第 10 部

ネットワークトラフィック統計情報の収集と解析

第 1 章

はじめに

WIDE NetStat WG は、広域分散環境におけるトラフィックデータの「収集」、「解析」、「保存」、「利用」等のために必要とされる技術に関する研究を行なうことを目的に活動を行なっている。

本年度も昨年度から引続き NNStat を用いた WIDE バックボーンネットワークの統計情報の収集と解析を行なって来た。またそれに加えて、IPANeMa の一部として開発された新しい統計収集、解析のツールであるスタットデーモン、ロギングデーモンを用いたトラフィック収集も一部で開始した。

本報告では、

1. 国際線のトラフィック解析
2. 東京藤沢間のバックボーントラフィック解析
3. スタットデーモン／ロギングデーモンによるトラフィック解析

の各々に関して報告を行なう。

第 2 章

国際線のトラフィック

2.1 国際線のトラフィック解析結果

表 2.1: 国際線のプロトコル別トラフィック

月		TCP	UDP	IP/IP	ICMP	IGMP	Other	合計	回線利用率
4 月	IN	1,340,237	129,588	0	14,317	848	1	1,484,991	71.61 %
	OUT	820,727	111,991	2,445	23,516	11,863	758	971,300	46.84 %
5 月	IN	1,369,390	153,334	34,458	9,417	1,935	0	1,568,534	75.64%
	OUT	852,399	115,397	101,902	33,784	9,817	97	1,113,396	53.69%
8 月	IN	1,003,239	107,749	5,441	12,235	1,870	0	1,130,534	54.52%
	OUT	1,122,979	123,752	17,268	8,635	10,754	0	1,283,388	61.89%
9 月	IN	1,013,340	155,094	3,029	17,985	1,540	1	1,190,989	57.44%
	OUT	975,435	166,902	5,218	18,330	10,748	1	1,176,634	56.74%
10 月	IN	1,053,180	169,008	55,899	22,917	8,268	0	1,309,272	63.14%
	OUT	825,450	251,236	72,162	9,850	21,709	2	1,180,409	56.93%
12 月	IN	3,714,116	279,378	120,386	63,449	13,939	481	4,191,749	25.27%
	OUT	914,283	190,799	11,398	67,998	18,737	451	1,203,666	7.26%
1 月	IN	3,844,209	240,544	82,676	43,214	11,181	162	4,221,986	25.45%
	OUT	1,100,458	218,722	3,215	69,033	11,501	251	1,403,180	8.46%
2 月	IN	4,691,820	344,003	227,175	38,103	12,186	555	5,313,842	32%
	OUT	1,304,233	173,931	12,397	75,544	12,053	677	1,578,835	9.52%
3 月	IN	4,929,174	359,825	125,158	30,689	16,888	728	5,462,462	32.93%
	OUT	1,341,833	247,385	3,302	40,227	13,737	1,144	1,647,628	9.93%

表 2.1は、1994 年度の IP プロトコル別の 1 日平均のトラフィック量をキロバイト単位で表したものである。また、図 2.1、図 2.2はそれをグラフ化したものである。

6 月 7 月、および 11 月は、データ収集を行なっていたホストのトラブルなどの為に十分なデータ収集が行なえなかったために、ここではデータとしてのせていない。

12 月 5 日から国際回線が 192Kbps から 1.5Mbps にアップグレードされた。これにより海外から国内へのトラフィックが一気に 3 倍以上に増えている。アップグレード以前の回線利用率をみると、1 日の平均でバンド幅の 60%-70%を利用しており、回線がボトルネッ

クとなっていたことが良く分かる。また、10 月と 12 月のトラフィックをプロトコル別に比較してみると全体で 3.2 倍であるのに対して、TCP のトラフィックが 3.5 倍、UDP のトラフィックが 1.6 倍とプロトコルによって増加の傾向が異なっている。これは、回線が混んでいることにより TCP を用いるインタラクティブなアプリケーションの利用をユーザが控えていたことによるものと考えられる。

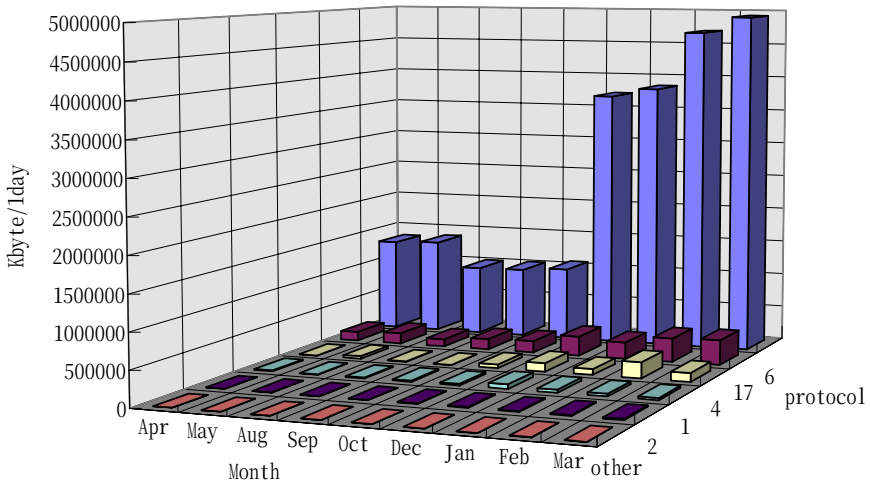

図 2.1: 国外から国内向けのプロトコル別トラフィック量推移 (1 日平均)

2.2　TCP ポート別トラフィック

表 2.2は、TCP ポート別の 1 日あたりのトラフィック量の推移をキロバイト単位で表したものである。SMTP や NNTP のようなアプリケーションによるトラフィックは大きな変化もなく安定しているのに対して、HTTP によるトラフィックを 3 月と 4 月のデータで比較すると、1 年間で、国外から国内向きには約 23 倍、 国内から国外向きには約 7.3 倍と飛躍的に増加している。また、4 月の時点で、国外から国内向きの HTTP のトラフィックは FTP-Data のトラフィックに比べて 10 分の 1 以下であったのに対して、3 月のデータでは、約 3 分の 2 程度にまで増加している。FTP-Data 自体のトラフィックも延びていることから考えると、情報の入手手段が FTP から WWW に変わったというわけではなく、むしろ WWW の出現によって新しい種類の情報の流通が生まれていると言ってよいだろう。また国内から国外への HTTP のトラフィックも月によっては FTP-Data を越える月もあり、国

