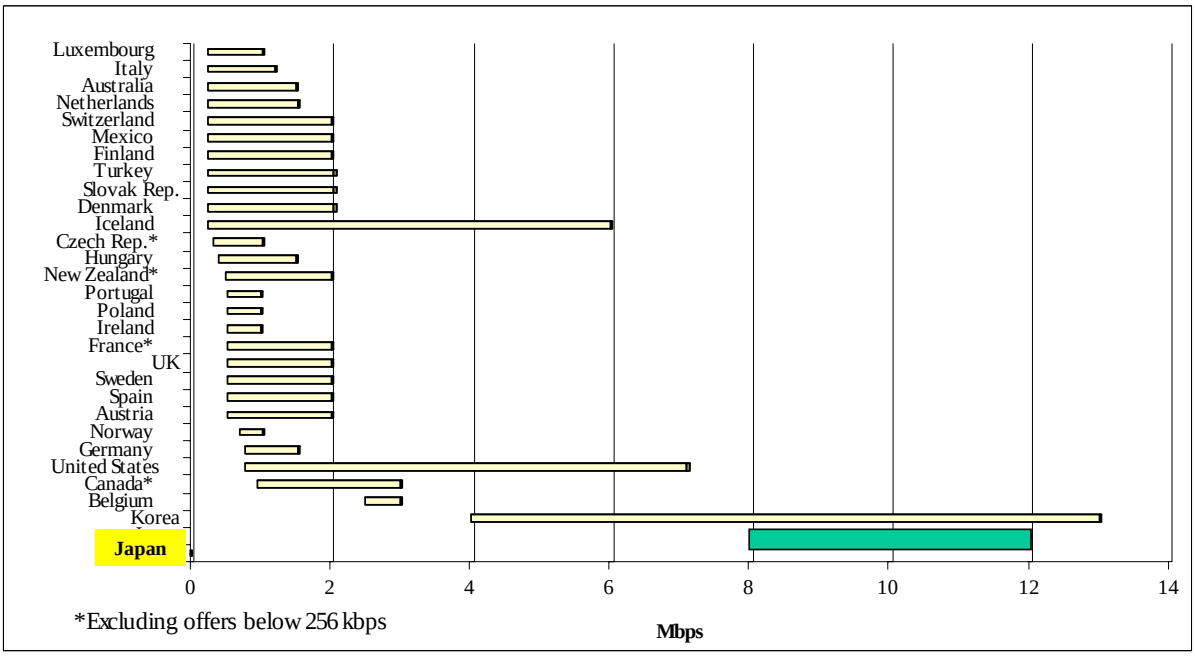
出典：“ITU Internet Reports 2003: Birth of Broadband” (2003年9月)

ブロードバンド通信速度



出典：“ITU Internet Reports 2003: Birth of Broadband” (2003年9月)

ＤＳＬ速度の国際比較



〔注1〕 日本の光ファイバ(100Mbps)及び韓国のVDSL(20Mbps)は除く。

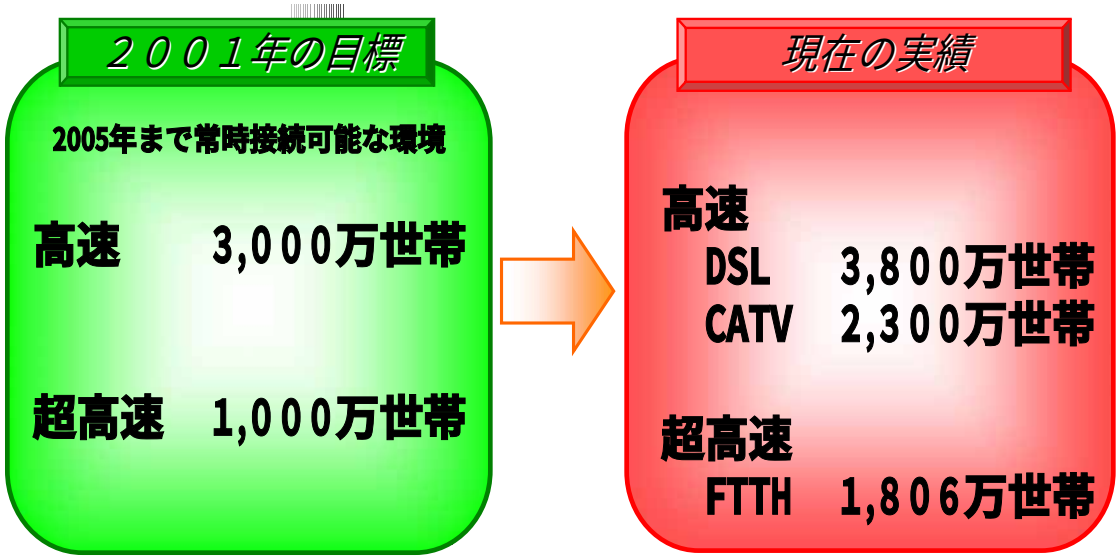
〔注2〕 アイスランド、アメリカで最大容量のサービスは、ビジネス利用者向け（例：ベライゾン: 7.1Mbps = 204ドル）。

（出典：「ITU Strategic Planning Workshop on Promoting Broadband Background Paper (2003年4月)」により総務省作成）

２．ブロードバンドの「加入可能」世帯数

電気通信事業者によるインフラ整備も進んでおり、「加入可能」世帯数でみると、ＤＳＬで３，８００万世帯、ケーブルインターネットで２，３００万世帯、加入者系光ファイバ（Fiber To The Home：ＦＴＴＨ）については１，８０６万世帯に達しており、２００１年１月に策定された「e-Japan 戦略」の目標を大幅に上回っている。

ブロードバンドの「加入可能」世帯数

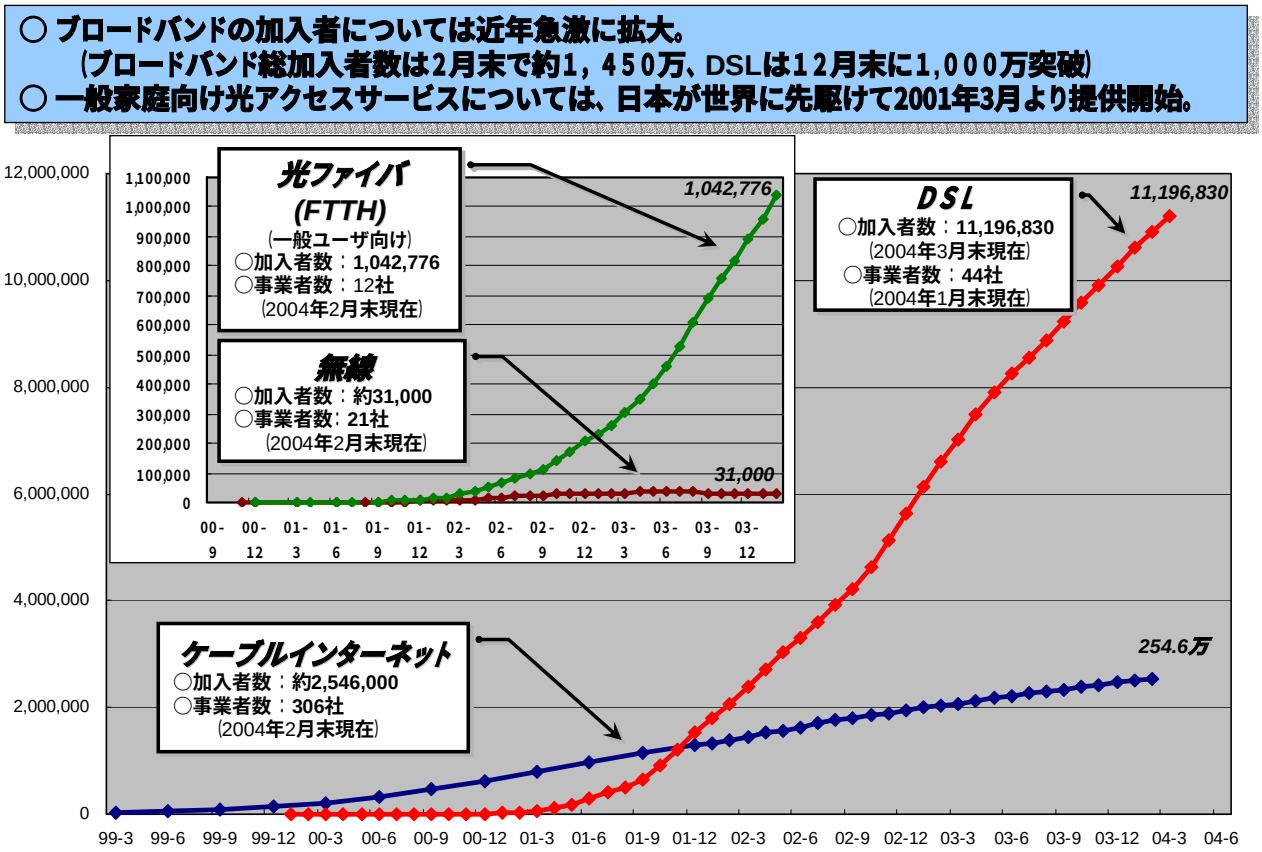


３．ブロードバンドの実加入者数

料金の低廉化とインフラ整備の進捗を受けて、ブロードバンド加入者も急速に増加しており、ＤＳＬ加入者は１，０００万を超え、ケーブルインターネット加入者は約２５０万、加入者系光ファイバ（ＦＴＴＨ）加入者は約１００万に達している。

また、現状では加入者数が少ないものの、ＦＷＡ（Fixed Wireless Access）や屋外又は屋内の無線ＬＡＮ等無線系のアクセスサービスも、ブロードバンド・サービスの一つとして期待されている。

我が国におけるブロードバンド加入者数の推移

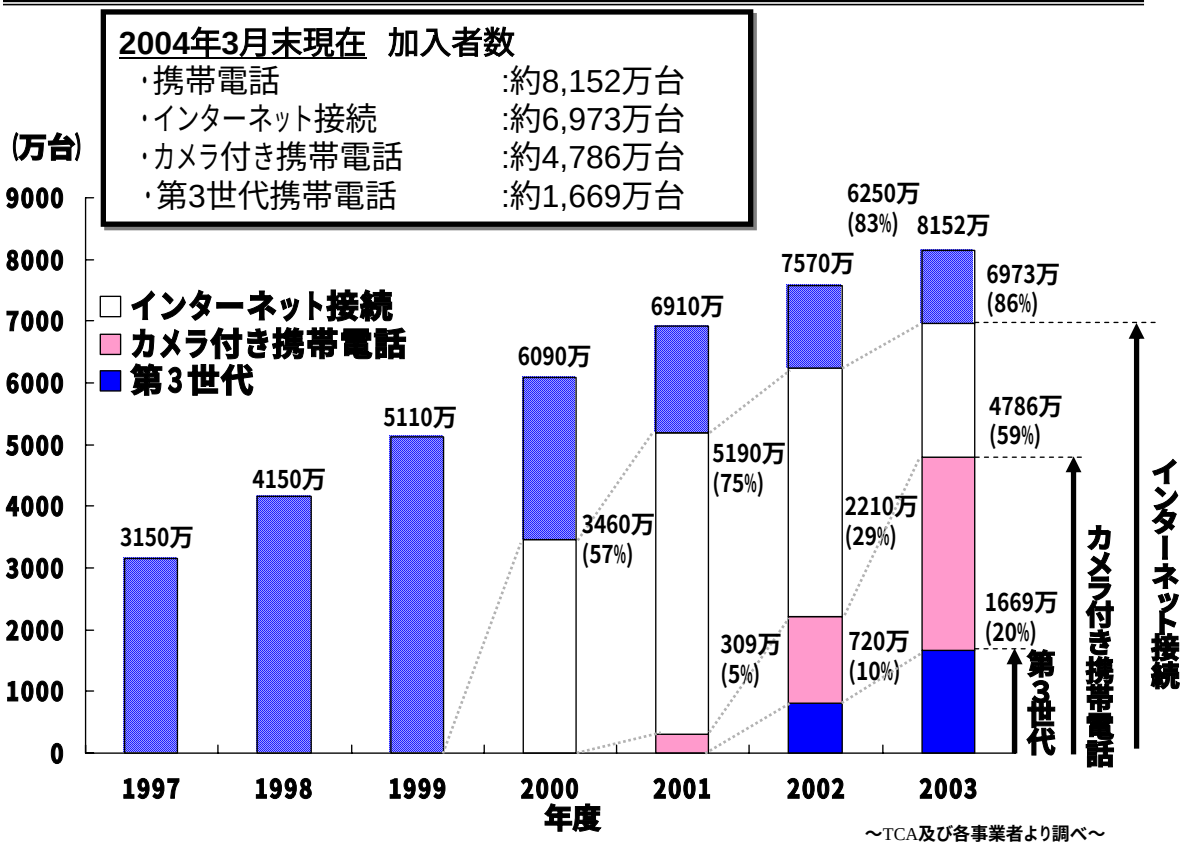


４．携帯電話からのインターネット接続のブロードバンド化

また、我が国では、インターネット接続が可能な携帯電話が８割を超え、第３世代携帯電話（３Ｇ）では写真のみならず動画も送ることができるまでにブロードバンド化している。

更に、２０１０年頃の実用化を目指して開発・標準化が進められている第４世代携帯電話（４Ｇ）では、１００Ｍ（メガビット毎秒）クラスの伝送を可能とすることが企図されており、有力なブロードバンド・アクセスの手段になるものと期待されている。

高機能携帯電話の普及の推移

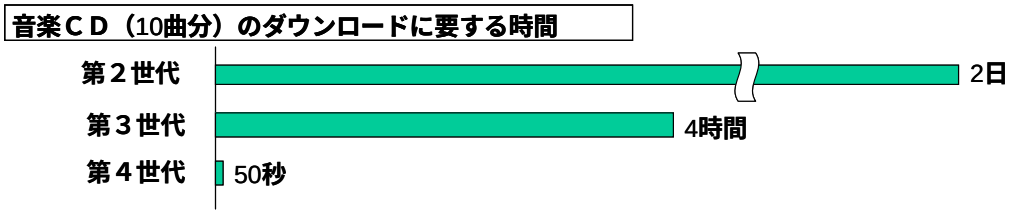


携帯電話サービスの高度化

携帯電話における技術の進歩

	サービス開始	データ伝送速度
第１世代	1979 年	**アナログ方式**
第２世代	1993 年	28.8kbps
第３世代 IMT-2000	2001 年	W-CDMA：384kbps、**最大** 14Mbps(HSDPA)※ CDMA2000 1x：144kbps CDMA2000 1x EV-DO：**最大** 2.4Mbps
Systems Beyond IMT-2000	2010 年頃	100Mbps

※現在、情報通信審議会において審議中



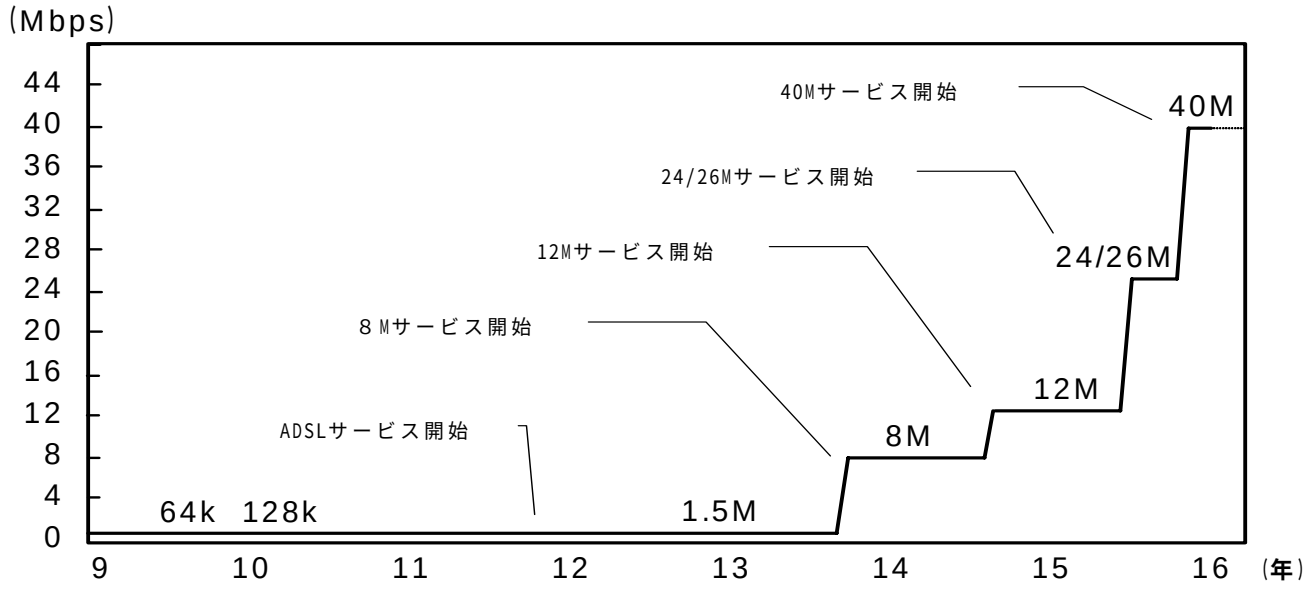
５．サービスの一層のブロードバンド化

一般に、ブロードバンドの加入者は、「速さ」や「品質」等のブロードバンドに対する要求水準を徐々に上げてくるものであり、インフラ整備とアプリケーションの関係は、インフラが整備されると今度はアプリケーションが進化し、アプリケーションが進化すると今度はそれに見合うインフラ整備への要望が生じるという関係にあると考えられるため、インフラの整備とアプリケーションの開発・振興は継続的に行われることが重要であると言える。

実際、電気通信事業者は、そのサービスを一層ブロードバンド化させており、ＤＳＬでベストエフォート(注)ベースで４５Ｍ（メガビット毎秒）クラス、加入者系光ファイバ（ＦＴＴＨ）で１００Ｍクラスのサービスが登場している状況にある。

（注）ベストエフォート：
可能な限り、高品質の情報伝送サービスの提供を行うこと。電話は、最低限のサービス品質(遅延や帯域幅など）を保障するものであるのに対し、ベストエフォートのサービスは、品質保証をするものではないが、品質保証がないために低品質のサービスを意味するものではない点には留意を要する。

アクセス網（メタル回線）のブロードバンド化



(各社HP等を参考に作成)

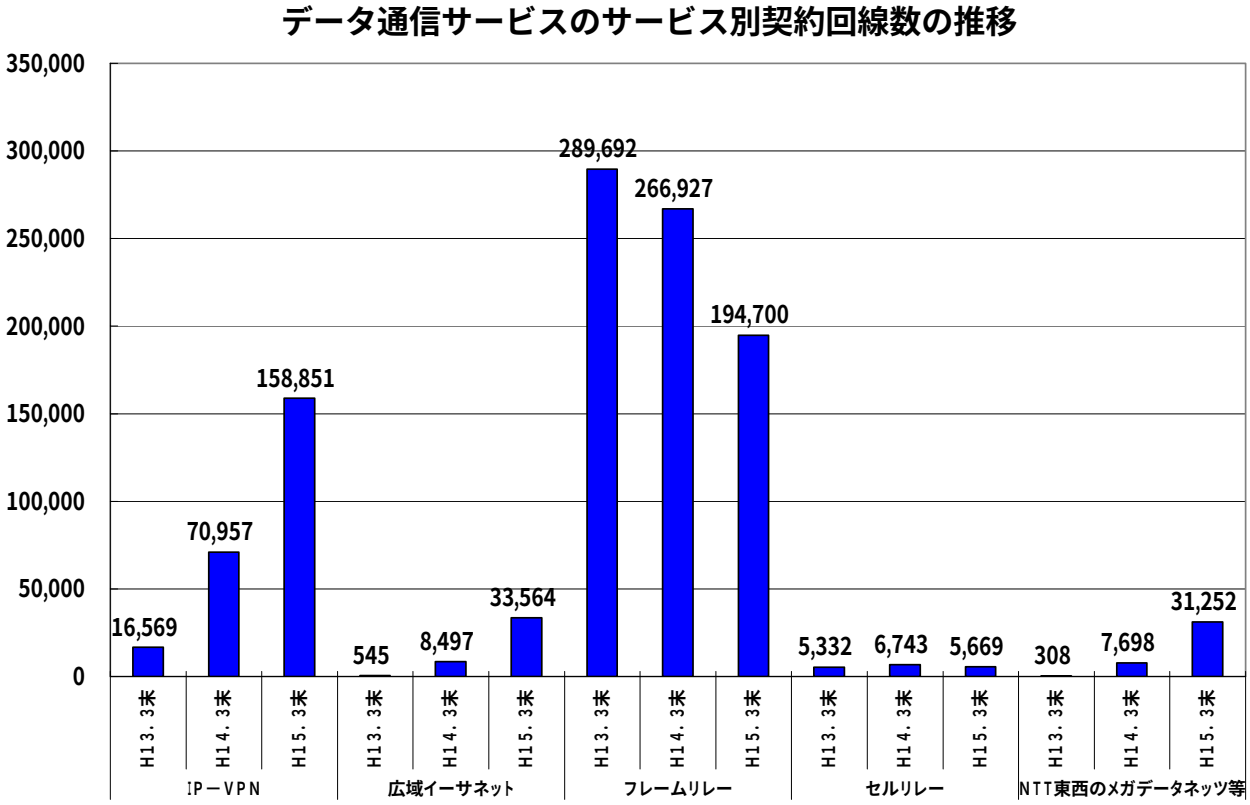
主な加入者系ネットワークの種類と伝送速度

分類		名称	伝送速度	サービス開始年
固定系	メタリックケーブル	固定電話	電話サービス：上り33.6kbps／下り56kbps	1890年
		ISDN(64kbps)	64kbps	1988年
		xDSL	ADSL：上り最大1Mbps／下り最大45Mbps程度 SDSL：1対で最大2Mbps HDSL：2対で最大2Mbps VDSL：上り2.3Mbps程度／下り52Mbps程度	1999年
	光メタル併用(HFC)	ケーブルインターネット	最大30Mbps程度	1996年
	光ファイバ	FTTH	最大100Mbps	2000年
	無線系	FWA	最大156Mbps	1999年
移動系	地上系	携帯電話・PHS	PHS　：32kbps～128kbps 携帯電話：28.8kbps(PDC)～64kbps(cdmaOne) IMT-2000：384kbps（DS-CDMA）、2.4Mbps（MC-CDMA)	携帯電話：1987年 PHS　：1995年 IMT-2000：2001年
		無線LAN(2.4G)	最大54Mbps	2002年
	衛星系	衛星移動電話	最大64kbps	1996年
		衛星通信	数kbps	1999年 （データ通信）

出典：総務省「平成15年度情報通信白書」(一部加工)

６．法人によるブロードバンド利用の拡大傾向

ブロードバンドによるＩＰ－ＶＰＮ等の品質向上に伴い、専用線やフレームリレーからＩＰ－ＶＰＮ、更にはより安価なインターネットＶＰＮに移行する法人利用者が増加している。国内のみならず海外拠点とのＩＰ－ＶＰＮ等の導入を検討する法人利用者もあり、ブロードバンドは個人利用者によるインターネット利用だけでなく、法人の業務用にも活用され、社会経済活動の基盤となっている状況にある。



出典：総務省「平成 15 年度　電気通信事業分野における市場の現況」

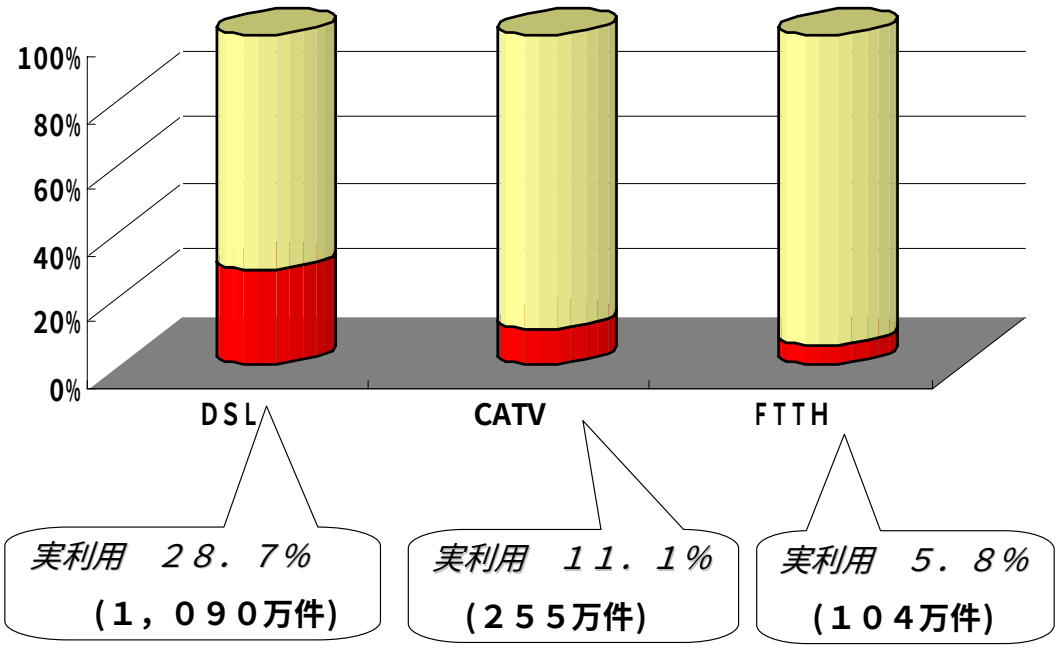
フレームリレー：転送するデータを可変長の「フレーム」という単位に分割して送受信する通信サービス。
ＩＰ－ＶＰＮ：Internet Protocol-Virtual Private Network の略。電気通信事業者の閉域ＩＰ網を経由して構築することによってセキュリティを高めた仮想的な閉域網サービス。
インターネットＶＰＮ：公衆網であるインターネットに接続する回線の両端に装置（ＶＰＮ装置）を接続すること等によって、インターネットを仮想的な閉域網として利用する。
広域イーサネット：ＩＥＥＥ（米国電気電子技術者協会）８０２．３委員会により標準化されたＬＡＮ規格であるイーサネットで使用されているスイッチング・ハブを組み合わせて構築した通信サービス。
セルリレー　：ＡＴＭ（非同期転送モード）により、伝送するデータを固定長の「セル」という単位に分割して送受信する通信サービス

７．ブロードバンドの実利用率

他方、実利用という観点からみれば、ブロードバンドの「実際の加入者数」は、「加入可能」数に比べると未だ低いと言わざるを得ない。例えば、ＦＴＴＨとＤＳＬの「実際の加入者数」は、それぞれ「加入可能」数の６％及び２９％に過ぎず、多くの人々にとって、ブロードバンドは、「利用可能だが、実際に対価を支払って利用するまでには至っていない」という状況にあると言える。

我が国におけるブロードバンドの実利用率

（2004年2月末現在）



（注）ブロードバンド加入者数の加入可能数に対する割合。

（出典：総務省調べ）

第２章　e-Japan 戦略Ⅱによる戦略の進化

１.「ＩＴ利活用」への戦略の進化

こうしたブロードバンドの普及状況をも踏まえ、２００３年７月に策定された「e-Japan 戦略Ⅱ」においては、第一期の「ＩＴ基盤整備」から、第二期の「ＩＴ利活用」へと、戦略を進化させている。

具体的には、「医療」、「食」、「生活」、「中小企業金融」、「知」、「就労・労働」、「行政サービス」という７つの分野において、ＩＴの高度利活用の取組を民と官が連携して実践することにより、ＩＴの利活用の成果を国民に広く提示することが提案されている。

