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おこなうことを目的に活動を行っている．また，トラフィックデータの収集・解析によって得られた情報をネットワーク管理において利用する技術に関する研究も合わせて行っている．

これまで当 WG では，WIDE Internet 上のトラフィックの統計情報の収集・解析を通して，WIDE バックボーンの利用状況を，その上を流れるトラフィックの観点から明らかにしてきた．また，WIDE の国際回線を通した国際的な通信の広がりについての考察を行ってきた．

本年度では，WIDE バックボーンの拡大，リンク上を流れるアプリケーションの多様化から，統計情報の収集範囲の増加，および測定内容の拡充を行った．

本報告では，93 年度の活動をもとに以下の内容を行った．

- トラフィック収集環境の紹介
- 国外のネットワークとのトラフィック解析
- WIDE バックボーン上のトラフィック解析
- TIX における，他のネットワークプロジェクト間とのトラフィック解析
- サイト間トラフィック解析
- IPIP トラフィック解析
- ネットワークモニター情報の自動統計機構

第 2 章

トラフィック収集環境

2.1 はじめに

WIDE バックボーンの拡大、及びアプリケーションの多様化にともない、NetStat WG では 93 年度計画の一貫として、国内線を中心にしたデータ収集地点の変更、測定サイトの増設、および測定内容の拡充をおこなってきた。本章では、トラフィック収集環境の変遷と現状を報告する。

2.2 トラフィック収集環境の変遷

NetStat WG ではここ数年の間、トラフィックの統計情報を収集するために、NNStat を利用している。このツールは概念的には、ある地点のトラフィックを測定する測定部分と各地点で測定されたデータを集める収集部分の 2 つから構成されている。サイトの増設とはある地点でのトラフィックを測定する部分の増設にあたる。

94 年の 3 月 6 日、および 3 月 16 日に国内のトラフィック収集環境を変更した。収集環境の変遷を以下に示す。

変更前

測定リンク TIX, TYO-SFC, SINET-TYO, TYO

測定対象物 Telnet, rlogin, FTP, FTP data, SMTP, NNTP, RIP, DNS, SNMP, IP, ICMP

1994 年 3 月 6 日

測定リンク TYO-SPK, SFC-SND, SFC-KYO を増設

測定対象物 Wais, HTTP, Gopher, Finger, Whois, Archie, IRC, NTP を増加

1994 年 3 月 16 日

測定リンク KYO-HIJ, KYO-NAKASU を増設

測定対象物 IP/IP を増加

2.3　現トラフィック収集環境の詳細

2.3.1　トラフィック収集トポロジー

現在、WIDE バックボーン及び、TIX におけるトラフィック測定リンクは 8ヶ所、収集地点は 2ヶ所という構成になっている。この構成を図 2.1に示す。収集地点は stat.nc.u-tokyo.ac.jp と endo.sfc.wide.ad.jp の 2ヶ所で行われ、TIX のデータは stat に、残りは endo に収集される。

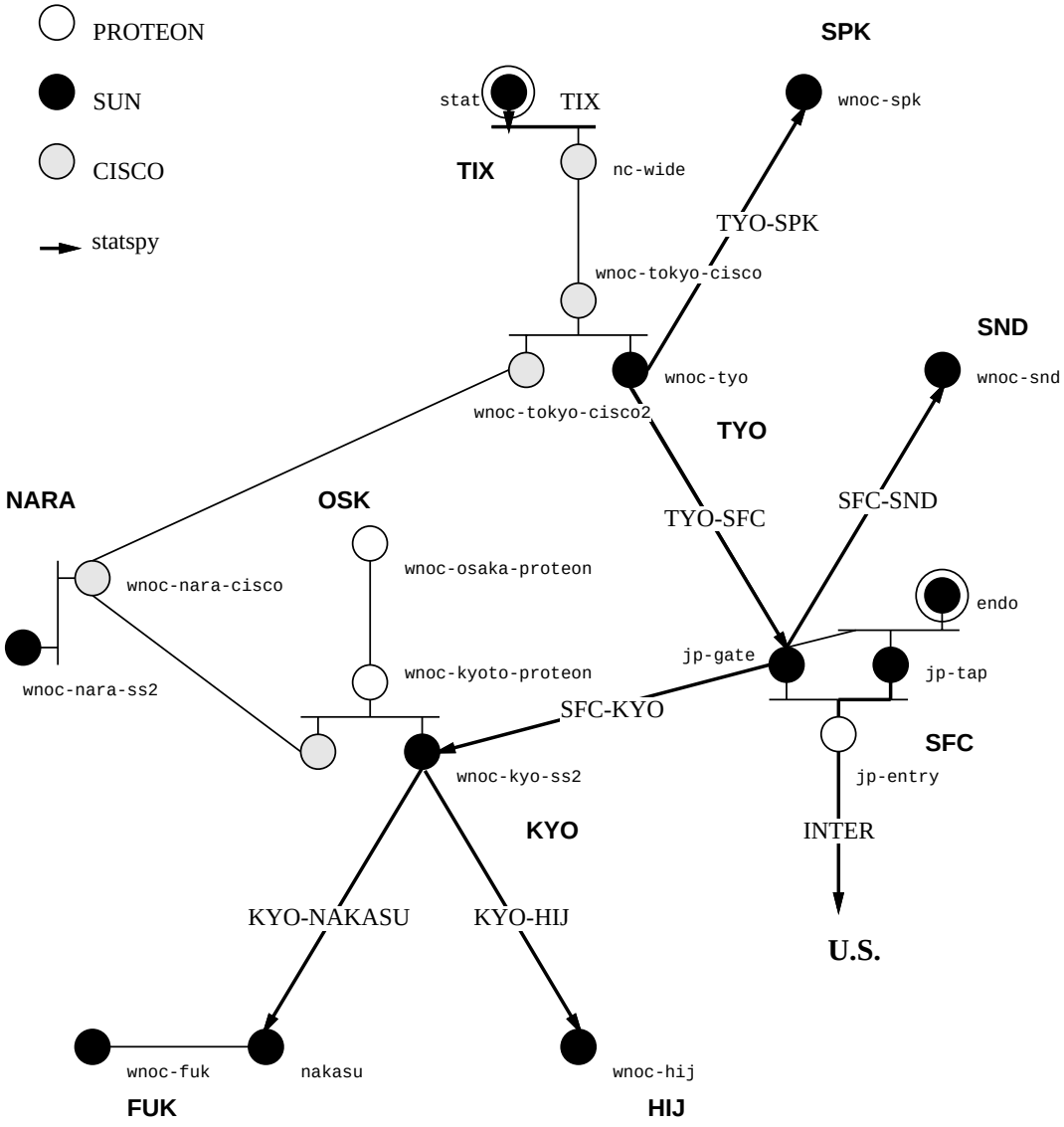

図 2.1: トラフィック収集トポロジー

測定されるリンクは矢印で示されている。矢印のもとのホストでは、そのリンクのト

ラフィック量を測定するためのデーモン statspy が稼働されている。現在、statspy は 5ヶ所のホストで稼働されている。

2.3.2 測定内容

測定内容を変更する以前は、Telnet, rlgoin, FTP, NNTP, RIP, DNS, SNMP, IP, ICMP など代表的なアプリケーションを中心に測定してきた。しかしながら、近年これらにあてはまらないデータが多く測定されるようになってきた。このため今年度では大幅に測定内容の拡充をおこなった。

拡充の対象は、急激に利用率が延びている gopher, WWW などの情報検索系を中心に、活発化する mbone の活動に応じてマルチキャストパケットなどに注目した。表 2.1には、測定の対象物とその対象物の測定内容を示した。

オブジェクト	測定内容
IP	・送信側、受信側のサブネットワークアドレスのマトリックスによるデータ量、パケット数 ・パケット長
ICMP	
OSPF	
BGP	
Telnet, rlogin/rwho	
SMTP	
NNTP	
DNS	
SNMP	
Finger	
Archie	
IRC	
NTP	
Whois	
gopher	・送信側、受信側のホストアドレスのマトリックスによるデータ量、パケット数 ・パケット長
Http	
Wais	
FTP	
RIP	・送信側のサブネットワークアドレスによるデータ量、パケット数 ・パケット長

表 2.1: 測定内容

第 3 章

93 年度のトラフィック解析の結果

93 年度は 92 年度と同様，WIDE バックボーンのうち，国際回線と，東京 NOC と藤沢 NOC 間のトラフィックについて NNStat を用いてデータを収集し解析を行った．また，WIDE のバックボーンの一部ではないが，TIX における各ネットワークプロジェクト間のトラフィックに関しても同様なデータ収集を行った．

残念なことに，データ収集を行っていたマシンのディスクトラブルのために，10 月分のデータの大部分が失われてしまったため，本年度のトラフィック解析のデータからは除外した．

本章では，1993 年 4 月から 1994 年 3 月までに収集されたデータをもとに行った解析の結果を示す．

3.1　国際回線のトラフィック

3.1.1　IP プロトコル別トラフィック

図 3.1は，93 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．

表 3.1: IP プロトコル別トラフィック (単位:キロバイト/日)