外から国内のトラフィックに比べて、より FTP-Data とのトラフィック的に見た差が少くなっている。

図 2.3、図 2.4は、表 2.2をグラフ化したものである。FTP-Data と HTTP のトラフィックが大半を占めていることが分かる。

2.3　UDP ポート別トラフィック

表 2.3は、UDP ポート別の 1 日あたりのトラフィック量の推移をキロバイト単位で表したものである。また、図 2.5、図 2.6はそれをグラフ化したものである。

UDP のトラフィックではどちらの方向に関しても DNS によるトラフィックが圧倒的に多い。その他には ARCHIE などのトラフィックもコンスタントに見られる。

2.4 WIDE 国際線の帯域増加によるトラフィックの検証

1994 年 12 月 5 日に WIDE 国際線は，192Kbps から 1.5Mbps に増加された．[1] 帯域増加前は，WIDE 国際線が国外との通信においてボトルネックリンクとなっていた．図 2.7は，海外から国内に入るトラフィックを帯域増加の数日前から数日後までの 1 日ごとの 1 秒あたりに流れるトラフィック量を示している．

帯域増加前の 12 月 4 日までは，回線の最大スループットである 192Kbps に近いトラフィックが流れていた．12 月 5 日の帯域の増加とともに，急激にトラフィックは増加した．図 2.8と図 2.9は、国外から国内へ、WIDE バックボーンを構成する各リンクに流れるトラフィックを示したものである。図内の太字の数字は各リンク上を 1 秒あたり流れるトラフィック量 (Kbps) を表し、細字の数字は各リンクの帯域幅を表している。

図 2.8は、帯域増加前である 199411 月 24 日から 30 日までのトラフィックの流れを示し、図 2.9は、帯域増加後である 1994 年 12 月 7 日から 13 日までの 1 週間のトラフィックの流れを示している。帯域増加による WIDE 国際線のトラフィック量の増加は、WIDE バックボーン上の各リンクに平均的に分散され増加している。

帯域増加によってスループットのような通信サービスが大幅に改善されたことはもちろん、RTT のようなサービスにも大きく影響を与えた。図 2.11、図 2.12は、帯域が増加される前の 1994 年 12 月 1、2 日、帯域が増加された後の 12 月 7、8 日における RTT の分布を示したものである。この RTT は、図 2.10のような実験環境のもと、jp-tap から NASA のゲートウェイである arc-nas-gw.arc.nasa.gov までの ping により得られたものである。計測は 64byte のパケット長で 1 分に 1 回コマンドを実行した。

図 2.11、2.12の横軸は RTT を示し、縦軸は計測期間中におけるその RTT の頻度を示している。WIDE 国際線が 192Kbps の頃は、RTT が分散しており TCP のようなタイマーを利用した通信プロトコルでは、多くの再送が行なわれる可能性がある。

[1] 物理的な接続は 12 月 3 日に行なわれたが，経路情報は 12 月 5 日に提供された．

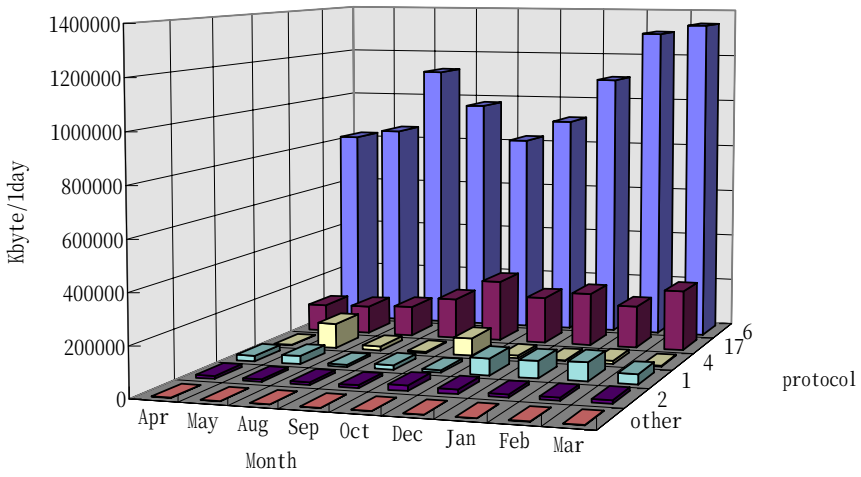

図 2.2: 国内から国外向けのプロトコル別トラフィック量推移 (1 日平均)

表 2.2: TCP ポート別トラフィック

		FTP-Data	HTTP	SMTP	NNTP	Gopher	Telnet	FTP	Other
4 月	IN	440,444	31,192	77,060	52,570	12,759	18,545	5,403	3,242
	OUT	211,598	29,149	61,560	16,232	45,962	11,885	4,891	3,775
5 月	IN	451,152	46,132	59,261	29,917	17,709	42,884	7,012	7,998
	OUT	239,047	37,252	80,534	19,883	11,720	14,038	5,640	3,279
8 月	IN	298,468	79,294	57,148	16,779	10,955	6,484	4,325	3,291
	OUT	141,671	323,118	38,265	21,438	8,676	8,925	4,044	4,953
9 月	IN	282,408	83,267	74,221	12,832	11,205	7,344	4,720	10,770
	OUT	121,571	266,670	41,568	17,240	11,360	9,004	4,372	11,422
10 月	IN	266,512	105,203	80,324	13,198	12,692	7,377	5,114	5,040
	OUT	108,456	191,386	49,370	16,848	15,770	7,986	4,682	5,856
12 月	IN	941,421	487,679	87,960	47,034	33,241	14,004	11,478	23,976
	OUT	183,652	110,565	43,141	27,919	13,644	11,116	7,564	5,682
1 月	IN	975,171	538,700	85,129	43,538	38,059	20,225	11,448	24,301
	OUT	235,543	161,543	39,839	20,363	15,757	12,554	8,473	4,835
2 月	IN	1,113,353	706,410	93,243	50,848	41,659	26,675	13,471	27,152
	OUT	267,862	196,875	61,497	15,962	16,919	18,328	9,155	7,079
3 月	IN	1,205,681	729,194	79,727	44,809	40,948	30,388	14,594	23,831
	OUT	276,824	212,987	40,168	20,333	14,574	16,935	9,175	9,552

