第 9 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 や IPANeMa 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た。また、得られた解析結果をビジュアライズする手法についても検討を行なった。

本報告では、以下の各項目に関して報告を行なう。

1. NNStat による国際線のトラフィック収集と解析
2. IPANeMa による東京藤沢間のバックボーントラフィック収集と解析
3. WWW を利用した、トラフィックデータのビジュアライゼーション

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	5,211,502	406,104	1,210,431	20,912	12,507	898	6,862,354	41.37%
	OUT	1,421,123	249,653	46,770	12,854	18,093	1,353	1,749,846	10.55%
5 月	IN	6,806,311	466,273	1,159,987	28,686	17,510	1,233	8,480,000	51.12%
	OUT	1,739,285	240,932	27,973	51,544	18,134	1,385	2,079,253	12.53%
6 月	IN	7,171,501	945,969	1,168,602	72,001	18,301	4,222	9,380,596	56.55%
	OUT	2,027,934	728,534	18,679	38,366	17,017	3,572	2,834,102	17.08%
7 月	IN	8,442,874	484,102	1,612,475	31,812	12,055	811	10,584,129	63.80%
	OUT	2,133,091	403,206	21,785	27,529	12,463	1,125	2,599,199	15.67%
8 月	IN	8,636,512	489,419	2,122	31,149	1,182	666	9,161,050	55.22%
	OUT	2,371,330	383,605	10,952	23,880	1,867	940	2,792,574	16.83%
9 月	IN	9,952,351	631,707	906	31,500	666	439	10,617,569	64.00%
	OUT	3,025,837	381,675	86,406	28,153	4,141	853	3,527,065	21.26%
10 月	IN	11,709,147	650,571	17,616	37,811	2,432	347	12,417,924	74.86%
	OUT	3,721,421	469,327	163,624	29,246	5,329	592	4,389,539	26.46%
11 月	IN	11,878,548	983,544	2,415	74,029	904	541	12,939,981	78.00%
	OUT	3,916,520	784,691	3,838	27,598	2,393	919	4,735,959	28.55%
12 月	IN	11,029,129	771,516	236	41,103	539	414	11,842,937	71.39%
	OUT	3,238,480	678,175	1,422	27,336	1,565	681	3,947,659	23.80%
1 月	IN	10,819,085	1,201,289	1,085	39,956	554	585	12,062,554	72.72%
	OUT	4,134,365	639,273	702	26,285	868	1,027	4,802,520	28.95%
2 月	IN	13,349,769	855,153	337	37,523	434	473	14,243,689	85.86%
	OUT	3,979,636	566,353	898	22,354	1,537	816	4,571,594	27.56%
3 月	IN	10,649,895	707,878	1,446	30,724	235	888	11,391,066	68.67%
	OUT	3,204,876	712,946	1,742	23,517	547	1,584	3,945,212	23.78%

国際線のトラフィックは、WIDE 藤沢 NOC と WIDE カリフォルニア NOC 間の 1.5Mbps の国際回線上を通るトラフィックを NNStat を用いて計測した。

表 2.1は、各 IP プロトコルについて、月毎のトラフィック量を 1 日当たりで平均したものである（単位：キロバイト）。各月ごとに、IN の行は国外から国内に向かうトラフィック、OUT の行は国内から国外に向かうトラフィックをそれぞれ表している。回線利用率は、1.5Mbps の国際回線を用いて 1 日に送信できる総トラフィック量に対する、各月の 1 日平均のトラフィック量の割合を求めることにより算出した。図 2.1、図 2.2は、表 2.1をもとに、国外から国内に向かう平均トラフィック量の推移、国内から国外に向かう平均トラフィック量の推移をそれぞれグラフ化したものである。

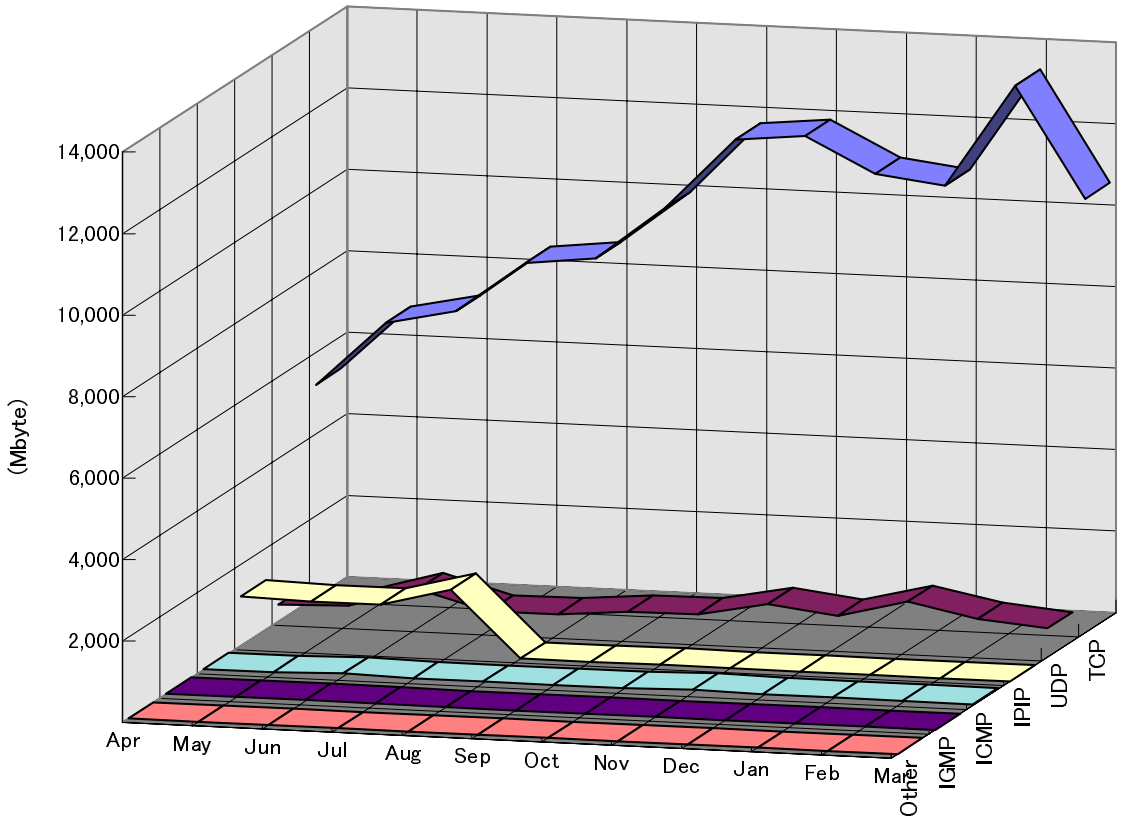

図 2.1: 国外から国内向けのプロトコル別トラフィック量推移 (1 日平均)

一年間で月の平均トラフィックが双方向とも約 2 倍に伸びている。また回線利用率をみると、国外から国内に向かう方向では、最も利用率が大きい月は 2 月で 85.86%、国内から国外に向かう方向では、最も利用率が大きい月は 1 月で 28.95% となっている。利用率の算出に用いたのが 1 日平均のトラフィックであることを考えると、非常に高い利用率であるとみなすことができる。

IP/IP と IGMP は、Mbone に関連するトラフィックである。双方とも 8 月を境に減少し

ているが、これは IMnet の国際線経由で日本と海外との Mbone のリンクをたちあげたことに起因するものであり、Mbone のトラフィック自体が減少しているわけではない。