月		ICMP	IGMP	IP/IP	TCP	UDP	その他	合計	回線利用率
4 月	IN	12,909	1,661	0	908,077	201,137	0	1,123,783	54.19%
	OUT	17,695	1,690	0	484,463	63,975	0	567,822	27.38%
5 月	IN	10,997	1,979	0	1,007,717	182,181	0	1,202,874	58%
	OUT	13,857	1,914	0	459,818	56,956	0	532,545	25.68%
6 月	IN	10,945	2,318	0	1,176,903	166,340	2	1,356,508	65.42%
	OUT	22,814	2,628	0	393,973	47,708	0	467,124	22.53%
7 月	IN	30,420	2,387	179,134	1,106,696	87,687	0	1,406,324	67.82%
	OUT	24,042	2,484	1,482	447,718	104,783	0	580,509	28%
8 月	IN	16,019	2,989	52,256	999,180	94,616	0	1,165,061	56.19%
	OUT	11,796	3,055	749	438,189	68,923	17	522,728	25.21%
9 月	IN	20,593	3,269	73,976	1,134,671	83,077	0	1,315,586	63.45%
	OUT	11,874	3,358	1,364	473,177	78,114	1,673	569,581	27.47%
11 月	IN	9,905	4,060	158,205	1,405,062	89,757	5,468	1,672,457	80.65%
	OUT	4,567	8,328	1,480	633,882	89,111	2,737	740,105	35.69%
12 月	IN	27,148	9,199	94,245	1,379,580	79,844	217	1,590,234	76.69%
	OUT	5,362	9,369	11,032	737,114	102,620	46	865,543	41.74%
1 月	IN	9,188	4,713	35,370	1,204,101	70,591	2,211	1,326,174	63.96%
	OUT	6,664	9,705	7,521	768,124	79,410	821	872,245	42%
2 月	IN	38,253	214	456	1,347,129	151,238	45	1,537,336	74.14%
	OUT	21,647	7,335	4,623	828,776	185,274	77	1,047,732	50.53%
3 月	IN	17,726	423	614	1,152,914	116,335	28	1,288,039	62.12%
	OUT	19,489	9,025	4,901	717,549	169,911	427	921,302	44.43%

図 3.1, 図 3.2は、図 3.1 をグラフ化したものである。グラフから分かように、93 年度後半には、国外から国内向けのトラフィックの 1 日の平均量は、概ね国際回線の容量の 60%を越え、また国内から国外のトラフィックについても、40%を越えている。

国内向けと国外向けのトラフィックの傾向としては、国内向けがそれほど大きな変動を見せていない反面国外向けのトラフィックは 1 年間で 2 倍弱の伸びを見せている。ただし、国内向けのトラフィックに関しては、回線容量的な限界が来ていると考えて良いだろう。

図 3.3は、各プロトコルの全体に占める割合である。国内向け国外向けともに TCP が 80%以上を占めている事が分かる。また、IP ／ IP のトラフィックが昨年に較べて増加しているが、これは MBONE のトラフィックがそれまでの IP オプションを用いてソースルーティングにより実現されていたのに対して、IP トンネリングを用いられるようになったためである。

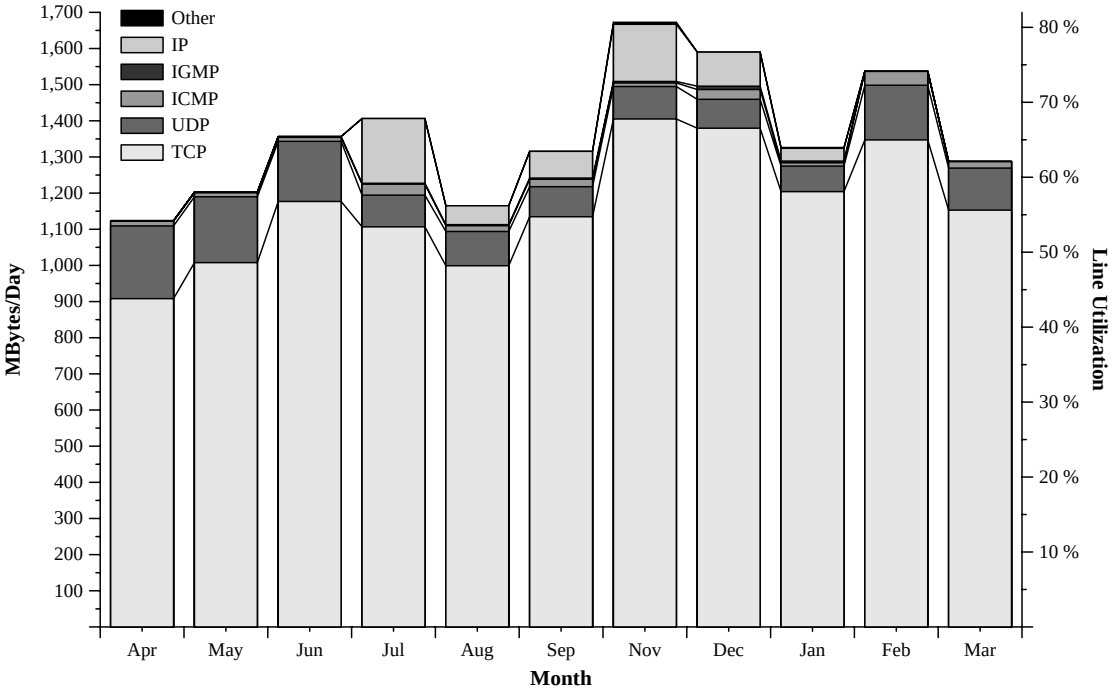

図 3.1: 国外から国内向けの，プロトコル別トラフィック量推移 (1 日平均)

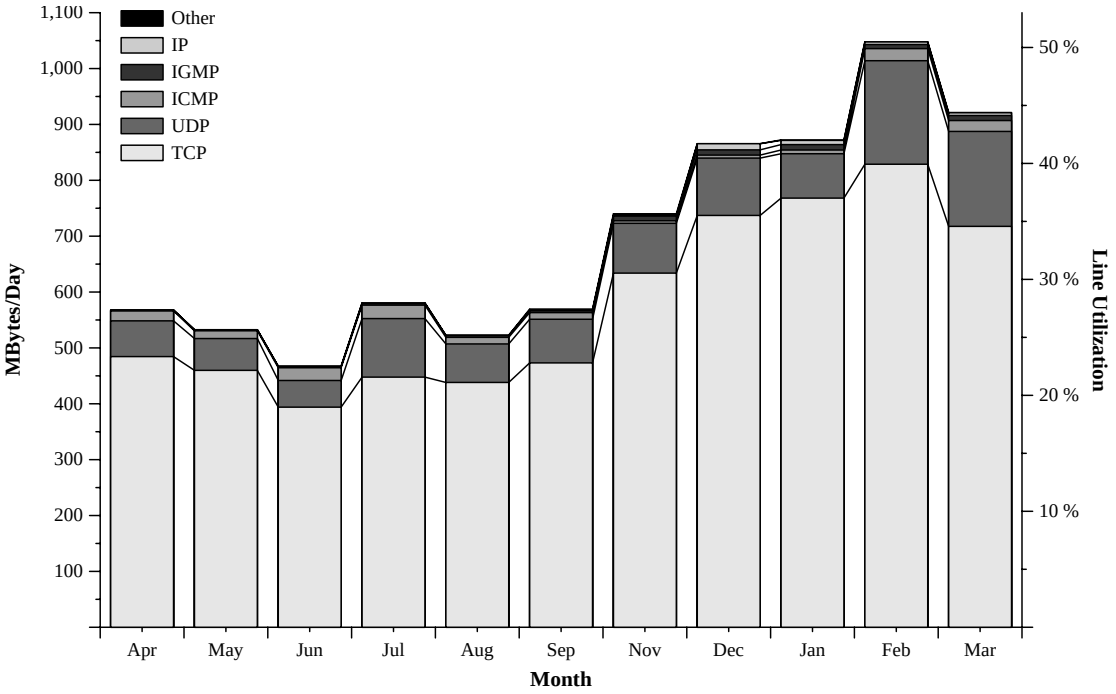

図 3.2: 国内から国外向けの，プロトコル別トラフィック量推移 (1 日平均)

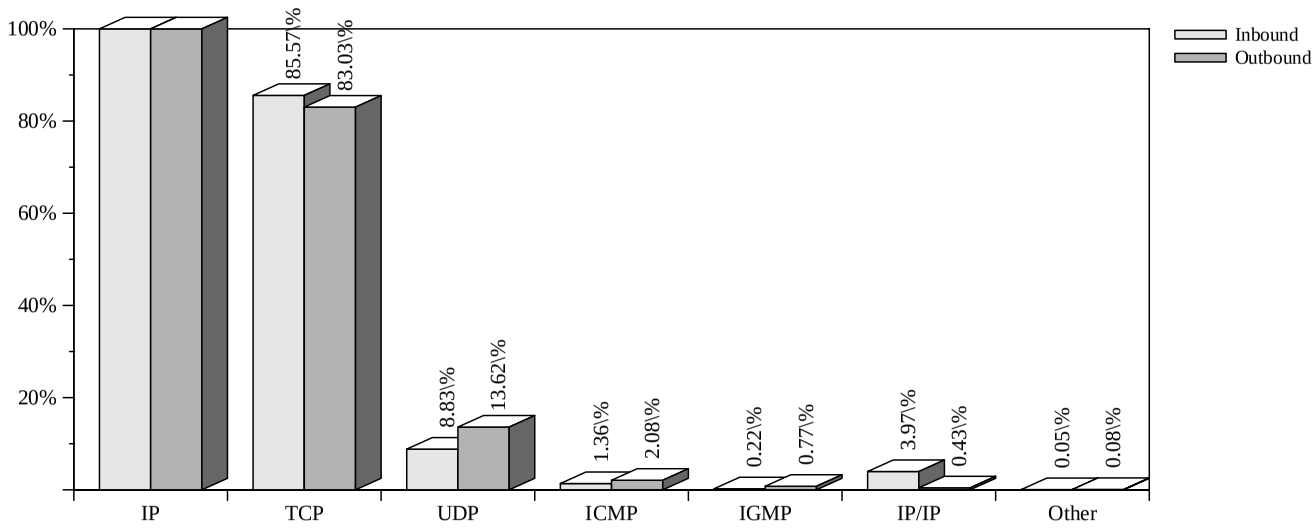

図 3.3: IP プロトコル別トラフィック量分布

3.1.2 TCP アプリケーション別トラフィック

表 3.2: TCP アプリケーション別トラフィック (単位:キロバイト/日)