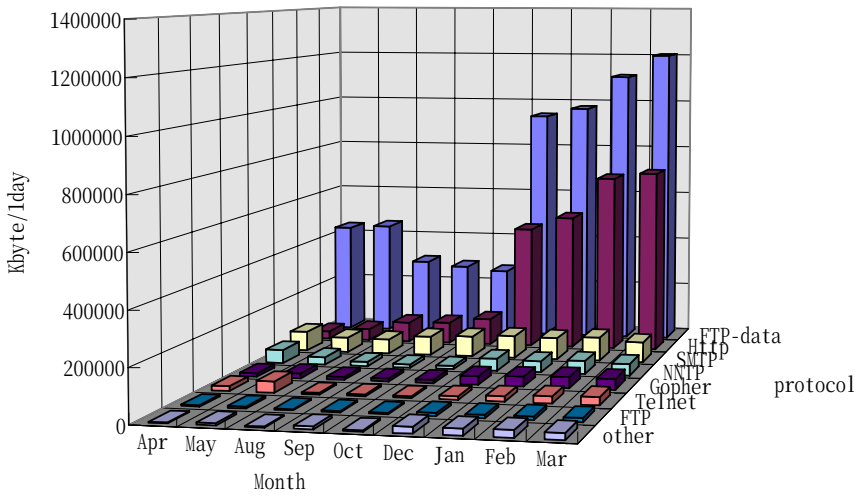

図 2.3: 国外から国内向けの TCP ポート別トラフィック量推移 (1 日平均)

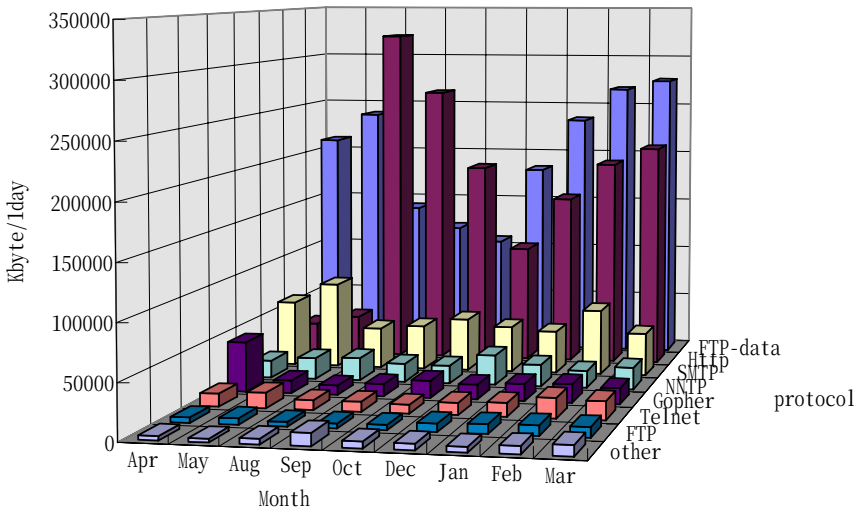

図 2.4: 国内から国外向けの TCP ポート別トラフィック量推移 (1 日平均)

表 2.3: UDP ポート別トラフィック

		DOMAIN	NTP	SNMP	Talk/Phone	ROUTE	ARCHIE	Other
4 月	IN	22,455	0	0	3,511	0	1,468	122
	OU	28,601	0	0	13,006	0	1,696	168
5 月	IN	26,417	0	0	2,460	0	385	177
	OUT	24,575	0	0	13,310	0	514	85
8 月	IN	17,713	0	0	1,206	0	462	228
	OUT	28,769	0	0	12,470	0	623	172
9 月	IN	18,472	0	0	3,068	221	412	736
	OUT	26,897	0	0	14,008	0	619	707
10 月	IN	25,240	0	0	1,912	1,895	762	1,468
	OUT	76,058	0	0	12,291	212	1,013	2,281
12 月	IN	34,659	20,276	5,089	2,917	11,821	642	962
	OUT	39,712	6,756	0	13,656	1,070	723	2,282
1 月	IN	49,185	21,869	11,597	2,766	10,919	0	4,212
	OUT	50,784	7,226	0	11,094	975	615	1,406
2 月	IN	74,533	24,687	2,680	4,117	3,723	0	2,254
	OUT	53,449	6,568	0	0	324	782	2,209
3 月	IN	62,649	28,448	1,420	3,456	0	701	12,722
	OUT	76,917	6,945	0	0	0	851	12,786

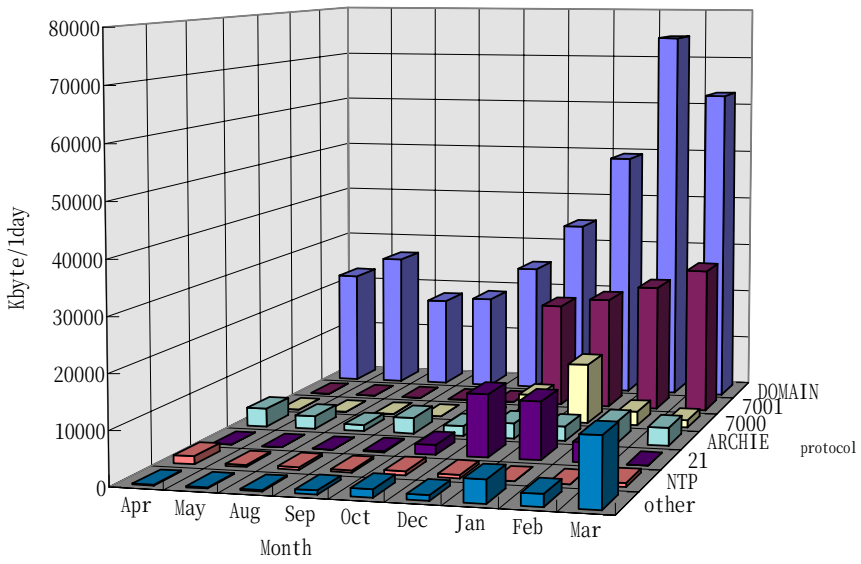

図 2.5: 国外から国内向けの UDP ポート別トラフィック量推移 (1 日平均)

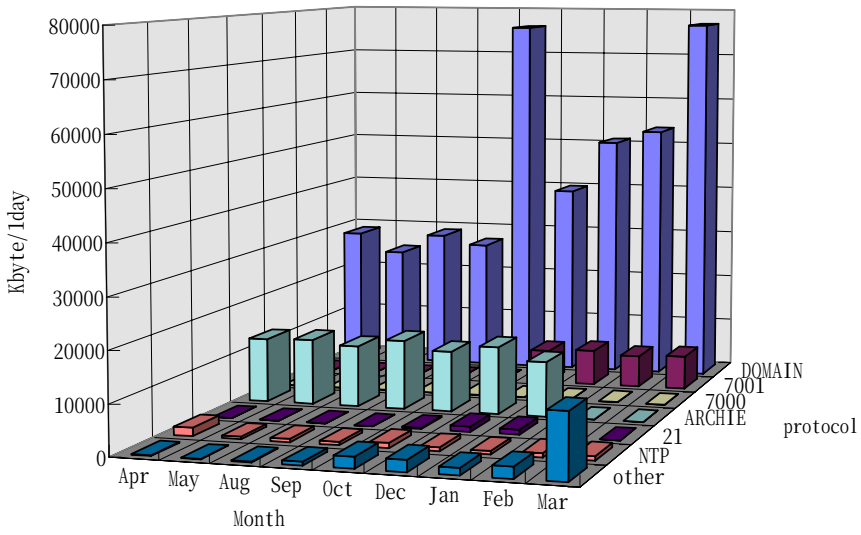

図 2.6: 国内から国外向けの UDP ポート別トラフィック量推移 (1 日平均)