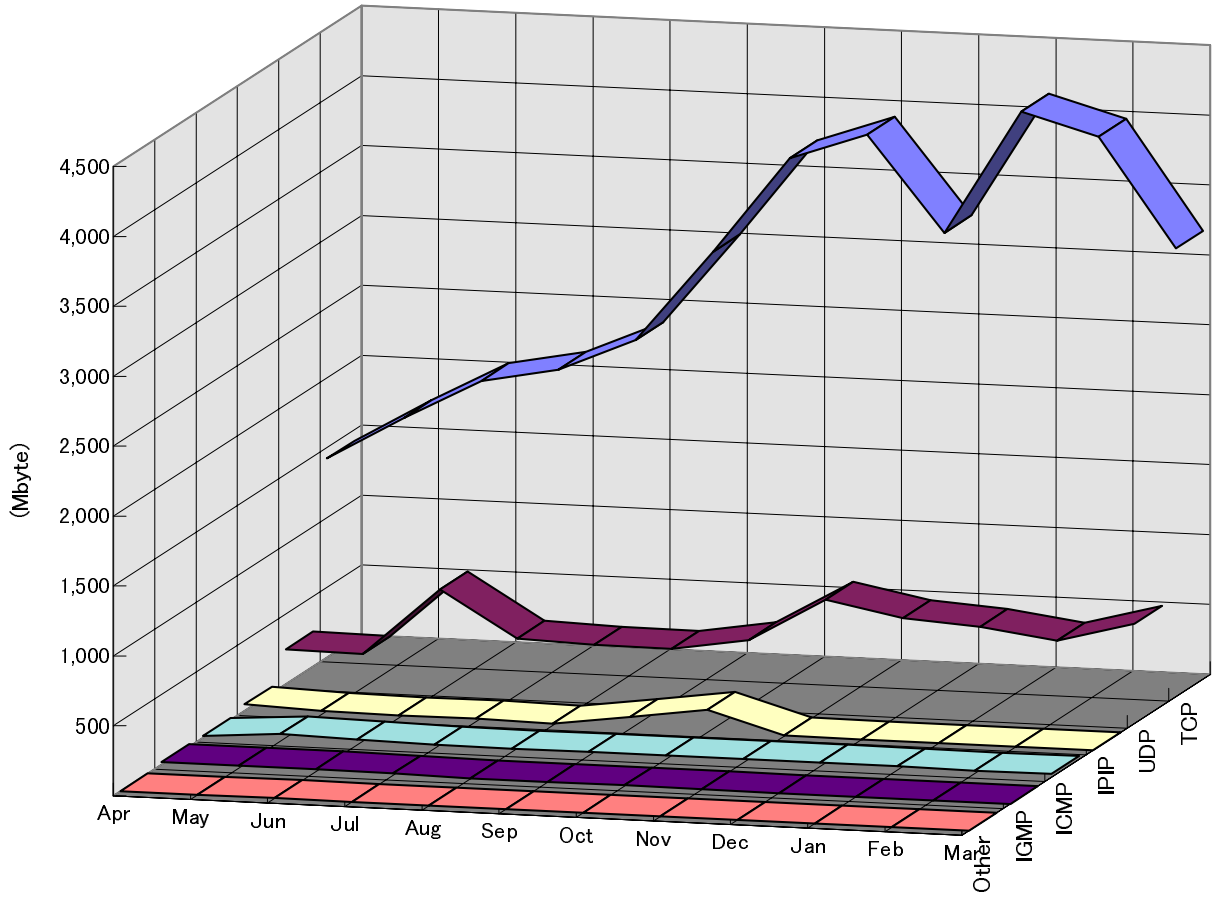

図 2.2: 国内から国外向けのプロトコル別トラフィック量推移 (1 日平均)

2.2　TCP ポート別トラフィック

表 2.2: TCP ポート別トラフィック

		HTTP	FTP-Data	SMTP	NNTP	Gopher	Telnet	FTP	Other
4 月	IN	1,796,660	2,253,999	151,571	81,722	88,660	73,563	27,347	737,980
	OUT	525,712	521,534	72,154	32,568	29,813	29,736	18,792	190,814
5 月	IN	2,801,729	2,559,118	188,612	113,823	100,187	70,527	31,069	941,246
	OUT	761,412	534,663	80,261	43,271	26,486	28,128	20,196	244,868
6 月	IN	2,421,174	2,069,909	154,286	70,902	76,599	46,523	25,332	2,306,776
	OUT	744,698	425,206	101,984	33,296	29,679	22,990	16,068	654,013
7 月	IN	4,134,875	2,262,550	185,118	68,794	90,685	77,036	31,849	1,591,967
	OUT	1,128,949	451,930	95,047	51,541	21,569	29,084	20,652	334,319
8 月	IN	4,441,338	2,550,801	151,893	71,007	67,159	40,375	28,714	1,285,225
	OUT	1,252,305	475,111	88,965	35,470	14,621	30,652	19,839	454,367
9 月	IN	5,139,097	2,530,361	175,309	94,275	73,359	49,928	36,010	1,854,012
	OUT	1,527,064	612,554	128,700	44,829	17,842	31,185	26,536	637,127
10 月	IN	6,570,520	3,089,065	229,048	104,000	63,141	64,722	42,970	1,545,681
	OUT	1,668,743	591,702	130,326	50,485	17,232	35,581	29,901	1,197,451
11 月	IN	6,967,755	2,436,392	237,762	181,084	70,403	53,167	38,763	1,893,222
	OUT	2,002,232	519,880	146,507	60,363	15,908	29,672	27,647	1,114,311
12 月	IN	6,709,993	1,970,148	204,757	87,705	51,868	51,365	32,629	1,920,664
	OUT	1,822,423	405,154	129,570	59,105	15,666	20,876	23,062	762,624
1 月	IN	6,189,058	1,679,929	210,830	98,827	45,905	42,469	33,446	2,518,621
	OUT	2,127,643	501,595	150,067	73,171	19,854	21,075	27,281	1,213,679
2 月	IN	8,418,227	2,267,805	329,594	118,355	39,240	37,176	39,777	2,099,595
	OUT	2,271,077	464,527	207,429	77,944	13,577	22,641	27,690	894,751
3 月	IN	6,438,887	2,157,377	198,021	92,379	27,824	37,041	28,157	1,670,209
	OUT	1,834,345	382,192	178,990	65,285	9,958	24,185	22,201	687,720

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。HTTP によるトラフィックは、1995 年 4 月の時点でのトラフィック量と、ピークにあたる 1996 年 2 月の時点でのトラフィック量を比較すると、1 年間で国外から国内向きには約 4.7 倍、国内から国外向きには約 4.3 倍とかなりの増加傾向を示している。また、1995 年 5 月を境に HTTP のトラフィックはそれまで最も多かった FTP-Data のトラフィックを追い抜いている。その後も HTTP のトラフィックはほぼ単調に増加しているのに対して、FTP-Data のトラフィックは頭打ちの傾向を示している。これは情報の取得や発信手段が FTP から WWW へと変化しようとしていることを示していると言えよう。

図 2.3、図 2.4は、表 2.2をグラフ化したものである。HTTP のトラフィックがかなりの増加傾向を示していることがわかる。また、Others に分類されるトラフィックが双方向とも

かなりの量を示すようになってきており、これまで特定のアプリケーションに集中していたインターネットの利用が多様化してきていることを示していると考えられる。

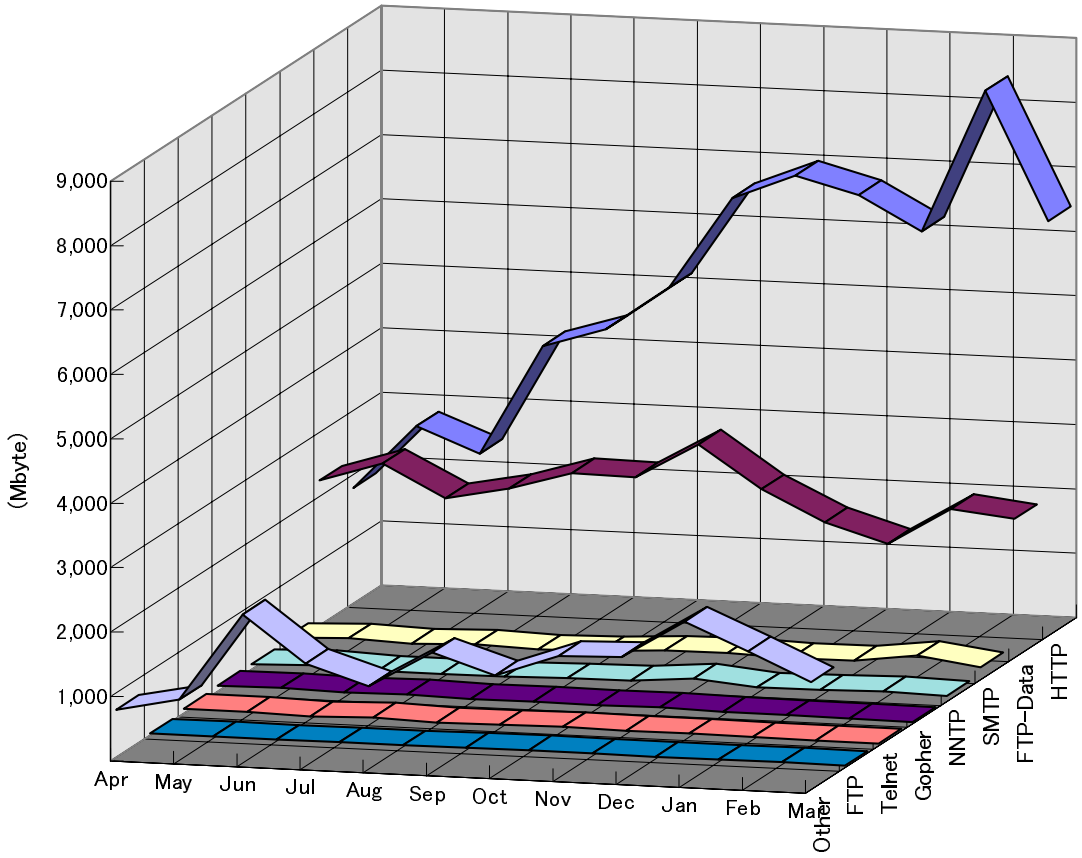

図 2.3: 国外から国内向けの TCP ポート別トラフィック量推移 (1 日平均)