このような先導的取組は、ＩＴの利活用を通じて、例えば、無駄な支出や待ち時間の縮減、安心で便利な生活環境の実現、一人一人の能力の発揮、効率的な資金調達、業務改善による生産性の向上、高付加価値化による新たなサービスと市場の創出等、社会的に大きな効果が期待できるものであり、民と官を挙げて取り組むべき課題と言える。

２．将来的なトラヒック増加とバックボーンの現状把握の必要性

他方、こうした先導的な取組は、大容量のトラヒックをネットワーク上に発生させるものである。

また、ユビキタス・ネットワーク社会のもとで、ブロードバンドの利用主体が、「ヒト」だけではなく「モノ」にまで拡張され、「モノ」と「モノ」との通信が２４時間行われる社会が想定されている点にも、留意しなければならない。

第１章で述べたとおり、アクセス網（加入者系ネットワーク(注)）におけるＤＳＬ、ケーブルインターネット及びＦＴＴＨの「実際の加入者数」と「加入可能」数とを対比してみると、確かにブロードバンドの実利用率は依然として低いと言える。

しかし、「e-Japan 戦略Ⅱ」に盛り込まれた先導的取組により、「実際の加入者数」が増え、かつ、個々の加入者が大容量のトラヒックを発生させた場合に、バックボーン（中継系ネットワーク(注)）はそれに対応し得るのか、ということは検証されていない。

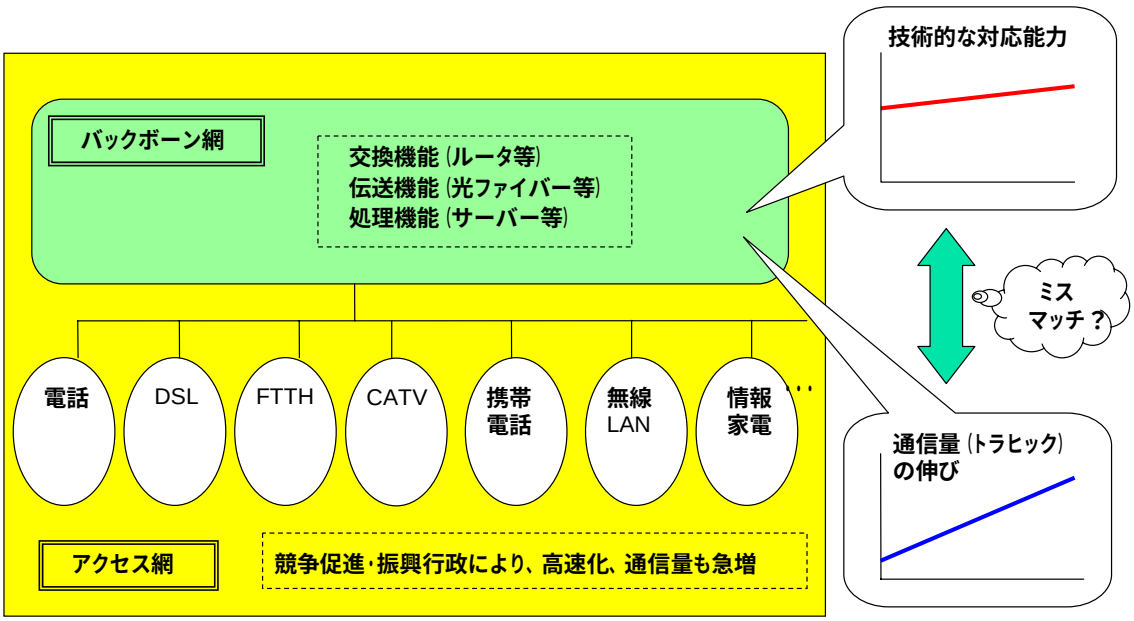
そこで、我が国のバックボーンの現状と課題を、第３章以下で見ていくこととする。

（注）「加入者系ネットワーク」とは、「加入者系配線」（集線点から加入者宅内の端末回線終端装置までの配線）及び「加入者系幹線」（加入者配線に分岐する集線点から加入者収容局内の端末系端局装置までの間の端末系幹線路）をいう。

「中継系ネットワーク」とは、「加入者系ネットワーク」を除く、電気通信事業者のネットワーク内の中継系伝送路、交換設備等をいう。

アクセス網とバックボーン

アクセス網からのトラヒック急増に対応できるバックボーンの確保が必要



３．高品質／高信頼性と情報セキュリティの確保

また、「e-Japan 戦略Ⅱ」では、「安全・安心な利用環境の整備」も提唱され、高品質／高信頼性と、情報セキュリティの確保が求められている。

そこで、トラヒック制御と品質保証及び障害連鎖防止策について、第６章及び第８章で検討することとする。

第３章　我が国のバックボーンの現状

１．各ＩＳＰのバックボーンへの関わり

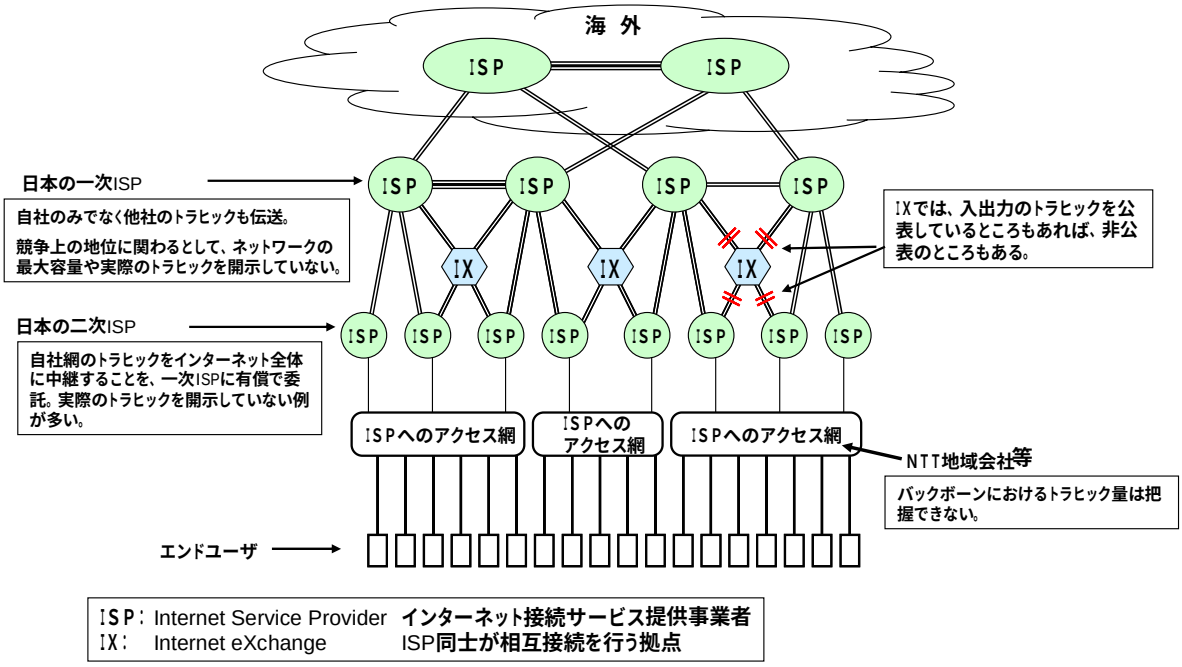
「インターネット」は、インターネット接続サービス提供事業者（ＩＳＰ；Internet Service Provider）のネットワーク、企業ネットワーク、学術ネットワーク、官公庁ネットワーク等々、多種多様なネットワークがInternet Protocol（ＩＰ）によって接続された、ネットワークの総称である。

ＩＳＰのネットワークだけをみても、日本全国及び国際的にネットワークを展開している一次ＩＳＰ、局所的に大きなネットワークをもつ二次ＩＳＰ、非常に小規模なＩＳＰなど、そのレベルは様々であり、現在、８，０００社以上のＩＳＰが林立している。

この他に、企業ネットワーク、学術ネットワーク、官公庁ネットワーク等があり、ネットワークによっては、小規模なＩＳＰよりも遙かに大規模なものもあって、インターネットの構造は複雑になっている。

ＩＳＰに限ってＩＳＰとバックボーンへの関わりを模式的に示してみたのが下図であるが、各ネットワークの容量やピーク時のトラヒックについては、競争上の地位に関わることもあって、各ＩＳＰが情報を開示していないことから、我が国のインターネット上でトラヒック量がどの程度あるのか、ネットワーク容量にどの程度余裕があるのかについては、これまで明らかにされていない。

各ISPのバックボーンへの関わり



２．ＩＸにおけるトラヒックの増勢傾向

しかし、ＩＸ（Internet eXchange；インターネット接続事業者間を相互に接続する相互接続点）の中には、トラヒックを公表しているところがあり、これにより増勢の「傾向」をうかがうことはできる。

日本の３大ＩＸであるＪＰＩＸ、ＪＰＮＡＰ、ＮＳＰＩＸＰの合計値の推移をみると、ここ数年、年間２～３倍のペースで増加しており、２００３年には最大で９０Ｇｂｐｓ（ギガビット毎秒）に達している。

我が国のＩＸにおけるトラヒックの最大値（単位：Ｇｂｐｓ）

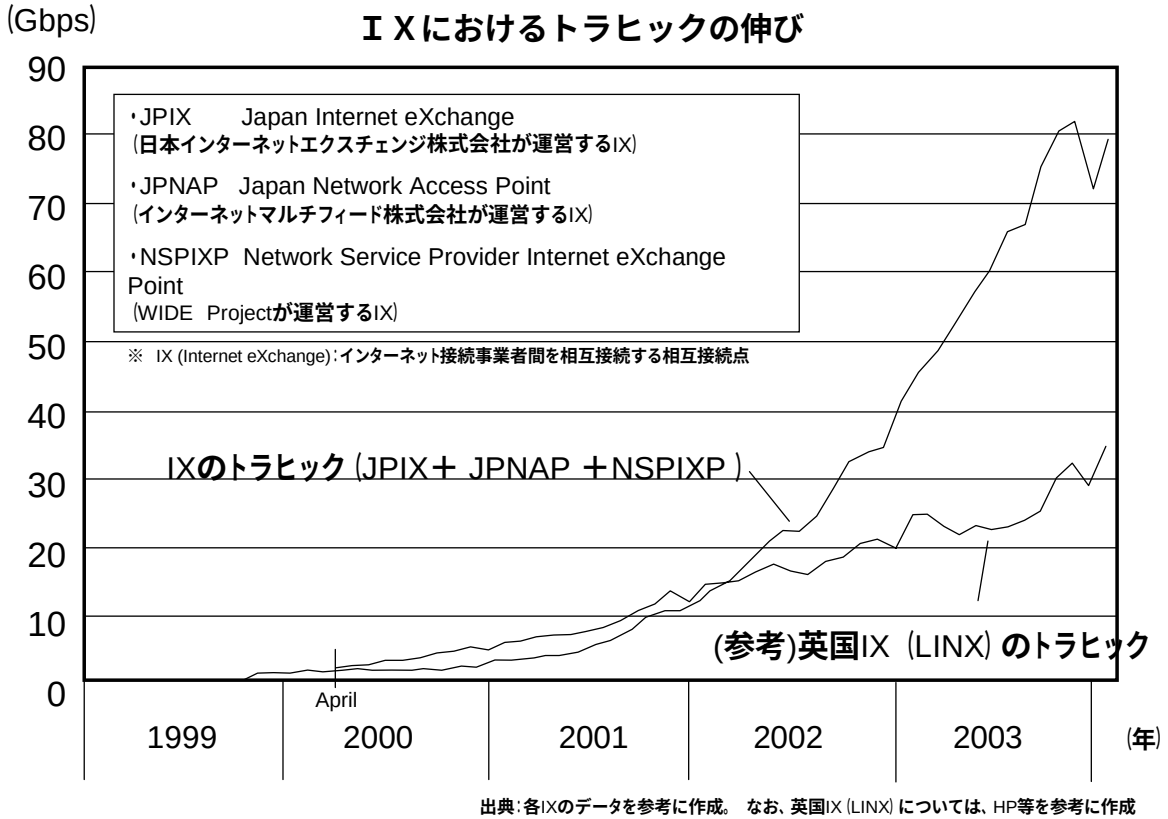
	２００１年末	２００２年末	２００３年末
NSPIXP（東京＋大阪）	５．５	１３．０	１８．６
JPIX（東京）	６．５	２０	３２
JPNAP（東京＋大阪）	２	１０．６	４０
合　計	１４．０	４３．６	９０．６

※　各年度におけるトラヒックの最大値

約３倍　約２倍

米国の大手ＩＸがトラヒック情報を開示していないため、米国との単純な比較は困難であるが、欧州最大のＩＸであるＬＩＮＸ（London INternet eXchange）はトラヒック情報を開示しており、ＬＩＮＸと比較してみると、我が国のバックボーンにおけるトラヒックの増勢傾向がより強いことがうかがえる。

ＩＸにおけるトラヒックの伸び



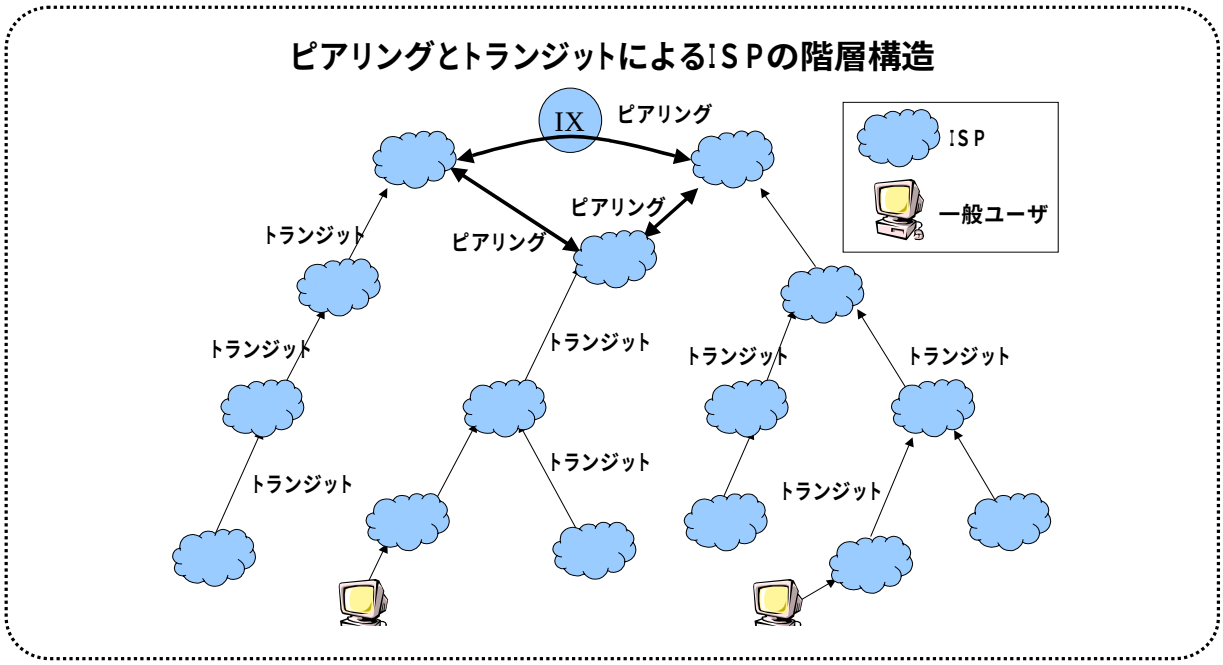
出典：各IXのデータを参考に作成。　なお、英国IX（LINX）については、HP等を参考に作成

※　LINX：The London Internet Exchange
※　1日のピークトラヒックの一ヶ月の平均値

なお、インターネット上のトラヒックは、ＩＸで行われるパブリック・ピアリング(注)だけではなく、ＩＸを介さないプライベート・ピアリング(注)やトランジット(注)によって伝送されるものもあり、実際には、より大量のトラヒックが伝送されていると考えなければならない。

（注）「ピアリング」：ＩＳＰ間でお互いに相手方ＩＳＰあてのトラヒックを交換しあうこと。一般的には無償接続。ＩＸで行われるピアリングを「パブリック・ピアリング」、ＩＸを介さないピアリングを「プライベート・ピアリング」という。

「トランジット」：他のＩＳＰからのトラヒックをインターネット全体に中継すること（他のＩＳＰに対してインターネットの経路を提供すること。）。一般的には有償サービス。



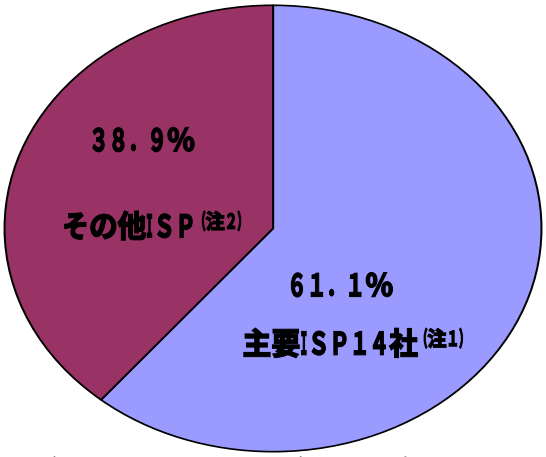
３．トラヒックの現状調査

当研究会では、我が国の主要なＩＳＰ１４社(注)に対して、ＩＸにおけるパブリック・ピアリングだけでなく、プライベート・ピアリング及びトランジットにおけるピーク時のトラヒックもアンケート調査した。

（注）インターネットイニシアティブ、ＮＴＴコミュニケーションズ、ケイ・オプティコム、ケーブル・アンド・ワイヤレスＩＤＣ、ＫＤＤＩ、ＪＥＮＳ、ソフトバンクＢＢ、ドリーム・トレイン・インターネット、日本テレコム、日本電気、ニフティ、パワードコム、ぷららネットワークス、松下電器産業

この主要ＩＳＰ１４社のトラヒックが我が国インターネット全体に占める割合を正確に計測することは困難であるが、１事業者のデータセンターから伝送されるトラヒックの割合という限定された形では、この主要１４社へのトラヒックが６割超を占めている状況にあり、ある程度の類推を働かせることは可能である。

データセンター事業者から発信されるデータの発信先比率



(注1) インターネットイニシアティブ、NTTコミュニケーションズ、ケイ・オプティコム、ケーブル・アンド・ワイヤレスIDC、KDDI、JENS、ソフトバンクBB、ドリーム・トレイン・インターネット、日本テレコム、日本電気、ニフティ、パワードコム、ぷららネットワークス、松下電器産業
(注2) その他ISPのAS数は7,110
(注3) ASとは、ある経路制御方針によって運営されるネットワークのことをいう。
全国展開しているISPもインターネット全体からみると一定の経路制御方針によって運営されている1つのネットワークであり、1つのASとして捉えられ、AS番号を割り当てられている。

出典:エスアールエス・さくらインターネットの調査結果(2004年4月8日 0時～1時、池袋データセンタ)を総務省にて加工

主要ＩＳＰ１４社へのアンケート調査結果は次のとおりである。

（１）ＩＸにおけるパブリック・ピアリング

ＩＸにおけるパブリック・ピアリングについては、主要ＩＳＰは東京地区のＩＸ、大阪地区のＩＸ及び海外のＩＸでのみ接続している状況にあり、ＩＸにおいて接続している各ＩＳＰの電気通信回線設備の容量（以下「回線容量」という。）の合計値は、東京地区で１８２Ｇ（ギガビット毎秒）、大阪地区で４３Ｇ、海外で５Ｇとなっており、東京と大阪の比率は４：１となっている。

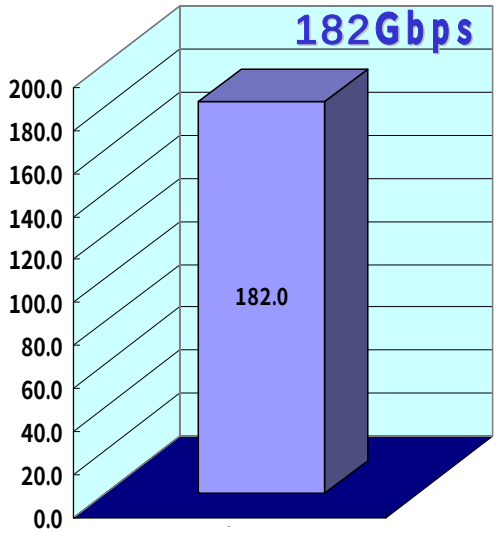


図　東京地区ＩＸ接続回線容量

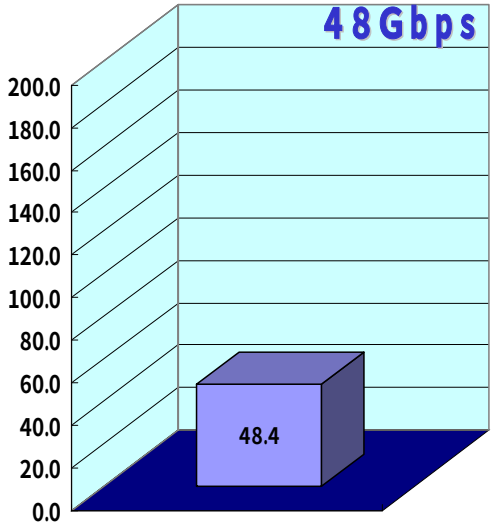


図　大阪地区及び海外でのＩＸ接続回線容量

また、ＩＸにおけるピーク時のトラヒックを回線容量の半分程度と見込んでいるＩＳＰが多いことを勘案すると、主要ＩＳＰがＩＸにおいて見込んでいるピーク・トラヒックの合計値は１１５Ｇと試算される。

（２）プライベート・ピアリング

プライベート・ピアリングについては、ほとんどのＩＳＰが東京で行っており、各社の回線容量を単純に合計した２７８Ｇのうち、２４７Ｇ（８９％）が東京でのものとなっている。

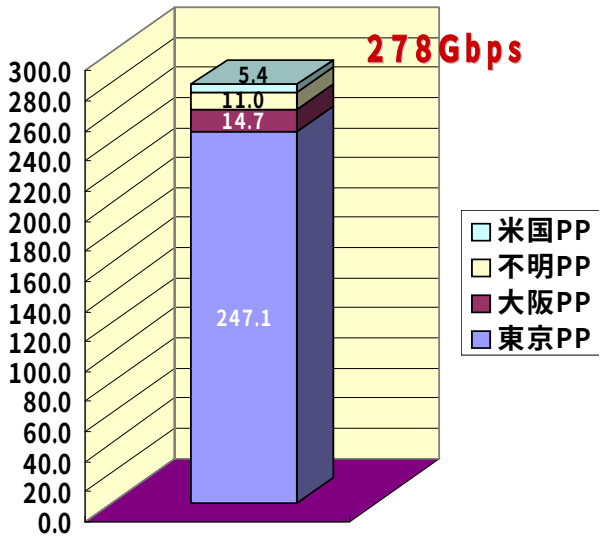


図　プライベート･ピアリング　回線容量

プライベート・ピアリングについても、ピーク時のトラヒックを回線容量の半分程度と見込んでいるＩＳＰが多いことを勘案すると、回線容量の合計値にあまり重複がないとすれば、主要ＩＳＰがプライベート・ピアリングにおいて見込んでいるピーク・トラヒックの合計値は１２０～１３０Ｇ程度と試算される。

（３）トランジット

トランジットについては、購入と販売について集計した。販売については、販売地点が不明な回答が多いが、購入については、各社の回線容量の合計値１１５Ｇ中東京地区でのトランジット購入が７８Ｇと６８％を占めている状況にある。

主要ＩＳＰにおいては、購入したトランジット１１５Ｇと販売したトランジット１５３Ｇに重複は少ないと仮定すれば、トランジットの回線容量の合計値は２００～２５０Ｇ程度と見込まれる。

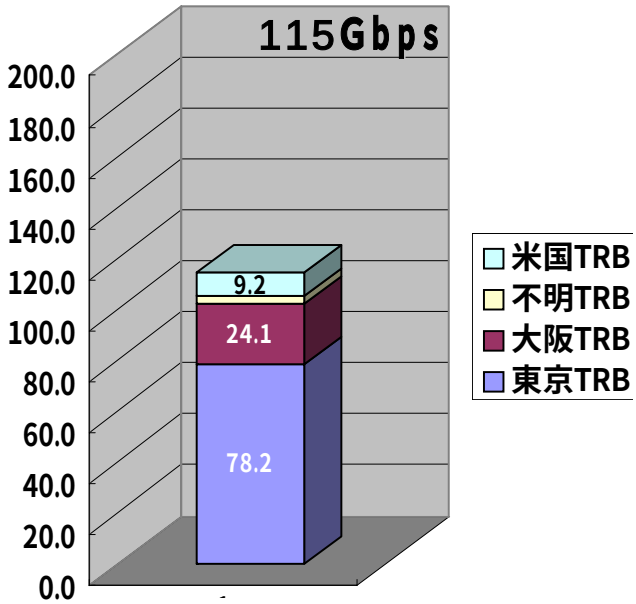


図　Transit 購入接続回線容量

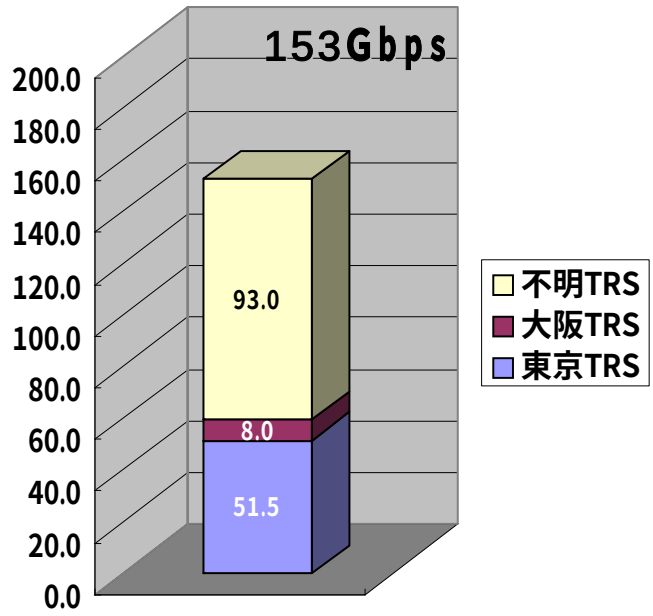


図　Transit 販売接続回線容量

また、ピーク時のトラヒックについてもＩＸ及びプライベート・ピアリングと同様に回線容量の半分程度と見込んでいるＩＳＰが多いと仮定すれば、トランジットにおいて見込まれているピーク・トラヒックの合計値は１００Ｇと試算される。

（４）トラヒックの把握の意義

（ア）主要ＩＳＰが他のＩＳＰとの間で接続している回線容量の合計値は、プライベート・ピアリング２７８Ｇ、トランジット２６７Ｇ、ＩＸにおけるパブリック・ピアリング２３０Ｇとなっており、プライベート・ピアリング及びトランジットにおける各社間の重複を勘案すれば、概ね１：１：１となっている。