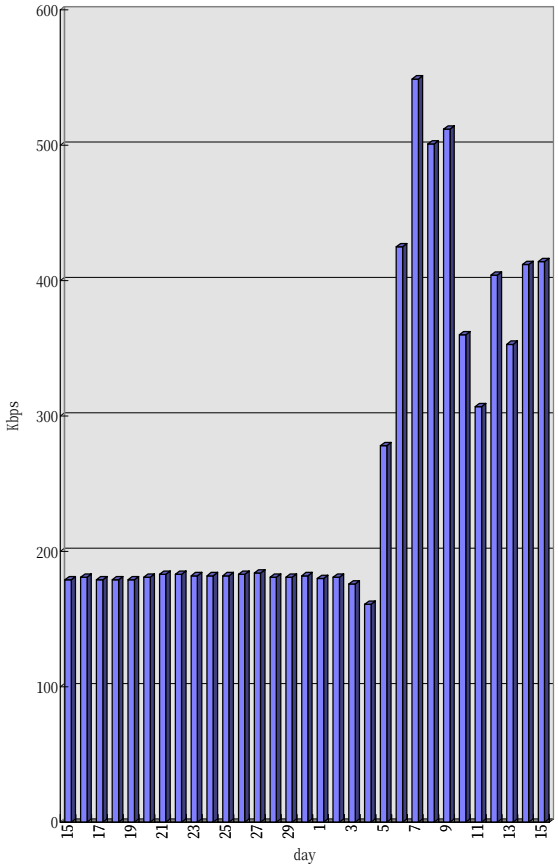

図 2.7: WIDE 国際線の帯域増加前と後のトラフィックの推移

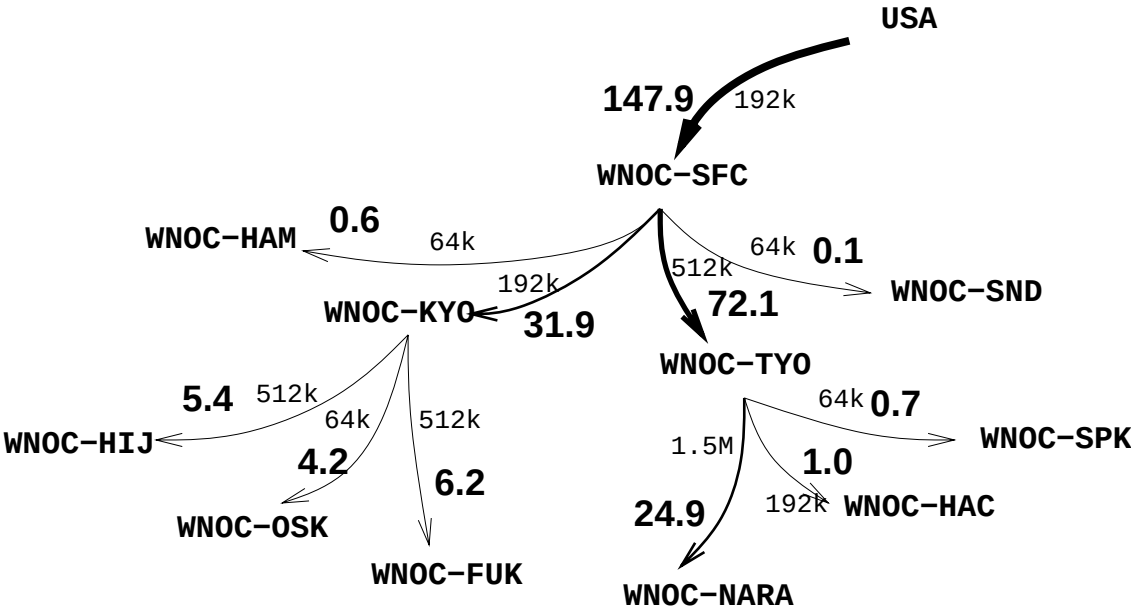

図 2.8: 国際線変更前の WIDE バックボーン上のトラフィックの流れ

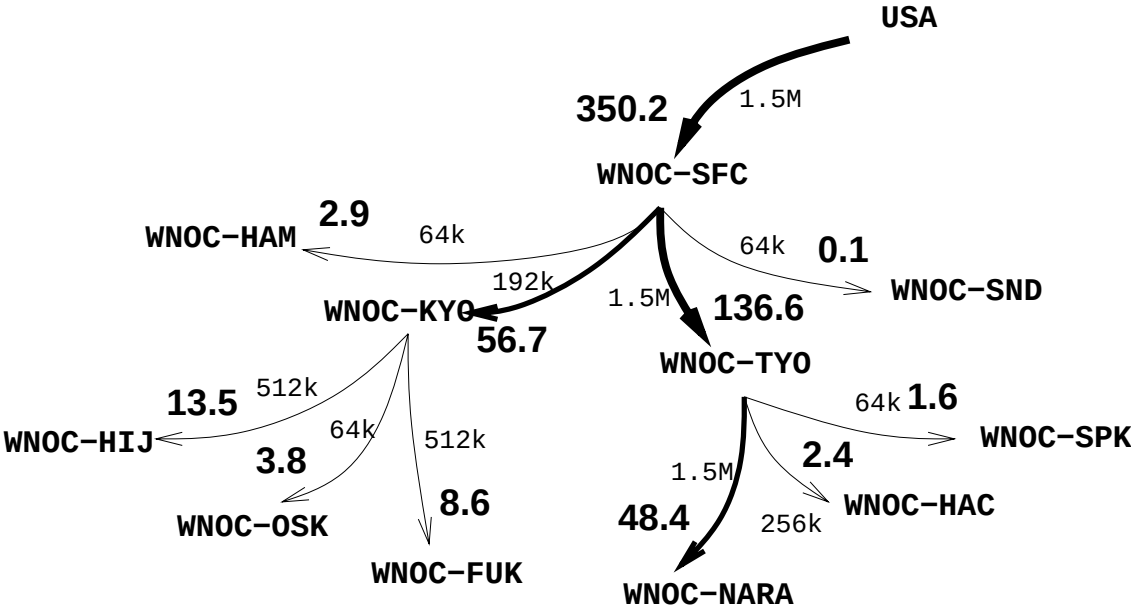

図 2.9: 国際線変更後の WIDE バックボーン上のトラフィックの流れ

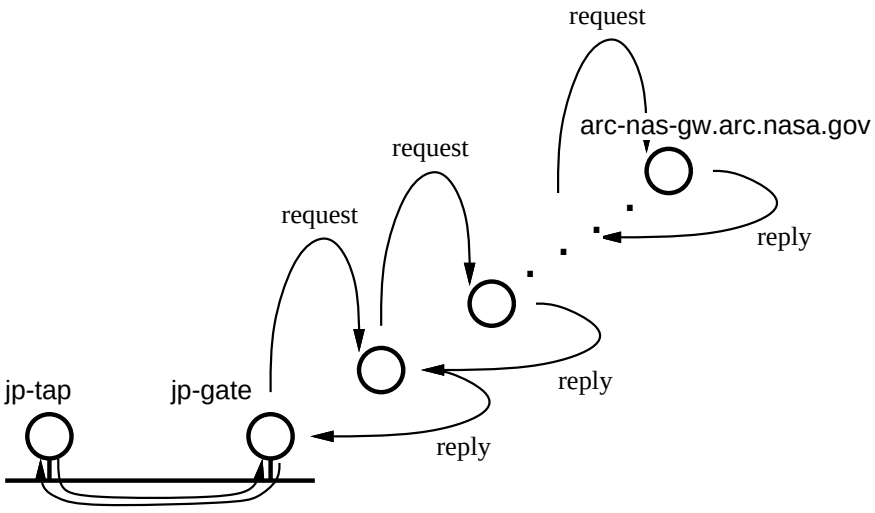
request
arc-nas-gw.arc.nasa.gov
request