2.3　UDP ポート別トラフィック

表 2.3: UDP ポート別トラフィック

		DNS	AFS	ARCHIE	SNMP	Talk/Phone	NTP	Other
4 月	IN	151,522	119,953	4,290	289	257	1,472	8,368
	OUT	113,213	29,779	40,511	4,031	1,028	2,130	29,182
5 月	IN	158,819	89,424	5,311	183	443	749	121,920
	OUT	125,792	24,350	44,600	2,186	717	2,286	16,651
6 月	IN	301,339	49,951	3,417	189	219	4,899	536,004
	OUT	281,205	22,563	523	25,703	23,005	6,184	346,788
7 月	IN	228,952	68,521	6,141	201	759	1,167	109,840
	OUT	208,641	21,453	30,715	26,233	10,708	1,922	82,081
8 月	IN	183,857	46,212	3,620	558	97	478	208,385
	OUT	171,438	7,992	36,221	53,670	1,465	1,916	102,911
9 月	IN	242,537	110,630	4,168	12,411	257	537	150,537
	OUT	210,653	32,896	24,439	41,199	873	2,452	36,267
10 月	IN	254,056	120,434	4,492	308	664	546	149,637
	OUT	282,997	40,183	6,759	117	2,132	2,217	94,739
11 月	IN	574,915	121,472	3,054	693	207	666	161,065
	OUT	533,979	41,344	22,334	549	13,000	1,524	130,617
12 月	IN	450,044	65,664	3,237	776	296	590	185,245
	OUT	417,962	29,478	214	720	588	1,525	198,210
1 月	IN	598,888	86,245	2,034	388	484	529	426,476
	OUT	499,858	33,393	8,053	451	1,030	1,551	61,544
2 月	IN	388,180	94,496	2,492	530	138	808	274,013
	OUT	413,615	18,101	32,218	608	404	2,682	80,624
3 月	IN	419,146	55,642	3,659	66	338	656	172,729
	OUT	592,018	4,804	37,484	26	668	2,919	70,223

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。

どちらの方向に関しても DNS によるトラフィックが相変わらず多いが、TCP の場合と同様に、Other に分類されるトラフィックがかなりの割合を示すようになってきている。特に UDP を用いて画像や音声を送信するアプリケーションがいくつか出現してきたこともOther のトラフィックが増大していることに寄与していると考えられる。これらの新しいアプリケーションのトラフィックの計測をいち早く開始するための手法を考案することが今後必要となってくるだろう。

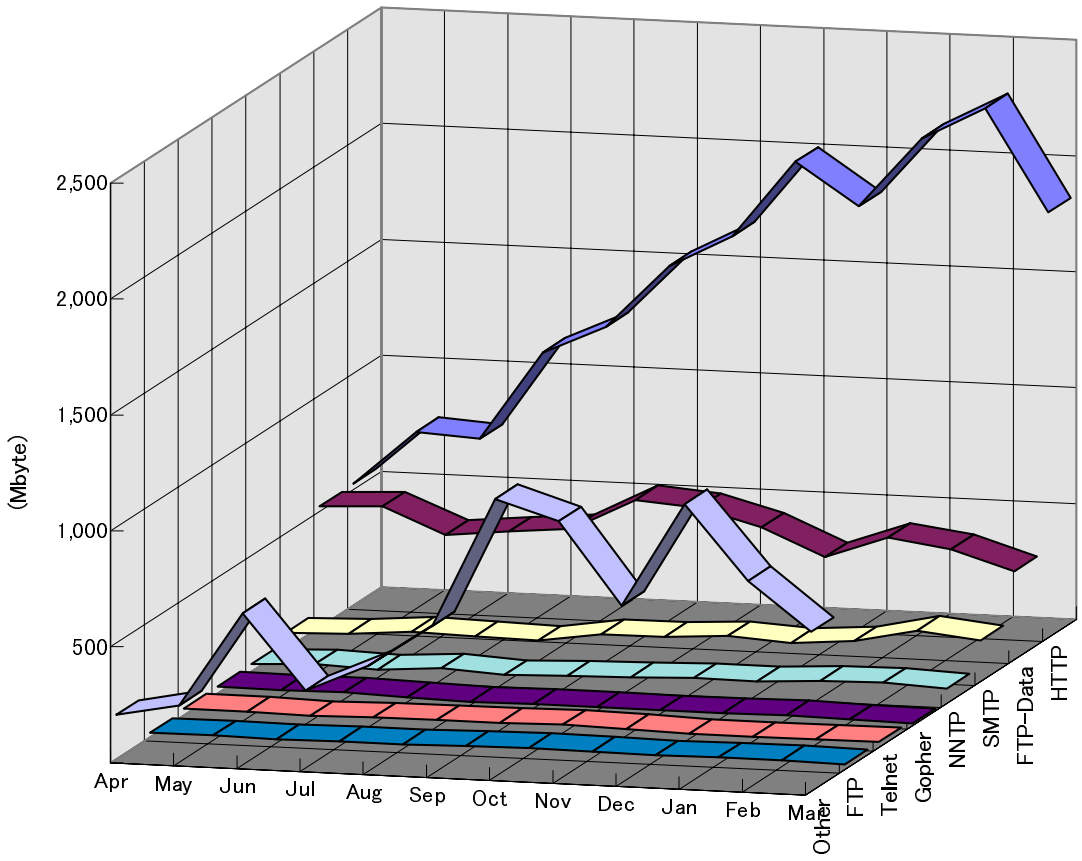

図 2.4: 国内から国外向けの TCP ポート別トラフィック量推移 (1 日平均)

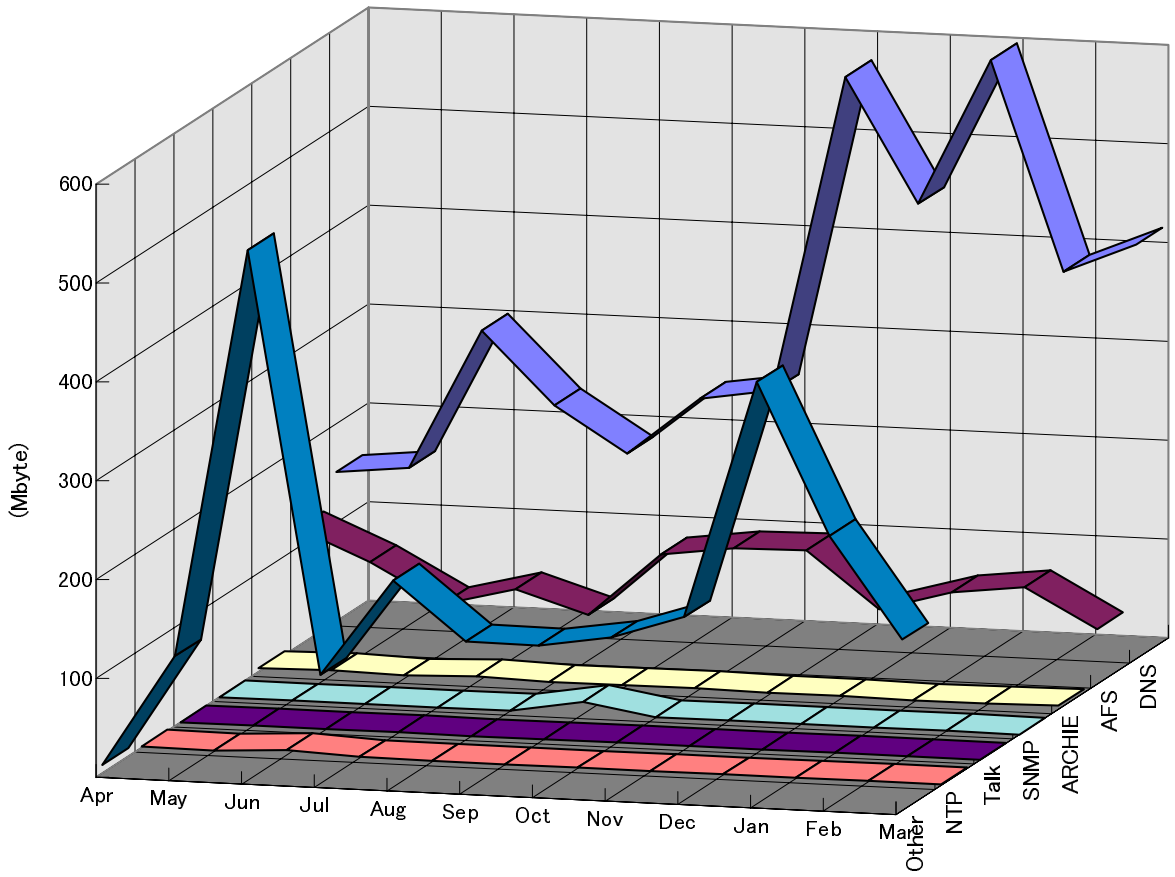

図 2.5: 国外から国内向けの UDP ポート別トラフィック量推移 (1 日平均)