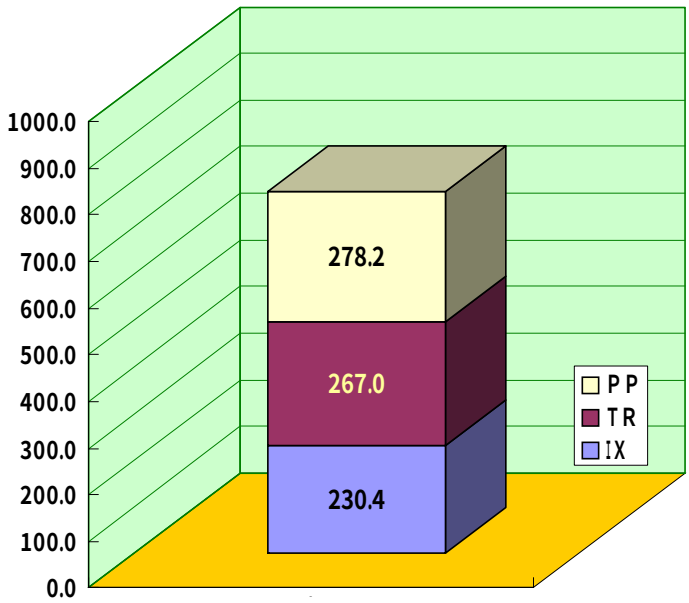


図　主要ＩＳＰ間の接続回線容量（Ｇｂｐｓ）

（イ）また、２００４年２月における主要ＩＳＰ各社の実際のピーク・トラヒックを合計してみると、ＩＮ（主要ＩＳＰへの上りのトラヒック）で６１％、ＯＵＴ（主要ＩＳＰからの下りのトラヒック）で５５％をプライベート・ピアリングが占めている状況にあり、

① 主要ＩＳＰ間のトラヒック交換については、プライベート・ピアリングがトランジットやＩＸにおけるパブリック・ピアリングよりも大きな役割を果たしていること、

② 公表されている主要ＩＸのトラヒック情報だけではインターネット全体におけるトラヒックを把握できず、プライベート・ピアリングやトランジットを含めてトラヒックを把握する必要があること、

が明らかになった。

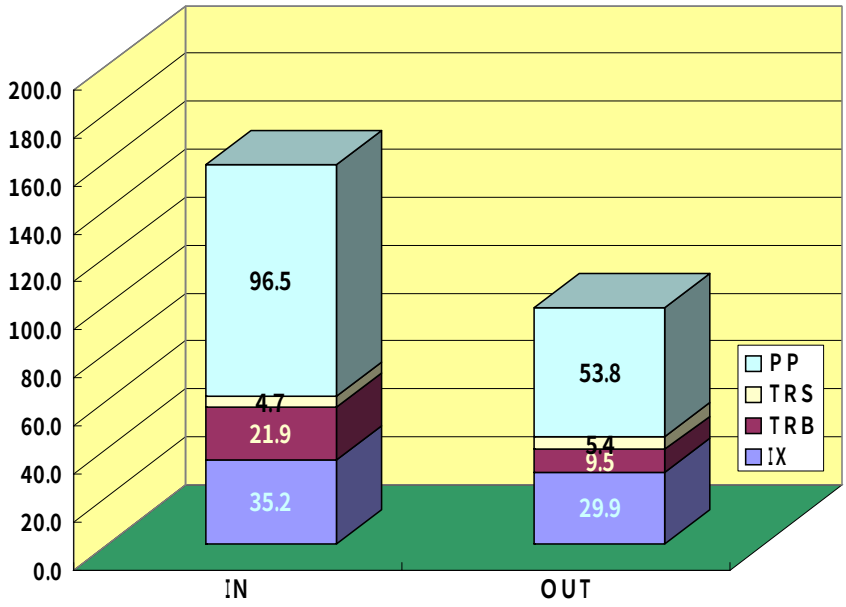
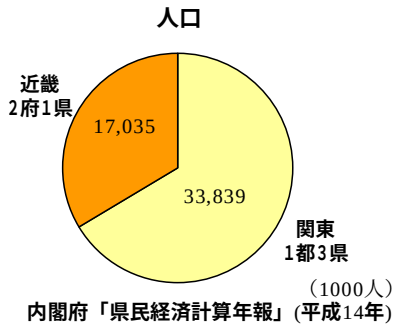


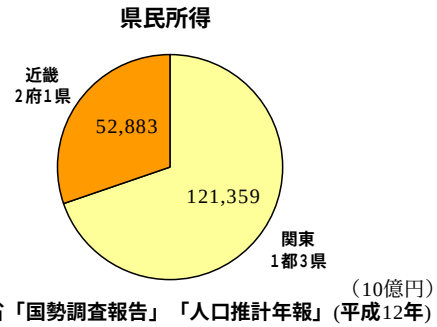
図 主要ISP間のピーク･トラヒックの合計値（２００４年2月、回答事業者のみ集計、Gbps）

（ウ）また、回線容量の合計値を東京と大阪とで比較してみると、ＩＸにおけるパブリック・ピアリングで東京：大阪＝４：１、プライベート・ピアリングで東京：大阪＝１７：１、トランジット購入で東京：大阪＝３：１と、いずれも東京一極に集中している状況にある。

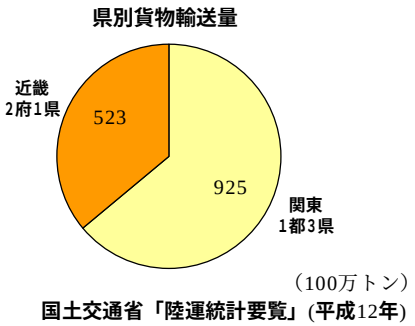
人口、県民総所得、県別自動車輸送量、県別輸送人員を見ても、関東の１都３県（東京・神奈川・埼玉・千葉）と近畿の２府１県（大阪・兵庫・京都）の比率は概ね２：１となっていることからしても、インターネットのトラヒックの東京一極集中は顕著であると言える。



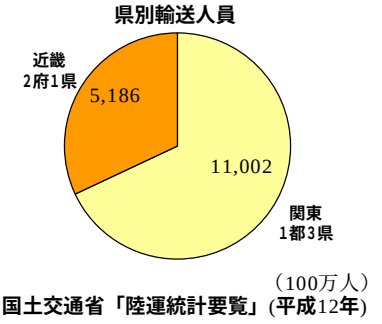
内閣府「県民経済計算年報」(平成14年)



総務省「国勢調査報告」「人口推計年報」(平成12年)



国土交通省「陸運統計要覧」(平成12年)



国土交通省「陸運統計要覧」(平成12年)

（エ）更に、固定電話や携帯電話のトラヒックと比較してみても、

① 同一都道府県内に終始するトラヒックは、固定電話発のトラヒックで７４．１％（２００２年度全国平均)、携帯電話発のトラヒックで８０．６％（同）となっていること、

② 地域ブロックに終始するトラヒックは、固定電話発のトラヒックで８３．６％以上（２００２年度)、携帯電話発のトラヒックでは８６．６％以上（同）となっていること、

から、東京を中心にトラヒックが交換されるインターネットは、固定電話や携帯電話とは、トラヒック・パターンを大きく異にしていると言える。

図　固定電話発：同一都道府県内に終始する通信回数の比率

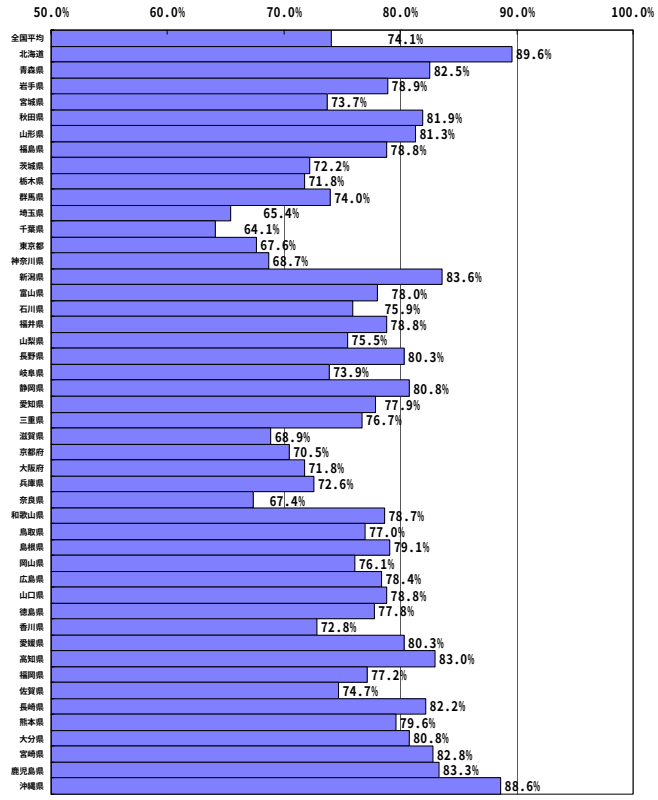
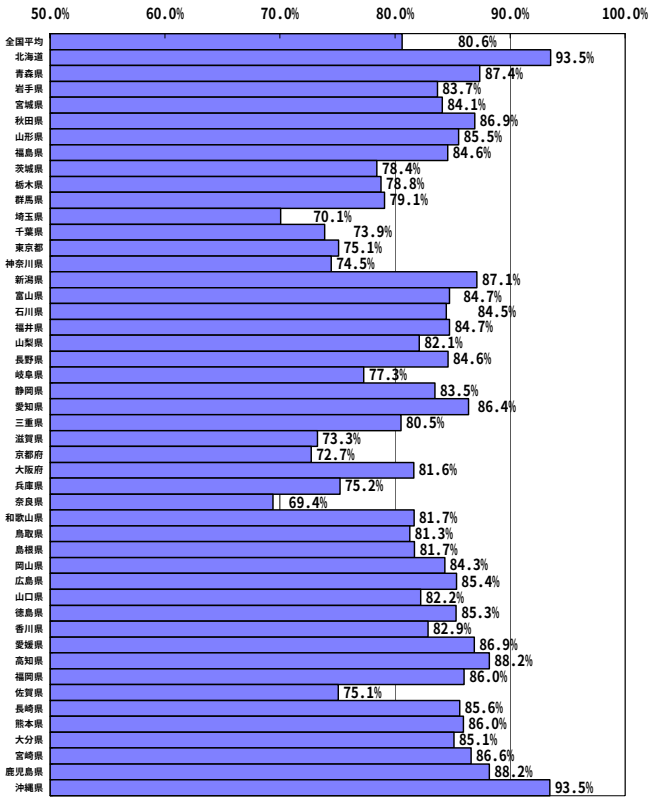


図　携帯電話発：各都道府県別同一都道府県内に終始する通信回数の比率



出典：総務省「トラヒックからみた我が国の通信利用状況（平成１４年度）」

図　固定電話発：地域ブロック間トラヒック交流状況

（単位：百万回）

	北海道	東北	関東	信越	北陸	東海	近畿	中国	四国	九州	沖縄	発信計
北海道	2,769	44	181	7	4	20	39	8	4	12	1	3,089
	(89.6%)	(1.4%)	(5.9%)	(0.2%)	(0.1%)	(0.7%)	(1.3%)	(0.3%)	(0.1%)	(0.4%)	(0.0%)	(100.0%)
東北	26	4,224	399	25	7	32	50	9	4	12	1	4,789
	(0.5%)	(88.2%)	(8.3%)	(0.5%)	(0.1%)	(0.7%)	(1.1%)	(0.2%)	(0.1%)	(0.3%)	(0.0%)	(100.0%)
関東	172	423	22,792	279	97	595	769	172	82	308	26	25,715
	(0.7%)	(1.6%)	(88.6%)	(1.1%)	(0.4%)	(2.3%)	(3.0%)	(0.7%)	(0.3%)	(1.2%)	(0.1%)	(100.0%)
信越	4	22	254	1,947	14	39	32	6	2	6	0	2,326
	(0.2%)	(1.0%)	(10.9%)	(83.6%)	(0.6%)	(1.7%)	(1.4%)	(0.3%)	(0.1%)	(0.3%)	(0.0%)	(100.0%)
北陸	3	5	84	15	1,300	42	82	5	2	5	0	1,543
	(0.2%)	(0.4%)	(5.4%)	(1.0%)	(84.1%)	(2.8%)	(5.3%)	(0.4%)	(0.2%)	(0.3%)	(0.0%)	(100.0%)
東海	16	31	551	45	43	7,082	260	24	24	49	4	8,129
	(0.2%)	(0.4%)	(6.8%)	(0.6%)	(0.5%)	(87.1%)	(3.2%)	(0.3%)	(0.3%)	(0.6%)	(0.0%)	(100.0%)
近畿	33	52	748	42	78	287	10,588	202	108	184	11	12,333
	(0.3%)	(0.4%)	(6.1%)	(0.3%)	(0.6%)	(2.3%)	(85.9%)	(1.6%)	(0.9%)	(1.5%)	(0.1%)	(100.0%)
中国	5	8	171	7	6	37	181	3,418	49	82	1	3,965
	(0.1%)	(0.2%)	(4.3%)	(0.2%)	(0.2%)	(0.9%)	(4.6%)	(86.2%)	(1.2%)	(2.1%)	(0.0%)	(100.0%)
四国	3	4	82	2	3	16	103	62	1,668	17	1	1,961
	(0.1%)	(0.2%)	(4.2%)	(0.1%)	(0.1%)	(0.8%)	(5.3%)	(3.2%)	(85.1%)	(0.9%)	(0.0%)	(100.0%)
九州	11	17	310	11	9	62	181	96	23	6,395	17	7,132
	(0.2%)	(0.2%)	(4.3%)	(0.1%)	(0.1%)	(0.9%)	(2.5%)	(1.3%)	(0.3%)	(89.7%)	(0.2%)	(100.0%)
沖縄	2	2	27	1	1	4	10	2	1	21	546	617
	(0.3%)	(0.3%)	(4.3%)	(0.2%)	(0.1%)	(0.6%)	(1.6%)	(0.4%)	(0.2%)	(3.3%)	(88.6%)	(100.0%)

（注）　上段は発信通信回数、下段は発信通信比率。

図　携帯電話発：地域ブロック間トラヒック交流状況

（単位：百万回）

	北海道	東北	関東	信越	北陸	東海	近畿	中国	四国	九州	沖縄	発信計
北海道	2,014	16	84	3	3	9	13	3	4	4	1	2,154
	(93.5%)	(0.7%)	(3.9%)	(0.1%)	(0.1%)	(0.4%)	(0.6%)	(0.1%)	(0.2%)	(0.2%)	(0.0%)	(100.0%)
東北	15	2,999	202	13	6	14	16	4	5	5	0	3,279
	(0.5%)	(91.5%)	(6.2%)	(0.4%)	(0.2%)	(0.4%)	(0.5%)	(0.1%)	(0.2%)	(0.2%)	(0.0%)	(100.0%)
関東	64	170	18,799	109	34	236	225	60	31	120	18	19,867
	(0.3%)	(0.9%)	(94.6%)	(0.5%)	(0.2%)	(1.2%)	(1.1%)	(0.3%)	(0.2%)	(0.6%)	(0.1%)	(100.0%)
信越	3	14	145	1,441	9	26	16	3	1	4	1	1,663
	(0.2%)	(0.8%)	(8.7%)	(86.6%)	(0.6%)	(1.6%)	(1.0%)	(0.2%)	(0.1%)	(0.3%)	(0.0%)	(100.0%)
北陸	2	6	48	9	1,125	37	39	4	3	3	1	1,276
	(0.2%)	(0.4%)	(3.7%)	(0.7%)	(88.1%)	(2.9%)	(3.0%)	(0.3%)	(0.3%)	(0.3%)	(0.0%)	(100.0%)
東海	10	16	293	26	25	6,109	126	20	20	22	5	6,672
	(0.1%)	(0.2%)	(4.0%)	(0.4%)	(0.4%)	(91.6%)	(1.9%)	(0.3%)	(0.3%)	(0.3%)	(0.1%)	(100.0%)
近畿	13	16	290	15	32	139	9,011	96	69	47	7	9,734
	(0.1%)	(0.2%)	(3.0%)	(0.2%)	(0.3%)	(1.4%)	(92.2%)	(1.0%)	(0.7%)	(0.5%)	(0.1%)	(100.0%)
中国	3	7	86	3	5	29	102	2,885	31	67	2	3,217
	(0.1%)	(0.2%)	(2.7%)	(0.1%)	(0.2%)	(1.0%)	(3.2%)	(89.6%)	(1.0%)	(2.1%)	(0.1%)	(100.0%)
四国	2	2	42	1	2	10	55	31	1,554	8	1	1,707
	(0.1%)	(0.1%)	(2.4%)	(0.1%)	(0.1%)	(0.6%)	(3.2%)	(1.8%)	(91.0%)	(0.5%)	(0.0%)	(100.0%)
九州	6	7	159	4	7	30	77	64	13	5,503	11	5,881
	(0.1%)	(0.1%)	(2.7%)	(0.1%)	(0.1%)	(0.5%)	(1.3%)	(1.1%)	(0.2%)	(93.6%)	(0.2%)	(100.0%)
沖縄	1	1	22	1	1	4	8	2	7	12	746	804
	(0.1%)	(0.1%)	(2.7%)	(0.1%)	(0.1%)	(0.5%)	(1.0%)	(0.2%)	(0.8%)	(1.4%)	(92.8%)	(100.0%)

（注）　上段は発信通信回数、下段は発信通信比率。

出典：総務省「トラヒックからみた我が国の通信利用状況（平成１４年度）」

（５）地域間トラヒック

全国主要地点間のトラヒックについても情報を集計した。地域間のトラヒックを計測するとしても、ルータで測る以上、トラヒックの始点・終点を特定しにくく、トラヒックの一部でしかない場合も多い。また、東京を経由してから戻ってくる折り返しのトラヒックもあり、集計された情報の解釈に困難な面はあるものの、報告されたデータのうち、東京－大阪間が上り（大阪→東京)、下り（東京→大阪）とも約７０％を占めている。

次に多いのは、大阪－福岡間であり、東北・北海道地区よりも西日本地域に人口１００万人規模の都市が多いこと等を反映したものと考えられる。

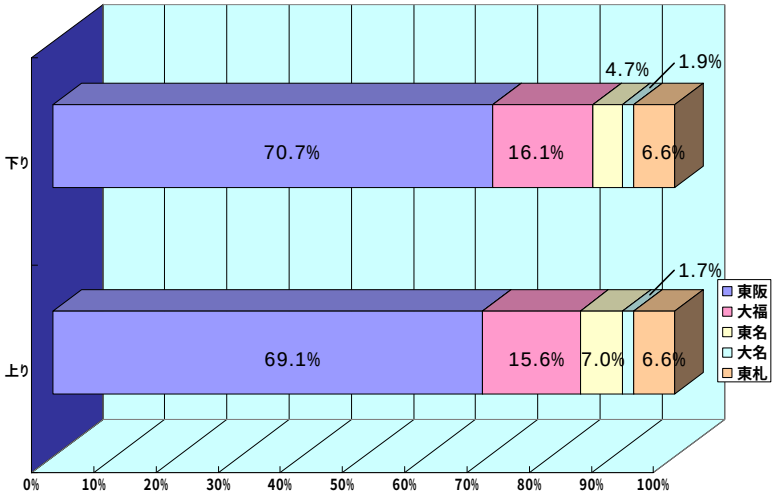


図　主要な地域間のトラヒックの割合
(回答事業者のみ集計)

（６）今後の課題

今回の調査は、我が国インターネットのバックボーンにおけるトラヒックを調査した初めての試みであり、主要各ＩＳＰ間のトラヒック交換について、ＩＸにおけるパブリック・ピアリング、プライベート・ピアリング及びトランジットに分けて回線容量等をアンケート調査したものである。

この結果、

① ＩＸにおけるパブリック・ピアリング、プライベート・ピアリング、トランジットについては、それぞれ同程度の回線容量が用意されていること、

② 主要ＩＳＰ間のトラヒック交換には、プライベート・ピアリングが多用されていること、

③ トラヒック交換は東京に集中していること、

④ 地域間トラヒックについても東京－大阪間が７割を占めていること、

等が明らかになった。

今後、我が国のインターネットの在り方を考える上では、国内全体でどの程度のトラヒックがどのように発生しているのかを把握すべきであるとの意見もある。

他方、トラヒック情報は、各ＩＳＰの経営情報に属するものであり、情報の開示を求めることが困難であることに加え、実際のトラヒックは、各ＩＳＰのネットワーク形態に依存しており、集計するトラヒック情報の様式を統一することにも難しい面がある。

このため、各ＩＳＰからのトラヒック情報を積み上げる方法ではなく、これまでに得られた情報と公開情報やサンプル調査を基に統計的な手法を駆使して、一定の仮定を置いてトラヒックの総量とパターンを推計するという方法を開発すべきであると考えられる。

また、トラヒック情報は定期的に集計し、分析してこそ意義をもつものであり、どういう情報をどこまでなら出せるかという点について、ＩＳＰ間で意思疎通を図ることが望ましい。

しかしながら、開示してよい情報と社外秘とすべき情報の区別については、各ＩＳＰの経営に関わる事項であり、ＩＳＰ相互間のトラヒック情報の交換には熟考が必要であろうし、その実施に当たっては、各ＩＳＰの経営者層のリーダーシップに基づくＩＳＰ間のコンセンサスが必要である。

特に各ＩＳＰがトラヒック情報の開示に踏み出しにくい初動期において、今回のトラヒックの現状調査のように、産官学で協力して個別のトラヒック情報の秘匿性を維持しつつ、各社のトラヒック情報を合計する形でインターネット全体としてのトラヒック情報を把握することは、重要な施策の１つであると考えられる。

いずれにしても、全体的なトラヒック情報を把握することは、各ＩＳＰにとっても今後の投資計画やネットワーク形態、更にはビジネス・モデルを検討する上で有用と考えられるが、一事業者だけでは把握できないものであり、今回のトラヒック調査のような取組みは、大きな意義を有するものと考えられる。

また、トラヒック情報の把握は、例えば半年に１回又は１年に１回というように定期的な集計と分析を行ってこそ意義をもつものであり、産学官で協力して、調査の趣旨や把握すべきトラヒック情報の範囲、秘匿性の維持方法等を明確化して、継続的な取組みをしていくことが必要と考えられる。

こうしたトラヒック情報の蓄積は、トラヒックの将来予想をする上での重要な基礎をなすものと考えられる。

４．国際的なトラヒック交換の変化

国内のトラヒック交換から国際的なトラヒック交換に目を転じると、１９９４年から９５年の時点では国内２割、国際８割であり、トラヒックの大半はＦＴＰ（File Transfer Protocol）等であったものが、１９９９年から２０００年の時点では国内６割、国際４割と逆転し、トラヒックの８割をＷｅｂが占めるようになり、２００３年から０４年の現時点では国内７割、国際３割であり、Ｐ２Ｐ（Peer to Peer）型ファイル転送のトラヒックが急増しているといったように、トラヒック構造の変化を把握することが必要との指摘も出されている。

なお、国際的なトラヒック交換の中では、アジア、特に韓国や中国とのトラヒック交換が増加しており、その背景として、韓国のブロードバンドの高い普及率と同国のゲームサイトとのトラヒックの増勢傾向、経済好況の続く中国で事業展開を図る法人利用者の急増等が指摘されている。

第４章　バックボーンにおける
トラヒックの将来予想

１．トラヒックの将来予想の有意性

将来的なトラヒック増加に対応し得るバックボーンの在り方について検討する際には、トラヒックや、インターネットの利用方法ごとのトラヒック・パターンについて予想することが有効と考えられるが、これについては、当研究会の下に設置された「次世代ＩＰ網ＷＧ」の構成員にアンケート調査を行ったところ、以下のとおり、意見が分かれた。

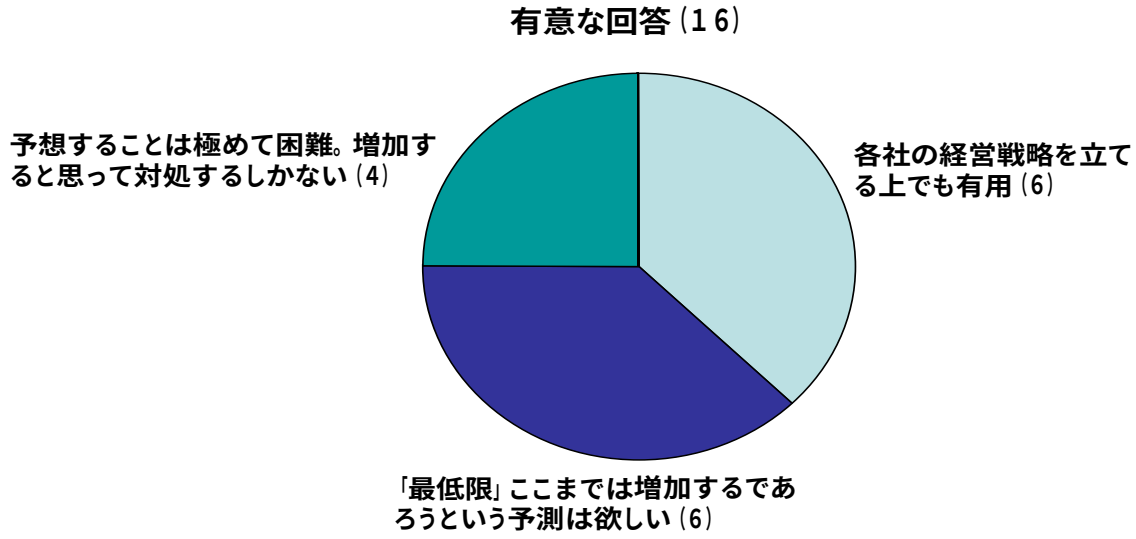
第１に、トラヒックやトラヒック・パターンは、利用者によるインターネットの使い方によって決まるものであり、利用者が今後どのようなインターネットの使い方をするかを、ＩＳＰが予想することなど到底できない、とする意見があった。

この意見は、トラヒックはむしろ予想を超えて増加するものであり、その時々で実用化されている技術を組み合わせ、それでも処理できない場合には、トラヒックを分散させ又は制御するしかない、とするものである。

第２に、過去のトラヒックの増勢傾向やＤＳＬ、ケーブルインターネット、ＦＴＴＨ等の利用人口の推移を踏まえ、将来的に、「最低限ここまではトラヒックは増加するであろう」という予想が欲しい、とする意見もあった。

第３に、現時点で想定される将来の主要なアプリケーションを勘案し、幾つかのシナリオのもとで、将来のトラヒックやトラヒック・パターンを検討しておくことは有用、とする意見もあった。

【トラヒックの将来予想についての意見】



２．将来のトラヒック試算

当研究会では、以上のアンケート結果を受け、日本の３大ＩＸ（ＮＳＰＩＸＰ、ＪＰＩＸ、ＪＰＮＡＰ）の公開情報である５分間平均トラフィックのピーク値を基に、次の前提のもとで、将来のトラヒック試算を試みた。

①　ＤＳＬ及びＣＡＴＶインターネットの利用者数については、合計値としてトラヒックを試算。

②　ＦＴＴＨの利用者数については、ＤＳＬやＣＡＴＶインターネットの利用者数とは独立させて試算。

③　利用者１人当たりの通信容量については、ＣＰＵクロック(注)を説明変数として使用。新聞等で１０Ｇ（ギガヘルツ毎秒）、２０ＧのＣＰＵクロックが公表されていることから、それらを参考に、トラヒックを試算。

（注）Central Processing Unit の略。パソコンにおいてあらゆる計算処理を行う部分。クロック周波数がＣＰＵの処理速度を表し、この数値が大きいほど、パソコンの動作スピードは速い。