request
reply
reply
jp-tap
jp-gate
reply

図 2.10: ping

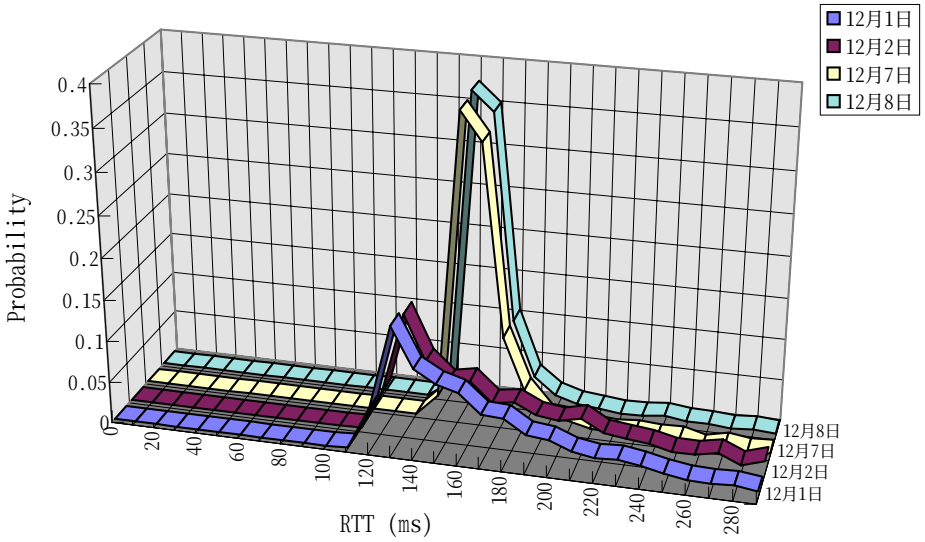

図 2.11: WIDE 国際線での RTT の分布 (part1)

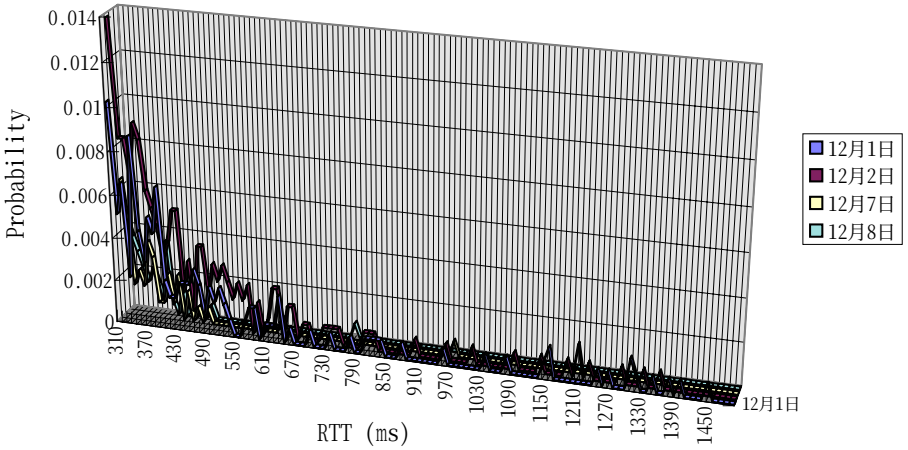

図 2.12: WIDE 国際線での RTT の分布 (part2)

第 3 章

WNOC-TYO と WNOC-SFC の間のトラフィック

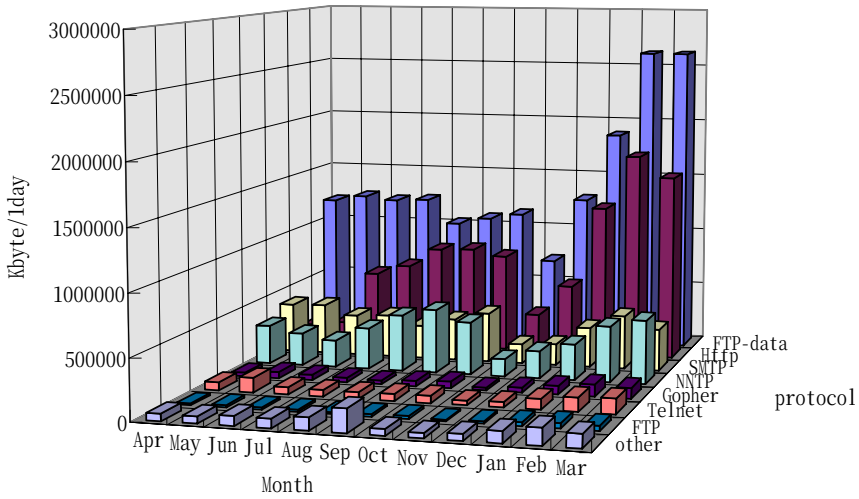

図 3.1: TCP ポート別トラフィック量推移 (1 日平均)