		FTP	Telnet	SMTP	DNS	HTTP	Gopher	NNTP	Z39.50	rlogin	Other
4 月	IN	683,600	22,234	85,962	2,243	0	0	59,798	584	5,826	47,830
	OUT	361,901	17,928	44,553	1,666	0	0	22,424	47	6,643	29,303
5 月	IN	774,550	23,403	90,884	3,471	0	0	59,576	1,223	5,302	49,307
	OUT	277,810	16,869	63,159	1,254	0	0	22,537	106	4,697	73,387
6 月	IN	874,124	26,715	116,896	2,952	0	0	73,782	1,179	5,528	75,728
	OUT	132,649	13,722	95,311	990	0	0	35,102	157	3,039	113,003
7 月	IN	809,807	26,653	116,668	3,638	0	0	67,224	908	4,786	77,011
	OUT	284,635	17,188	68,739	718	0	0	47,325	80	4,729	24,305
8 月	IN	705,572	33,607	108,114	3,021	0	0	56,092	553	3,364	88,857
	OUT	294,244	20,581	61,476	600	0	0	34,297	40	4,230	22,720
9 月	IN	820,793	34,968	109,503	3,420	0	0	62,629	898	4,550	97,910
	OUT	318,915	21,748	53,661	616	0	0	20,662	99	6,432	51,044
11 月	IN	1,005,147	37,465	134,539	3,047	0	0	107,993	739	3,990	112,143
	OUT	446,710	21,957	83,458	969	0	0	26,581	90	4,436	49,681
12 月	IN	1,005,503	36,585	101,631	3,111	0	0	103,859	597	3,312	124,982
	OUT	557,880	18,925	76,294	2,294	0	0	28,316	108	4,299	48,999
1 月	IN	802,677	49,256	118,319	3,334	0	0	103,252	779	3,859	122,624
	OUT	527,264	25,464	89,170	2,393	0	0	30,949	99	4,082	88,704
2 月	IN	927,988	56,143	132,850	5,425	15,456	51,710	94,194	392	3,317	59,653
	OUT	334,975	21,840	90,199	2,025	24,185	25,104	42,831	79	2,643	284,893
3 月	IN	756,226	38,548	169,031	2,585	15,897	37,858	88,695	495	2,552	41,028
	OUT	395,360	21,345	109,669	1,114	64,301	38,576	37,730	77	3,355	46,022

表 3.2は、93 年度の国際線のトラフィックのうち TCP アプリケーションによるもののデータ量をキロバイト単位で表した物である。また、図 3.4、図 3.5は、それらの月毎の推移をグラフで表した物である。

図 3.6では、これらの TCP アプリケーションの月毎の平均量を TCP 全体に対する割合で表しているが、例年と同様、FTP のトラフィックが占める割合が最も多く、TCP 全体に対して、国内から国外向きが約 62%、国外から国内向きが約 71%となっている。これらは IP のトラフィック全体に対して、それぞれ 51%、61%となっている。月毎の推移としても、コンスタントに FTP のトラフィックが最大となっている。まだまだ FTP はインターネット上の情報交換の手段として主流となるアプリケーションである事が分かる。

新しい TCP アプリケーションプロトコルとして、HTTP と Gopher についてもデータの収集を開始した。表 3.2で、これらの値は 94 年 1 月迄は 0 となっているが、これは単にデータを収集し始めたのが 94 年の 2 月からであったためである。これらの新しく収集を始めたプロトコルのトラフィック量が、TCP アプリケーションの中でも比較的上位を占めるようになって来ている。HTTP も Gopher も、インターネット上での情報の検索を行うタイプのアプリケーションであるが、旧来からある NNTP や Z39.50(WAIS) と較べても、トラフィック量的には、同等以上となっている事が分かる。これらのアプリケーションのトラフィックは今後増加していくことが予想される。

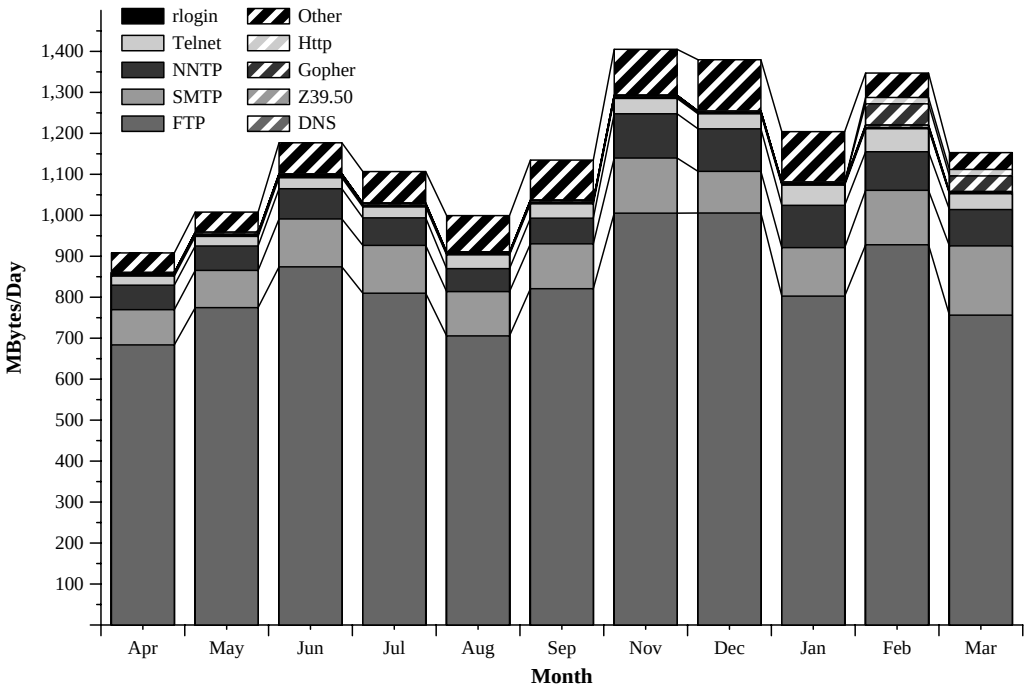

図 3.4: TCP アプリケーションのトラフィック (国外から国内)

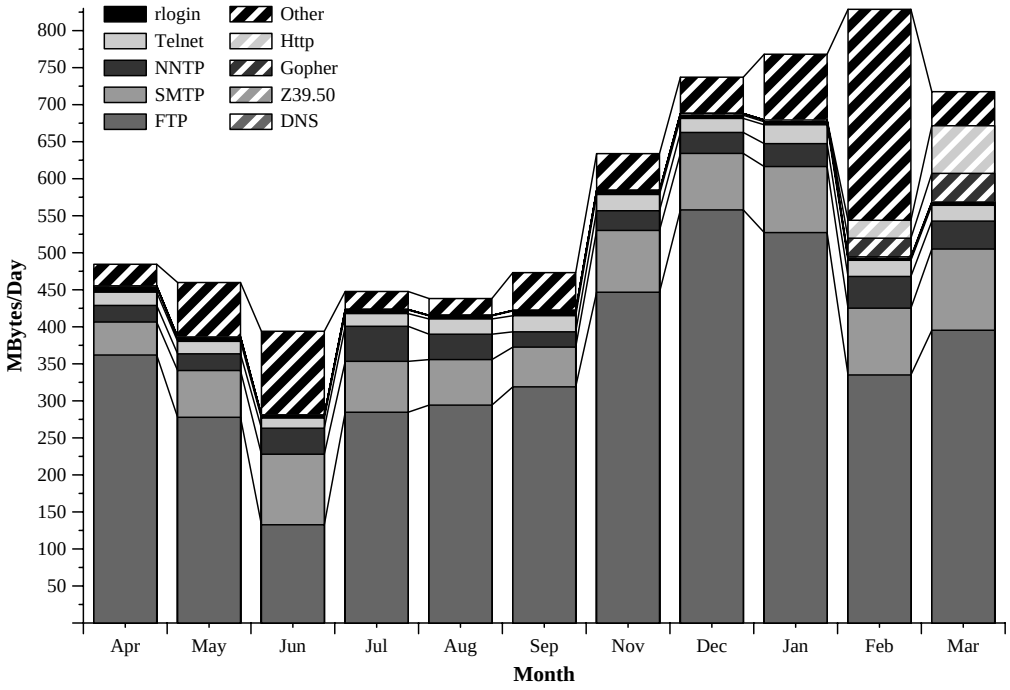

図 3.5: TCP アプリケーションのトラフィック (国内から国外)