④　新しい利用方法が登場することは考慮しない。

⑤　ヒト対ヒトの通信のみならず、ヒト対モノ、モノ対モノの通信が普及することによる影響は考慮しない。

⑥　利用者数について、次の２つの想定を用意。

想定１　ＤＳＬ及びＣＡＴＶインターネットの利用者数については、これまでの増加スピード（年間５００万件増）が当面継続し、後にＦＴＴＨ利用者数の増加速度がこれらを上回ると想定。また、両者を合わせたブロードバンドの世帯普及を３，８００万世帯で頭打ちと想定（２０１０年の総世帯数４９１４万と推計）。

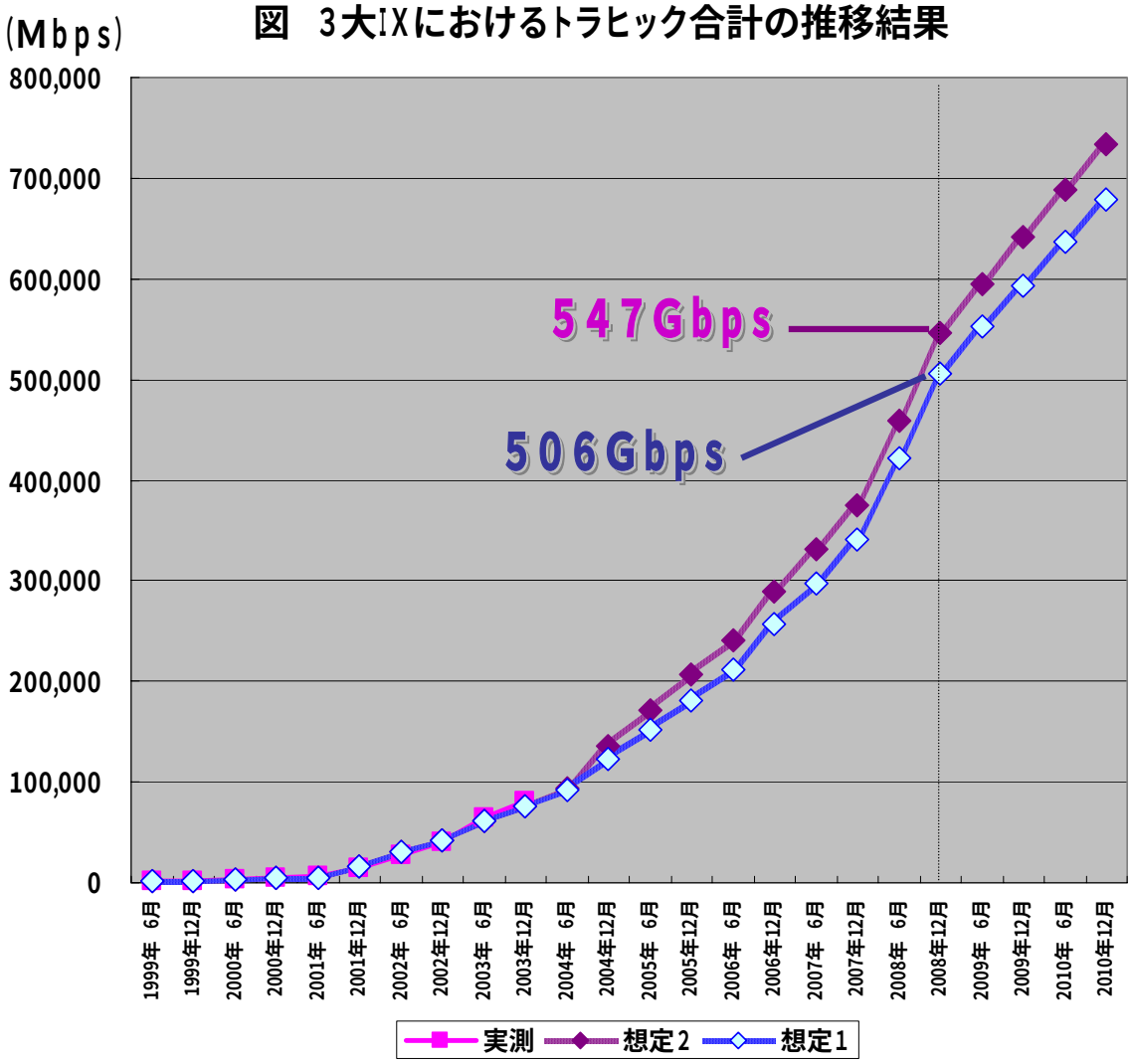
想定２　e-Japan 評価専門調査会中間報告（２００４年3月３０日）に基づき、３０Ｍ（メガビット毎秒）以下（主としてＤＳＬ及びＣＡＴＶインターネット）の利用者が４０００万、３０M超（主としてＦＴＴＨ）の利用者が１０００万と想定。

上記の前提及び想定の下で３大ＩＸにおけるトラヒック合計を試算すると、想定１の下で２００８年末に５０６Ｇ（ギガビット毎秒）、想定２の下では５４７Ｇとなった。これまでの３大ＩＸにおけるトラヒックは９０Ｇであるので、その５～６倍の水準ということになる

しかしながら、上記の試算値は、新しい利用方法が登場することを考慮していないことや、ヒト対モノ、モノ対モノの通信が普及することによる影響も考慮していないことから、これらのインパクト次第では、トラヒックはより一層増大するものと考えられることころであり、堅目の見積もりによる試算値と位置付けることが適当と考えられる。

また、第３章のトラヒックの現状調査にみたように、ＩＸでのパブリック・ピアリングと同等又はそれ以上のトラヒック交換がプライベート・ピアリングやトランジットによって行われており、実際のトラヒック総量はより大きいものと捉える必要がある。

図　3大IXにおけるトラヒック合計の推移結果



３．将来的なトラヒック増加への３つの対応策

２．において将来のトラヒック試算を行ったが、「トラヒックは増えることはあっても減ることはない。」又は「予想を超えて増える。」という点では、研究会構成員の意見に大きな差異はない。

次に問題となるのは、将来的なトラヒックの増加に対してどのように対応するか、という点である。

これについては、次の３つの対応策があると考えられる。

①　ネットワークを増強する

②　トラヒックを制御する

③　トラヒックを分散させる

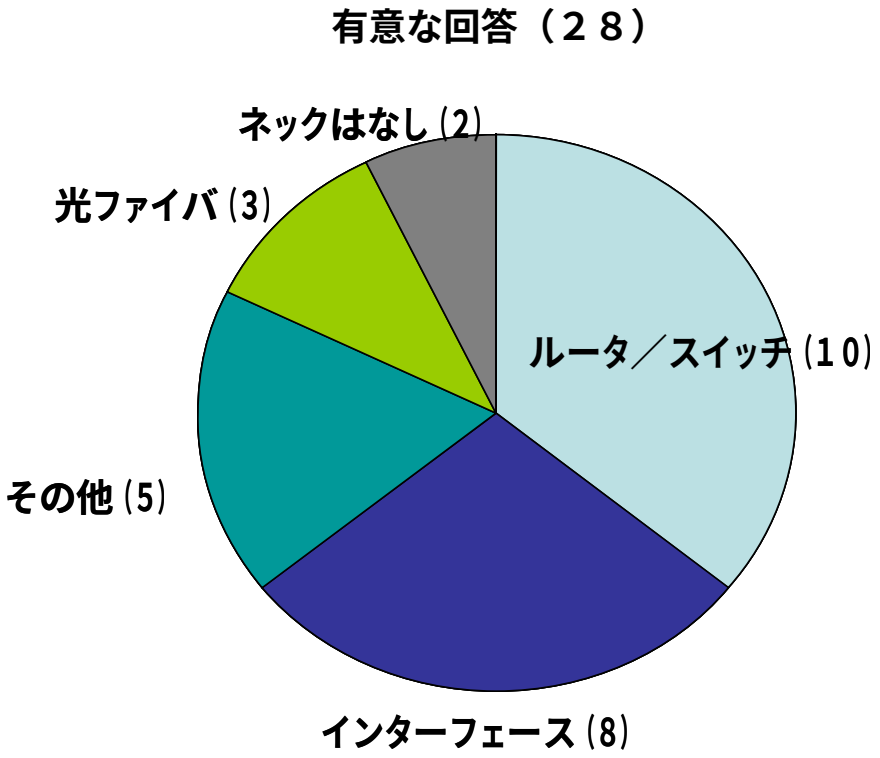
そこで、以下、①については第５章で、②については第６章で、③については第７章で、それぞれ検討を行うこととする。

第５章　トラヒック増加に対応するための
ネットワークの増強と技術開発

１．バックボーンのネックになる部分

将来的なトラヒックの増加に対して、バックボーンのどの部分がネックになるのかについて、当研究会の下に設置された「次世代ＩＰ網ＷＧ」構成員の意見を聴取したところ、その結果は次のとおりである。

【将来的なトラヒック増に対してバックボーンのどの部分がネックになるか】



なお、「その他」の意見の中には、①通信容量の大容量化に伴う設置スペースや給電・空調設備等の機器環境がネックである、②設備投資資金をどうやって確保するかがネックである、等の意見があった。

そこで、バックボーンのうち交換機能を担う部分と伝送機能を担う部分とに分けて現状と今後の課題を検討してみたところ、以下のとおりである。

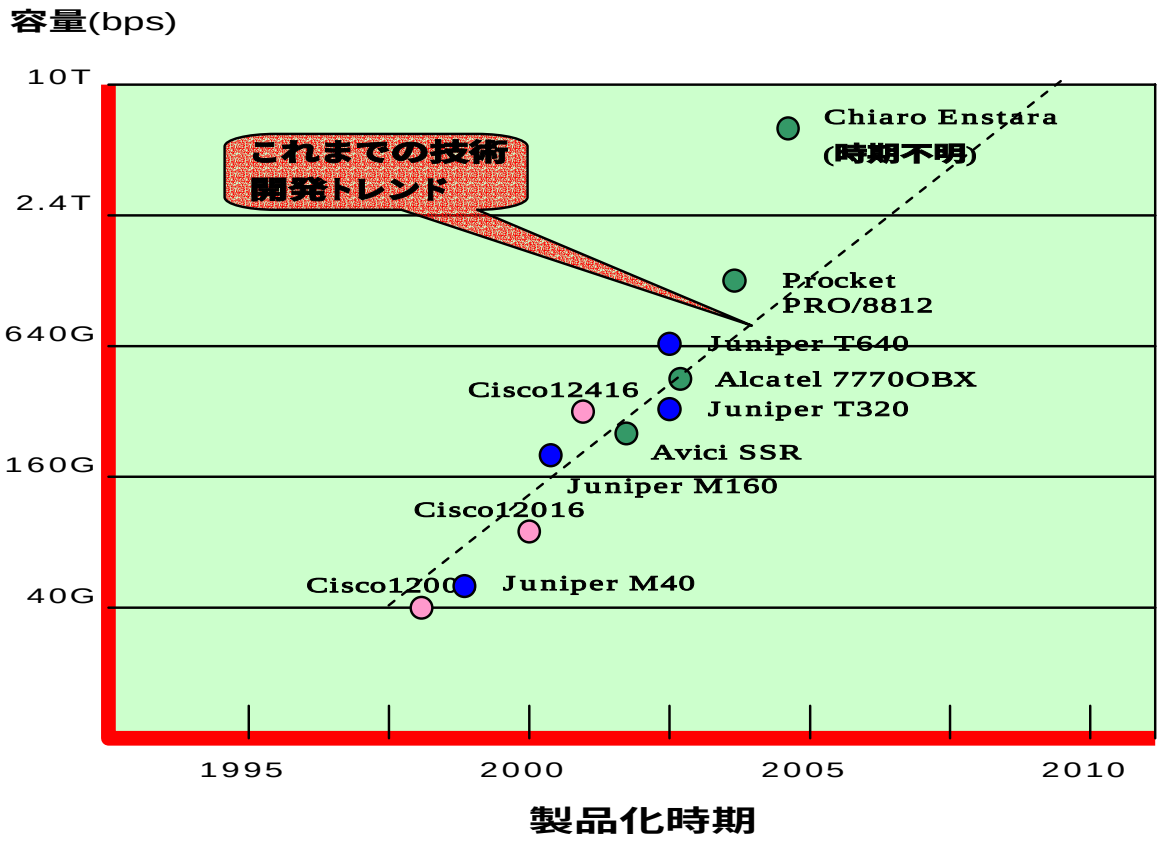
２．交換機能を担う部分（ルータ／スイッチ／インターフェース等）

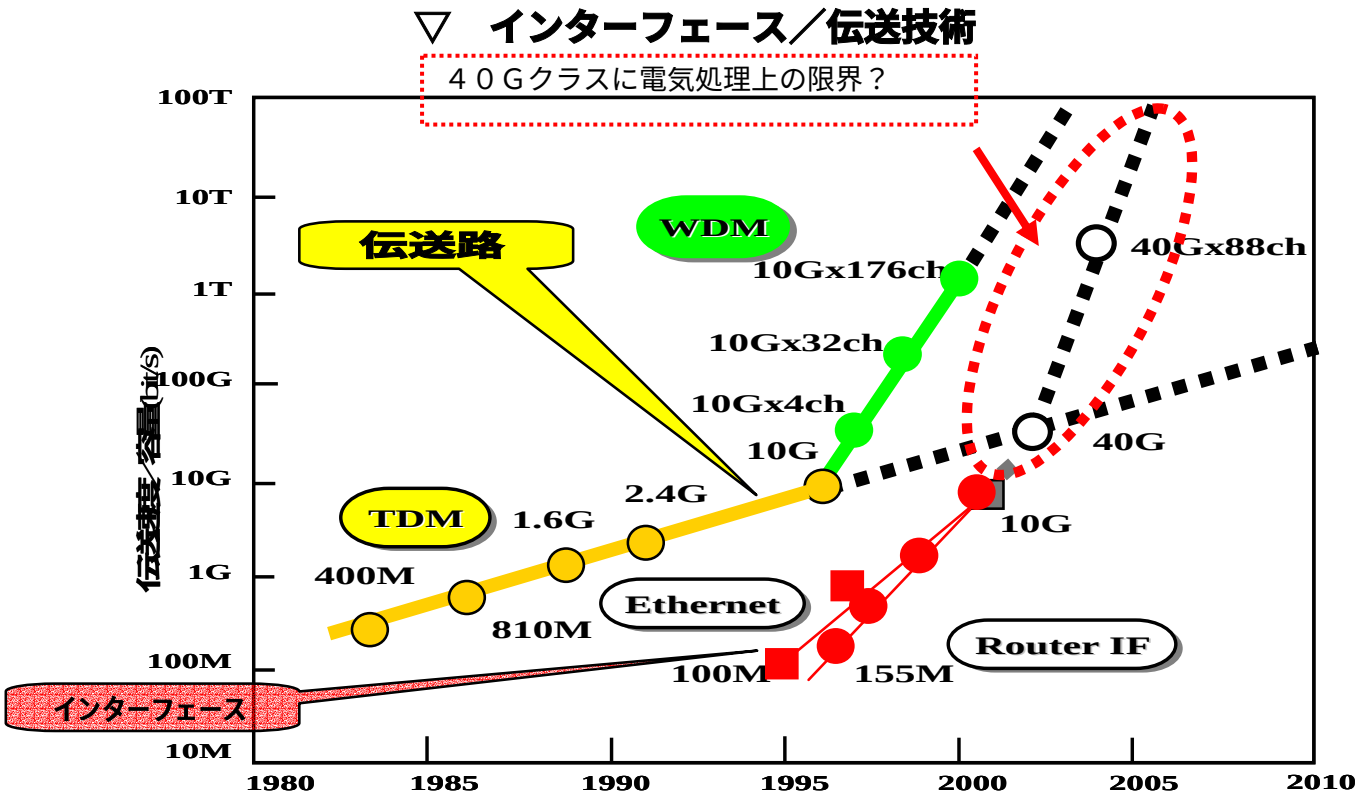
（１）技術開発の現状と課題

インターネットの交換機能を担うルータ、スイッチ、インターフェース等について、技術開発の現状と課題をまとめてみると、次のとおりである。

要素技術	現状	課題
ルーティング	現在のネットワーク規模でも、安定した対応はできていない。	○プロトコルのチューニングを含め、開発が必要。 ○ルーティング情報をリアルタイムでバックアップする技術も必要。
大容量スイッチ	電気スイッチ；１～２Ｔ 光スイッチ：～１００Ｔ	光スイッチによるパケットスイッチングについては、技術が確立していない。
パケット処理	１０Ｇ	１０Ｇで高度な処理を行うネットワーク・プロセッサは製品化されていない。
インターフェース	～４０Ｇ：開発済み ４０Ｇ超：未開発	４０Ｇ超のインターフェースの開発
(参考)伝送技術 波長分割多重 （ＷＤＭ）	～２Ｔ：製品化済み １０Ｔ：実験レベルで開発済み	

▽　ルータ





（２）技術的なブレークスルーの必要性

以上のように、インターネットの交換機能を担うルータ、スイッチ、インターフェースの部分については、電気処理上の限界が見えてきているとの意見もあり、光技術との融合も含め、これまでの延長線上にとどまらない実用化及び商用化に向けた研究開発が必要である。なお、既に米国のいくつかの通信機器メーカにおいては、製品化に向けた具体的な研究開発が推進されているところである。

（３）ルータ、スイッチ、インターフェースに関する開発要望

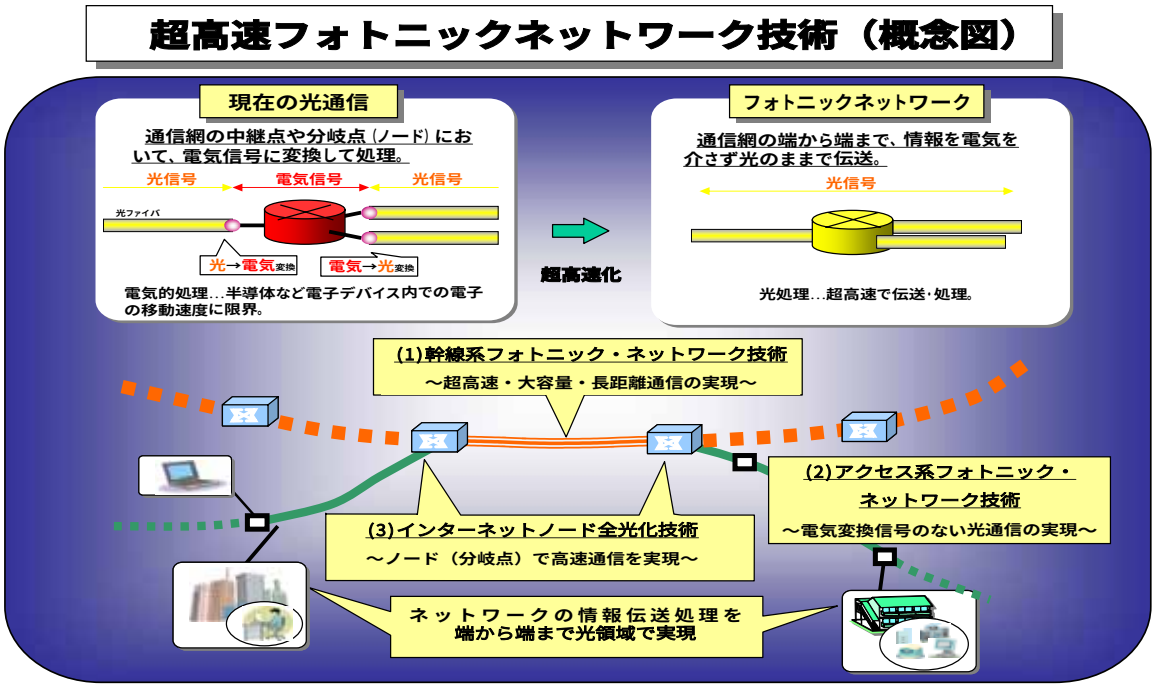
実際、当研究会において、ＩＳＰやＩＸ事業者から、ルータ、スイッチ、インターフェースの開発・実用化に関し、次のような要望が寄せられた。

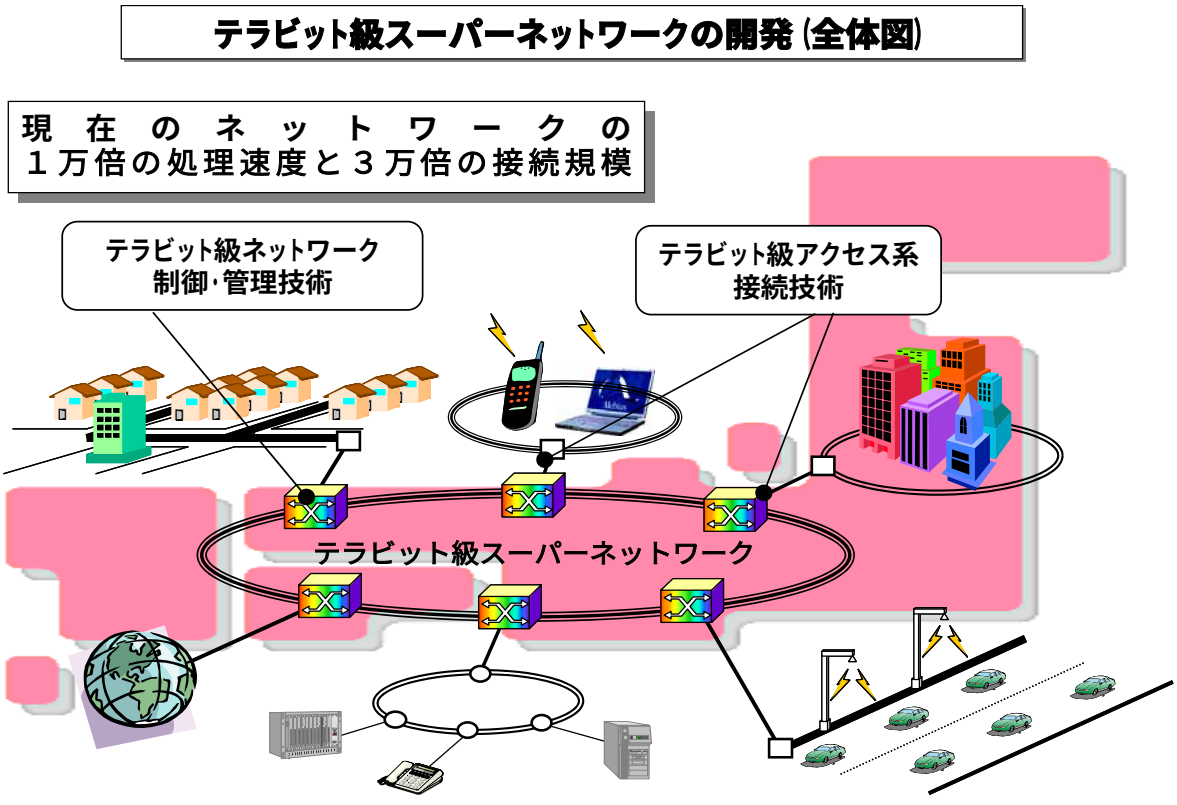
【ルータ、スイッチ、インターフェースに関する開発要望】

２００６年　４０Ｇ（ギガビット毎秒）のインターフェースを持つ装置の出荷
２００７年　４０Ｇのインターフェースの実用化
２００８年　４０Ｇルータの単価が２００４年時点の１０Ｇのものと同一の単価まで低下
２０１０年　４０Ｇルータの単価が２００４年時点の１Ｇのものと同一の単価まで低下
米国等の海外メーカの最高性能ルータやスイッチと同等もしくは同等以上の性能・機能を持つ機器を、国内メーカにおいても開発することで、選択肢の幅が広がることが望ましい。

（４）政府による研究開発の総合的・計画的な取組

また、光ルータや光スイッチの研究開発については、総務省においても、２００１年度より「超高速フォトニック・ネットワーク技術に関する研究開発」を５ヶ年で、ネットワークの制御・管理技術等の開発については、２００２年度より「テラビット級スーパーネットワークの開発」を４ヶ年で推進しており、今後とも、こうした研究開発に総合的かつ計画的に取り組むとともに、実用化及び商用化に向けたニーズをこうした研究開発活動にも反映させていくことが必要と考えられる。





また、（３）に掲げた開発要望に応えられるよう、①１００Ｔ（テラビット毎秒）程度の情報の伝送を実現するスイッチ技術、②１０Ｇ（ギガビット毎秒）を超えるインターフェース実現のための超高速パケット処理技術、③高速大容量の情報の伝送を低消費電力で実現する技術等についても、研究開発を推進していくことが必要と考えられる。

（５）ＩＳＰ等の対処

しかし、こうした基礎的な研究開発には、多額の費用と長い期間を要するのも、また事実である。

このため、ＩＳＰやＩＸ事業者にとっては、研究開発を待ってはいられないのが実状であり、トラヒックの増加に対して、既に実用化されている製品を束ね、並列処理させること等により対応しているが、設置台数と処理能力は単純な倍数関係にはなく、台数を２倍にして処理能力は１．５倍程度、台数を４倍にして処理能力は２倍程度にすぎない。

また、デバイス数の増加により通信機器からの発熱が増大しており、発熱は機器の動作に悪影響を与えるため、空調を２４時間稼働させることが不可欠となっていることから、スペース当たりに必要となる電力消費量が増え、ＩＳＰやＩＸ事業者にとって大きな負担となっているとの指摘がある。

（６）通信機器メーカ側の考え方

他方、開発を担当する通信機器メーカ側には、我が国の現在のインターネットのように、トラヒックを東京一極に集中させる極端なスター型のネットワーク形態のもとでは、極めて高性能なルータやスイッチを開発したとしても、一次ＩＳＰや主要なＩＸ事業者の中核機器として販売できるにすぎず、基礎研究レベルからの開発費をごく少数のルータの販売収入で賄うことは困難であるとの意見がある。

（７）ネットワーク形態の検討

このため、各ＩＳＰ側においても、極端なスター型のネットワーク形態を採用することはできず、高性能なルータを「ある程度」分散配置してメッシュ型のネットワーク形態を採用し、トラヒックを分散させることが求められる。

この点については、第７章で取り上げることとする。

３．伝送機能を担う部分

（１）中継系光ファイバの投資規模と利用状況

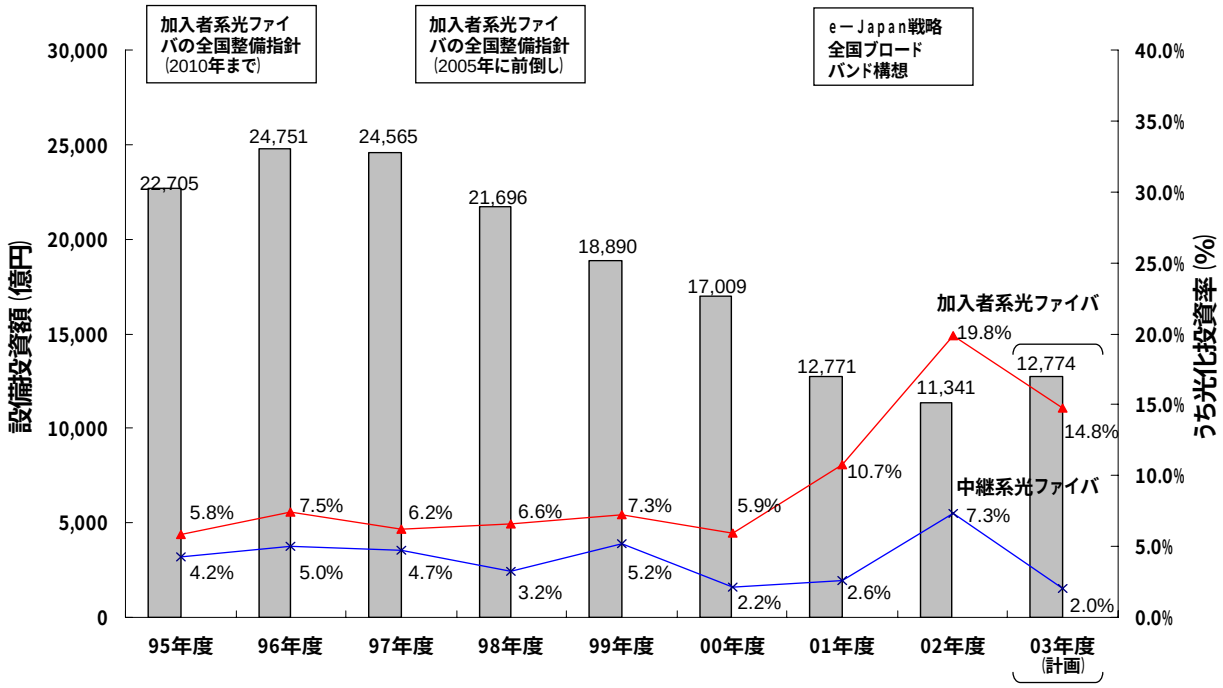
（図１）は、設備投資の総額並びに加入者系光ファイバ及び中継系光ファイバへの投資率を示したものであり、これを見ると次の３点がうかがわれる。