図 3.1は、WNOC-TYO と WNOC-SFC の間の TCP ポート別の 1 日あたりのトラフィック量をキロバイト単位でグラフ化したものである。

トラフィックの傾向としては国際線のトラフィックと同様で、SMTP、NNTP のトラフィックはおおむね安定しているが、FTP-Data、HTTP などのトラフィック量は増加の傾向にある。とくにこれらのトラフィックは国際線のアップグレードに伴い確実に増加していることがわかる。

図 3.2は、WNOC-TYO と WNOC-SFC の間の UDP ポート別の 1 日あたりのトラフィック量をキロバイト単位でグラフ化したものである。こちらもトラフィックの傾向は国際ト

ラフィックに類似しており、DNS によるトラフィックが圧倒的となっている。しかし、国際線のアップグレードによるトラフィックの変化としては、TCP の場合程あきらかではない。

RIP によるトラフィックが 10 月をピークに徐々に減少して来ている。これは、WIDE バックボーン内での経路制御が RIP によるものから OSPF によるものへと移行されていることを反映している。

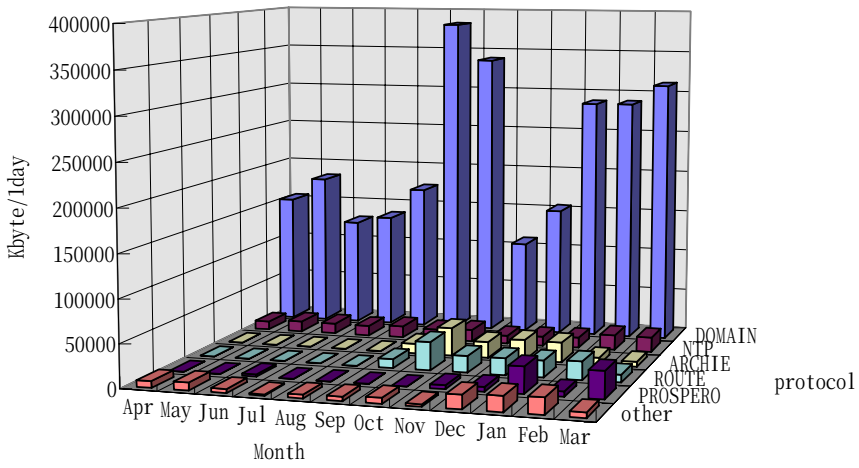

図 3.2: UDP ポート別トラフィック量推移 (1 日平均)

1994 年度は NNStat によるトラフィックデータ収集に加えて、IPANeMa による統計解析も開始した。以下の章ではこちらの方法による統計収集に関して報告する。これにより、従来行なっていたものとは違う観点からの統計処理が可能になっている。

第 4 章

WNOC-TYO モニター報告

4.1 はじめに

昨年度報告した、ネットワークモニター情報の自動統計機構によって、WNOC-TYO のモニターを行なった。1995 年 1 月から本格的に運用を開始したので、その報告を行なう。このネットワークモニター情報の自動統計プログラムは、IPA からフリーソフトウェアとしてリリースされている。 (ftp://ftp.mgt.ipa.go.jp/pub/IPANeMa)

また、WNOC-TYO モニター報告は、www.wide.ad.jp 上で公開されている。

4.2 1995 年 1 月 - 3 月 各月ごとの統計

表 4.1: Monthly Figures by upper protocol (1 月)

	packets/sec	bytes/sec
TOTAL	735.69	178963.77
OTHER	11.76	4261.19
1:ICMP	28.46	2163.84
6:TCP	554.33	147776.55
17:UDP	81.07	12509.83
89:OSPFIGP	5.31	1003.84
4:IP in IP	54.76	11266.48