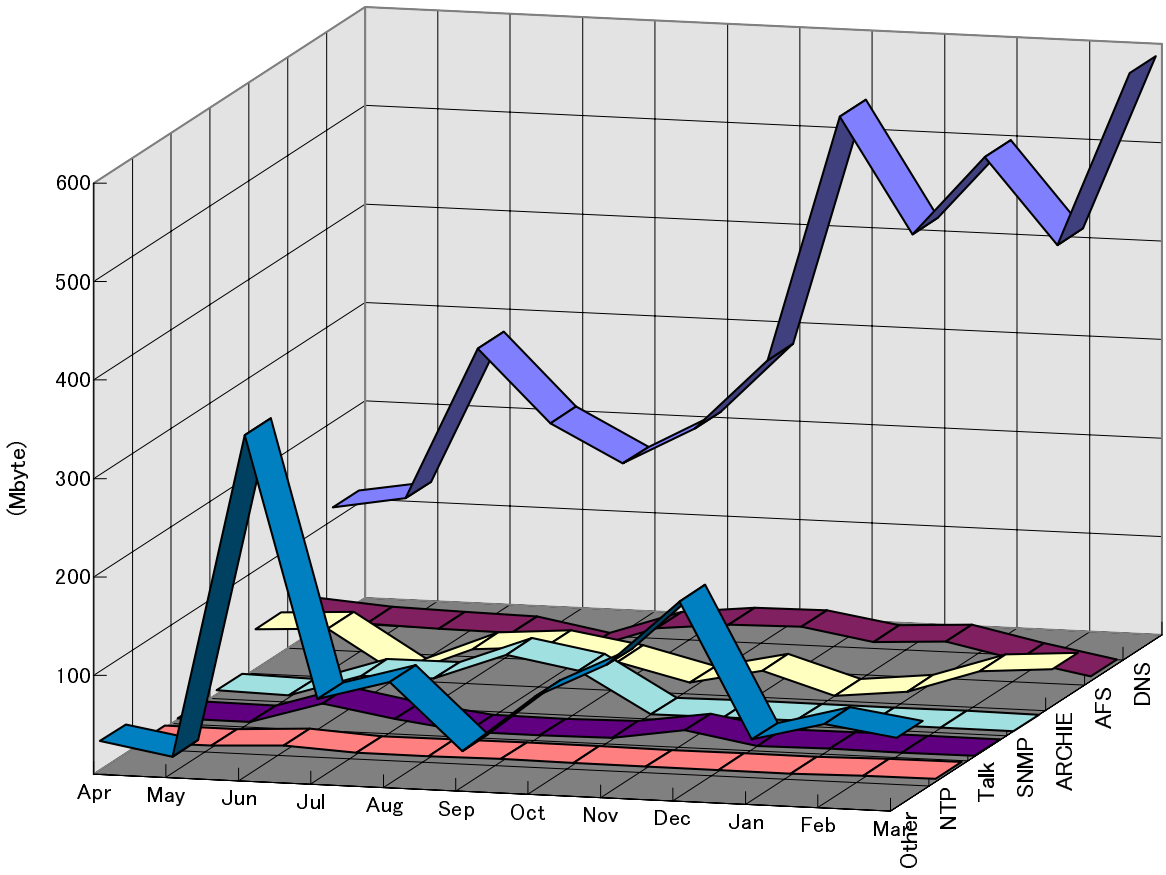

図 2.6: 国内から国外向けの UDP ポート別トラフィック量推移 (1 日平均)

第 3 章

WNOC-TYO モニター報告

3.1 はじめに

1993 年度に報告した、ネットワークモニター情報の自動統計機構によって、1995 年 1 月から 7 月まで WNOC-TYO のモニターを行なった。1995 年 8 月にイーサースイッチが導入されたため、モニター活動は終了した。ここでは、1995 年 1 月から 7 月までのモニター報告を行なう。このネットワークモニタープログラムは、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。

3.2 1995 年 4 月 - 7 月 各月ごとの統計

1995 年 1 月から 3 月までについては、昨年度報告したので、ここでは省略する。まず、IP の上位プロトコルごとに色分けされた 1 日ごとの平均トラフィックのグラフを示す。

上位プロトコル番号	上位プロトコル名
1 :	ICMP
6 :	TCP
17 :	UDP

次に、1 日ごとの最大トラフィックのグラフを示す。このグラフは、１時間ごとの平均トラフィックが最大の値、つまり、24 個の平均トラフィックのうち最大の値と、その時間帯を示している。たとえば、”9 May 1995 6:00:01 am” は、5 月 9 日 6:00 から 7:00 までの平均トラフィックが、その日の最大であることを意味している。