① 設備投資の総額は１９９６年度の２４，７５１億円をピークに減少傾向が続いていること。

② 中継系光ファイバよりも加入者系光ファイバへの投資率が高いこと。

③ 設備投資の総額に占める中継系光ファイバへの投資率は数%であり、しかも逓減傾向にあること。

(図1) 電気通信事業者の設備投資の推移



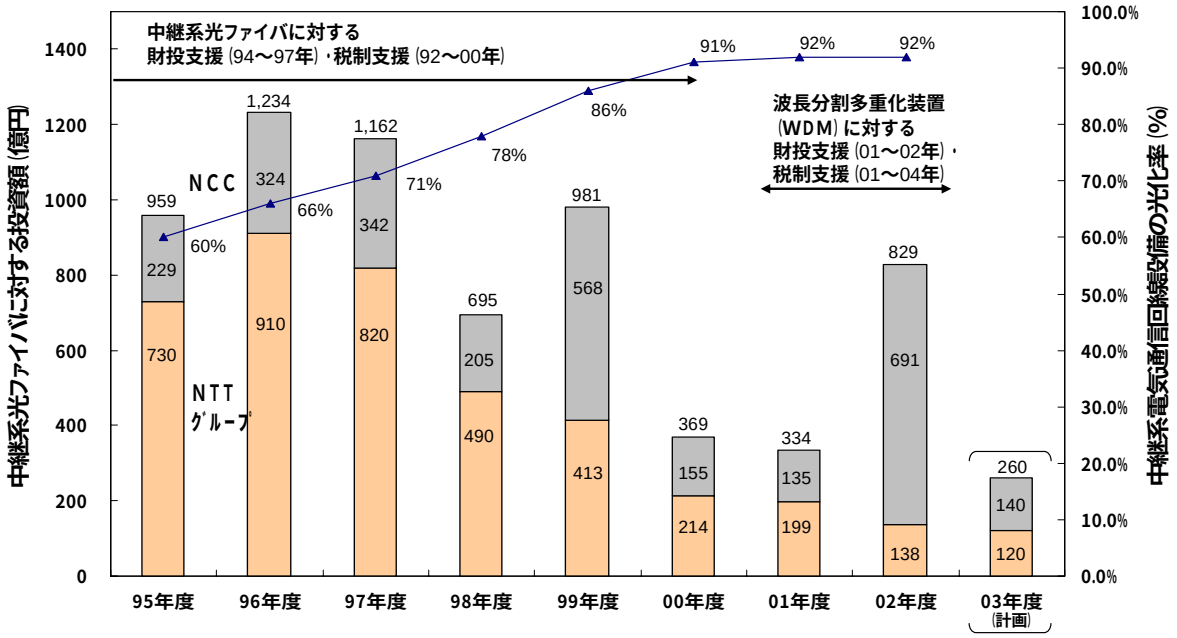
(注) 1．電気通信事業者へのアンケート調査による。衛星系事業者、移動系事業者及びＣＡＴＶを兼営する電気通信事業者を除く。
2．光化投資率は、光ファイバ及び管路に対する投資額の全設備投資額に占める割合。
3．中継系光ファイバとは、加入者系配線（集線点から加入者宅内の光端末回線終端装置までの配線）及び加入者系幹線（加入者配線に分岐する集線点から加入者収容局内の端末系光端局装置までの間の端末系幹線路）を除く中継系伝送路のうち、光ファイバで敷設されているものをいう。

（図２）は、「中継系光ファイバに対する投資額」及び「中継系電気通信回線設備の光化率」を示しているものであり、これを見ると次の２点がうかがわれる。

① 中継系光ファイバに対する投資額も、１９９６年度の１，２３４億円をピークに、総じて減少していること。

② これは、中継系電気通信回線設備の光化率が２０００年度には９０%を超え、回線設備に関する光化投資が一巡したことによるものであると考えられること。

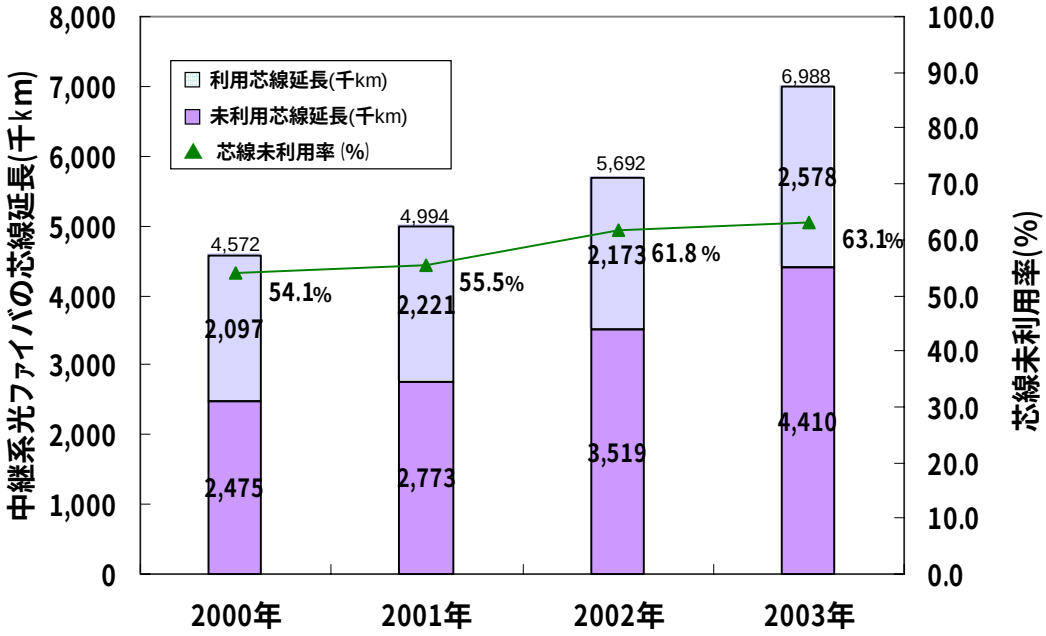
（図2）中継系光ファイバに対する投資規模の推移



（注）1．電気通信事業者へのアンケート調査による。衛星系事業者、移動系事業者及びCATVを兼営する電気通信事業者を除く。
2．光化投資率は、光ファイバ及び管路に対する投資額の全設備投資額に占める割合。
3．中継系光ファイバとは、加入者系配線（集線点から加入者宅内の光端末回線終端装置までの配線）及び加入者系幹線（加入者配線に分岐する集線点から加入者収容局内の端末系光端局装置までの間の端末系幹線路）を除く中継系伝送路のうち、光ファイバで敷設されているものをいう。

（図３）は、中継系光ファイバの「芯線延長」及び「芯線の未利用率」について、２０００年度以降の推移を示したものであり、これを見ると「芯線の未利用率」が54%～63%で推移していることがわかる。

（図3）中継系光ファイバの利用状況の推移



（注）1．光ファイバを設置（IRUによる設置は含まない）している電気通信事業者へのアンケート調査による。
2．中継系光ファイバとは、加入者系配線（集線点から加入者宅内の光端末回線終端装置までの配線）及び加入者系幹線（加入者配線に分岐する集線点から加入者収容局内の端末系光端局装置までの間の端末系幹線路）を除く中継系伝送路のうち、光ファイバで敷設されているものをいう。
3．2000～2001年における芯線延長及び未利用芯線延長は20社の合計値。2002年における芯線延長及び未利用芯線延長は22社の合計値。2003年における芯線延長及び未利用芯線延長は23社の合計値。
4．芯線延長及び未利用芯線延長には、各社の設備投資計画等に基づき算出した概算値を含む。
5．芯線延長及び未利用芯線延長は四捨五入により算出しているため合計値と一致しないことがある。

このように「芯線の未利用率」が６割前後で推移していることは、商用ネットワークの運用上、中継系光ファイバに関する需給逼迫感をもたらさないという観点からは、

健全なことと考えられる。

また、１９９０年代半ば以降、波長分割多重（WDM）技術が開発・実用化され、光ファイバの容量を増幅させることが可能となっていることも、中継系光ファイバの需給を逼迫させないことに寄与しているものと考えられる。

（２）ＩＳＰやＩＸ事業者の懸念

しかし、それにもかかわらず、特に、電気通信回線設備を自ら設置している電気通信事業者（以下「通信キャリア」という。）から中継系光ファイバを借りて事業を運営しているＩＳＰや、ＩＸ事業者の中には、次のような懸念が存在することも、また事実である。

（ア）マクロでは余裕があるにしても、東名阪などトラヒックが集中する肝心なところは足りなくなるのではないか。

（イ）光はエネルギーなので、出力を上げるとファイバに負担がかかることなど多重化には様々な制約がある。１０Ｇの光ファイバを多重化するにしても、現在商用化されているものは１６０波までであり、せいぜいＴ（テラビット毎秒）クラスの伝送しか実現できないことから、いずれ限界を迎えるのではないか。光ファイバ１芯あたりの伝送容量を上げるには、①現在使われていない波長を使う、②波長多重の高密度化を図る、という方法が考えられるが、これらを実現するためには基礎研究が必要であり、将来のトラヒック増加を睨んで今から取り組んでおく必要があるのではないか。

（３）上記懸念に対する考え方

こうした懸念については、次のように考えることができる。

（ア）まず、主要通信キャリア(注)が東名阪で確保している電気通信回線設備の容量並びに自己設置している光ファイバの芯線数及び未利用率を調査してみると次のとおりであり、全国主要地点間のうち最もトラヒックの多い東京－大阪間において、光ファイバの未利用率は７４％となっている。

▽　主要通信キャリア(注)の東名阪の電気通信回線設備・自己設置光ファイバ

2003年	回線容量	自己設置光ファイバ	
12月末	(音声＋データ＋専用)	芯線数	未利用率
合計値	１．７T(テラビット毎秒)	７９８芯	７４％

（注）NTTコミュニケーションズ、ケイ・オプティコム、ケーブル・アンド・ワイヤレスIDC、KDDI、日本テレコム、パワードコムの6社。

このように、トラヒックが集中するような特定区間であれば、通常は、トラヒックの増大に応じて、中継系光ファイバに対する投資が行われるものと期待されるところである。

更に、既設の光ファイバを波長分割多重（WDM）技術で増幅させることにより、トラヒックの増大に対応することも考えられる。

ただし、新規に中継系光ファイバを設置しなければならない場合には、区間にもよるが、既設の局舎のない地域に光ファイバを設置するときには、工事計画協議から工事完了に至るまでに約２年、場合によっては３年以上を要することもあるので、中継系光ファイバを設置する通信キャリアにおいては、将来的なトラヒック増を見越して投資することが求められる。

新規設置を判断する際の基準は、各通信キャリアによって様々であるが、これまでの経験則に基づき、特定の区間で実際に発生したトラヒックが当該区間に設置されている電気通信回線設備の最大容量の５割に達する等一定の割合を占めるようになれば新設のための手続を開始する、という対応をとっている通信キャリアが多いようである。

しかしながら、今後は、ブロードバンド化の一層の進展やＩＴの高度利活用により、予想を超えてトラヒックが急増する事態も想定され得るところである。

このため、各通信キャリアにおいては、これまでの経験則のみにとらわれずに電気通信市場の動向を十分に見極め、中継系光ファイバへの投資が後手に回らないように留意することが求められる。

他方で、我が国は、米国におけるＩＴバブル崩壊の歴史にも学ばなければならない。

米国のＩＴバブル崩壊は２０００年３月に始まり、インターネット関連の株価指数は２００２年１１月までに９３％下落したが、その要因の１つに１９９７年以来のバックボーンへの過大な設備投資の反動があったと指摘されている。

その投資ブームの１つの契機となったのが、自社のバックボーンにおけるトラヒックが「１００日で倍増」したという UUNet の幹部による１９９７年の発言であり、この説は、米国商務省「新生デジタル・エコノミー98」という報告書にも引用された。

商務省の報告書にも取り上げられたことが投資ブームに与えた影響は定かではないが、投資リスクを負うのは、あくまで通信キャリアであって政府ではない。

本研究会によるトラヒックの将来予想も、一定のシナリオのもとでの数値であり、各通信キャリアにおいては、あくまで１つの参考値として利用することが適当と考えられる。

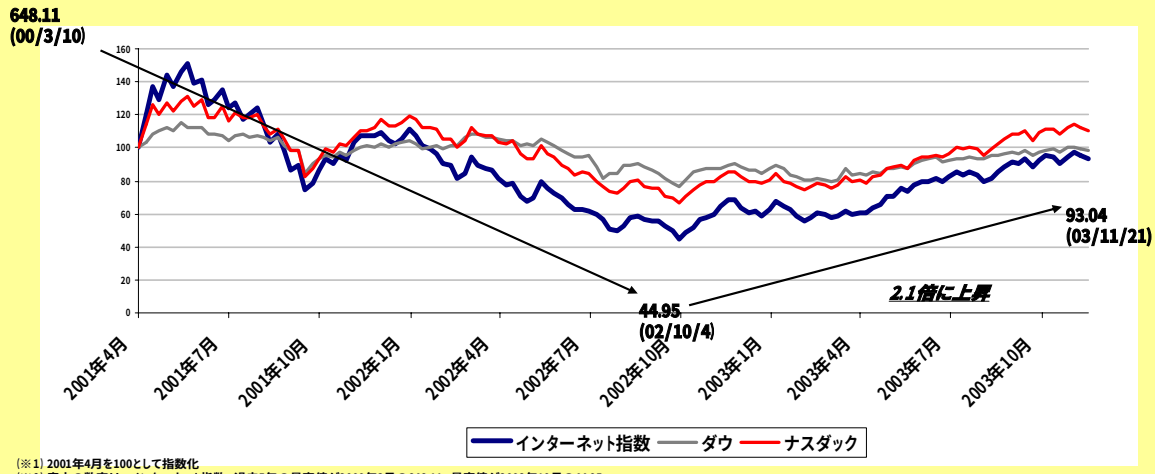
今後求められるのは、むしろ、トラヒックの増加を実感しているＩＳＰやＩＸ事業者から、通信キャリアに対して、中継系光ファイバの将来需要をきちんと伝えることである。

また、中継系光ファイバを設置しているのは通信キャリアだけではなく、地方公共団体や電気事業者、鉄道事業者、国等も存在しているが、これらの主体の光ファイバを利用するに当たっては、接続可能な地点が少ない、利用希望区間から先の光ファイバを用意することが困難な場合がある等、利用に当たっての利便性に改善の余地を残していると考えられることから、これらの主体とＩＳＰとの間で、中継系光ファイバの需要に関する情報交換を行う枠組みを設けることも検討に値すると考えられる。

更に、光ファイバの設置場所となる電柱・管路等の設備の使用については、電柱・管路等を保有する公益事業者（電気通信事業者、電気事業者、鉄道事業者等）と電柱・管路等を使用したい電気通信事業者とが遵守すべき標準的な取扱方法が「公益事業者の電柱・管路等使用に関するガイドライン」（平成１３年４月総務省策定、平成１６年４月改定）として取りまとめられており、このガイドラインの運用の徹底等を通じて、光ファイバの設置を更に円滑化していくことが求められると考えられる。

米国IT不況（2000～2002年）

インターネット関連の株価指数は、２０００年３月をピークに２００２年１０月までに９３％下落



（※1）2001年4月を100として指数化
（※2）表中の数字は、インターネット指数。過去5年の最高値が2000年3月の648.11、最安値が2002年10月の44.95

（注）Bloomberg U.S. Internet Index：米国における上場・公開企業のうち、インターネット関連事業を主な事業とする企業の株価動向を指数化したもの

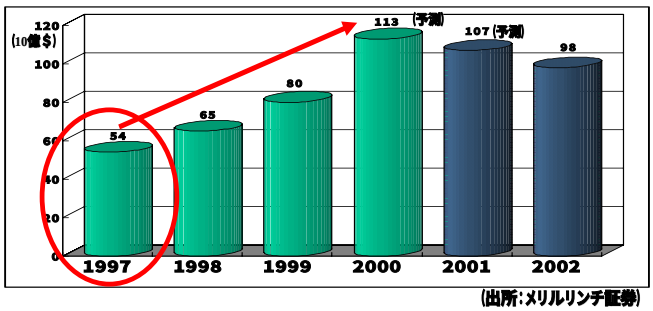
米国IT不況の要因

- **通信事業者のリストラ・倒産、収益悪化**
  要因 ⇒ 競争の激化による通信料金の低廉化（注）、長距離通信需要の低迷等

（注）新興通信事業者淘汰後、既存地域通信事業者はDSL等の通信料金を値上げ（例 ﾍﾞﾗｲｿﾞﾝ DSL料金を＄39.95→＄49.95 (2001.3)）

- 長距離通信事業者の設備投資減
  要因 ⇒ 97年以来のバックボーンへの過大な設備投資の反動等

[米国通信事業者の設備投資の動向]



（出所：メリルリンチ証券）

[ビジネスモデルの機能不全]

○広告収入依存型ビジネスモデルが中心
○巨額の先行投資を行い、ブランド力の確立を期待
○商品の保管・配送等におけるノウハウの欠如

巨額の先行投資により市場シェアを奪うというビジネスモデルはトップ・グループを除くと明らかに「間違い」。
ブランドネームは金で買えない。
（Thomas Eisenman教授(Harvard Business School)）

米国商務省"THE EMERGING DIGITAL ECONOMY" (April 15,1998)より抜粋

INTRODUCTION

Examples showing the growth of the Internet and electronic commerce this past year are numerous:

• Traffic on the Internet has been doubling every 100 days.

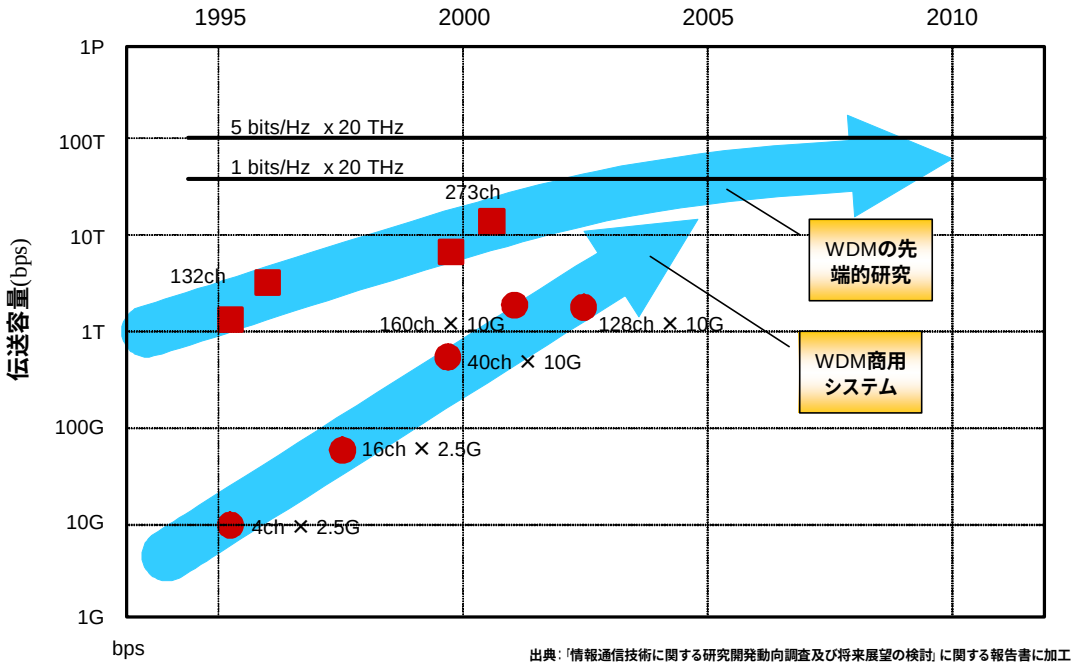
CHAPTER TWO : BUILDING OUT THE INTERNET

UUNET, one of the largest Internet backbone providers, estimates that Internet traffic doubles every 100 days.

（イ）次に、光ファイバネットワークの伝送容量を上げるための基礎研究に今から取り組んでおく必要があるのではないかという懸念については、２．で述べた「超高速フォトニック・ネットワーク技術に関する研究開発」（２００１年度～２００５年度）の中で既に取り組まれているところであり、今後も、こうした研究開発に総合的かつ計画的に取り組むとともに、実用化及び商用化に向けたニーズをこうした研究開発活動にも反映させていくことが必要と考えられる。

また、研究開発の目標も時間軸とともに示されているところであり、今後とも、ベンチャー企業における動向も含めた研究開発の進捗状況や電気通信市場におけるニーズを踏まえて、こうした目標を適時に更新していくことが必要であると考えられる。

光ネットワークの高度化ロードマップ



出典：「情報通信技術に関する研究開発動向調査及び将来展望の検討」に関する報告書に加工

現在の光ファイバの中にはＷＤＭ技術を用いずに利用されているものもあることから、伝送能力を向上させるためには、必要に応じてＷＤＭ技術を活用することが有効であるが、ＩＳＰの中には、ブロードバンドが普及する以前から整備されてきた波長当たり１０Ｇ（ギガビット毎秒）クラスまでの光ファイバによってバックボーンを構築するのではなく、今後一層普及するブロードバンド・サービスを展望して、波長当たり４０Ｇ超の光ファイバでバックボーンを構築することが必要であるとの意見がある。

こうしたニーズを踏まえて研究開発を推進していくとともに、商用ネットワークだけでなく、研究開発ネットワークや地方公共団体のネットワークを含めて、総合的な視点に立った通信インフラの設計及び運用の協調についても検討を行う必要がある。

第６章　トラヒック制御と品質保証

１．トラヒックに関する考え方

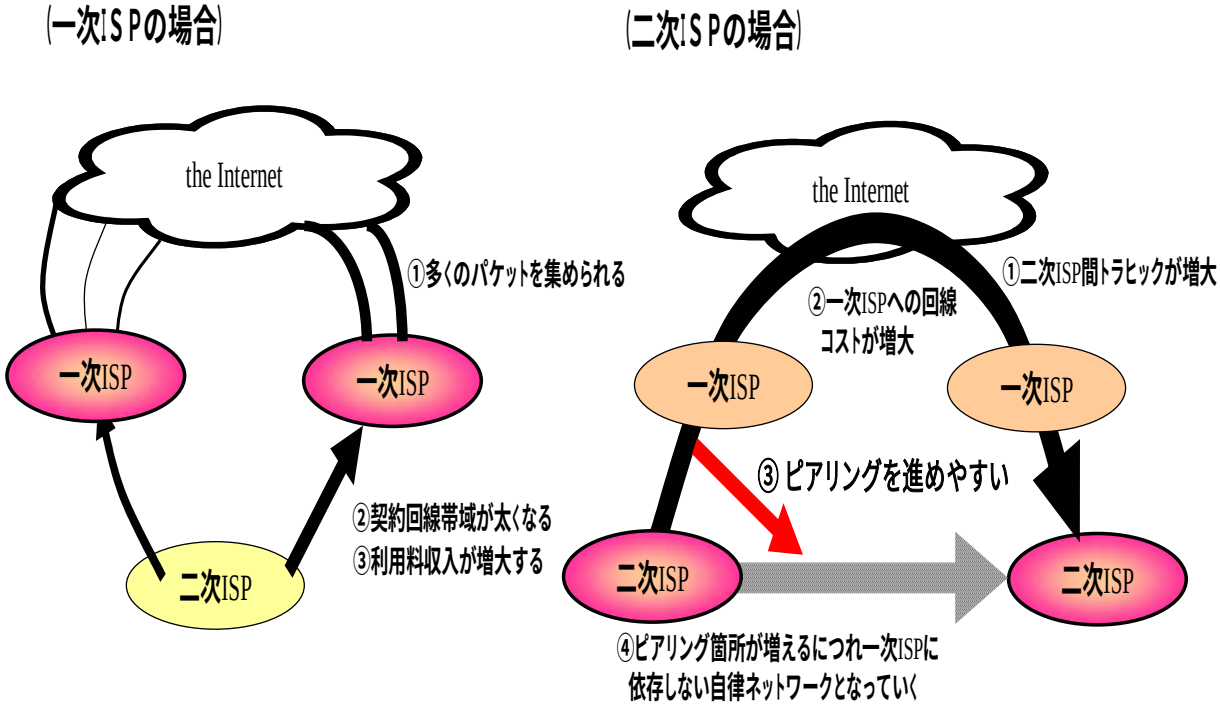
第５章では、「将来的な」トラヒックの増加に対してバックボーンのどの部分がネックになるのかという点について検討したが、各ＩＳＰは、「将来的な」問題としてではなく、まさに「足許の」問題として、トラヒック増加にどのように対処すべきかについてジレンマを抱えている。

そこで、当研究会では、インターネットの利用方法に応じたトラヒック制御と品質保証に関してどのように考えるべきかについても検討を加えた。

その内容は、以下のとおりである。

まず、一般論として、電気通信事業者が多くの顧客と多くのトラヒックを獲得することにより、ネットワークの規模を大きくし、スケール・メリットを活かして低廉なサービスを提供することは、電気通信の健全な発達及び国民の利便の確保の観点から望ましいことと考えられる。

特に、より多くのトラヒックを取り扱うことは、一次ＩＳＰにとっては下位ＩＳＰからのトランジット料金収入の増大が見込めることとなり、また、二次ＩＳＰ等にとっても、トランジットからプライベート・ピアリングへの移行を進め、一次ＩＳＰに依存しないネットワーク形態の構築が可能となる点で、事業運営上のメリットがあるものである。