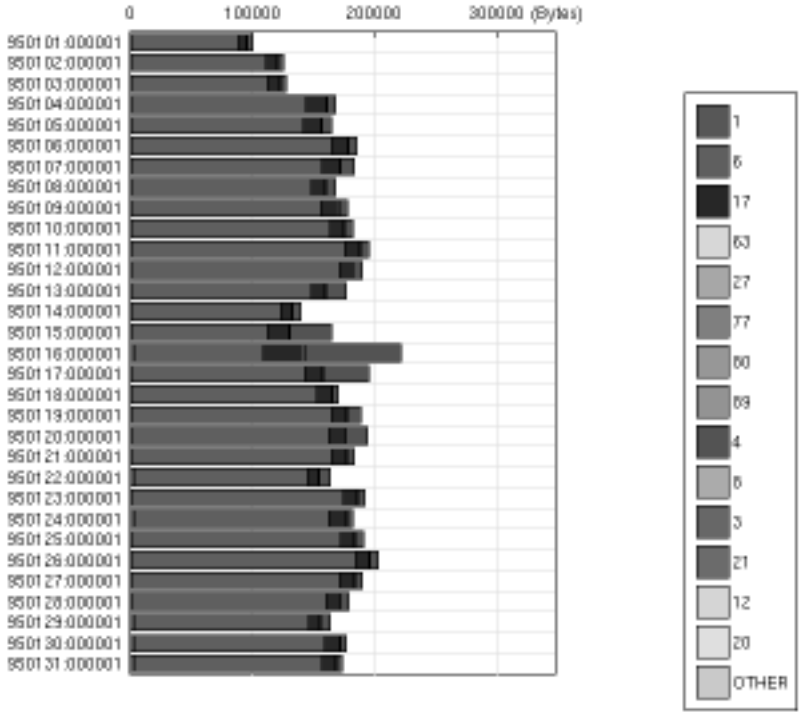

図 4.1: daily mean traffic (bytes/sec) - 1 月

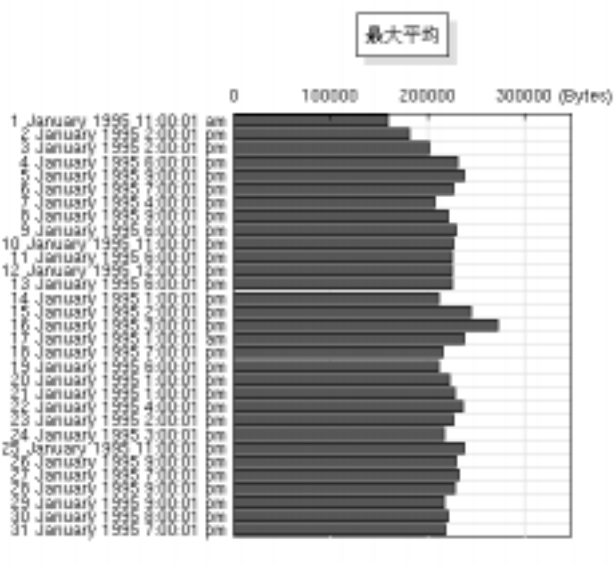

図 4.2: daily max traffic (bytes/sec) - 1 月

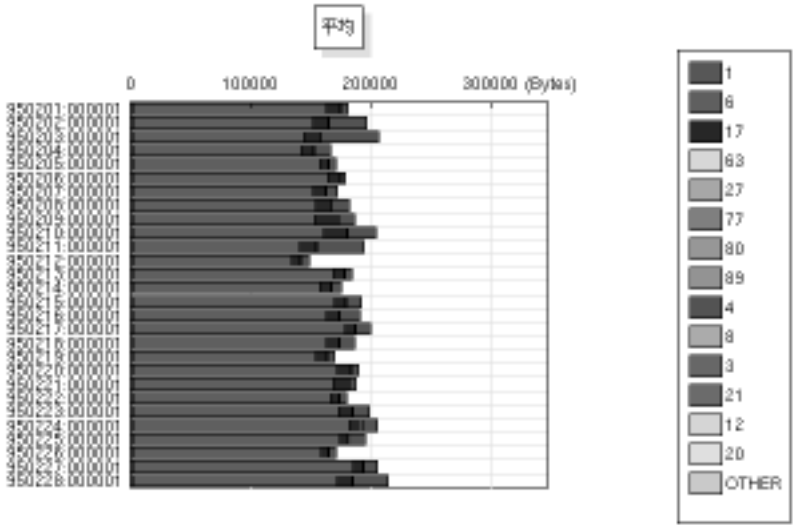

図 4.3: daily mean traffic (bytes/sec) - 2 月

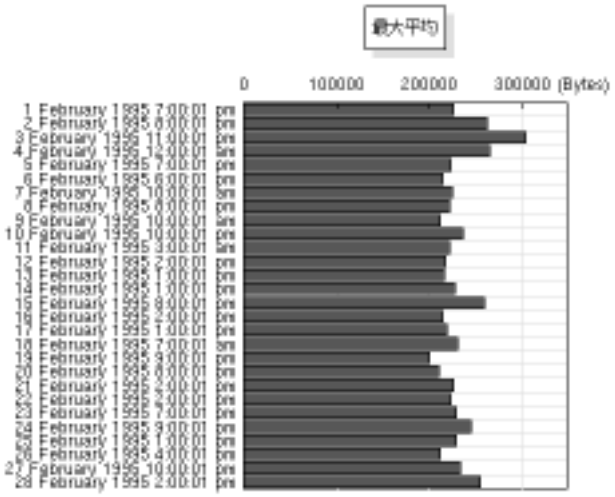

図 4.4: daily max traffic (bytes/sec) - 2 月

表 4.2: Monthly Figures by upper protocol (2 月)

	packets/sec	bytes/sec
TOTAL	786.25	190947.66
OTHER	10.54	3745.67
1:ICMP	32.71	2409.04
6:TCP	595.86	159637.38
17:UDP	75.66	10470.79
89:OSPFIGP	5.33	1038.87
4:IP in IP	66.15	13693.41
3: GGP	0.00	0.00

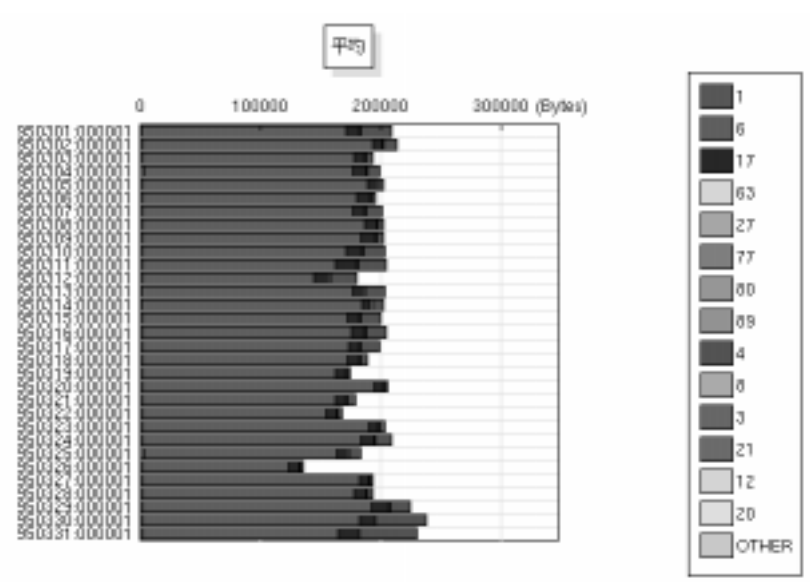

図 4.5: daily mean traffic (bytes/sec) - 3 月

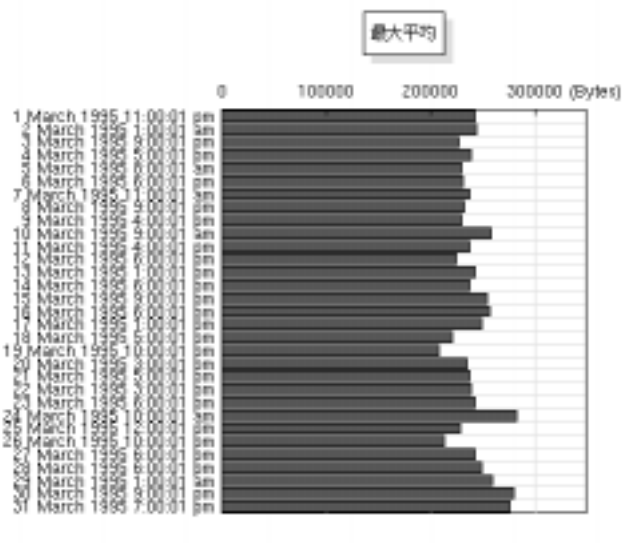

図 4.6: daily max traffic (bytes/sec) - 3 月

表 4.3: Monthly Figures by upper protocol (3 月)

	packets/sec	bytes/sec
TOTAL	791.08	202867.70
OTHER	12.22	4617.81
1:ICMP	28.98	2108.18
6:TCP	623.91	172286.97
17:UDP	68.96	10289.45
89:OSPFIGP	5.27	1188.36
4:IP in IP	51.73	12407.25
3: GGP	0.00	0.00