3.3 1995 年 1 月 - 7 月 7 ケ月分の統計

６月は２０日以降、７月は２８日まで、データがとれなかった。特に、７月は３日分の統計でしかない。

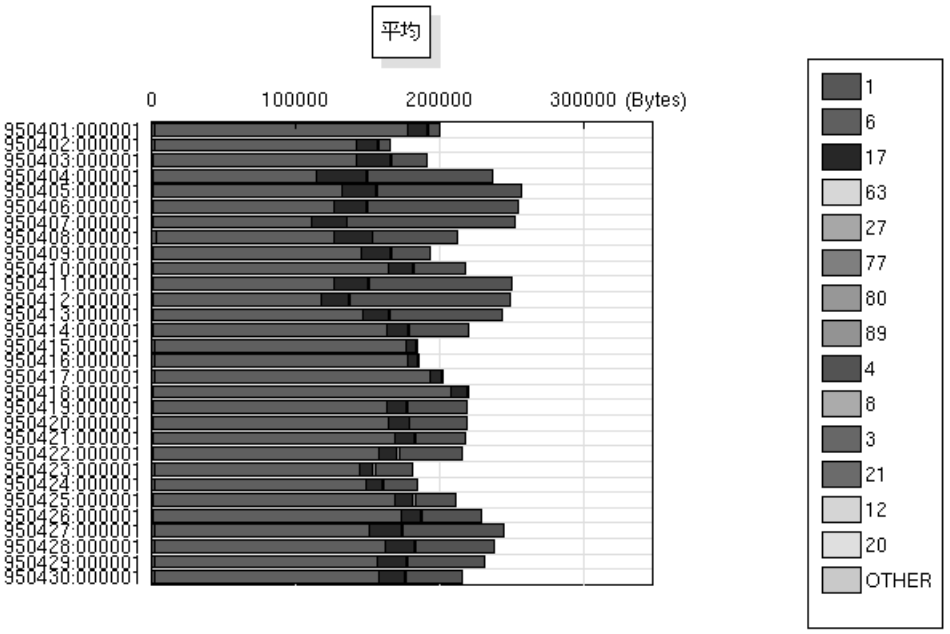

図 3.1: daily mean traffic (bytes/sec) - 4 月

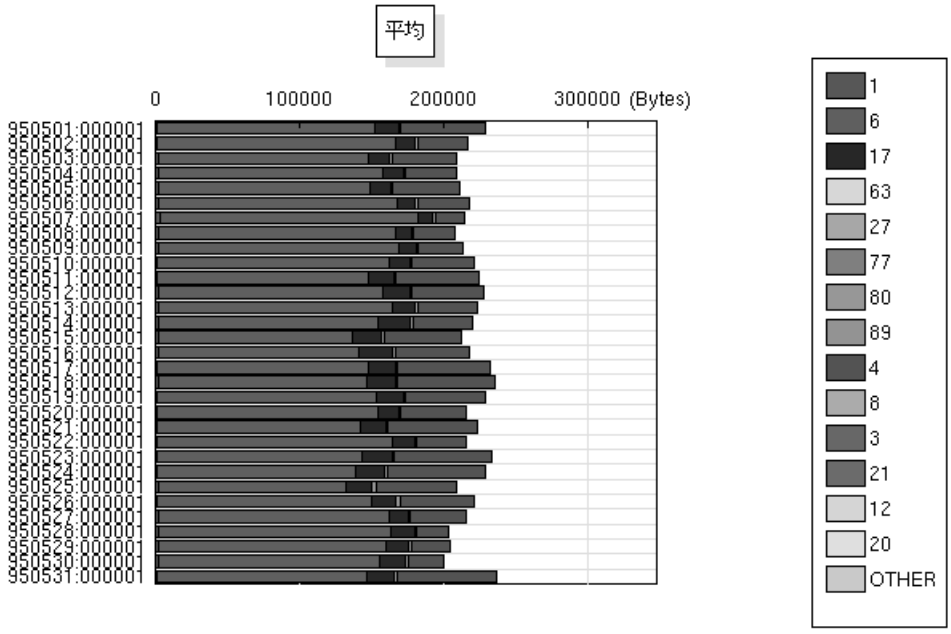

図 3.2: daily mean traffic (bytes/sec) - 5 月

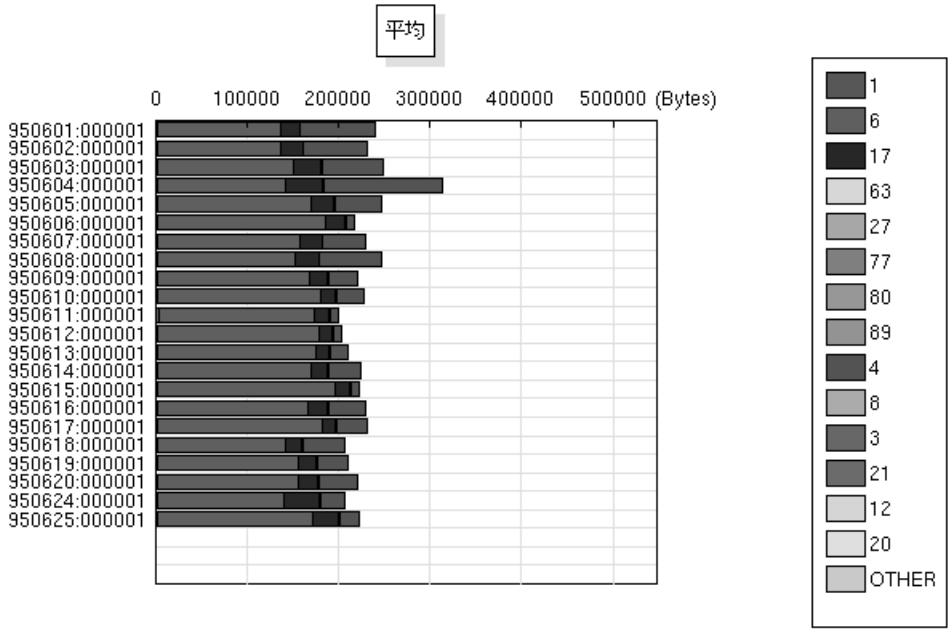

図 3.3: daily mean traffic (bytes/sec) - 6 月

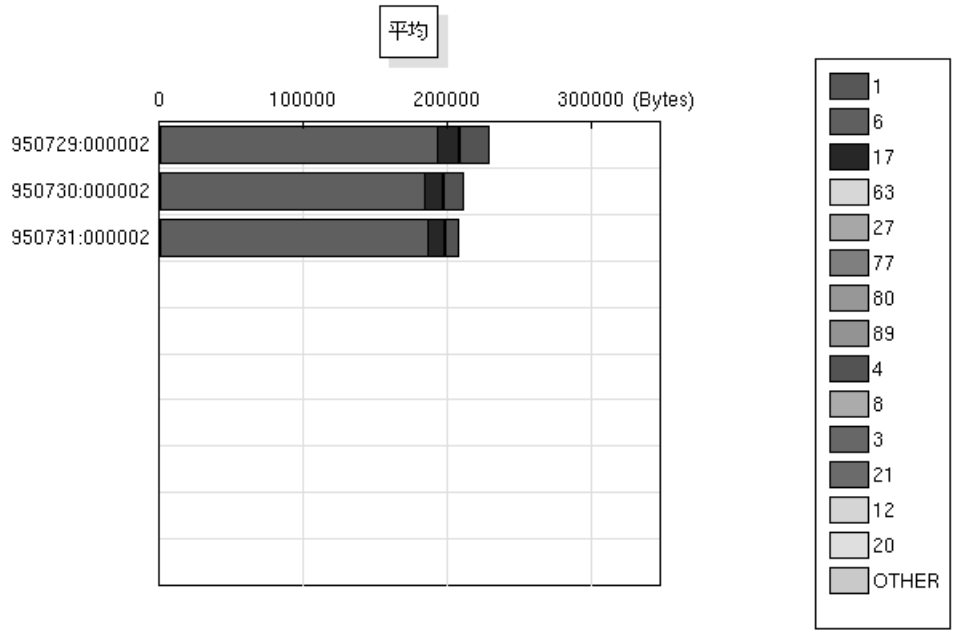

図 3.4: daily mean traffic (bytes/sec) - 7 月

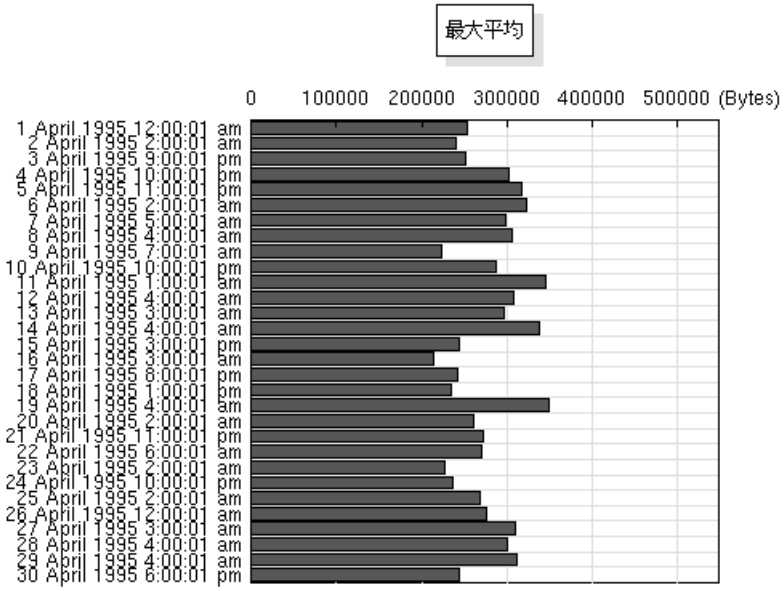

図 3.5: daily max traffic (bytes/sec) - 4 月

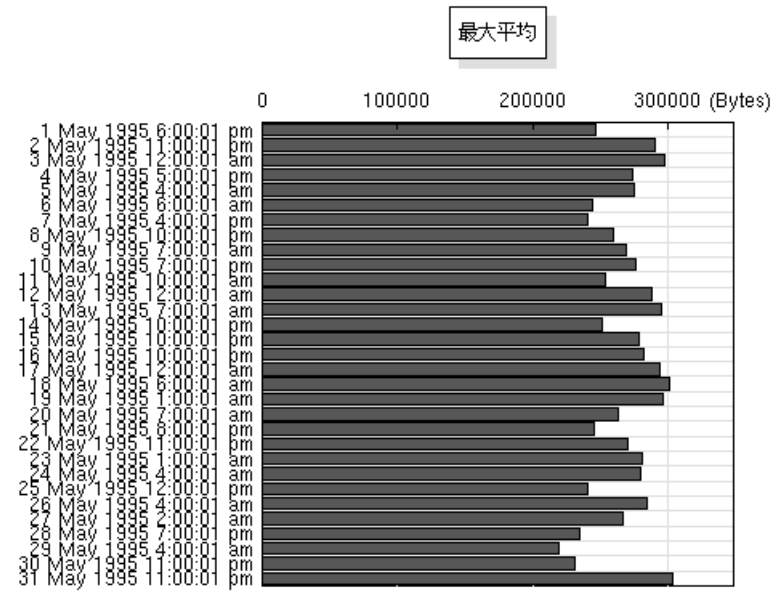

図 3.6: daily max traffic (bytes/sec) - 5 月

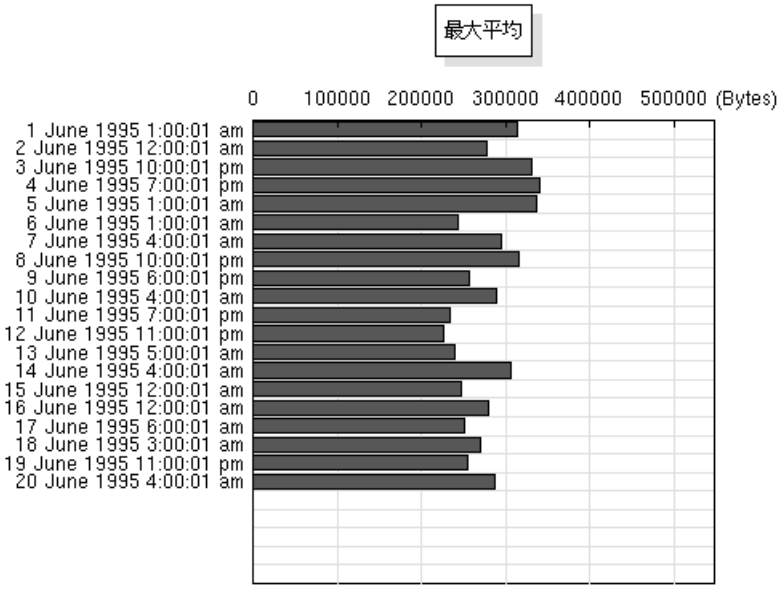

図 3.7: daily max traffic (bytes/sec) - 6 月

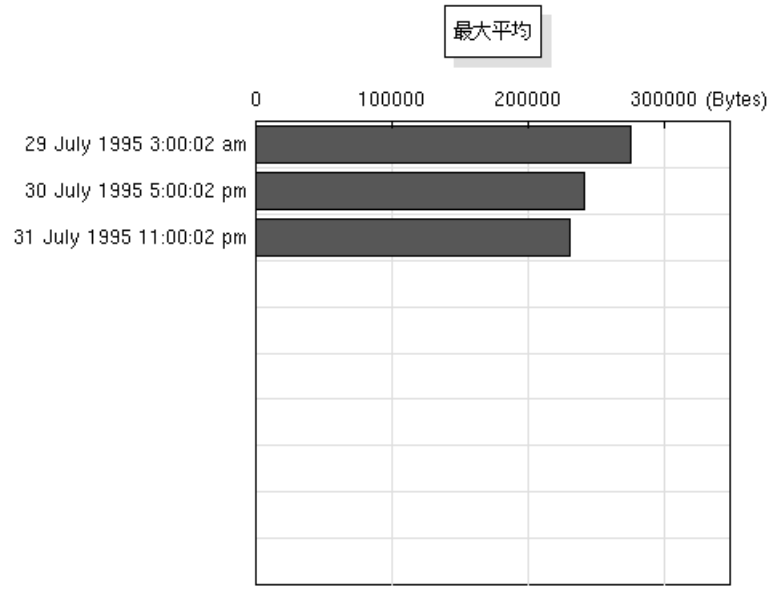

図 3.8: daily max traffic (bytes/sec) - 7 月

表 3.1: Monthly Figures by TCP port (bytes/sec)

TCP Port	4 月	5 月	6 月	7 月
OTHER	16615.70	15814.99	15690.78	19602.84
23:telnet	2699.81	2510.17	2258.35	1972.45
20:ftp-data	34345.00	32596.98	39228.51	36476.97
21:ftp	572.13	611.43	651.86	628.21
25:smtp	5087.68	5299.27	6016.58	5585.39
37:time	0.12	0.11	0.15	0.13
42:name	0.00	0.00	0.00	0.00
43:whois	4.81	6.18	3.18	3.77
53:domain	547.17	414.41	455.30	79.15
70:gopher	844.32	968.95	1201.56	1128.77
79:finger	110.44	93.59	112.38	63.35
80:http	19243.92	25176.15	33178.34	54928.27
103:x400	0.18	0.07	0.02	0.01
104:x400-snd	0.18	0.07	0.00	0.00
109:pop2	0.00	0.01	0.01	0.01
110:pop3	13.62	17.57	18.99	14.20
111:sunrpc	0.03	0.18	0.02	0.08
115:sftp	0.01	0.02	0.02	0.01
119:nntp	70447.27	68202.47	60544.52	65712.55
153:sgmp	0.00	0.00	0.00	0.00
210:z39.50	4.91	4.84	2.68	0.44
512:exec	0.02	0.04	0.02	0.01
513:rlogin	462.34	447.29	424.92	392.74