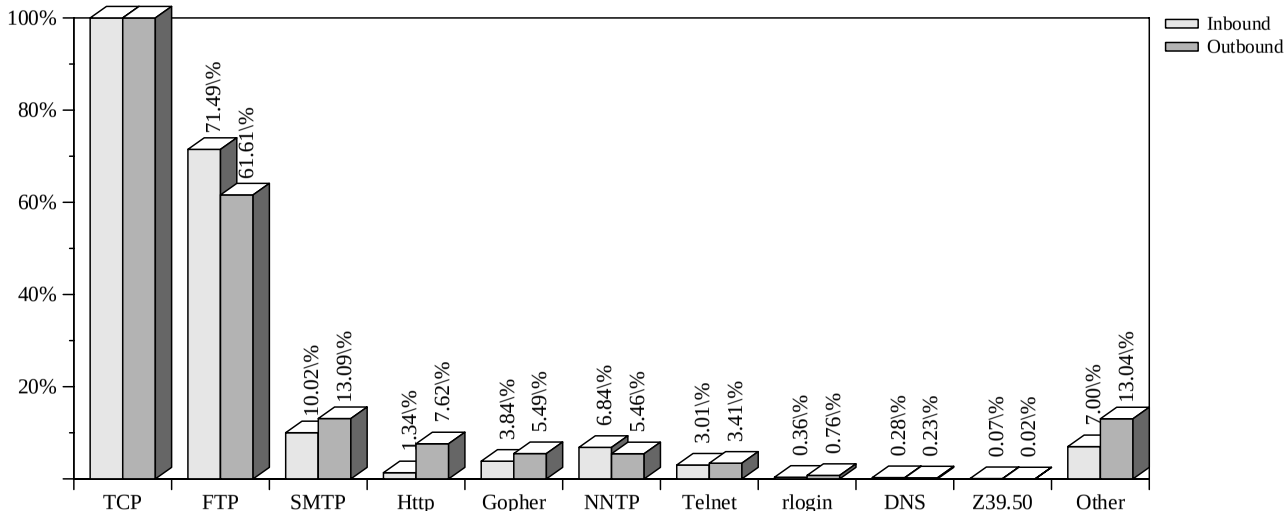

図 3.6: TCP アプリケーション別トラフィック量分布

3.1.3 UDP アプリケーション別トラフィック

表 3.3: UDP アプリケーション別トラフィック (単位:キロバイト/日)

		DNS	NTP	SNMP	Talk/Phone	ROUTE	ARCHIE	Other
4 月	IN	38,414	1,178	218	460	2	1,287	159,577
	OUT	45,670	906	737	523	14	6,906	9,219
5 月	IN	32,562	1,362	268	548	607	2,822	144,014
	OUT	31,606	906	199	516	295	8,728	14,706
6 月	IN	29,820	1,361	218	795	0	2,431	131,715
	OUT	29,980	927	36	475	9	11,901	4,380
7 月	IN	36,315	1,259	194	923	0	4,412	44,584
	OUT	52,089	714	1	929	7	11,888	39,155
8 月	IN	49,470	1,185	209	280	0	3,893	39,578
	OUT	42,328	613	10	433	27	10,346	15,167
9 月	IN	32,828	1,424	189	1,878	0	4,402	42,355
	OUT	30,427	692	60	269	7	9,319	37,340
11 月	IN	36,121	1,954	258	825	1	4,006	46,592
	OUT	35,284	1,120	0	1,197	491	19,499	31,520
12 月	IN	31,454	1,098	185	802	3	4,956	41,346
	OUT	65,728	935	24	2,269	9	13,434	20,222
1 月	IN	33,620	630	230	991	3	4,504	30,613
	OUT	41,117	693	12	1,969	56	20,405	15,158
2 月	IN	54,502	5,001	214	669	345	6,957	83,550
	OUT	55,409	5,141	5	252	86,177	27,898	10,392
3 月	IN	49,444	918	582	797	36	10,464	54,095
	OUT	81,409	1,011	63	548	38,203	35,728	12,949

表 3.3は、93 年度の国際線のトラフィックのうち UDP アプリケーションによるもののデータ量をキロバイト単位で表した物である。また、図 3.8、図 3.9は、それらの月毎の推移をグラフで表した物である。

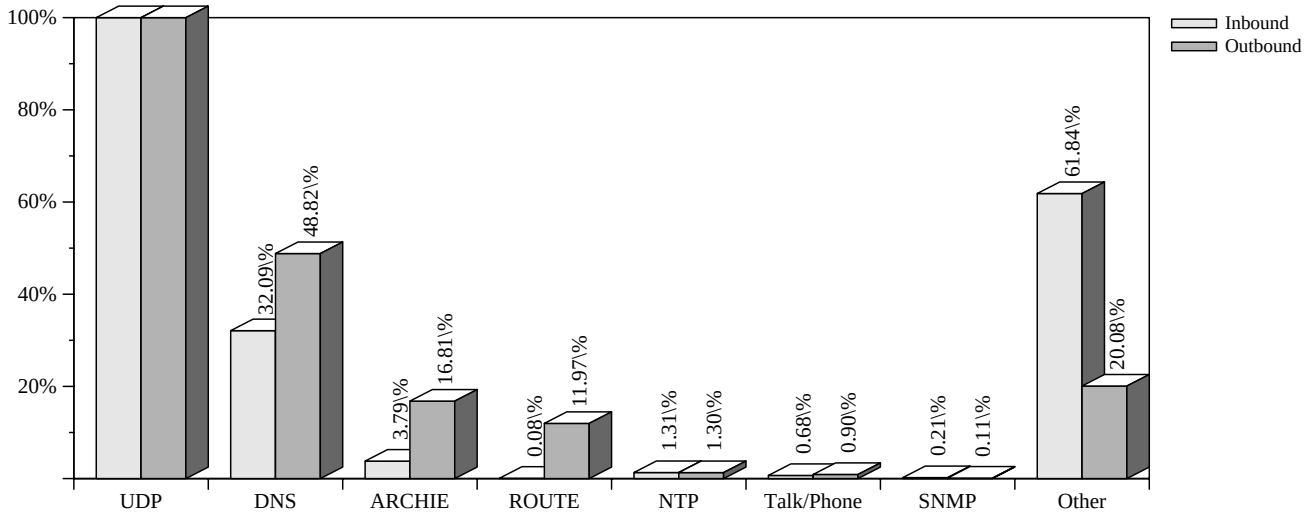

図 3.7: UDP アプリケーション別トラフィック量分布

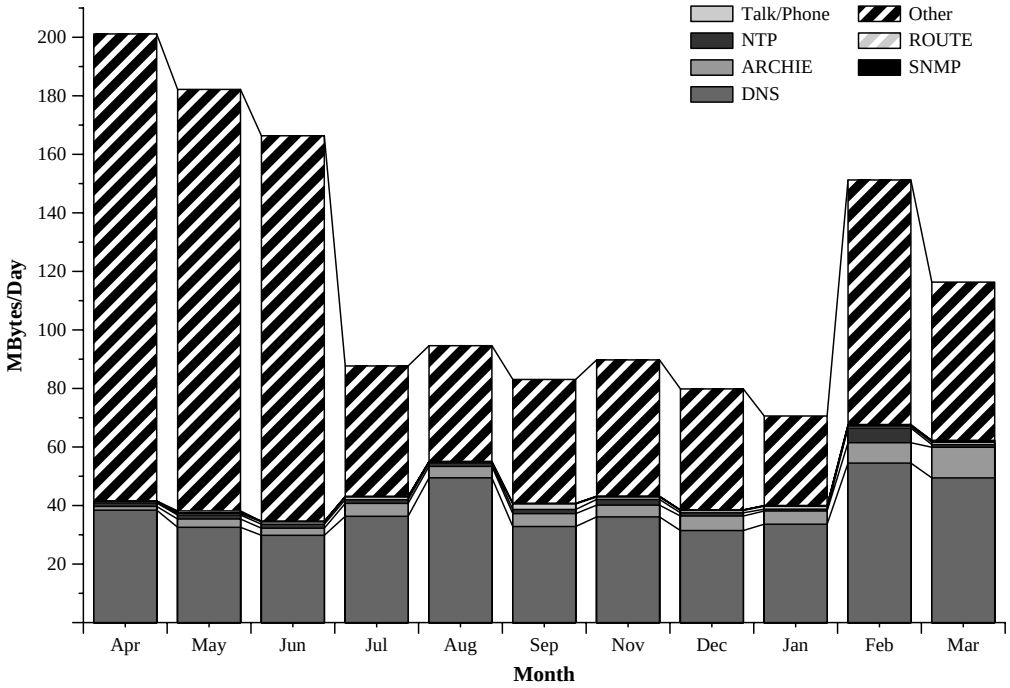

図 3.8: UDP アプリケーションのトラフィック (国外から国内)

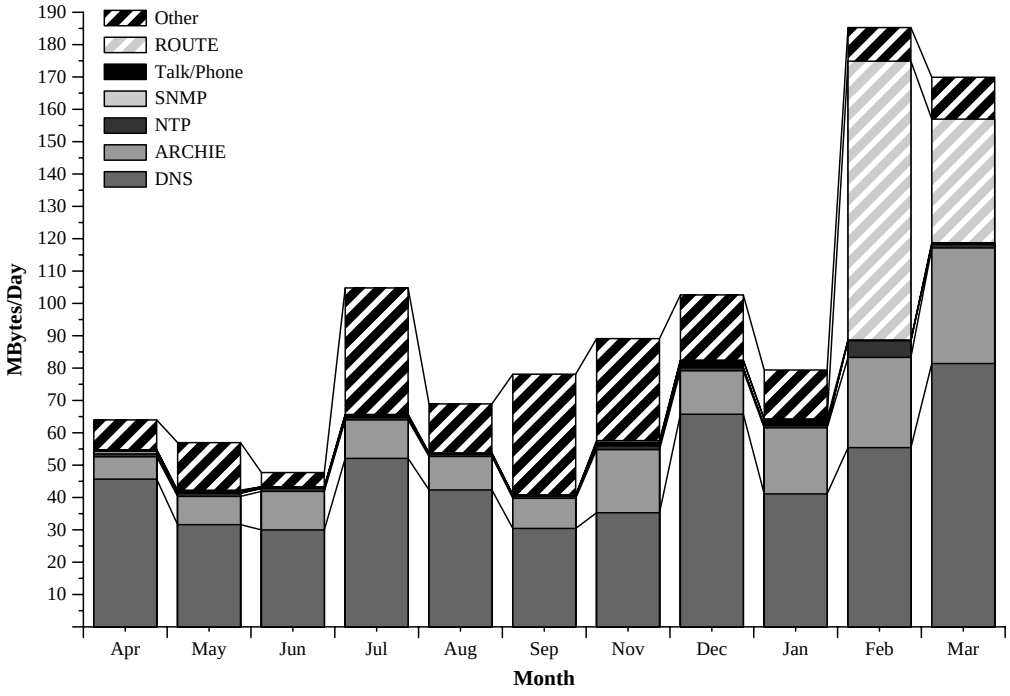

図 3.9: UDP アプリケーションのトラフィック (国内から国外)