4.3 ３ケ月分の統計

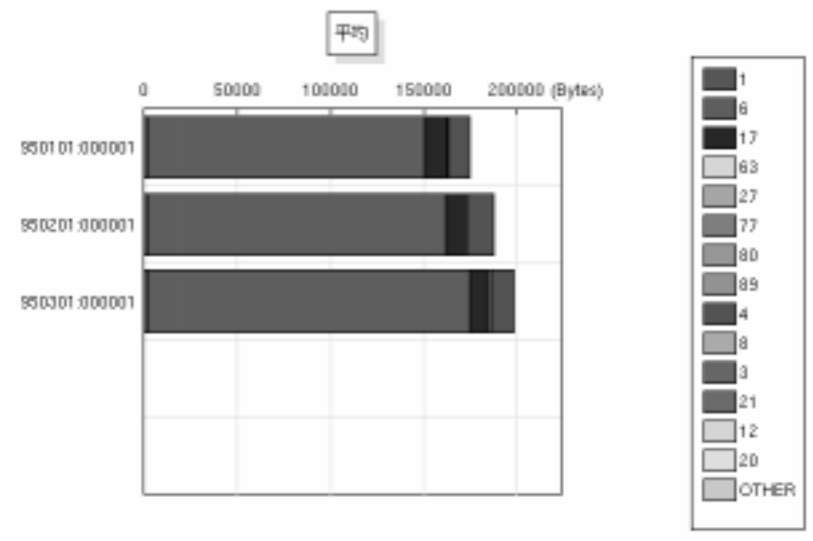

図 4.7: Monthly mean traffic (bytes/sec) 1 月- 3 月

表 4.4: Figures by upper protocol (3 ケ月分平均)

	bytes/sec
TOTAL	190925.66
OTHER	4223.64
1:ICMP	2220.95
6:TCP	159909.05
17:UDP	11110.66
89:OSPFIGP	1078.30
4:IP in IP	12414.46
3: GGP	0.00

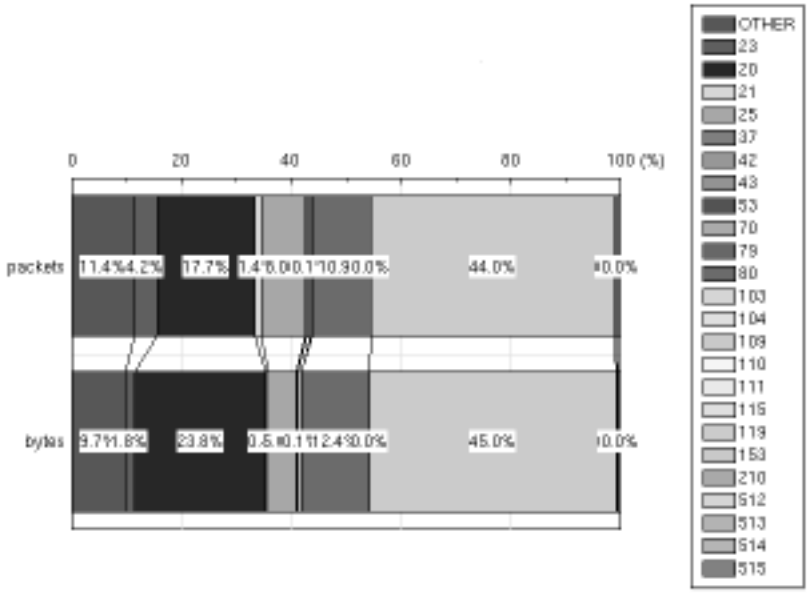

図 4.8: TCP port ratio

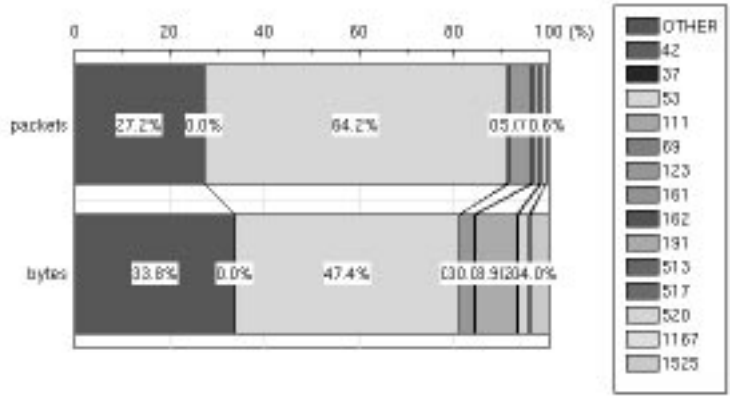

図 4.9: UDP port ratio

表 4.5: Figures by TCP port (3 ケ月分平均)

	bytes/sec
OTHER	15486.13
23:telnet	2807.16
20:ftp-data	38092.02
21:ftp	687.66
25:smtp	8067.36
37:time	0.18
42:name	0.05
43:whois	20.15
53:domain	463.39
70:gopher	1086.23
79:finger	79.95
80:http	19790.09
103:x400	0.14
104:x400-snd	0.11
109:pop2	0.03
110:pop3	14.61
111:sunrpc	0.04
115:sftp	0.02
119:nntp	71803.84
153:sgmp	0.01
210:z39.50	7.66
512:exec	0.05
513:rlogin	532.93
514:shell	809.41
515:printer	3.84

表 4.6: Figures by UDP port (3 ケ月分平均)

	bytes/sec
OTHER	3760.63
42:name	0.00
37:time	0.08
53:domain	5249.26
111:sunrpc	4.53
69:tftp	0.34
123:ntp	339.36
161:snmp	20.27
162:snmp-trap	0.27
191:PROSPERO	985.16
513:who	16.29
517:talk	16.13
520:route	260.39
1167:phone	12.94
1525:archie	444.11

第 5 章

まとめと今後の課題

本報告では 1994 年度に収集されたトラフィックデータの解析結果に基づき WIDE インターネット上のトラフィックに付いての考察を行なった。とくに、WIDE の国際回線のアップグレードの前後でのトラフィックの比較も行なった。

また、従来の NNStat によるトラフィック収集に加えて、IPANeMa の一部であるスタットデーモン／ロギングデーモンを用いた統計収集も一部で開始した。

今後は新しい統計収集方法をバックボーン全体に広げていく。またバックボーン回線が高速になるにしたがい全てのトラフィックを収集して解析すると言う方法が、ルータに与える負荷の問題などから現実的ではなくなりつつある。そろそろ NSFNET バックボーンで行なわれていたような、サンプリングによる統計処理を行なう手法を確立していく必要がある。

また、試験的に WWW によるトラフィックデータの公開も行なった[1]。今後はこの様な情報公開を自動的に行なう手法に付いて考察して行く予定である。

[1] http://www.wide.ad.jp/wg/stat/nnstat/index.html