514:shell	1062.17	314.53	1306.89	392.74
515:printer	0.23	24.84	1.75	0.00

表 3.2: Monthly Figures by UDP port (bytes/sec)

UDP Port	4 月	5 月	6 月	7 月
OTHER	10094.24	10350.39	12812.96	6616.56
42:name	0.00	0.01	0.00	0.00
37:time	0.07	0.06	0.06	0.07
53:domain	4817.24	4714.94	7167.10	4644.63
111:sunrpc	5.31	11.03	5.75	25.22
69:tftp	0.02	0.05	0.04	0.01
123:ntp	295.98	263.39	328.85	325.70
161:snmp	36.28	19.44	29.22	122.23
162:snmp-trap	0.17	0.20	0.24	0.25
191:PROSPERO	697.42	262.24	1408.30	96.03
513:who	25.56	11.75	13.38	23.44
517:talk	7.62	12.86	141.26	23.84
520:route	55.19	50.29	27.26	25.64
1167:phone	0.18	0.47	0.25	5.19
1525:archie	692.44	793.26	79.19	681.77

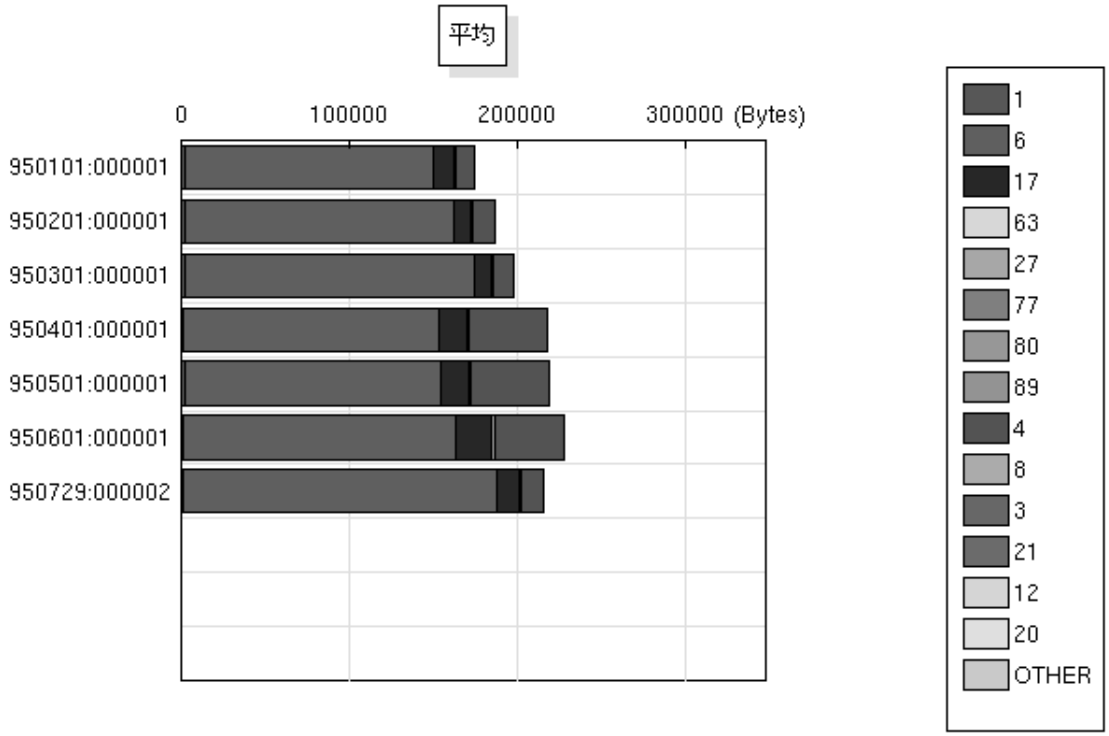

図 3.9: monthly mean traffic (bytes/sec)

第 4 章

WWW を利用したネットワーク・トラフィックのビジュアライゼーション

4.1 はじめに

NetStat ワーキンググループでは、WIDE バックボーンのトラフィック統計を実施しているが、その統計結果を効果的に表示させる方法についてはいまだ確立されていないといえる。ネットワーク・トラフィックのような情報は、その詳細な情報からいかに簡単にネットワークの状態を知ることができるかという点が重要である。そのためには 1 時間毎、1 日毎のようなトラヒックを人間が直感的に判断できるようにグラフで表示し、しかもネットワーク管理者、時にはエンドユーザもが必要なときにいつどこにいても確認できるようにしておくことが重要である。

ネットワークの状態をいつどこにいても確認できるようにしておくためには UNIX、Windows、Macintosh 等の様々な OS 上で利用でき、かつ既に広く普及している WWW を利用すれば実現が可能になる。ネットワークの状態を知りたい時には WWW ブラウザさえあればいつでもその情報を参照できるわけである。また、WWW であれば情報をビジュアルに表現することも容易である。

そこで本章では、NNStat のようなトラフィック統計ツールから得られる情報を WWW を利用してビジュアルに表示する方法について述べる。

4.2 Java アプレットを使用したグラフ表示

トラヒック統計情報を WWW を利用して公開することは以前からおこなわれており、NetStat ワーキンググループにおいても WIDE のホームページ上で実施している。

このような従来の表示法では、NNStat 等のトラヒック統計ツールから得られたデータを gnuplot や MS-Excel 等のアプリケーションを用いてグラフにし、そのグラフを GIF 等のフォーマットの画像ファイルにして WWW サーバ上に置くという手法が一般的である。しかし、例えば 1 日毎にデータを処理してグラフを作成する場合、その画像ファイルの量は膨大なものとなり、ディスク容量の面で問題が生じてくる。