3.1.4　ICMP の種類別トラフィック

表 3.4: ICMP タイプ別トラフィック (単位:パケット数/日)

		Echo Reply	Net Unreach	Host Unreach	Port Unreach	Source Quench	Redirect Host	Echo Request	Time Exceeded In Transit	Other
4 月	IN	6,024	72,381	27,957	44,983	1,948	11,811	32,924	13,923	48
	OUT	27,454	10,974	9,716	223,343	187	34	9,195	28,557	92
5 月	IN	4,979	39,437	47,234	29,912	1,900	7,567	26,568	21,559	60
	OUT	5,742	1,441	2,857	147,626	78	1	3,944	8,990	51
6 月	IN	12,781	41,808	27,752	34,078	2,243	34,755	14,941	17,056	95
	OUT	10,854	795	532	11,434	206	431	12,368	3,609	3,997
7 月	IN	155,682	173,720	42,594	43,051	2,892	2,118	22,991	28,864	212
	OUT	28,274	6,165	4,874	73,185	430	1,658	204,246	21,198	8,377
8 月	IN	58,711	85,654	83,816	9,531	1,184	2,375	6,257	16,983	287
	OUT	1,663	2,160	8,301	56,190	419	170	64,334	22,138	1,472
9 月	IN	7,400	168,418	38,582	32,267	1,668	93,611	6,877	20,931	203
	OUT	5,249	7,633	5,236	54,034	217	33	90,571	19,039	112
11 月	IN	4,901	64,459	34,208	43,693	3,222	236	2,607	17,636	3,008
	OUT	1,308	515	4,531	75,070	98	625	9,344	18,794	209
12 月	IN	5,639	69,986	69,306	298,270	7,060	2,291	15,693	22,978	947
	OUT	8,117	561	5,171	52,989	259	4,883	24,006	30,733	1,541
1 月	IN	3,899	38,521	32,867	29,474	4,006	25,801	5,922	18,776	2,668
	OUT	44,139	479	5,780	39,021	276	175	9,221	27,253	4,376
2 月	IN	2,648	19,781	12,677	27,838	3,767	56,062	158,204	331,425	3,101
	OUT	1,017	2,101	1,205	11,876	122	165	22,461	69,131	1,363
3 月	IN	12,007	43,608	17,434	42,024	3,336	22,835	80,394	44,224	3,586
	OUT	15,863	3,677	15,810	76,984	392	41,216	86,635	61,328	5,576

表 3.4は、93 年度に国際線上をやりとりされた ICMP メッセージの種類別パケット数である。また、図 3.10、図 3.11は、それらの月毎の推移をグラフで表した物である。

傾向としては、国内から国外に向かっては、Port Unreach、Echo Request の ICMP メッセージが多く、国外から国内に向かっては、Net Unreach、Port Unreach、Host Unreach の Unreach 系の ICMP メッセージが多い。国外から国内に向かって Net Unreach のメッセージが多いのは、国外の組織へのルーティングを default route に頼っている事にも起因している。また双方向とも Port Unreach が比較的多いのは、traceroute 等のツールによるトラフィックが原因として考えられる。ただ、traceroute によるものが多いとすれば、Time Exceeded in Transit もそれに対応して多くなるはずなので、一概にこれらの Port Unreach が traceroute による物ばかりとは考えにくい。例えば、TCP や UDP のポートへのアクセスををしらみつぶしに試みる等の不正なアクセスの可能性等も考慮しなければならないだろう。

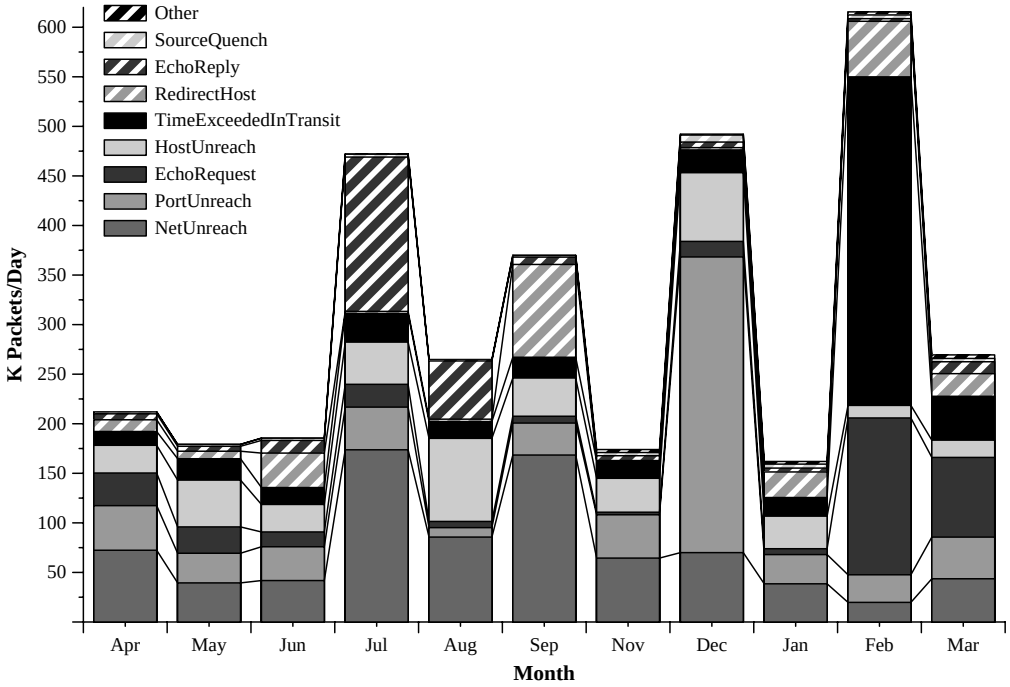

図 3.10: ICMP のトラフィック (国外から国内)

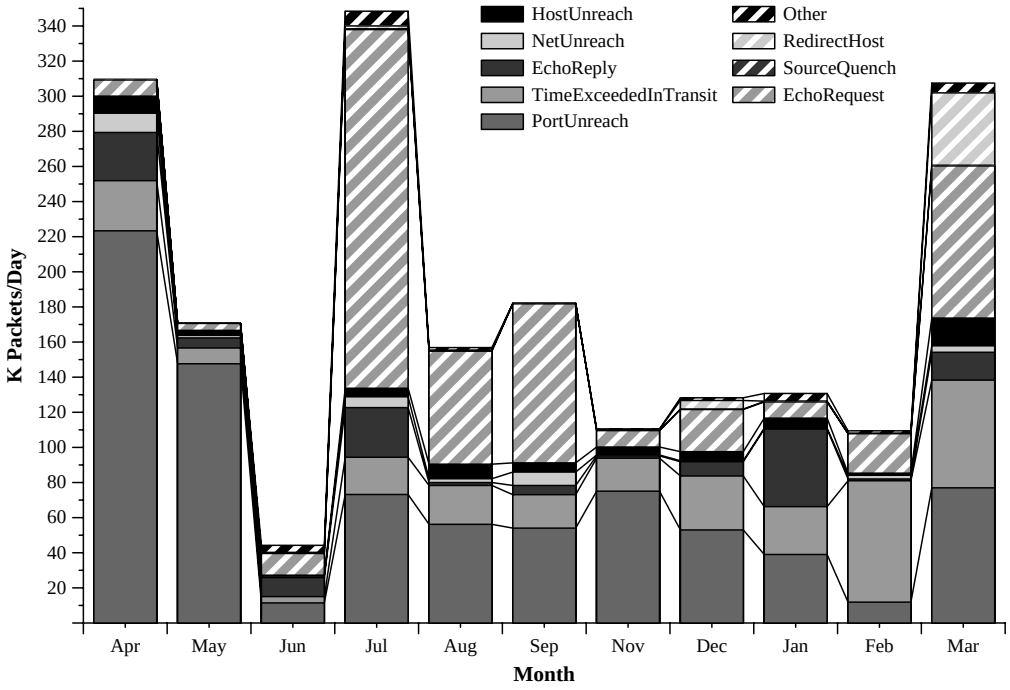

図 3.11: ICMP のトラフィック (国内から国外)