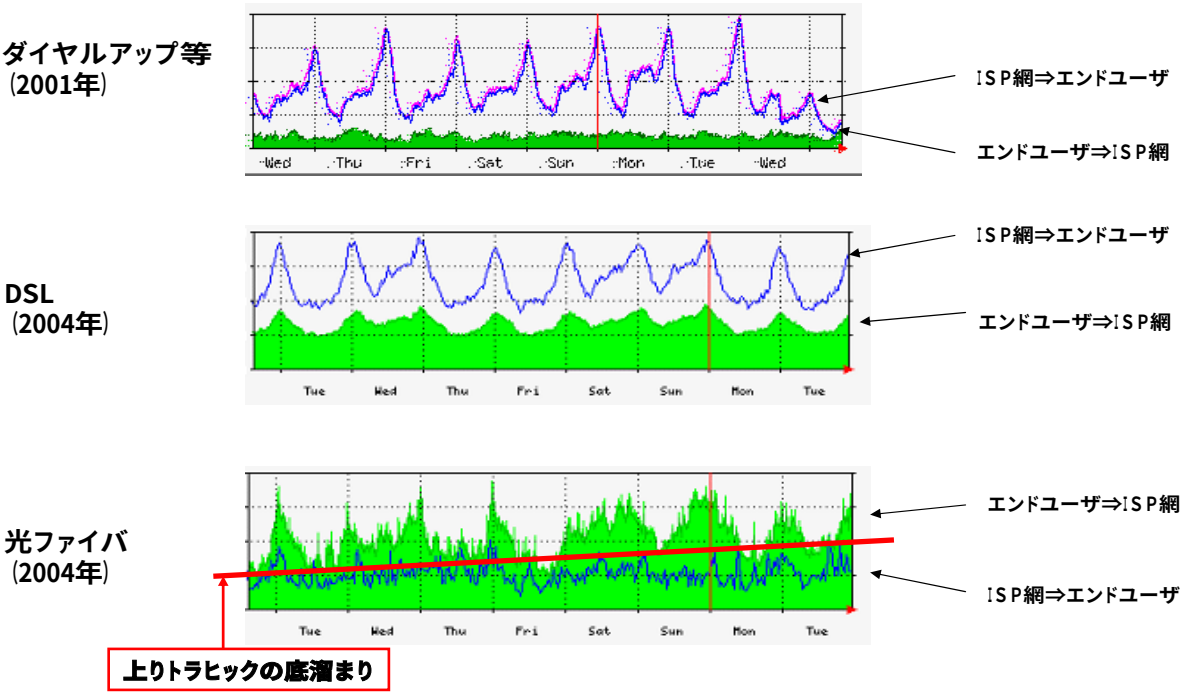
２．加入者系光ファイバ（ＦＴＴＨ）サービスにおけるトラヒックの特徴

しかし、光ファイバサービスを開始しているＩＳＰの中には、ダイヤルアップやＤＳＬとは異なる次の特徴を持つ利用者・利用形態が出てきているところである。

① ＩＳＰから利用者への「下り」のトラヒックよりも、利用者からＩＳＰへの「上り」のトラヒックの方が上回る利用者が出てきていること。

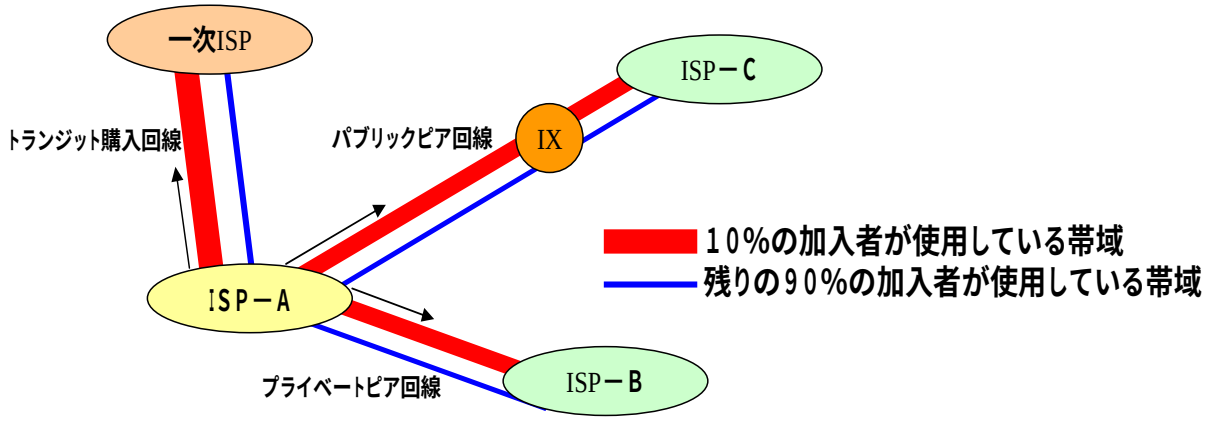
② 時間軸を通してみても、「上り」のトラヒックが一定水準以下には落ち込まず、トラヒックの大きな「底溜まり」ができていること。

あるISPにおけるトラヒック・パターンの変化



３．一部の利用者による回線容量の占有

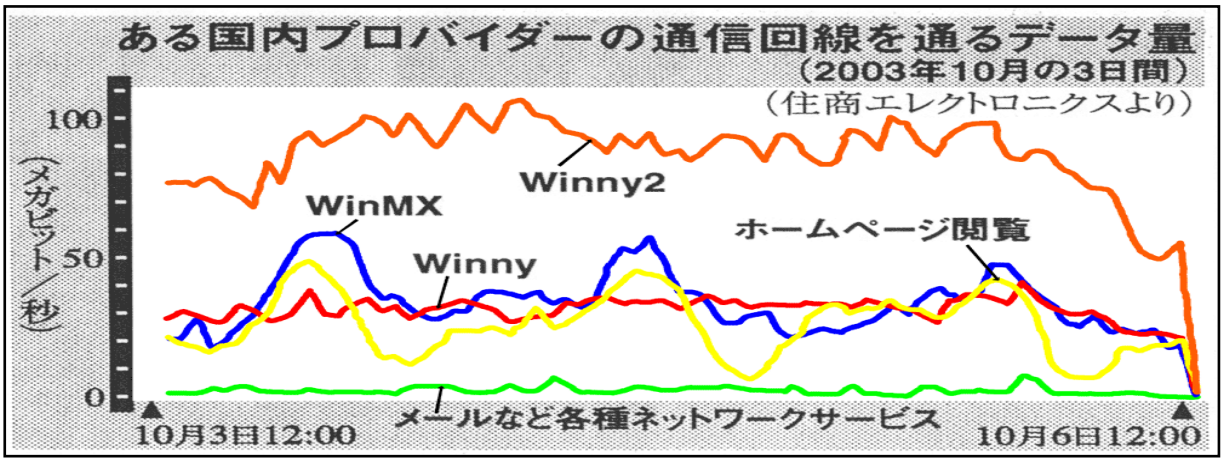
光ファイバサービスの提供によるトラヒック・パターンの変化は、上記にとどまらない。「上り」が「下り」のトラヒックよりも多い利用者は、光ファイバの全利用者の約１割しか占めないにもかかわらず、この約１割の利用者がバックボーンへの全転送量の８割以上を占め、利用者によっては１月当たり７Ｔ（テラビット）を超えるトラヒックを発生させているという指摘が、一部のＩＳＰからなされている。



４．Ｐ２Ｐ型ファイル転送のインパクト

「上り」のトラヒックが「下り」のトラヒックを上回っている利用者の多くは、現状では、利用者間でコンテンツ等をやりとりするＰ２Ｐ（Peer to Peer）型のファイル転送を行っている利用者であると指摘されている。

Ｐ２Ｐ型のファイル転送は、あるコンテンツの配信を既に受けているコンピュータから他の利用者のコンピュータに直接配信するもので、ＩＳＰが明示的に介在しない形で行われる場合もある。



（２００４年１月２７日読売新聞夕刊８面より抜粋・加工）

P2Pファイル共有ソフトの扱うデータサイズ（米国調査）

Univ. of Washingtonでの実測－ファイルサイズ分布

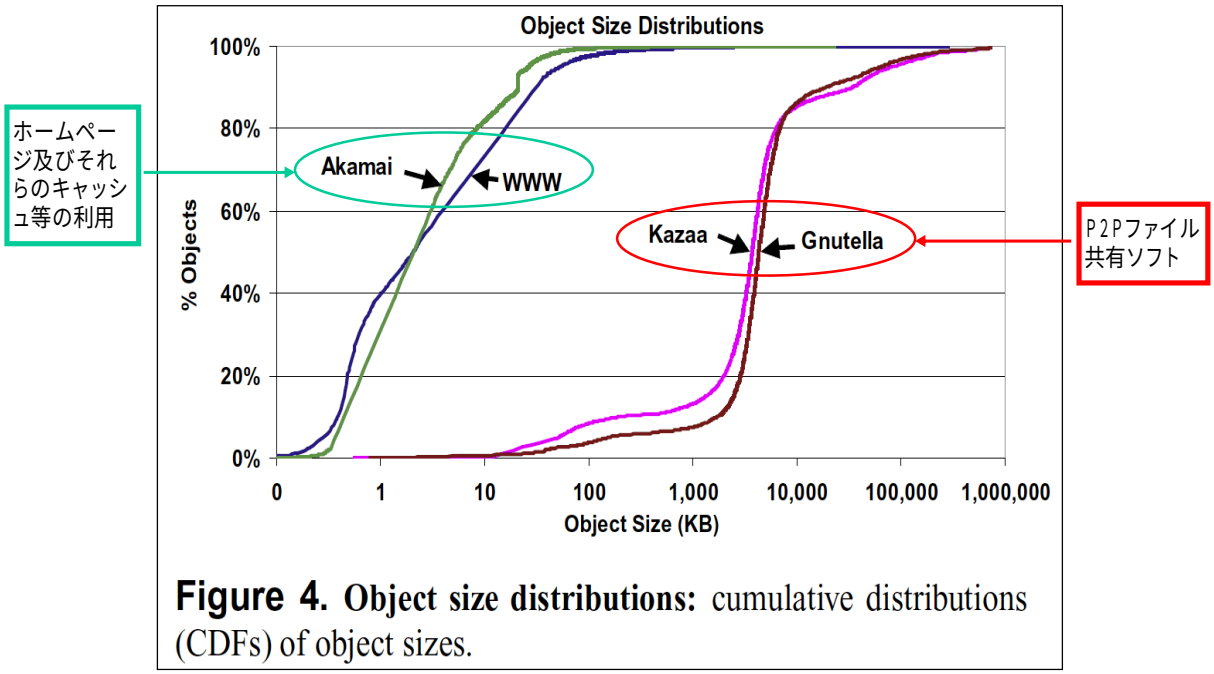


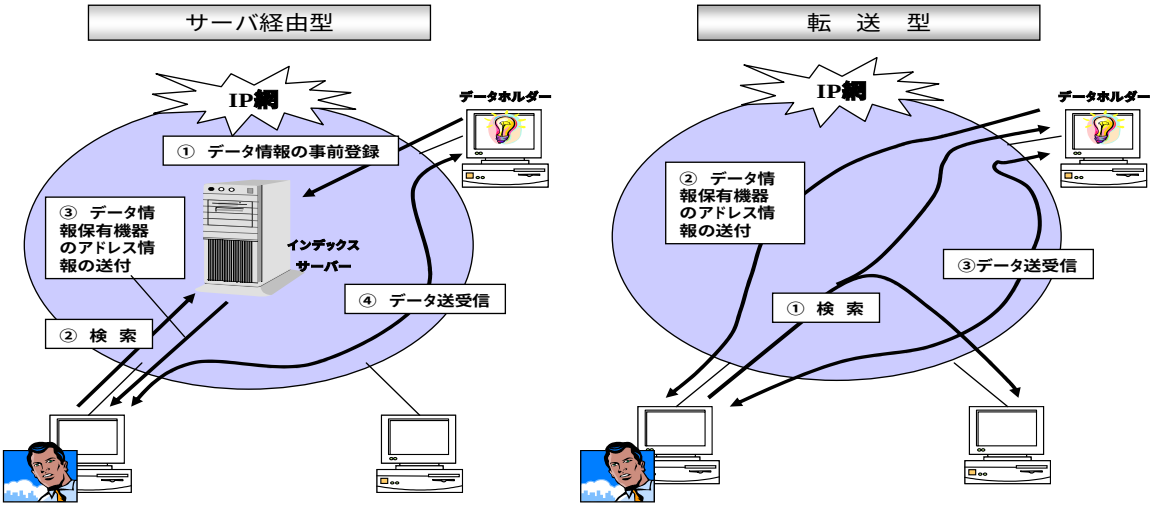
Figure 4. Object size distributions: cumulative distributions (CDFs) of object sizes.

- **調査範囲**： 大学と外部との接続点で測定。 学生、職員数計6万人 9日間(2002.5.28-6.6) のトレース、5億個のデータ。
- **調査方法**： SWのモニタリングポートを利用してパケットをキャプチャ。 アプリケーションの識別にはポート番号を利用。
- **出典**： Proceedings of the 5th Symposium on Operating Systems Design and Implementation, December 2002 （http://www.usenix.org/events/osdi02/tech/saroiu/saroiu.pdf）

Ｐ２Ｐ (Peer to Peer)通信の概念図

■　ファイルなどの必要な情報（データ）が保管されている場所を突き止め、直接その場所にアクセスし、情報（データ）を入手すること。

■　サーバ経由型のほか、サーバへの負荷集中を回避する転送型がある。



（注）日経コンピューター（０２年２月２５日号）等を基に作成。

５．トラヒック制御に関するＩＳＰのジレンマ

このような大容量のトラヒックを発生させる一部の利用者に対して、トラヒック制御を実施すべきか否かについて、多くのＩＳＰは次のようなジレンマを抱えているのが実状である。

ＩＳＰのジレンマ（各考え方の○はメリット、●はデメリット）

制御すべき	制御すべきではない
○「使い放題」ではなく「使った者勝ち」になる。 ○他の利用者へのサービスに遅延等が生じかねない。 ○「ベスト・エフォート」という言い訳にも限界。 ○仮にネットワークを増強するとなれば、一部の利用者が発生させた費用を全ての利用者で負担することになる。 ○大容量トラヒックを発生させる利用方法をそもそも想定しておらず、事業性の問題も発生。 ○制御すれば、既存のネットワーク資源には余裕ができ、料金を引き下げて利用者を拡大させることもできる。 ●利用方法は大容量のトラヒックを発生させないものに限定され、多様な利用方法が発展する可能性を摘んでしまう。	○トラヒックを制御しないことによって、ブロードバンド化は益々進展し、ネットワークの高度利用も進み、多様な利用方法が発展する。 ●ネットワーク増強のための投資が必要になる。

６．技術的な対応

この点に対する技術的な対応としては、ＴＶ会議やＩＰ電話などリアルタイムでのサービス提供が求められるものと、Ｐ２Ｐファイル転送のように蓄積系のサービスとに分けて、前者には品質保証をかけ、後者についてはそのパケットの長さや識別子により分別し、トラヒックの状況によっては、これを制御して、他のサービスへの悪影響が出ないようにするという方法が考えられている。

しかし、こうした技術を事業として実装するための投資が多額に上ることに加え、仮に技術を実装できたとしても、利用者はＩＳＰ側には予想のつかない新たな利用方法を生み出すものであり、対症療法でしかないとの指摘がある。

実際、１９９０年代前半には、ＦＴＰ（File Transfer Protocol）がトラヒックの大宗を占め、ネットワーク資源を浪費していると指摘された。ネットワーク利用上のマナーとして、ファイル交換はネットワーク上ではしないで、フロッピーディスクで行うべきと指摘された程である。その後、１９９０年代後半にＷｅｂの利用が広まると、そのトラヒックが大宗を占めた。

現在はＰ２Ｐファイル交換によるトラヒックが大宗を占めていると言われているが、今後ユビキタス・ネットワーク社会が進展してくると、ヒト対ヒトだけでなく、ヒト対モノ、モノ対モノの通信にまで拡大してくるので、Ｐ２Ｐファイル交換だけに焦点を当てて議論しても、ネットワークの新たな利用方法が登場し、いわゆる「いたちごっこ」に終わるおそれがある。

７．契約上の対応

（１）大容量のトラヒックを発生させる利用者への対応

このため、一部の利用者が大容量のトラヒックを発生させている点について、技術的な対応ではなく、制度上又は契約上の対応をとるべきとの指摘もなされている。

まず、Ｐ２Ｐファイル転送を行っている利用者が、非合法のコンテンツ転送を行っているのであれば関係法令に基づき規制されるべきものであるが、それ以外でも、業としてファイル転送を行っているのであれば、法律でそうした行為を規制すべきではないかとの意見も、当研究会では提示された。

しかし、法規制によって保護される法益が特定されにくいことに加え、実際にＰ２Ｐファイル転送を行っている者は、一般的な個人利用者であることから、法による規制は困難であるとの意見が多い。

他方、ＩＳＰによっては、下表のような対応をとり始めたところも散見されるようになってきている。

ＩＳＰ各社の対応

	概要
A社	平均的な利用を大幅に超えて利用し、本サービス（インターネット接続サービス）の運用に支障を来すと判断した場合は、当該会員に事前に連絡し、改善しない場合は３０日以上前に通知して、個別サービス契約を解除できるものとする。
B社	月間転送量が１００Ｇを超えた場合は契約者に警告し、効果がなければサービスを停止し、状況によっては契約解除もあり得る。
C社	２４時間当たり１５Ｇ以上のトラヒックを送信するなど、サービスに重大な支障を与える場合に、利用を停止又は制限することがあり、その場合、速やかに理由及び期間を通知する。
D社	本サービスの運営上必要であると判断したときなどに、契約者の当該通信に割り当てる通信を制限することがある。

（２）課金体系の工夫

上記（１）のような対応に関しても、やはり対症療法的な対応であり、Ｐ２Ｐファイル転送のような大容量のトラヒックを発生させる利用方法に対しては、①ネットワークを増強する、②課金体系を見直す、という２つの方法しか根本的な解決はあり得ないのではないかという意見が、ＩＳＰの中には存在する。

しかし、ＩＳＰ間の競争が激しい現状において、他のＩＳＰが定額料金によってサービスを提供している以上、対抗上、自社のみが課金体系を見直すことは困難であるとの意見や、利用者に定着している定額料金制を維持すべきであるとの意見もあり、ＩＳＰ各社は課金体系の採否においても、ジレンマを抱えているのが実態である。

また、いざ電話サービスのような従量課金をブロードバンドで広く採用しようとしても、

① 通信の伝送処理（トランザクション）の回数が既存の電話に比べて格段に多いため、既存の電話と同様の課金システムでは巨大になりすぎる、

② 発信側なのか受信側なのかを検知しないデータ転送システムの場合、発信者以外の利用者に対しても課金が発生してしまうおそれがある、

③ 常時接続のサービスの場合、通信「時間」に応じた従量課金は採用できず、あくまで通信「量」に応じた従量課金となることから、そのための課金システムを整備しておく必要がある、

等の問題がある。

いずれにしても、課金体系の採用は各ＩＳＰのビジネス・モデルやコスト・モデルに関わる事項であるが、定額料金は次の課題を抱えており、利用者間の公平性と正当性の確保の観点から、各ＩＳＰにおいて課金体系に工夫を加えることも１つの対処方法と考えられる。

① 「使い放題」であるがゆえに、迷惑メールやＤｏＳ（サービス否定）攻撃のような利用も出てきている側面がある。

② 一部の利用者によるトラヒック増によりバックボーンの増強を迫られる場合、定額料金では、利用者が増えない限り収入が増えず、また、全ての利用者に費用負担を求めることになってしまう。

そこで、例えば、トラヒックを大量に発生させる契約者に対しては、一定のトラヒック量を超えたら追加料金を徴収するというように、他の契約者とは異なる料金体系を採ることも１つの方策と考えられる。

８．複数事業者間でのトラヒック制御・品質保証

他方、ＴＶ会議やＩＰ電話などリアルタイム系のサービスの提供のために品質保証をかける場合については、現在は１つの事業者のネットワーク内でのみ可能であり、今後は、複数事業者間でのトラヒック制御や品質保証に関する技術の研究開発を進めていく必要があると考えられる。

その際には、帯域保証や遅延保証といった側面だけでなく、パケットが損失した場合並びにパケットの伝送誤り（エラー）や破棄が発生した場合でも利用可能性を確保する技術の研究開発に取り組むことが必要である。特に、最近急速に普及しているＶｏＩＰ（Voice over IP）等について、通信機器相互間及びネットワーク相互間の接続性の確保のための取り組みを強化することが重要である。

更に、有線網と無線網との相互統合運用や協調の実現に関する研究開発を進める必要がある。

第７章　トラヒック分散と
ネットワーク形態

１．トラヒックの東京一極集中

将来的なトラヒックの増加への対応策のうち、ネットワーク増強については第５章で、トラヒック制御と品質保証については第６章で、それぞれ検討を加えた。

ここでは、将来的なトラヒック増加への第３の対応策として、トラヒック分散とトラヒック分散に対応するためのネットワーク形態について検討することとする。

第３章３．のトラヒックの現状調査で見たとおり、プライベート・ピアリング、ＩＸにおけるパブリック・ピアリング、トランジットいずれについても、トラヒックは東京に集中している状況にある。

すなわち、既存の電話網は、ネットワーク形態としては統合型のツリー型ネットワークであるが、トラヒックは市内や県内に閉じるものが多く、ツリーの上部まで上ってくる呼数は相対的に減少するのに対し、インターネットは、ネットワーク形態としては非統合型の分散型ネットワークと言われるが、トラヒックは東京一極に集中しているのが実情である。

２．トラヒックの東京一極集中の要因

このように、インターネットのトラヒックが東京一極に集中する要因としては、次のような点が指摘されており、各要因の相乗効果で集中化のスパイラルが生じている状況にある。

トラヒックの東京一極集中の要因

（１）人口も利用者数も東京が圧倒的に多いこと。
（２）我が国の経済機能が東京に集中していること。
（３）魅力あるコンテンツが東京や米国・アジア等の外国に集中しており、コンテンツや国際回線が集中している東京にアクセスする必要があること。
（４）コンテンツや各種アプリケーションを設定・運営できる技術者も、東京に集中していること。
（５）電話では一呼当たりのトラヒック量が決まっているためトラヒック理論に基づくトラヒック予想が可能だが、インターネットではアプリケーションに応じてトラヒック量が大きく変動するため、トラヒック需要に応じたネットワーク設計・構築が困難であったこと。
（６）上記（１）～（５）を受けて、全国規模のＩＳＰのネットワークも東京を中心に構成され、他のＩＳＰとのトラヒック交換も、回線費用節減のため、できるだけ短い距離で伝送したいとの観点から、東京の主要ＩＸ及びその近辺で行うことが最も効率的となっており、地方のＩＳＰとの間でも、東京でのみプライベート・ピアリングに応じている場合が多いこと。
（７）我が国最初のＩＸが東京に実験用として設置され、商用ＩＸも上記（１）～（５）を受けて、まず東京に設置され、発展したこと。

３．トラヒックの東京一極集中に係る問題点

しかしながら、上記のようなトラヒックの東京一極集中に対しては、次のような問題点も指摘されている。

（１）地域におけるブロードバンド・サービスの品質低下

本来、地域内に終始するトラヒックが東京を経由することは、トラヒックの伝送効率だけを考えれば非効率である。

例えば、本来は北海道内に終始するトラヒックを東京で折り返す現在のネットワーク形態の下では、往復の転送時間に３０ミリ秒を要しているとの指摘が、一部のＩＳＰからなされている。

５０ミリ秒以内の遅延であれば、現在提供されているサービスについては、利用者からの苦情を招くものではないと言われているが、今後、テレビ電話等のリアルタイム性が求められ、かつ、大容量のサービスが提供される場合に、本来は地域内に終始するトラヒックが東京経由で伝送されることにより、地域の利用者に遅延を実感させることになるとすれば、東京とそれ以外の地域における新たなディジタル・デバイド問題になるおそれがある。

（２）サイバー攻撃や大規模災害等に対する脆弱性

サイバー攻撃や大規模災害の発生等により、東京のトラヒック交換機能に障害が発生した場合には、我が国のインターネット全体に影響が及ぶおそれがあり、危機管理の観点から、最低限、大阪等との分散は必要であると指摘されている。実際、主要なＩＳＰやＩＸ事業者の中には、危機管理の観点から、東京だけでなく大阪等でもトラヒック交換を行っているところが多い。

（３）通信設備に対する過剰負荷

１つの通信設備が処理しなければならないトラヒックが増大しているにもかかわらず、故障やバグ（ソフトウェアの不具合）等の信頼性が、従前から変わっていないとの指摘が、一部のＩＳＰからなされている。

過去にも、トラヒックの増加に通信設備の機能が追いつかずに、処理速度の低下やパケットの損失を起こしたことがあるが、今後も、例えば障害が発生した場合の復旧時間の短縮等といった通信設備の機能向上が見られないとすれば、障害が発生した際に処理速度の低下やパケットの損失が発生するおそれがある。

このため、通信機器メーカにおいては、通信機器の容量向上、高速化だけでなく、信頼性向上のための開発も求められている。

４．トラヒック分散に当たっての課題

３．に挙げた問題点は、トラヒックが東京に集中すればするほど、より大きな問題になるが、他方、トラヒックを分散させるためには、次の点が課題となっている。

（１）地域における技術者の不足

地域においてトラヒック交換を行うためには、一定レベル以上の能力を有する技術者を相当数確保することが必要であるが、地方においてはこのような人材が不足している。

（２）ＩＳＰ側にとっての費用増

一般に、全国規模のＩＳＰは、次の理由から、プライベート・ピアリングにしても、ＩＸにおけるパブリック・ピアリングにしても、地方では行わない場合が多いと言われている。なお、その結果として、東京以外の地域を拠点とするＩＳＰは、東京でトラヒック交換をするため、東京までの回線費用を負担している状況にある。

① 仮にプライベート・ピアリングやＩＸにおけるパブリック・ピアリングを地方でも行うとすれば、相互接続拠点の分散化に伴う拠点間バックボーンを増強する必要があるが、トラヒックの交換量について東京と地方との間で大きな差がある現状では、拠点間バックボーンの増強は、東京におけるルータ等の増強よりも、却って費用がかかる。したがって、相互接続拠点の分散については、危機管理の観点から、大阪等との間で分散させる程度しか意義を見出せない。

② ＩＰｖ４（Internet Protocol Version 4：インターネットで現在使われているアドレス）のもとでは、ＩＳＰのアクセス・ポイントに細分化されたアドレスが割り当てられている場合が多く、ＩＳＰの中には、地域性を考慮してアドレスの経路情報を集約し、他のＩＳＰと交換するためには、各アクセス・ポイントでのアドレスの地域分けを改めて行う必要があり、相当の費用がかかるところもある。

（３）ＩＳＰ間の協調の不足

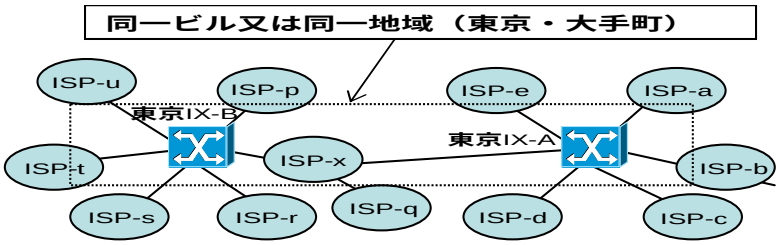
トラヒックを分散させるに当たっては、トラヒックの流れを制御し、ネットワークの利用効率を最適化するトラヒック・エンジニアリングの分析をはじめとして、地域性を考慮した経路制御等、技術的に検証が必要な課題があり、こうした課題検証にはＩＳＰ間の協調が必要であるが、これまでのところＩＳＰ間の協調は必ずしも十分ではない状況にある。

（４）ＩＳＰのネットワーク以外のネットワークの積極的活用

インターネット全体で効率的なトラヒック分散を図るには、光ファイバやＤＳＬを中心とする、いわゆる有線ネットワークだけではなく、衛星等の無線ネットワークやＩＳＰの商用ネットワーク以外の通信インフラを含めた、総合的な視点に立った通信インフラ全体の設計や運用、運用の協調についても検討を行う必要がある。