そこで本手法では、グラフを画像ファイルとして保管しておくのではなく、１日毎の数値データとその数値データからグラフを作成する Java アプレットを用意しておくことによって、WWW でアクセスされるたびにグラフを作成する方法を採用する。

グラフを作成する Java アプレットは、Sun Microsystems Inc. から公開されているグラフ作成用アプレット'Chart.java' を改良し、階層グラフを描けるようにしたものを使用している。

4.3 方法と仕組み

NetStat ワーキンググループでは、以前から NNStat による WIDE バックボーンのトラフィック統計を実施しており、本手法ではこの NNStat の出力するデータを利用している。

NNStat の出力するログの集計は１時間毎のトラヒックを IP,TCP,UDP について各プロトコル毎におこない、その処理は夜中に１日分をまとめておこなっている。ここで集計した結果は Java アプレットに引数として渡す形式で保存していく。

統計結果を参照したい場合には、WWW でアクセスすることにより図 4.4のようなメニュー画面を表示させる。ここで、日付、参照したい WIDE バックボーンのリンクなどを入力するとグラフ表示用 Java アプレットと対応する数値データがダウンロードされ、グラフが作成・表示される仕組みになっている。

4.4 表示結果

本手法によって、１日分のトラフィック情報を表示させた結果を図 4.4 、図 4.4、図 4.4 に示す。トラヒック情報は WIDE バックボーンの各リンクについて IP,TCP,UDP レベルでの各プロトコルの占める割合をバイト数およびパケット数単位で１時間毎に表示するようにしている。

4.5 考察

4.5.1 表示速度

本手法では、Java アプレットをダウンロードすることによりクライアント側で数値データを処理しグラフを描画しているため、画像データを直接ダウンロードする場合とはグラフを表示する速度に当然差が生じてくる。Java を利用した場合には、ダウンロードするデータ量が画像ファイルそのものを転送する場合に比べて少なくなるため、ネットワークへの負荷は小さくなるが、クライアント側でアプレットを実行させる時間が生じてしまう。

しかし、クライアントの CPU に Pentium 等の高速プロセッサを用いた場合には快適にグラフを表示することが可能であった。表示速度の面においてはどちらの方法が優れてい

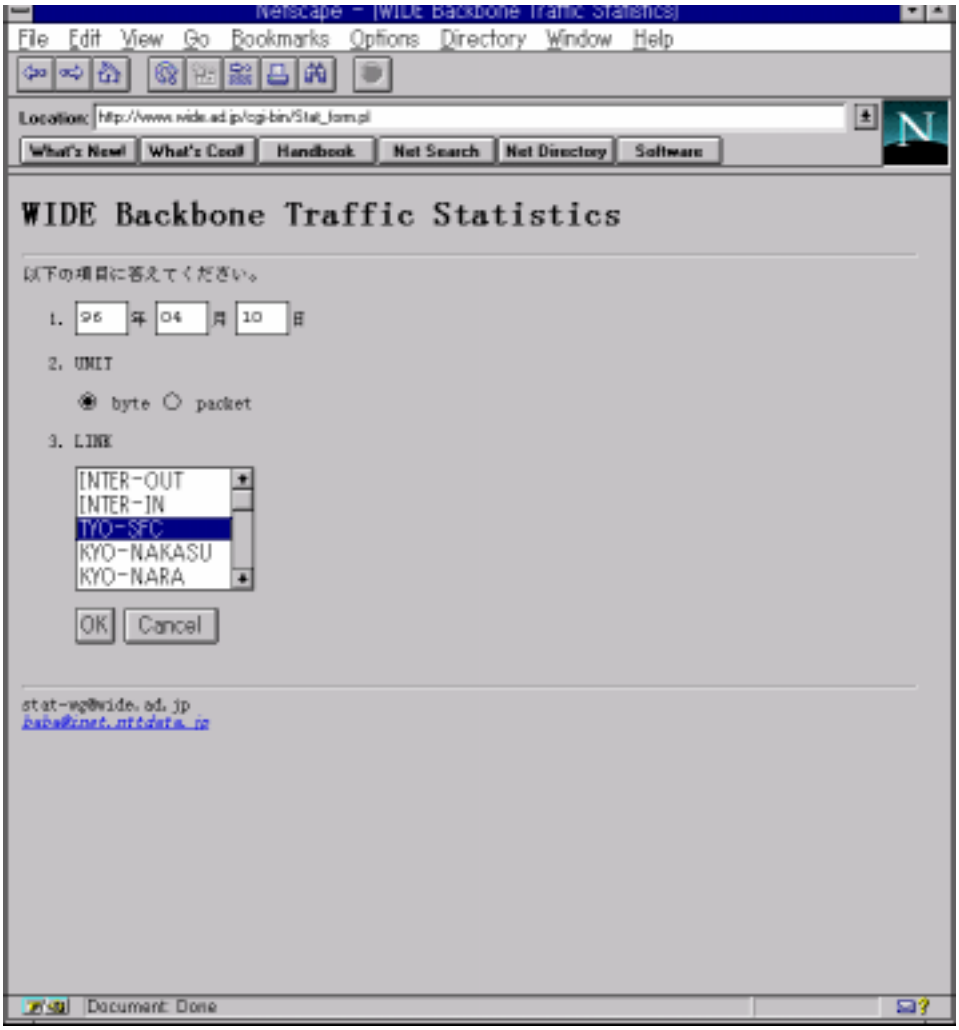
File Edit View Go Bookmarks Options Directory Window Help
Location: http://www.wide.ad.jp/cgi-bin/Stat_form.pl
What's New! What's Cool! Handbook Net Search Net Directory Software
WIDE Backbone Traffic Statistics
以下の項目に答えてください。
1. 96 年 04 月 10 日
2. UNIT
byte packet
3. LINK
INTER-OUT
INTER-IN
TYO-SFC
KYO-NAKASU
KYO-NARA
OK Cancel
stat-wg@wide.ad.jp
Document: Done

図 4.1: メニュー画面

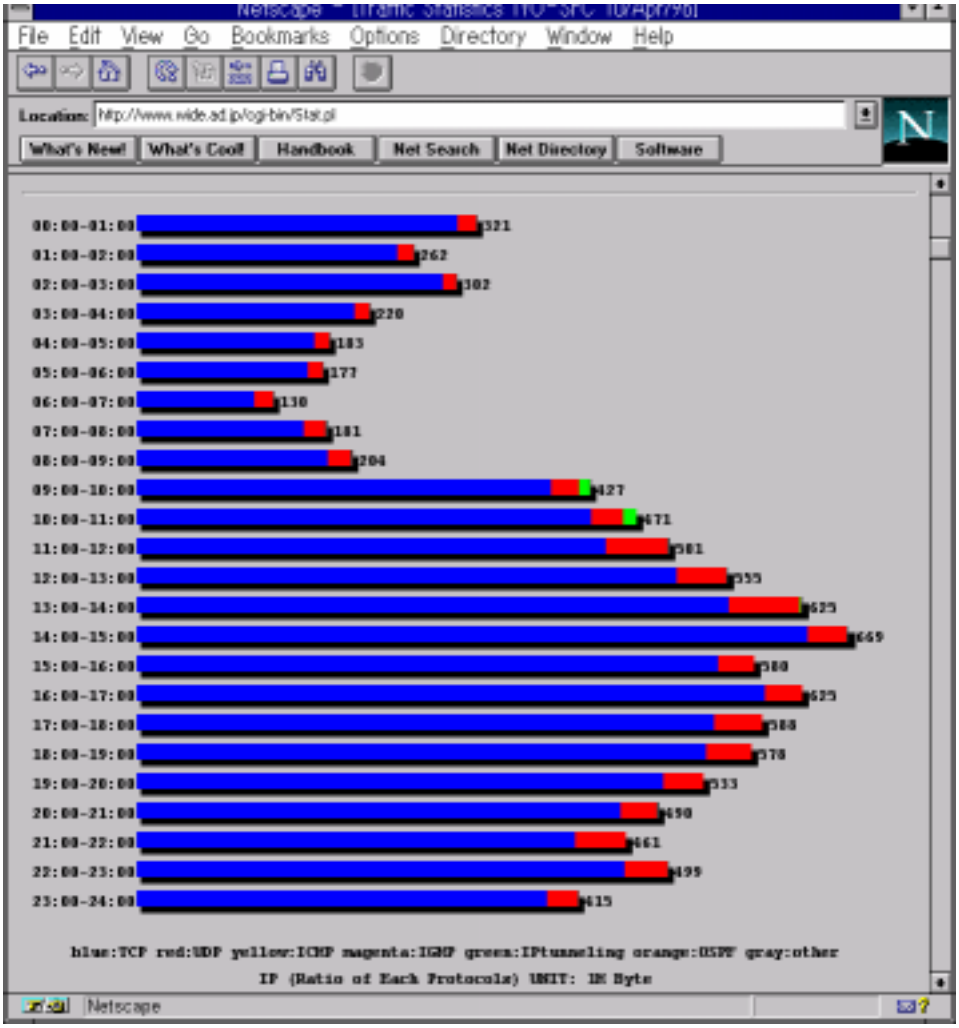

図 4.2: トラフィック表示結果 (IP)