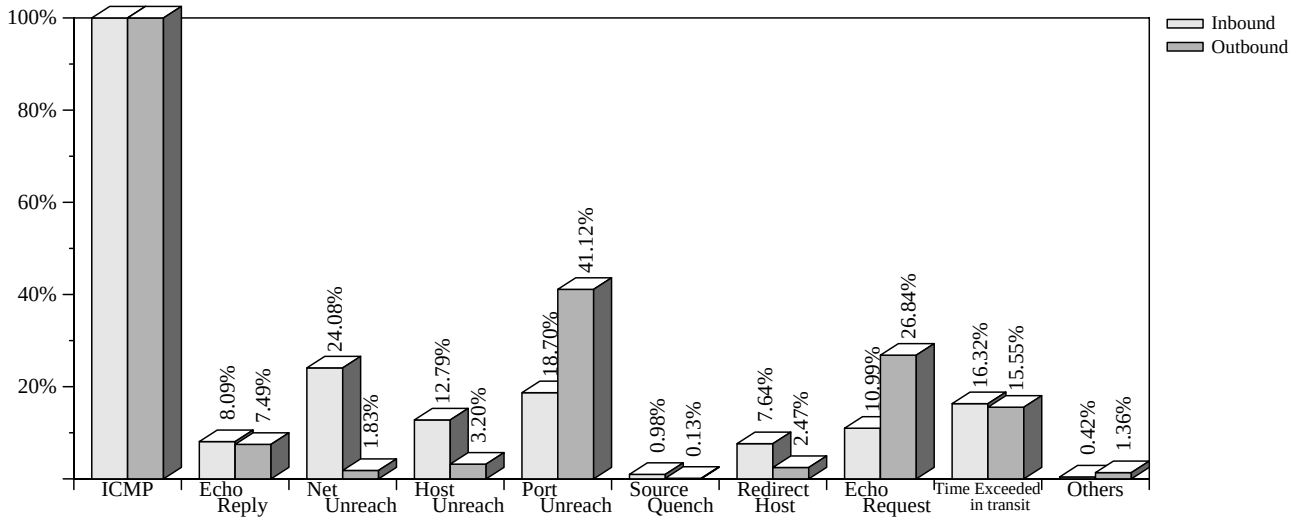

図 3.12: ICMP の種類別トラフィック量分布

3.2　WIDE バックボーンのトラフィック

WIDE バックボーンのトラフィックとして、WNOC-TYO と WNOC-SFC の間のトラフィックを定常的に収集した。

図 3.13は、TCP のトラフィックのアプリケーション別の分布、図 3.14は、UDP のトラフィックのアプリケーション別の分布を各々グラフ化した物である。

TCP では FTP のトラフィックが、UDP では DNS のトラフィックが最も多くなっている。

また、94 年 3 月より、WIDE バックボーンのトラフィック収集の範囲を拡張して WNOC-TYO と WNOC-SFC の間以外のトラフィックに関しても収集を開始した。まだデータの量としては十分ではないが、これらのバックボーントラフィックに関しても解析結果を後の章で示す。

今後は、これらの解析結果をもとに、WIDE バックボーン上で各 NOC 間のトラフィックがどこに集中しているのか等に焦点を当てて解析を行い、バックボーントポロジの最適化や、NOC 間を結ぶ回線に必要なバンド幅等の予測等のための構成管理等に役立てられるようなデータを提供していくことも予定している。

3.3　TIX のトラフィック

東京大学大型計算機センター内に、TIX(Tokyo Internet eXchange) と呼ばれるイーサネットセグメントを設け、このイーサネットセグメント上で、WIDE、TISN、JAIN、TRAIN 等のネットワークプロジェクト間の相互接続を現在行っている。本章では、このイーサネットセグメント上での各プロジェクト間でやりとりされているトラフィックの解析を

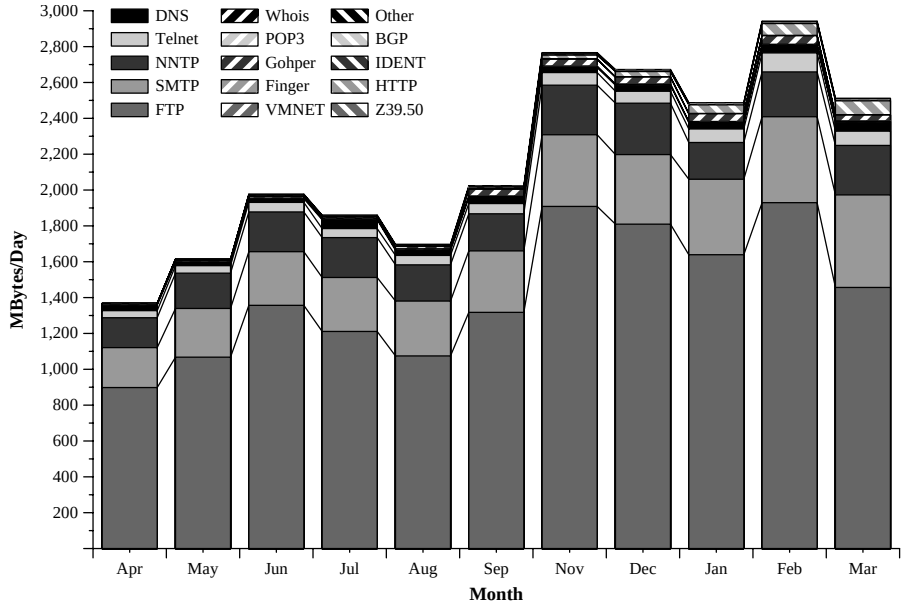

図 3.13: 東京 NOC–藤沢 NOC 間の TCP アプリケーションのトラフィック

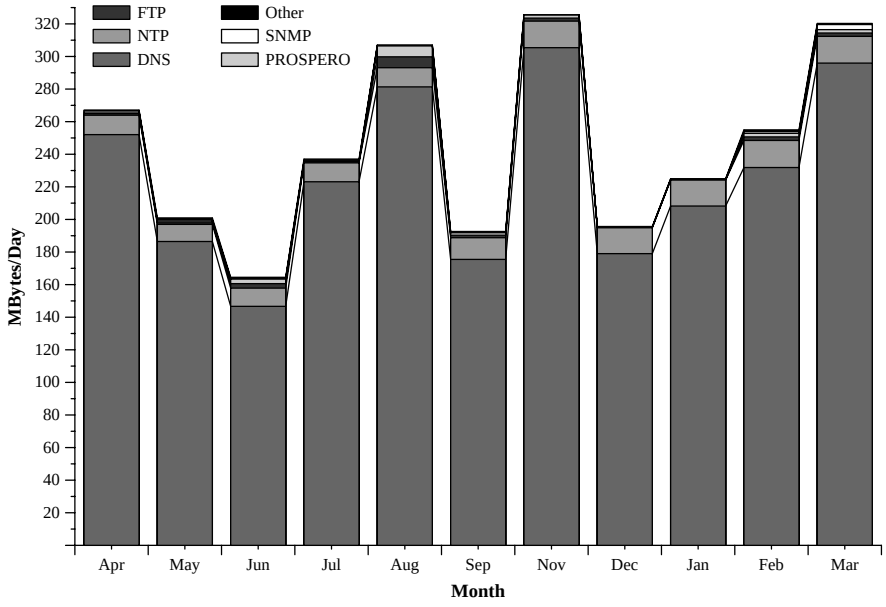

図 3.14: 東京 NOC–藤沢 NOC 間の UDP アプリケーションのトラフィック

行った結果を示す。

どの 2 つのプロジェクト間のトラフィックを見ても、FTP のトラフィックの占める割合がやはり最も大きくなっている。また、ネットワークプロジェクトの観点から見ると、JAIN とその他のネットワークとの間のトラフィックが減少傾向にあり、反面、TRAIN とその他のネットワークとの間のトラフィックが増加の傾向にある。

中でも WIDE-TRAIN 間と、WIDE-TISN 間のトラフィックが最も多い。ただし、WIDE と TISN の相互接続は、TIX 以外の場所でも行われているので、今後は、TIX 以外の場所での相互接続のトラフィックの調査も併せて行っていく必要があるだろう。

また、どのネットワークプロジェクト間のトラフィックにおいても、Other のカテゴリが占める割合が増加しつつある。新しいプロトコルによるトラフィックが増加した時に、それに柔軟に対応しより正確なデータ収集を行っていくことは現在の NNStat を用いいたデータ収集のみではもはや難しくなって来ている。このような新しいプロトコルのデータを柔軟に収集していくための手法を考案していくことは今後の課題である。

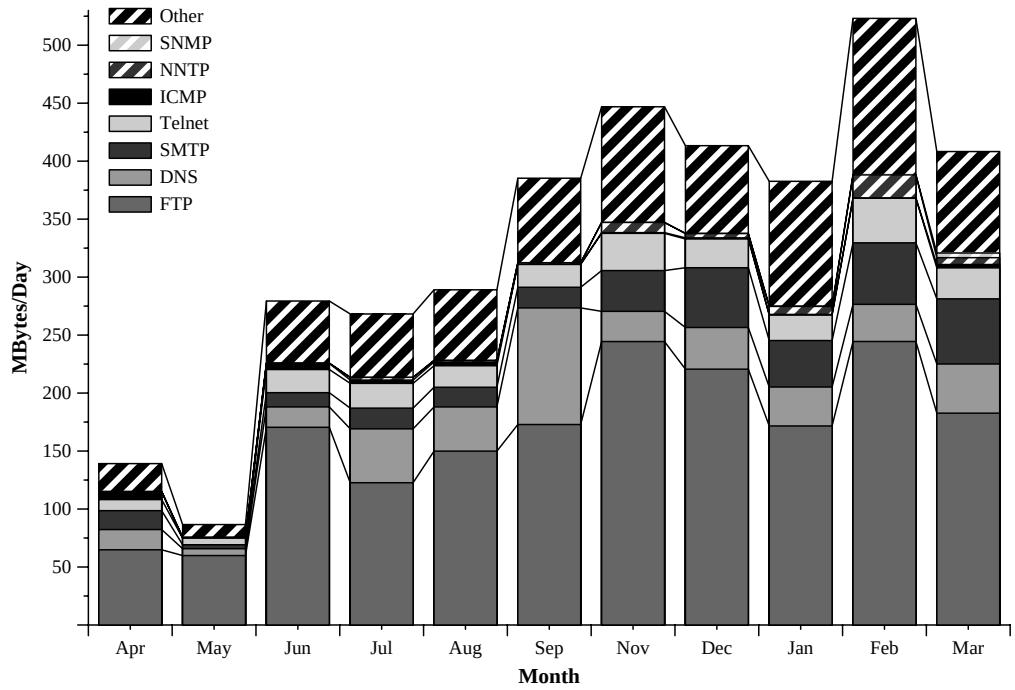

図 3.15: WIDE-TISN 間のトラフィック (バイト数/日)