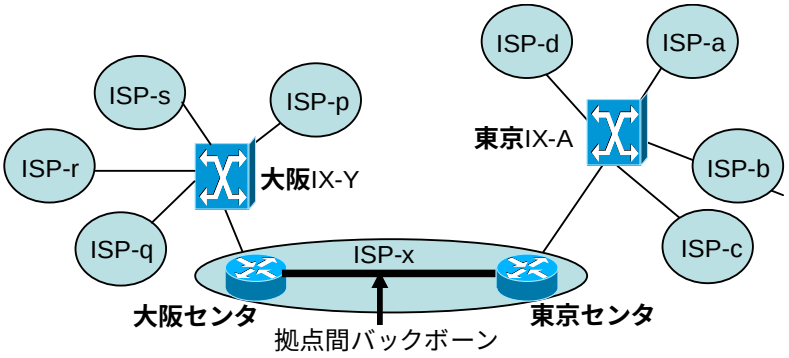
以上を踏まえて、東京一極集中型ネットワーク形態と分散型ネットワーク形態のメリット／デメリットを整理すると、以下のとおりである。

▽　東京一極集中型ネットワーク形態のメリット／デメリット



メリット	デメリット
○多くのＩＳＰが集まっているためトラヒック交換が容易 ○大量のトラヒック交換ができるため、費用対効果が大	●地域内に終始するトラヒックに遅延が発生するおそれ ●東京一極集中は危機管理上問題 ●集中するトラヒックを処理できるだけの通信設備の性能向上がないと、処理速度の低下やパケット損失が発生するおそれ ●東京以外のＩＳＰにとっては、東京でトラヒック交換をするため、東京までの回線費用を負担

▽　分散型ネットワーク形態のメリット／デメリット



メリット	デメリット
○地域内に終始するトラヒックの伝送効率が高い（遅延が少ない） ○危機管理に資する ○超高性能の通信設備は不要 ○東京以外のＩＳＰにとって、東京までの回線費用を節減可能	●地域における技術者の不足 ●地域でトラヒック交換するＩＳＰが集まらないと却って費用が嵩む ●東京と地方とでトラヒック交換量が不均衡な場合、ＩＳＰにとっては、拠点間のバックボーン費用負担が大 ●アドレス・ブロックの地域分けに相当の費用がかかるＩＳＰも存在

５．ネットワーク形態に関する考え方

４．でトラヒック分散に当たっての課題、東京一極集中型ネットワーク形態と分散型ネットワーク形態のメリット／デメリットを整理した。

しかしながら、「ではどの程度分散型にすべきなのか」、また「最適なネットワーク形態はどのようなものなのか」、という点については、一律には論ぜられないところである。

というのも、各ＩＳＰが現在採用しているネットワーク形態は、利用者の分布、コンテンツの配置、アプリケーション、更にはこれらを受けたトラヒックの状況等に大きく依存しており、経営上の必然性があるからである。

ＩＳＰ、ＩＸ事業者及び通信機器メーカのために求められるのは、むしろ、第３章に記述したトラヒックの現状や第４章に記述した将来のトラヒック予想について、信頼するに足りる情報が今後とも提供されることであり、これらを踏まえてどのようなネットワーク形態を採用すべきかについては、各ＩＳＰの経営判断に委ねられるべき事項であると考えられる。

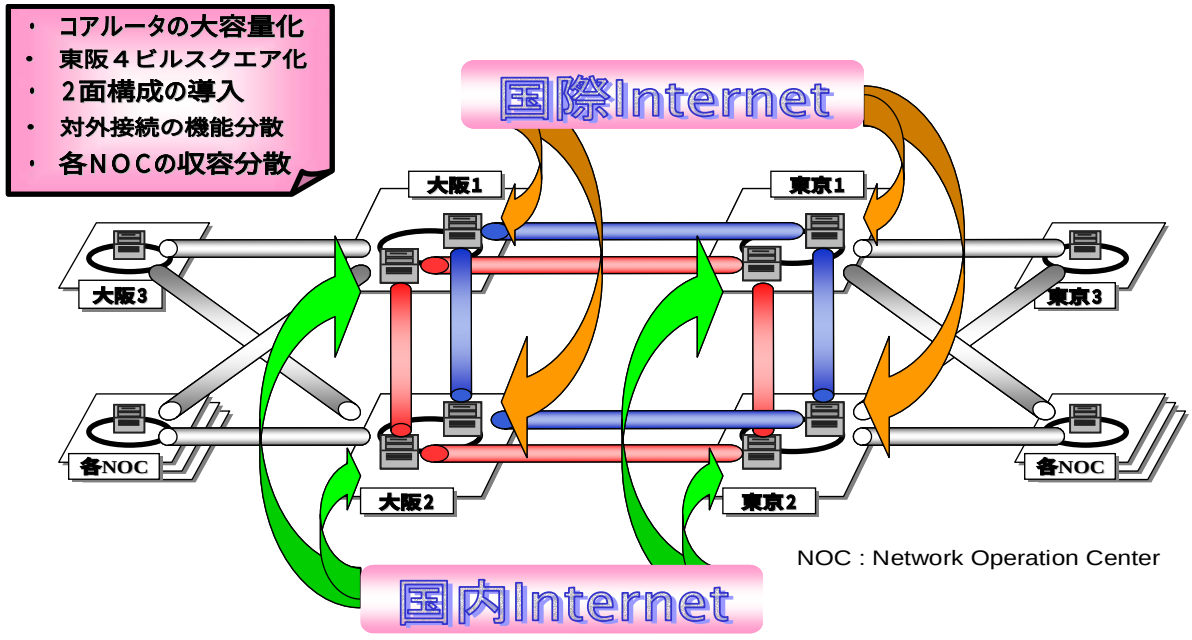
その上で、ここでは、インターネット全体の安定運用の観点から、次の点を各ＩＳＰ側の課題として指摘しておくこととする。

（１）危機管理の観点

東京でサイバー攻撃や大規模災害が発生する場合に備え、東京の中でトラヒック交換拠点を分散するとともに、例えば大阪など東京以外の地域でもトラヒック交換を可能とするネットワーク形態を採用することが必要と考えられる。

既に主要なＩＳＰでは、このような危機管理の観点から、分散型のネットワーク形態を採用している。

▽　ＯＣＮにおけるネットワーク形態の分散化

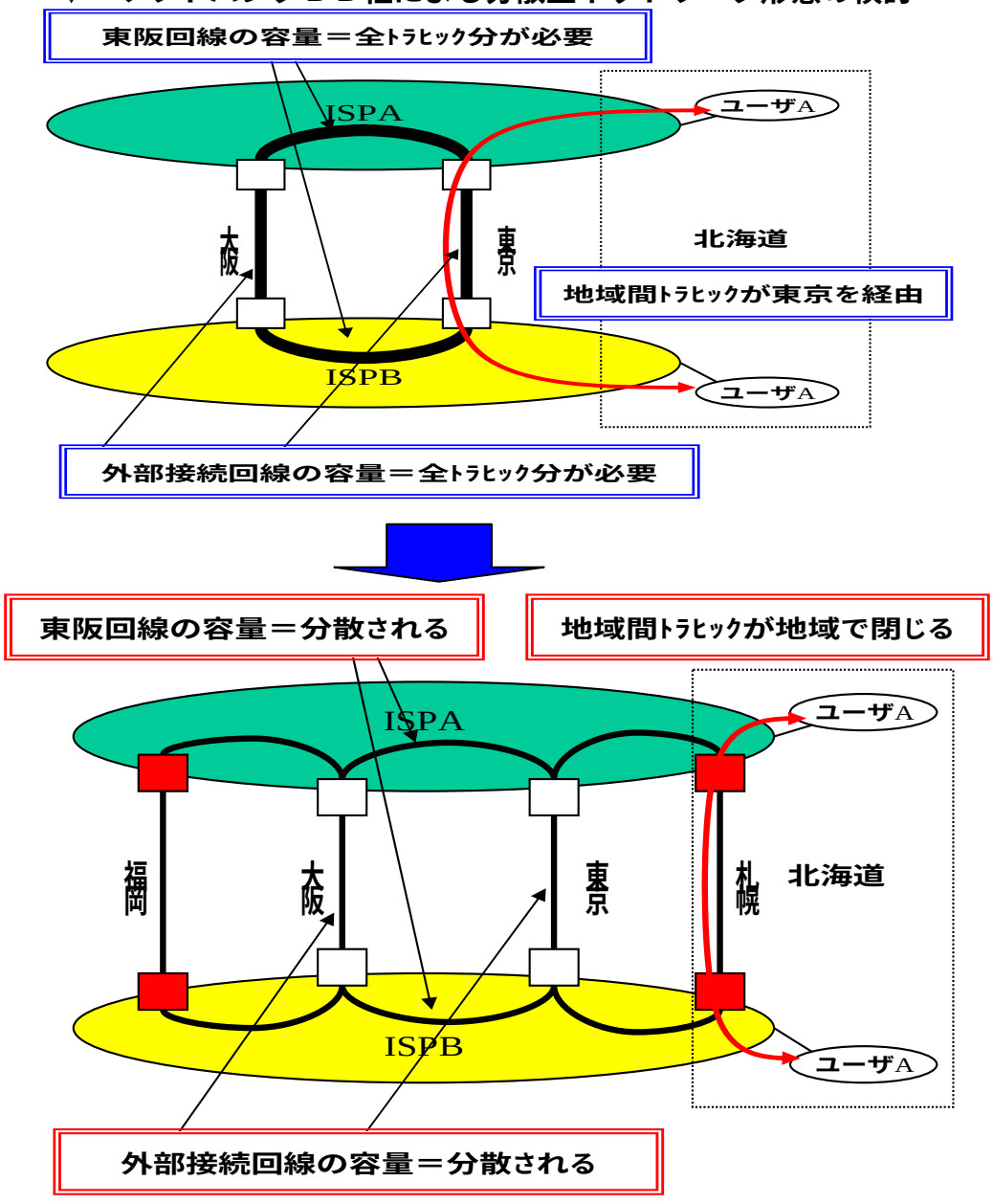


（２）地域におけるブロードバンド・サービスの遅延防止

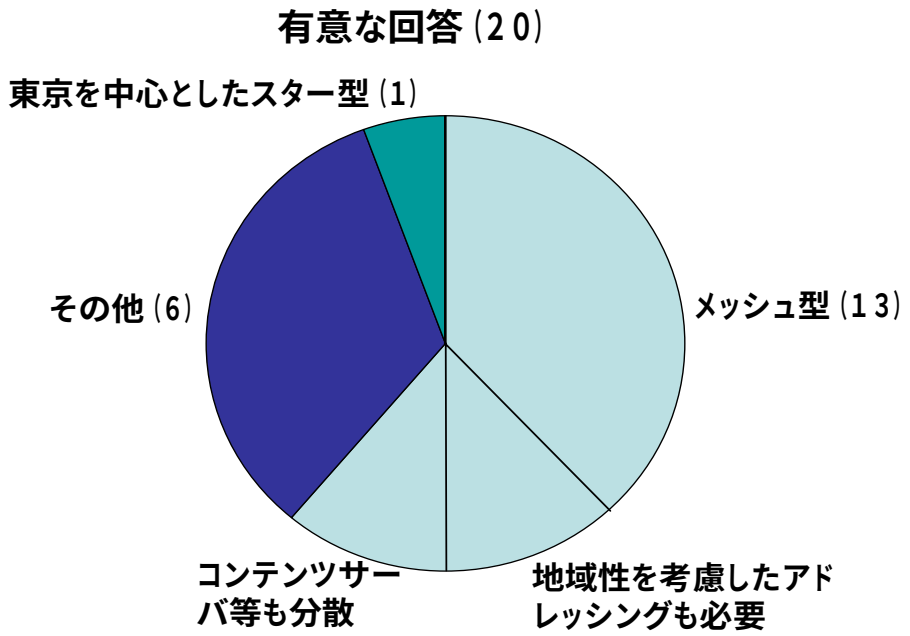
３．で述べたとおり、東京一極集中のネットワーク形態を採用しているがために、本来は地域内に終始するトラヒックも東京を経由し、結果として、地域の利用者に遅延を実感させることになるとすれば、東京と地方における新たなディジタル・デバイド問題になるおそれがあることから、各ＩＳＰにおいては、このような事態を招かないよう、ブロードバンド・サービスの進展に応じてトラヒック・エンジニアリングの分析を行い、適時適切にネットワーク形態の分散化を進めていくことが必要と考えられる。

既に一部のＩＳＰでは、①最短経路でのトラヒック交換による遅延の防止、②トラヒックの集中回避、③バックアップ用回線容量の分散の観点から、分散型ネットワーク形態の採用が検討されている。

▽　ソフトバンクＢＢ社による分散型ネットワーク形態の検討



実際、将来的なトラヒックの増加に対してどのようなネットワーク形態が有効かについて、本研究会の下に設置された「次世代ＩＰ網ＷＧ」の構成員の意見を聴取したところ、「地域性を考慮したアドレッシングも必要」、「コンテンツサーバ等の分散も必要」といった一定の条件を付したものも含めて、分散型（メッシュ型）のネットワーク形態を挙げる意見が多数を占めた。



また、そのうち、ネットワーク形態をどの程度まで分散させるべきかについては、地域ブロック単位まで分散させるべきではないかとの意見が多かったところである。

６．実証実験プロジェクトの推進による諸課題の検証

上記のように、アンケート調査では分散型ネットワーク形態が将来的には適当とする意見が多いところであるが、東京を中心としたスター型の形態となっている現在の我が国のインターネットの構造を分散型ネットワーク形態に移行させて行くためには、トラヒックの流れを制御し、ネットワークの利用効率を最適化するトラヒック・エンジニアリングの分析をはじめとして、ＩＰアドレスの割当て、地域性を考慮した経路制御、アドレスによる識別機能と経路制御機能とを分離した階層型のトラヒック制御技術の開発等の技術上の課題を検証する必要がある。

また、分散の程度についても、将来的には、地域ブロック単位ではなく、例えば都道府県単位まで進めた方が適当となる事態も想定されるところであり、ネットワーク形態の分散化を議論する際には、より詳細な分散化が進む可能性を考慮する必要がある。

更に、ネットワーク形態の分散化を進めるに際しても、単に東京を中心としたスター型のネットワーク形態から分散型のネットワーク形態に一律に移行するものではないと考えられる。

すなわち、現在の東京規模の設備が全国で展開されるということは想定し難く、各

地域のトラヒック規模に応じた設備が、全国レベルでは分散型ネットワーク形態の一部を構成し、各地域ではスター型のネットワーク形態を構成するという事態も考えられる。

いずれにしても、インターネットは、これまでにも多くの課題を克服し発展してきたネットワークであり、今後も更なる発展に向けて、各ＩＳＰ共通の課題として、次の事項を検証する必要がある。

①　トラヒック・エンジニアリングの分析、ＩＰアドレスの割当て、地域性を考慮した経路制御、アドレスによる識別機能と経路制御機能とを分離した階層型のトラヒック制御技術の開発等の技術上の課題

②　①の検証を踏まえたネットワーク形態の分散化の程度（ネットワーク形態の最適化）

このため、第６章で取り上げたトラヒック制御と品質保証に関する技術的な課題とともに、分散型ネットワーク形態に移行するに当たっての技術的な課題についても、ＩＳＰ間で協調して検証していくとともに、必要に応じて、その解決に必要な支援を国が行うことが有効と考えられる。

第８章　障害連鎖防止

１．通信障害連鎖の事例

第２章で述べたとおり、「e-Japan 戦略Ⅱ」に盛り込まれたＩＴの利活用を進めていくためには、将来的なトラヒック増加に対応するだけでは十分ではない。

多数のネットワークが多様に接続することによって成り立っているインターネットにおいては、一つのネットワークにおける通信障害が全体に波及するおそれがあり、インターネット全体の安定した運用を確保する観点から、障害連鎖を防止するためにどのような方策（ＩＳＰ間の連携、技術開発等）が必要かつ有効か、という点も検討しておかなければならない課題である。

インターネットは、発展を続けるオープンなネットワークであり、様々なサービスやコンテンツが生まれるワークベンチであるというメリットを有する一方、「隣人が信じている隣人（第三者）を信用する」ということを前提として成り立っているネットワークであり、適切な対策を講じなければ障害や攻撃に対して無防備であるというデメリットを有している。

実際、インターネット上では、様々な通信障害が起こっており、各ＩＳＰでは、いわゆる「モグラ叩き」のように対策を講じてきているのが実状である。

通信障害連鎖の事例

原因	内容
経路情報の誤り（海外）	1997 年 4 月、ある米国 ISP から大量の経路情報が逆流。これにより、インターネットは 12 時間以上にわたり経路が混乱。
	1997 年 10 月、UUNET が誤った経路情報を大量に広報。
	2003 年 2 月、ある海外 ISP から日本のある ISP の誤った経路情報が広報されたため、 当該 ISP のネットワークオペレーションに支障を来した。
経路情報の誤り（日本）	1994～95 年、NSPIXP における誤った国際経路情報の広報により、ルータに過負荷。
	2000 年 9 月、ある ISP から IX を含む経路情報を誤って広報。１つの誤った経路情報で IX におけるパブリック・ピアリングがダウン。
	2002 年 1 月、ある ISP から誤った国際経路情報が大量に広報。
DDoS 攻撃(分散拠点からのサービス否定攻撃)	1997 年、Cisco 社のルータの工場出荷時設定の不備をついた攻撃
	2001 年、Yahoo!、Microsoft 等、特定の有名サイトを狙った DoS 攻撃
	2002 年 10 月、インターネットのドメイン・ネームを管理する 13 台のルートサーバを狙った攻撃
	2003 年、メールやセキュリティ・ホールをついたワーム (*) が流行。韓国では、インターネットの大規模な停止が発生。

（＊）通常のコンピュータウイルスは感染の対象となるファイルといっしょになってパソコン間を移動するが、そのようなファイルを必要とせずに、自力で多くのパソコンに感染するウイルスのことを「ワーム」という。

２．通信障害の定義と種類

通信障害とは、ＩＳＰの電気通信設備の故障やネットワーク運用時のオペレーションミス等により通信に支障が生じることをいい、障害により、①通信ができなくなる、②回線容量に対して過度のトラヒックが集中し輻輳が発生する、といった事態を招く場合が多い。

通信障害には、障害の範囲が１つのＩＳＰ内にとどまり他のＩＳＰに影響が波及しないものと、他のＩＳＰに障害が連鎖して被害が拡大するものとがあるが、本研究会では、後者の通信障害への対応策について検討した。

３．連鎖する通信障害の種別と原因

通信障害の原因には、ＩＳＰ側で不適切な経路情報を広報してしまう場合と、端末設備からのＤｏＳ攻撃やウイルスによる場合とがある。

連鎖する通信障害の種別をその原因ごとに整理すると、下表のとおりである。

▽　通信障害の種別と原因

種別	内容	原因
経路障害	・不適切な経路情報が広報され、通信ができなくなる。 ・経路の確立・切断が頻繁に行われる等により、ルータ間の接続が不安定になる。	・通信装置の故障やバグ ・ＩＳＰの運用ミス ・不正アクセス、不正制御
パケット転送障害	・異常なトラヒックが発生することにより、回線が輻輳する。	・利用者の端末設備がウイルス等に感染し、不正なトラヒックを送出 ・ＤｏＳ攻撃　　等
アプリケーション障害	・ドメインネーム・サーバの障害により、名前解決ができなくなる（実際には希少）。	・ＩＳＰの運用ミスや不正アクセス、不正制御

４．通信障害が発生した場合における対処の実状

それでは次に、通信障害が発生した場合に、実際にどのような対処がとられているかを見ておくこととする。

通信障害が発生した場合には、何よりもまず障害の状況を把握しなければならない。

障害状況把握の手段としては、接続しているＩＳＰ同士での情報交換、ＩＸ事業者やＪＡＮＯＧ（JApan Network Operators' Group）で運営しているメーリング・リストの活用等があるが、実際には、各ＩＳＰのシステム担当者同士が携帯電話等で直接連絡し合うことにより、緊急対応している場合が多い。

障害が実際に発生した場合に、各ＩＳＰが講じている主な対処方法を挙げると、次のとおりである。

（１）経路情報の誤り

経路情報の誤りには、電気通信設備の障害とは異なり、①アラームが出ないことから監視が困難である、②「経路が不安定」という点に関する定義や認識がＩＳＰごとに異なる、③障害の認識とその対策について人間の判断が介在するため迅速な対応が困難である、という課題を抱えている。

こうした中で、各ＩＳＰにおいては、次のように対処している。

▽　経路情報の誤りへのＩＳＰの対処

（ア）他のＩＳＰのネットワークとの責任分界点に設置されるゲートウェイにおいて、不適切な経路情報を分別（フィルタリング）して廃棄する。
（イ）経路の確立・切断が頻繁に行われる等により、ルータ間の接続が不安定になった場合には当該ルータでのプライベート・ピアリングそのものを一時停止する。

しかしながら、この方法を採用するためには、正常なトラヒックまで止めてしまわないようにするため、バックアップとして他のＩＳＰへの通信経路を複数確保しておく必要があり、ＩＳＰにとっては費用が嵩む１つの要因となっている。

また、正常か異常かの判断自体が困難な場合が多いことに加え、約款上接続を一時停止できる旨の規定があったとしてもＩＳＰには営業上の配慮も働くことから、上記のうち、（ア）のフィルタリングはまだしも、（イ）のプライベート・ピアリングの一時停止については実施しにくいとの指摘が、一部のＩＳＰからなされている。

（２）ＤｏＳ攻撃やウイルス

ＤｏＳ攻撃において、攻撃先がＩＳＰのネットワーク内にある場合は、攻撃先である特定アドレス向けのパケットを一時的に破棄するという対処がなされている。

また、攻撃元が特定でき、かつＩＳＰのネットワーク内にある場合には、攻撃元の端末の管理者に対応を依頼するとともに、攻撃元の特定アドレスからのパケットをＩＳＰ側で破棄するという対処がなされている。

５．障害連鎖の予防

上記４．では、通信障害が発生した場合の「対処の実状」を見た訳であるが、それだけではなく、障害連鎖をどのように「予防」するかという点も重要である。

現在、各ＩＳＰに採用されている主な予防策は、以下のとおりである。

（１）フィルタリングの活用

連鎖する通信障害のうち、予防の対策を講じることが可能なものとしては、不適切な経路情報の受信の予防がある。

実際には、ＢＧＰに一定のフィルタリング機能を設定することにより、予防策を講じているＩＳＰが多い。

フィルタリングの種類とその内容

種類	内容
AS-path フィルタリング	AS-path 情報を交換し、AS(Autonomous System)(*)間の責任分界点に置かれるルータの設定において、AS-path 情報にあった経路のみを受け取るようフィルタリング。
Prefix フィルタリング	Prefix(**)情報を交換し、AS 間の責任分界点に置かれるルータの設定において、Prefix 情報にあった経路のみを受け取るようフィルタリング。
Maximum prefix フィルタリング	受信する Prefix 数の上限を設定し、それを超える経路を受け取った場合に、アラーム発出又は接続停止を行うようフィルタリング。
不適切情報のフィルタアウト	デフォルトルート、プライベートアドレス、マルチキャストアドレス、ループバックアドレス等インターネット上へ流すべきでない経路をフィルタリングして破棄。

（＊）ＡＳとは、ある経路制御方針によって運営されるネットワークのことをいう。全国展開しているＩＳＰもインターネット全体からみると一定の経路制御方針によって運営されている１つのネットワークであり、１つのＡＳとして捉えられ、ＡＳ番号を割り当てられている。

（＊＊）Prefix 情報とは、ISP 間で経路情報の交換を行う場合、アドレス空間を指定するための情報。アドレス空間の開始位置とアドレス空間の大きさの２つを組み合わせて指定される。

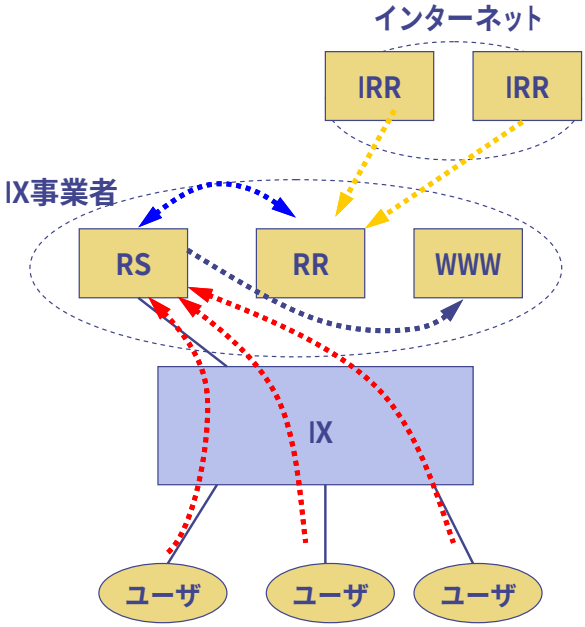
（２）ＩＲＲ (Internet Routing Registry)の活用

ＩＲＲ（Internet Routing Registry）とは、インターネット上でのデータの経路情報、どの接続からどのようなデータをどのように優先的に流すかについての情報、また、その経路が誰に管理されているかについての情報を蓄積したデータベースのことをいい、既に多くのＩＲＲが存在している。

ＩＳＰにとってＩＲＲは、他のネットワークから受信した経路情報をＩＲＲに登録されているものと比較して経路情報を確認する場合や、ＩＳＰ間でフィルタリングを行う場合等に活用されている。

ＩＲＲを活用した経路情報の確認の仕組み（JPIXにおける事例）

- IRRに登録されている正しい(と思われる)経路情報をIXのRouting Registry（ＲＲ）にコピー
- IXのRoute Server（ＲＳ）は、ＩＳＰから経路情報を受信
- RSで受信した経路とRR上の経路情報とを比較
- 比較した結果をWebサイトにてＩＳＰに提供



http://www.nic.ad.jp/ja/materials/irr/20030724/05_jpirr-bof-research.pdf

（３）ＩＳＰ間の協調

障害の連鎖を予防するためには、ＩＳＰ間の情報共有や連携が不可欠である。

現在では、ＮＡＮＯＧ（North American Network Operators' Group）、ＪＡＮＯＧ等の任意団体で情報交換が行われているほか、ＩＸ事業者が主催するメーリング・リストやミーティングなどにおいて、障害情報や障害連鎖防止のためのノウハウに関する技術交流等が行われている。

６．障害連鎖防止に向けての課題

（１）不適切な経路情報による障害連鎖に対する予防

第１に、各ＩＳＰにおいて経路情報の設定ミスや運用ミスにより、障害連鎖が発生しないようにすることが求められる。

このためには、Prefix フィルタリングを導入することが望ましいと考えられるが、その導入にはコストがかかる等、ＩＳＰ側に運用面で負担がある。

第２に、我が国においては、ＩＸを経由した経路情報の広報による障害連鎖が多いことから、相互接続における運用や接続方針を明確化することも求められる。

第３に、ＩＲＲの活用も有効であると考えられているが、全てのＩＳＰが登録している訳ではないので、その適用範囲が限定されている状況にあることから、多くのＩＳＰがＩＲＲに登録するよう、インターネットの安定運用のためにＩＲＲがどれほど有効かという点についての普及・啓蒙活動を行うこと等により、未登録ＩＳＰにＩＲＲ登録へのインセンティブを与えていくことを検討すべきであると考えられる。