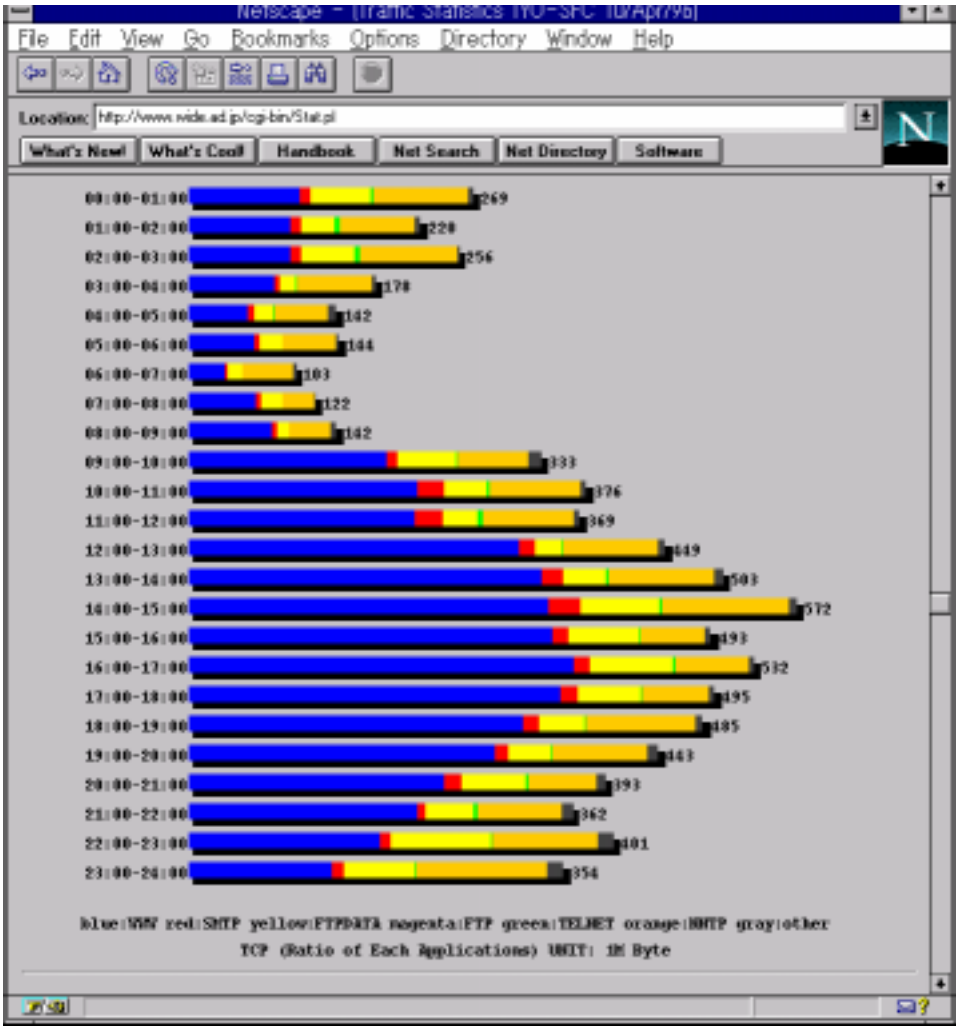

図 4.3: トラフィック表示結果 (TCP)

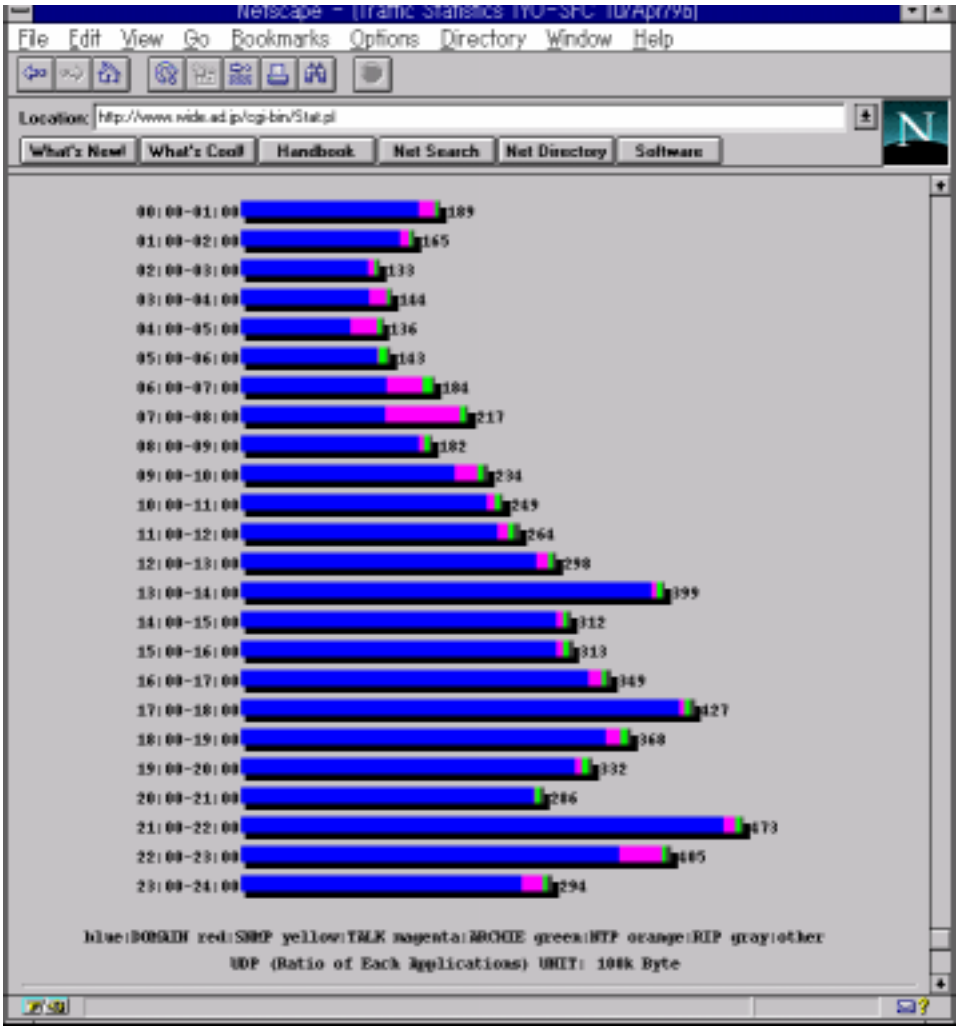

図 4.4: トラフィック表示結果 (UDP)

るという判断はネットワーク、マシン等の環境によるので一概には言えないが、ネットワーク・トラフィックを削減できるという面ではかなりの効果が期待できると思われる。

4.5.2　トラフィック表示のリアルタイム化

現在は１時間毎のトラフィックを１日分まとめて処理をしているため、一昨日前までのデータしか確認することができない。

しかし、今現在のトラフィックを知りたいという要望も当然あると思われる。本手法では Java を利用しているが、Java にはソケットを使用することによりホスト間通信を容易に実現できるという特徴がある。

今後 Java アプレットにトラフィック集計マシンとの通信機能を持たせることによりリアルタイムでトラフィック情報を確認することが可能となると思われる。

4.6　まとめ

以上、NNStat 等のトラフィック統計ツールから得られたデータを WWW を利用してビジュアルに表示する方法について述べた。

これにより、Java 対応の Web ブラウザのある環境でネットワークの状況をいつでも簡単に把握することが可能となった。

今後の課題を以下に示す。

- グラフ表示メニューの充実 － １時間毎/１日毎/１ヶ月毎の統計表示 等
- トラフィック表示のリアルタイム化

以上の課題について今後検討していき、さらに利用しやすい仕組みを考えていくつもりである。

第 5 章

まとめと今後の課題

本報告では 1995 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。

また、今回トラフィックの情報をリアルタイムにビジュアライズするための試みについても報告した。

今後インターネットの利用方法が多様化し、バックボーンネットワークが高速化するに従い、リアルタイムにネットワークの利用状況を知りたいと言う要求が増大していくだろう。今後これらの要求に対してより意味のある情報をより早く提供するための手法を確立していくことが、NetStat ワーキンググループに与えられた一つの大きな課題である。

また、バックボーン回線の高速化にともない、全てのトラフィックデータを収集し、解析することが困難になりつつある。またそれらの収集されたデータの保管に関しても、より大容量で高密度な二次記憶媒体の利用を検討していく必要があるだろう。今後は、全てのデータを集める方法ではなく、統計的に有意なデータのサンプリングの手法なども検討していく。