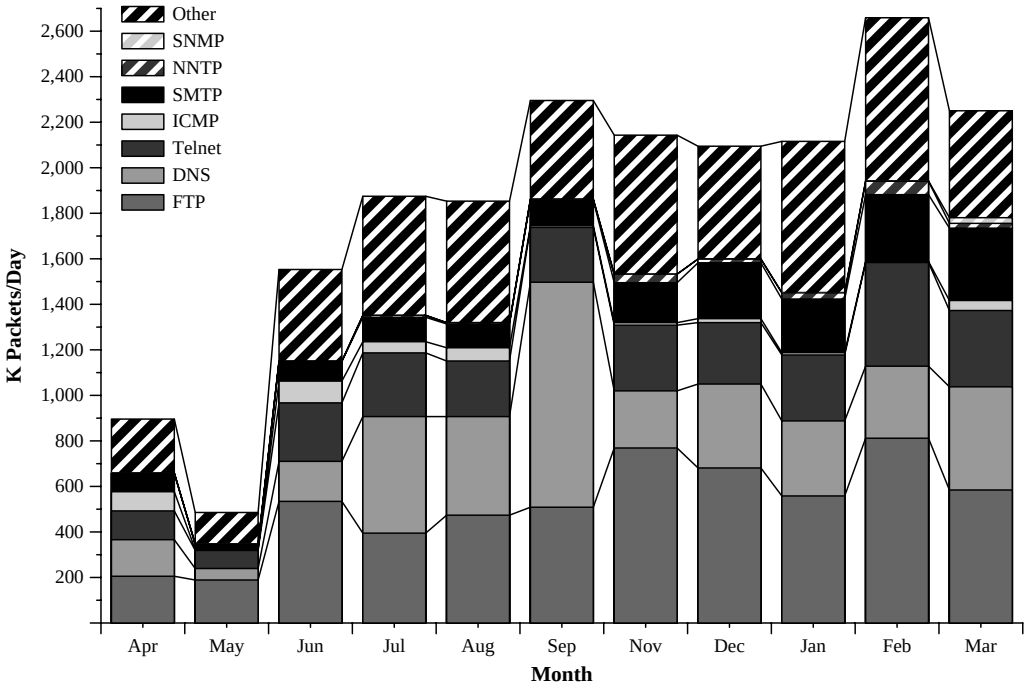

図 3.16: WIDE-TISN 間のトラフィック (パケット数/日)

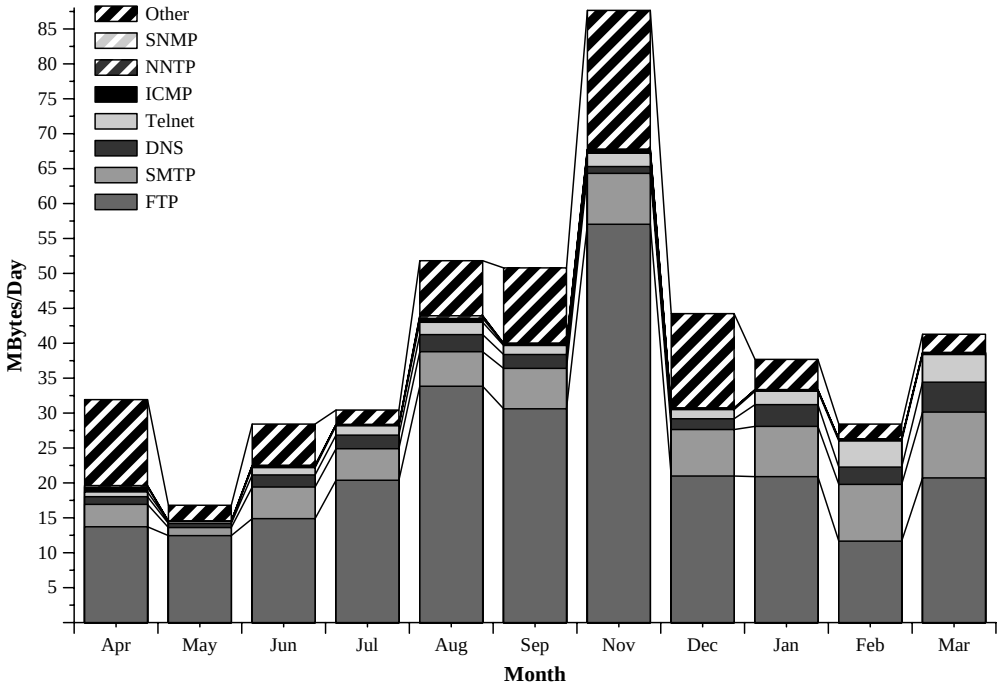

図 3.17: WIDE-JAIN 間のトラフィック (バイト数/日)

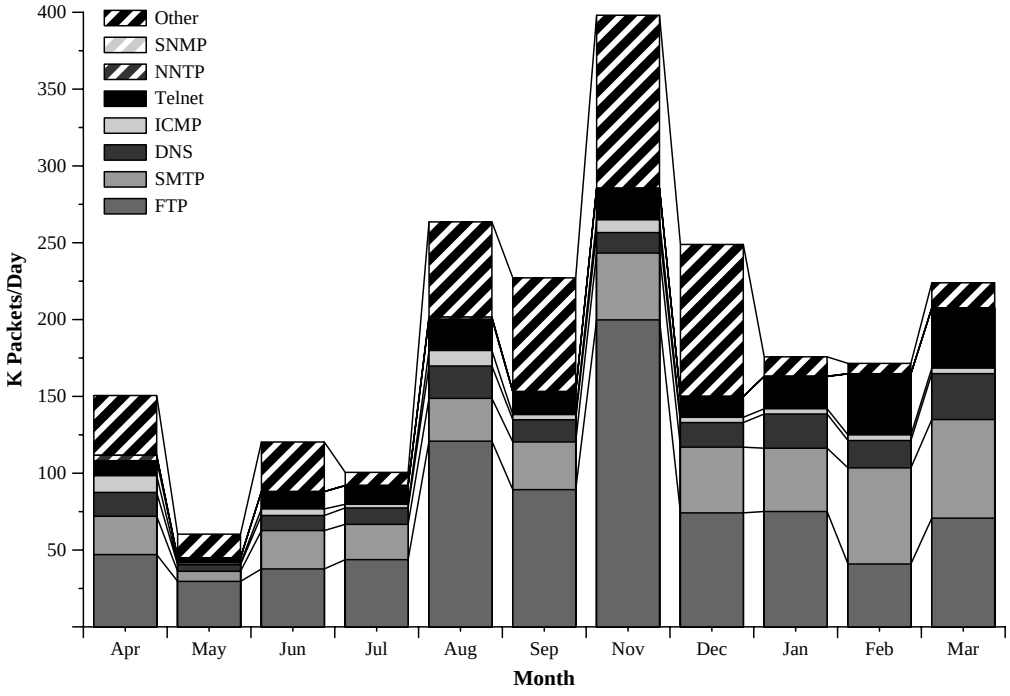

図 3.18: WIDE-JAIN 間のトラフィック (パケット数/日)

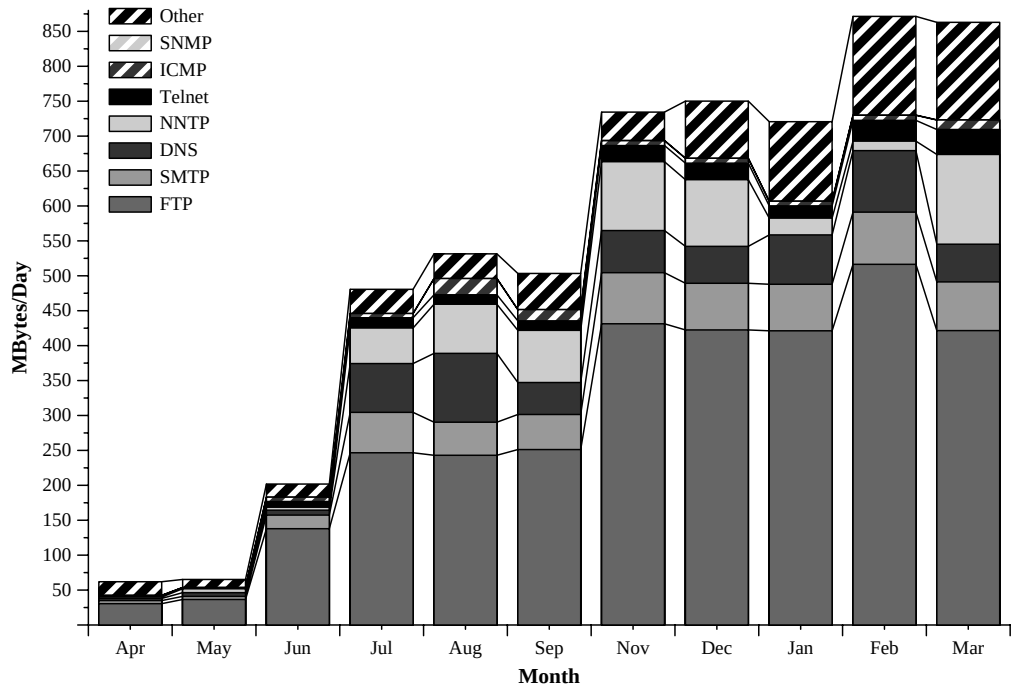

図 3.19: WIDE-TRAIN 間のトラフィック (バイト数/日)