また、ＩＲＲの情報が適切に更新されていないため、ＩＲＲのデータベースの信憑性の向上自体が課題であるとの指摘もある。

この点については、ＩＲＲのデータベースの維持・更新・管理を随時行うこと等により、その信頼性を高めていくことが必要である。

この点については、我が国でＩＰアドレスの管理を行っているＪＰＮＩＣ（JaPan Network Information Center）において、ＩＲＲ企画策定専門家チームが設立され、ＩＲＲの活用促進策が検討されているが、今後とも、こうした活動が充実・強化されていくことが期待される。

第４に、ＩＳＰとして最低限守るべき運用方針やネットワーク品質の明確化を図ることも有効であると考えられる。

この点については、例えば、現在ＪＡＮＯＧ等の任意団体において情報交換や技術交流が行われているが、事業を開始したばかりのＩＳＰやこれから事業を開始しようとするＩＳＰに対して、障害連鎖防止のための運用のノウハウを普及・啓蒙させていくための施策も必要と考えられる。

インターネットの安定運用は、各ＩＳＰやＩＸ事業者の技術者がＪＡＮＯＧ等の民間団体における活動等を通じて情報交換や技術交流を行うことにより支えられてきているのが実情であり、こうした活動を肯定的に認知し支援することは、インターネットの信頼性を向上させていく上で重要である。

また、障害発生時には、自社の情報を他社と共有することが必要となるが、他方で、インターネット全体の安定運用を確保する観点から、自社の情報をどこまで出して良いか、また出すべきかについての基準は明確ではなく、各ＩＳＰやＩＸ事業者の技術者はジレンマに陥る場合も多い。

このため、障害発生時に自社情報をどこまで出して良いかについて、各 ISP や IX 事業者において経営レベルまで話を上げて、一定の基準を作っておくことが望ましいと考えられる。

いずれにしても、ＪＰＮＩＣやＪＡＮＯＧ等の活動は、費用がかかる一方で収益には直結せず、にもかかわらずインターネット全体の安定運用に資するものであることから、政府による政策支援の在り方を検討すべきであると考えられる。

第５に、インターネットにおける障害連鎖は、国境を越えて広がり得るものであり、国内のみならず、国際的な連携も必要である。

この点については、例えば、我が国で行われているＩＳＰ間の協調を国際間でも行い、国際レベルでのＩＲＲのデータベースの信憑性の確保や、障害連鎖防止のための運用ノウハウの途上国ＩＳＰへの提供等を推進していくこと等を検討すべきである。

（２）ＤｏＳ攻撃やウイルスへの対応

ＤｏＳ攻撃への対応としては、まず攻撃元の検出方法を確立することが有効であると考えられる。

しかしながら、攻撃元がアドレスを偽れば、技術的な対処をとりようがないのが実情であり、ＤｏＳ攻撃やウイルスに対応できるシステムの導入について、研究開発・実証実験の推進をするとともに、ＤｏＳ攻撃やウイルスが発生した際のＩＳＰ間の協力体制についても検討すべきである。

また、端末設備側のセキュリティの向上も重要であり、端末設備やアプリケーション・ソフトそれ自体のセキュリティを高めるとともに、ＩＳＰ、通信機器メーカ、システムインテグレータ、国、自治体等において、利用者のセキュリティ意識を高め、セキュリティ対策が適切に実行されるための方策を見出す必要がある。

第９章　総括

以上、当研究会におけるこれまでの検討を総括すると、次のとおりである。

１．トラヒックの現状把握

当研究会では、我が国のインターネットのバックボーンにおけるトラヒックについて現状把握を行った。

こうした作業を進めるに当たっては、どういう情報をどこまでなら出せるかという点について、ＩＳＰ間で意思疎通を図っておくことが望ましい。

しかしながら、開示してよい情報と社外秘とすべき情報の区別については、各ＩＳＰの経営に関わる事項であり、トラヒック情報の交換には熟考が必要であろうし、その実施に当たっては、各ＩＳＰの経営者層のリーダーシップに基づくＩＳＰ間のコンセンサスが必要である。

特に各ＩＳＰがトラヒック情報の開示に踏み出しにくい初動期においては、今回のトラヒックの現状調査のように、産学官で協力して個別のトラヒック情報の秘匿性を維持しつつ、各社のトラヒック情報を合計する形でインターネット全体としてのトラヒック情報を把握することは、重要な施策の１つであると考えられる。

また、実際のトラヒックは、各ＩＳＰのネットワーク形態に依存しており、集計するトラヒック情報の様式を統一することにも難しい面がある。

そこで、これまでに得られている情報と公開情報やサンプル調査を基に統計的な手法を駆使して、一定の仮定を置いてトラヒックの総量とパターンを推計するという方法を開発する必要がある。

いずれにしても、全体的なトラヒック情報を把握することは、各ＩＳＰにとっても今後の投資計画やネットワーク形態、更にはビジネス・モデルを検討する上で有用と考えられるが、一事業者だけでは把握できないものであり、今回のトラヒック調査のような取組みは、大きな意義を有するものと考えられる。

また、トラヒック情報の把握は、例えば半年に１回又は１年に１回というように定期的な集計と分析を行ってこそ意義をもつものであり、産学官で協力して、調査の趣旨や把握すべきトラヒック情報の範囲、秘匿性の維持方法等を明確化して、継続的な取組みをしていくことが必要と考えられる。

こうしたトラヒック情報の蓄積は、トラヒックの将来予想をする上での重要な基礎をなすものと考えられる。

２．ネットワークの増強

当研究会では、将来的なトラヒックの増加にどのように対応すべきかについても検討を行った。

第１に考えられる方策は、ネットワークの増強である。

この点については、ルータ等交換機能を担う部分と光ファイバ等伝送機能を担う部分とに分けて検討を行った。

（１）交換機能を担う部分

ルータ／スイッチ／インターフェースの大容量化が懸念事項であるとの指摘が当研究会の多数を占めた。

この点については、総務省においても２００１年度から研究開発に取り組んでいるところであるが、今後は、実用化及び商用化に向けたニーズをこうした研究開発活動にも反映させていくことが必要である。

（２）伝送機能を担う部分

当研究会では、中継系光ファイバの芯線の未利用率についても調査を行い、未利用率が６割前後で推移しているという点を確認した。

このように芯線の未利用率が６割前後で推移していることは、商用ネットワークの運用上、中継系光ファイバに関する需給逼迫感をもたらさないという観点からは、健全なことと考えられる。

また、波長分割多重（ＷＤＭ）技術が開発・実用化され、光ファイバの容量を増幅させることが可能となっていることも、中継系光ファイバの需給を逼迫させないことに寄与しているものと考えられる。

しかしながら、将来的なトラヒック増加に対応するには、中継系光ファイバの需要に関する情報交換を行うことや、光ファイバ１芯当たりの伝送容量を上げるための研究開発を、実用化及び商用化に向けたニーズを反映しつつ引き続き推進することが重要である。

３．トラヒック制御

将来的なトラヒックの増加に対して第２に考えられる方策は、トラヒックの制御である。

この点については、一部の利用者が大量のトラヒックを発生させ、回線を占有している場合において、そもそもトラヒックを制御すべきなのか、また、インターネットにおいてトラヒック制御は可能なのか、技術的な対応や契約上の対応として何が有効か、といった点に関し、多くのＩＳＰが事業運営上の悩みを抱えていることが確認された。

課金体系に工夫を加えることもトラヒック制御の１つの手段であり、トラヒックを大量に発生させる契約者に対し、例えばトラヒックの上限値を超えたら追加料金を徴

収するというように、他の契約者とは異なる料金体系を採ることも考えられる。

いずれにしても、課金体系の採否は、各ＩＳＰのビジネス・モデルやコスト・モデルに関わる事項であるが、一部の利用者が発生させる大量のトラヒックに伴うネットワーク増強費用を、利用者全体で負担することは、却って公平を失すると考えられることから、各ＩＳＰにおいては、利用者間の公平性と公正性を確保し得る料金モデルを採用することも１つの対処方法と考えられる。

また、トラヒック制御のため、ＩＰ電話やＩＰテレビ電話等のリアルタイム系サービスの提供のために品質保証をかける場合についても、現在は１つの事業のネットワーク内でのみ品質保証が可能であり、今後は複数事業者間でのトラヒック制御や品質保証に関する技術の研究開発を進めていく必要がある。

その際には、帯域保証や遅延保証といった側面だけでなく、パケットが損失した場合でも利用可能性を確保する技術の研究開発に取り組むことが必要である。特に、最近急速に普及しているＶｏＩＰ（Voice over IP）等について、通信機器相互間及びネットワーク相互間の接続性の確保のための取り組みを強化することが重要である。

４．トラヒック分散

将来的なトラヒックの増加に対して第３に考えられる方策は、トラヒックの分散である。

この点については、まず、多くのＩＳＰが東京を中心としたスター型のネットワーク形態を採用しており、トラヒックが東京一極に集中している現状が確認された。

しかしながら、ネットワーク形態は、利用者の分布、コンテンツの配置、アプリケーション、更にはこれらを受けたトラヒックの状況等に大きく依存するものであり、各ＩＳＰの経営判断に委ねられるべき事項であると言える。

また、一部のＩＳＰでは、危機管理の観点又は地域におけるブロードバンド・サービスの遅延防止の観点から、既に分散型ネットワーク形態を採用している又は採用を検討していることも確認された。

実際、将来的なトラヒックの増加に対してどのようなネットワーク形態が有効かについて、当研究会の下に設置された「次世代ＩＰ網ＷＧ」構成員の意見を聴取してみると、分散型ネットワーク形態が有効とする意見が多い。

しかしながら、東京を中心としたスター型のネットワーク形態から分散型ネットワーク形態への移行を進めて行くためには、トラヒックの流れを制御し、ネットワークの利用効率を最適化するトラヒック・エンジニアリングの分析をはじめとして、ＩＰアドレスの割当て、地域性を考慮した経路制御、アドレスによる識別機能と経路制御機能とを分離した階層型のトラヒック制御技術の開発等の技術上の課題を検証する必

要がある。

また、光ファイバやＤＳＬを中心とする、いわゆる有線ネットワークだけではなく、無線ネットワークやＩＳＰの商用ネットワーク以外の通信インフラを含めた、総合的な視点に立った通信インフラ全体の設計や運用、運用の協調についても検討を行う必要がある。

いずれにしても、インターネットは、これまでにも多くの課題を克服し発展してきたネットワークであり、今後も更なる発展に向けて、各ＩＳＰ共通の課題として、こうした技術上の課題やネットワーク形態の分散化の程度を検証していくことが必要である。

５．障害連鎖防止

インターネット全体の安定した運用を確保する観点から障害連鎖を防止するためには、①各ＩＳＰ間の情報共有、②経路情報のフィルタリング、③経路情報等のデータベースであるＩＲＲの活用が必要である。

なお、このうちＩＲＲについては、データベースの維持・更新・管理を随時行うこと等により、その信頼性を高めていくことが必要である。

更に、ＩＳＰとして最低限守るべき運用方針やネットワーク品質の明確化については、現在ＪＡＮＯＧ等の任意団体において継続されている情報交換や技術交流が行われているが、事業を開始したばかりのＩＳＰやこれから事業を開始しようとするＩＳＰに対して、障害連鎖防止のための運用のノウハウを普及・啓蒙させていくための施策も必要と考えられる。

端末設備側のセキュリティの向上も重要であり、端末設備やアプリケーション・ソフトそれ自体のセキュリティを高めるとともに、ＩＳＰ、通信機器メーカ、システムインテグレータ等において、利用者のセキュリティ意識を高め、セキュリティ対策が適切に実行されるための方策を見出す必要がある。

以上

用語集

名称	用語解説	掲載頁
ブロードバンド	ｘＤＳＬ（digital subscriber line）、ＣＡＴＶ、ＦＴＴＨ（fiber to the home）、ＦＷＡ（fixed wireless access）など数百ｋビット/秒以上の広帯域のアクセス回線サービスやその帯域を指す。	1,2,3,4,6,7,8,9,11,25,28,36,39,42,47,49,53,57,71
ＩＳＰ：Internet Service Provider	インターネット･サービス･プロバイダのこと。インターネットへの接続サービスを提供する事業者。	14,16,17,18,19,20,23,24,27,33,35,38,39,40,42,44,45,46,47,48,49,50,52,53,54,55,56,57,59,61,62,63,64,65,66,67,69,70,71,72
バックボーン	一般的に、電気通信事業者の中継設備を相互に接続した基幹通信回線のことを指す。	11,12,13,14,15,23,26,27,31,39,41,42,44,45,50,54,69
ＩＸ：Internet eXchange	インターネット･サービス･プロバイダ相互間を接続する接続点。	15,16,17,18,19,20,23,27,28,29,33,35,39,52,53,54,55,56,61,63,65,66
ＩＴＵ：International Telecommunication Union	国際電気通信連合。電気通信に関する国連の専門機関であり、多国間の円滑な通信を行うため、世界各国が独自の通信方式を採用することによる弊害の除去、有限な資源である電波の混信の防止、電気通信の設備が不十分な国に対する技術援助等を実施している。	2,3
ＦＴＴＨ:Fiber To The Home	電話局等から家庭までの加入者線を光ファイバー･ケーブルにすること。家庭で最大１００Mbps の高速大容量のブロードバンド通信が可能になる。	3,4,6,7,9,11,27,28,44
ＦＷＡ:Fixed Wireless Access	加入者系無線アクセスシステムのこと。利用者と通信事業者の加入者回線を無線で接続する固定通信システム。	4,7,12
ケーブルインターネット	ケーブルテレビ用のケーブルを用いて提供するインターネット接続サービス。これにより高速の常時接続サービスを提供。	3,4,11,27
Ｗ－ＣＤＭＡ：Wideband Code Division Multiple Access	広帯域（5MHz 幅）の直接拡散 CDMA 方式の無線規格。ITU の勧告による IMT-2000 の無線方式の一つであり、日本と欧州がそれぞれ ITU に提案した方式を一本化したもの。	6
ＨＳＤＰＡ：High Speed Downlink Packet Access	NTT ドコモなどが採用している第 3 世代(3G)携帯電話方式「W-CDMA」のデータ通信を高速化した規格。3G 方式の改良版であることから「3.5G」とも呼ばれている。	6

名称	用語解説	掲載頁
CDMA2000	狭帯域（1.25MHz 幅）の直接拡散 CDMA（Code Division Multiple Access）方式の無線規格。第3世代移動通信システム「IMT-2000」の規格案として、米国が ITU（電気通信連合）に提案した方式の一つ。	6
CDMA2000 1x	CDMA2000 方式のうちの一つで、1.25MHz 幅の周波数を使って音声通話や最大 153.6kbps のパケット通信が可能。	6
CDMA2000 1x EV-DO	CDMA2000 1x 方式を拡張した高速無線データ通信規格。通信速度は下りが最大 2.4Mbps で、音声通話とデータ通信を混在させている 1x と異なり、データ通信だけで帯域を占有し、その帯域を一定時間毎に任意の1ユーザに割り当てる。	6
ベスト・エフォート	品質保証のない通信ネットワーク又は通信サービスのことをいう。ＤＳＬサービスでは通信速度の上限はあるが、最低速度の保証はされていないという意味で用いられる。	6,47
IMT-2000：International Mobile Telecommunications-2000	第 3 世代移動通信システムのこと。携帯電話初の世界共通仕様で、W-CDMA、CDMA2000 など5つの無線アクセス方式からなり、日本では、W-CDMA、CDMA2000 の2つの方式が採用されている。2GHz の周波数帯の電波を用い、最大 2Mbps の高速データ通信が可能。	7
ＰＤＣ：Personal Digital Cellular	日本の携帯電話に使われているデジタル無線通信方式。800MHz/1.5GHz の周波数帯を電波を利用している。	7
cdmaOne	符号分割多重接続(CDMA：Code Division Multiple Access)方式を利用した、第 2.5 世代携帯電話規格(2.5G)のひとつ。PDC（Personal Digital Cellular）など従来の携帯電話方式に比べ、音声品質が良く、データ伝送速度が速いなどの特徴を持つ。	7
ＤＳ－ＣＤＭＡ：Direct Spread Code Division Multiple Access	IMT-2000 規格の 1 つで、通称名は W-CDMA。（解説は W-CDMA を参照。）	7
ＭＣ－ＣＤＭＡ：Multi-Carrier Code Division Multiple Access	IMT-2000 規格の 1 つで、通称名は CDMA2000。（解説は CDMA2000 を参照。）	7
ＡＤＳＬ：Asymmetric Digital Subscriber Line	一般の電話において音声伝送に利用しない高い周波数帯を使ってデータ通信を行なう、xDSL 技術の一種。電話局から利用者方向(下り)の通信の最高速度と利用者から電話局方向(上り)の通信の最高速度が非対称(asymmetric)になっているのが特徴。	7

名称	用語解説	掲載頁
ＳＤＳＬ：Symmetric Digital Subscriber Line	1対の電話線を使って通信するxDSLの一つ。ADSLやVDSLと異なり、電話局から利用者方向と利用者から電話局方向が同じ速度で通信できる。	7
ＨＤＳＬ：High-bit-rate Digital Subscriber Line	2対の電話線を使って通信するxDSL技術の一つ。ADSLやVDSLと異なり、電話局から利用者方向と利用者から電話局方向が同じ速度で通信できる。	7
ＶＤＳＬ：Very high-bit-rate Digital Subscriber Line	1対の電話線を使って通信する。ADSLと同じく、伝送速度は電話局から利用者方向(下り)と利用者から電話局方向(上り)が非対称速度になっている。	7
フレームリレー	転送するデータを可変長の「フレーム」という単位に分割して送受信する通信サービス。	8
ＩＰ－ＶＰＮ：Internet Protocol-Virtual Private Network	電気通信事業者の閉域IP網を経由して構築することによってセキュリティを高めた仮想的な閉域網サービス。	8
インターネットＶＰＮ	公衆網であるインターネットに接続する回線の両端に装置（ＶＰＮ装置）を接続すること等によって、インターネットを仮想的な閉域網として利用する。	8
広域イーサネット	IEEE（米国電気電子技術者協会）802．3委員会により標準化されたLAN規格であるイーサネットで使用されているスイッチング・ハブを組み合わせて構築した通信サービス。	8
セルリレー	ATM（非同期転送モード）により、伝送するデータを固定長の「セル」という単位に分割して送受信する通信サービス。	8
ＩＰ:Internet Protocol	インターネットを構成する通信機器が共通に使用する通信プロトコル。	8,14,27,31,48,50,54,59,66,71
ユビキタス・ネットワーク	「いつでも、どこでも、誰でもアクセスが可能」なネットワーク環境。なお、ユビキタスとは「いたるところに遍在する」という意味のラテン語に由来した言葉。	11,48
トラヒック	ネットワークの特定の経路上を一定時間に流れる情報の量。	11,12,14,15,16,18,19,20,2123,24,25,26,27,28,29,30,31,35,38,39,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,61,62,63,69,70,71

名称	用語解説	掲載頁
ピアリング	ISP間でお互いに相手方ISPあてのトラヒックを交換しあうこと。一般的には無償接続。IXで行われるピアリングを「パブリック・ピアリング」、IXを介さないピアリングを「プライベート・ピアリング」という。	16,17,18,19,20,23,28,44,52,54,63
トランジット	他のISPからのトラヒックをインターネット全体に中継すること（他のISPに対してインターネットの経路を提供すること。）。一般的には有償サービス。	16,18,19,20,23,28,44,52
ＣＰＵ：Central Processing Unit	パソコン作業に必要なあらゆる計算処理を行う部分。クロック周波数がＣＰＵの処理速度を表し、この数値が大きいほど、パソコンの動作スピードは速い。	28
ＦＴＰ：File Transfer Protocol	インターネットやイントラネットなどのTCP/IPネットワークでファイルを転送するときに使われるプロトコル。	25,48
Ｗｅｂ	World Wide Web の略。インターネットやイントラネットで標準的に用いられるドキュメントシステム。HTML という言語で文書の論理構造などを記述し、文書の中に画像や音声など文字以外のデータや、他の文書の位置(ハイパーリンク)を埋め込むことができる。インターネットで最も多く利用されるアプリケーションである。	25,48
プロトコル	コンピュータとコンピュータが、互いにデータをやりとりするための手順や仕組みを定めた約束事。	32
ルーティング	ネットワーク上の目的地までの転送経路を選択するプロセス。ルータなどのネットワーク構成機器同士が情報交換することで実行する。経路制御ともいう。	32
光ルータ	光信号を電気信号に変換せず光のまま経路制御処理を行うルータ。	34
光スイッチ	光信号を光のまま経路変更するＷＤＭ伝送路向けの中継装置「光クロスコネクト」で利用する基幹部品又は技術のこと。入力してきた光信号を鏡などで反射して別の経路に出力する。	34
インターフェイス	一般的には、二つのものの間に立って、情報のやり取りを仲介するもののこと。ルータ・スイッチ等の通信機器におけるインターフェースとは、複数の通信機器を接続して通信する際の規約で、コネクタの形状や電気信号の形式などを定めているもの。	21,31,32,33

名称	用語解説	掲載頁
中継系光ファイバ	加入者系配線（集線点から加入者宅内の光端末回線終端装置までの配線）及び加入者系幹線（加入者配線に分岐する集線点から加入者収容局内の端末系光端局装置までの間の端末系幹線路）を除く中継系伝送路のうち、光ファイバで敷設されているもの。	36,37,38,39,40,70
ＩＲＵ：indefeasible Right of User	関係当事者すべての合意がない限り、破棄したり終了させることができない回線使用権のこと。「破棄し得ない使用権」ともいう。 破棄し得ない使用権（indefeasible right of user）のこと。破棄し得ない使用権とは、契約（契約以外の協定等の形式を含む。）によって定められ、関係当事者の合意がない限り破棄又は終了させることができない長期安定的な使用権のこと。 　他者の所有する光ファイバ等についてIRUの設定を受けた事業者は、当該光ファイバ等を継続的に支配・管理している状態にあると認められる。	37
ＷＤＭ：Wavelength Division Multiplexing	波長分割多重。複数の異なる波長の光信号を同一の光ファイバに合波及び分波することにより、光ファイバの伝送容量を飛躍的に増大する方式。	32,33,37,38,39,42,70
Ｐ２Ｐ:Peer to Peer	従来のクライアント・サーバ型のシステムのようにサーバに集められたデータを引き出して複数の端末(クライアント)で利用するのではなく、パソコン等のあらゆる端末に保存されたデータを直接やりとりするシステム及びサービス	46,47,48,49
サイバー攻撃	インターネット経由で他のコンピュータに不正アクセスを行い、相手の国家や企業にダメージを与えようとする行動のこと。	53,56
経路情報	ルータや端末が保持するパケットの伝送先に関する情報。	54,61,62,63,64,65,72
ＤＤｏＳ攻撃:Distributed Denial of Service	分散型サービス否定攻撃のこと。多数のサーバを踏み台にしてコンピュータやルータに大量のデータを同時に送り、システムをダウンさせる攻撃。DoS 攻撃のうち多数のサーバから攻撃するもの。	61
ＤｏＳ攻撃:Denial of Service	サービス不能攻撃のこと。標的となるコンピュータやルータに大量のデータを送りつけてシステムをダウンさせる攻撃。	61,62,63,67
ドメイン・ネーム	インターネットに接続されたコンピュータを識別するためのもので、いわば、インターネット上の住所。コンピュータの識別番号を数字だけで表記するIPアドレスコード（例：211.133.250.131）を、人間が判りやすいアルファベットに置き換えた名称で、コンピュータを、存在する地域や所有する組織の属性などを用いて標記。	61,62

名称	用語解説	掲載頁
ルートサーバ	ルートネームサーバ、ルートDNSサーバともいう。インターネット上のドメイン名とIPアドレスを対応させるシステムがDNS(Domain Name System)であり、このドメイン名とIPアドレスを対応させるための情報を提供するネームサーバがインターネット上には無数に存在し、ドメイン名に対応した階層構造をなしている。この最上位にあるのがルートネームサーバで、世界13か所にある。	61
セキュリティ・ホール	コンピュータ上のアプリケーション等に存在する、情報セキュリティの不備。これを悪用することでネットワークへの不正アクセス等が可能となる。	61
ワーム	通常のコンピュータウイルスは感染の対象となるファイルといっしょになってパソコン間を移動するが、そのようなファイルを必要とせずに、自力で多くのパソコンに感染するウイルスのことを「ワーム」という。	61,62
ウイルス	電子ファイル、電子メール等を介して次々と他のコンピュータに自己の複製プログラムを潜伏させていき、その中のデータやソフトウェアを破壊するなどの害を及ぼすコンピュータプログラム。	62,63,67
ＪＡＮＯＧ：JApan Network Operators' Group	日本ネットワーク･オペレーターズ･グループ。日本のインターネット技術者･利用者などが参加し、インターネット技術やオペレーション技術に関する話題を議論･検討する。インターネット接続事業者（プロバイダ）関係者らが多く参加するメーリングリストでは、インターネットを安全･安定的に運営するための情報交換が活発に行われている。	63
ＢＧＰ：Boder Gateway Protocol	AS間で利用するルーティングプロトコルであるEGPs（Exterior gateway protocols）の一つで、ＡＳ間で経路情報を交換する際に用いるプロトコル。	64
ゲートウェイ	ネットワーク上で、媒体やプロトコルが異なるデータを相互に変換して通信を可能にする機器。通信媒体や伝送方式の違いを吸収して異機種間の接続を可能とする。	63
フィルタリング	特定の条件に合致するデータを通過又は破棄する行為や機能のこと。	64,65,72
ＡＳ：Autonomous system	ＡＳとは、ある経路制御方針によって運営されるネットワークのことをいう。全国展開しているＩＳＰもインターネット全体からみると一定の経路制御方針によって運営されている１つのネットワークであり、１つのＡＳとして捉えられ、ＡＳ番号を割り当てられている。	64

名称	用語解説	掲載頁
AS-path 情報	ある AS に到達するための経路を示した AS 番号リスト。	64
AS-path フィルタリング	AS-path 情報を交換し、AS(Autonomous System)間の責任分界点に置かれるルータの設定において、AS-path 情報にあった経路のみを受け取るようフィルタリング。	64
Prefix 情報	ISP 間で経路情報の交換を行う場合、アドレス空間を指定するための情報。アドレス空間の開始位置とアドレス空間の大きさの2つを組み合わせて指定される。	64
Prefix フィルタリング	Prefix 情報を交換し、AS 間の責任分界点に置かれるルータの設定において、Prefix 情報にあった経路のみを受け取るようフィルタリング行為や機能のこと。	64,65
デフォルトルート	パケットの転送先が登録されていない場合のパケットの転送先。	65
プライベートアドレス	社内ネットワークなど組織内に閉じたネットワーク上で、自由に利用できる IP アドレス。	64
マルチキャストアドレス	一つのパケットを同時に特定の複数のコンピュータに送信するためのアドレス。	64
ループバックアドレス	ネットワーク上において自分自身を表す仮想的なアドレスであり、IPv4 においては「127.0.0.0」のこと指す。	64
ＩＲＲ ：Internet Routing Registry	インターネット上でのデータの経路情報、どの接続からどのようなデータをどのように優先的に流すかについての情報、また、その経路が誰に管理されているかについての情報を蓄積したデータベース。	64,65,66,72
ＮＡＮＯＧ：North American Network Operators’ Group	インターネット運用技術全般に関して技術的な議論を展開しているグループ。1994 年に発足し、主に北米地域のネットワーク管理者が参加している。活動の主体はメーリング･リストによる情報交換だが、年に3回の定例ミーティングがある。	65
ＪＡＮＯＧ：JApan Network Operators’ Group	日本ネットワーク･オペレーターズ･グループ。日本のインターネット技術者･利用者などが参加し、インターネット技術やオペレーションに関する話題を議論、検討する。	63,65,66,72