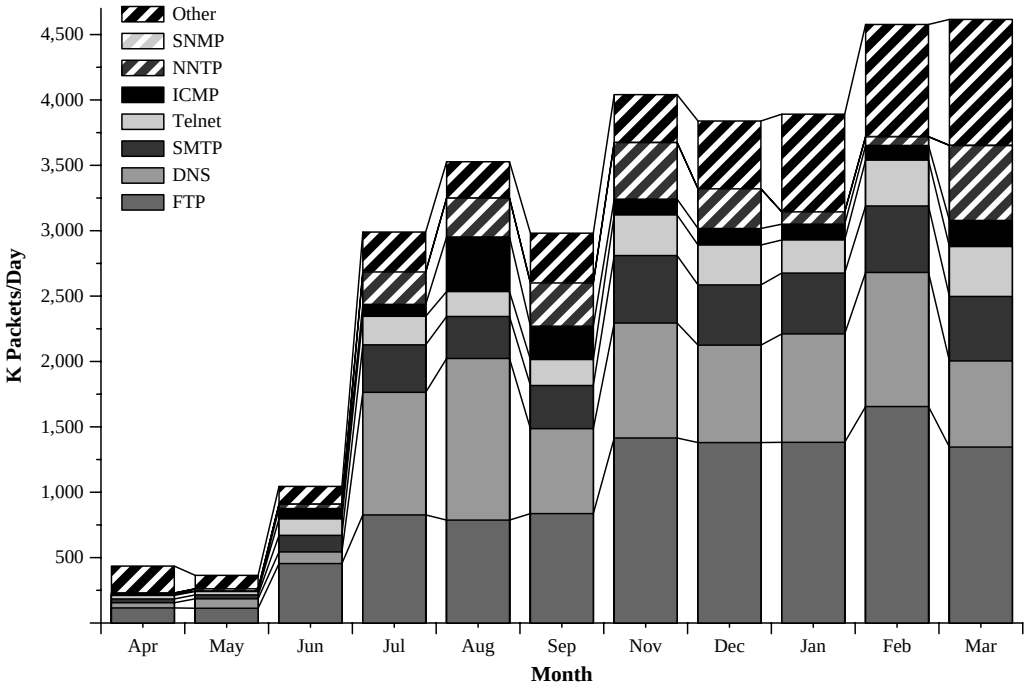

図 3.20: WIDE-TRAIN 間のトラフィック (パケット数/日)

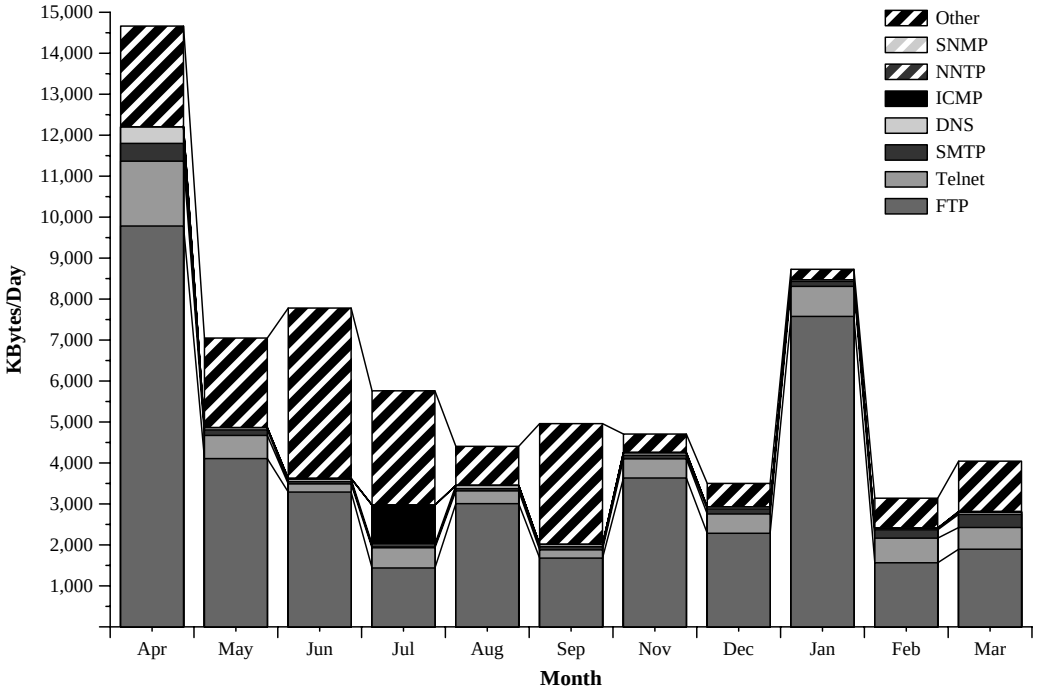

図 3.21: TISN-JAIN 間のトラフィック (バイト数/日)

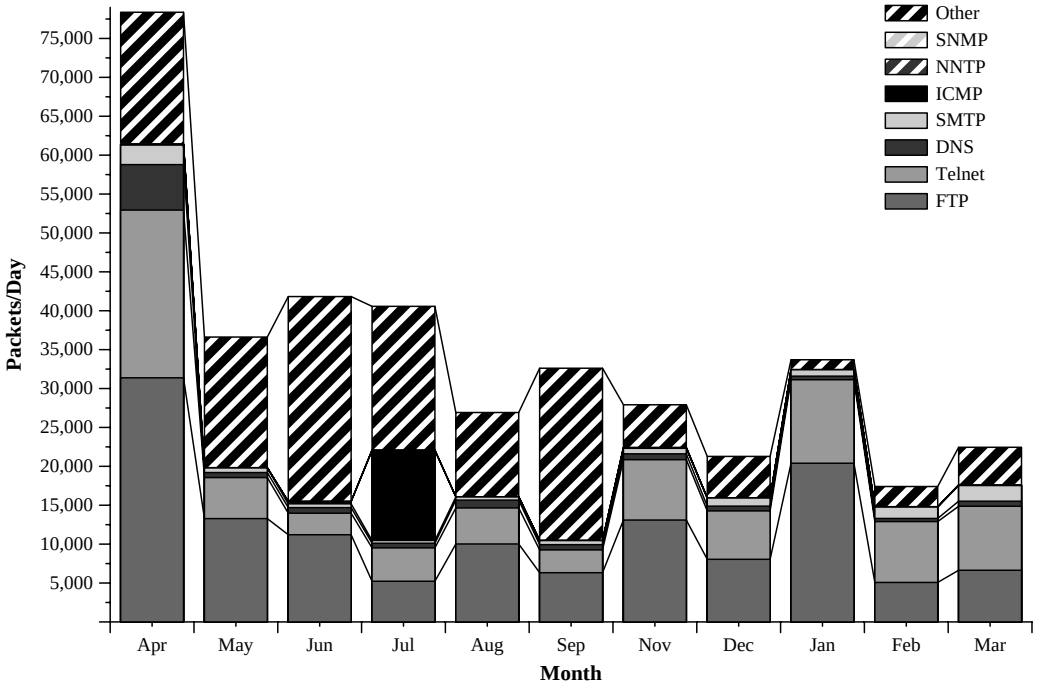

図 3.22: TISN-JAIN 間のトラフィック (パケット数/日)

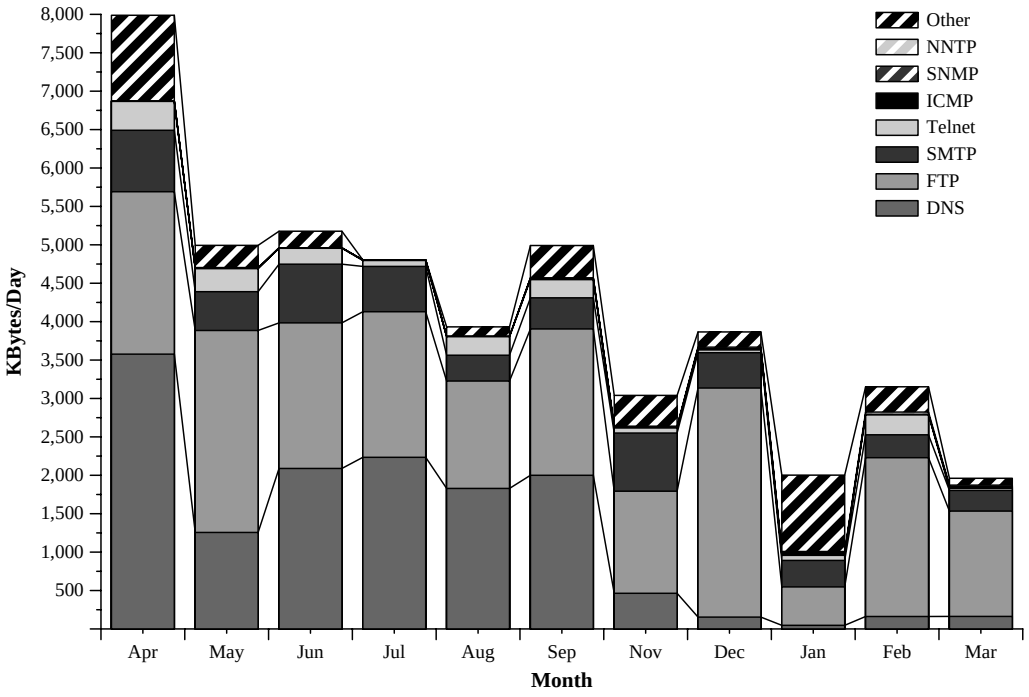

図 3.23: TRAIN-JAIN 間のトラフィック (バイト数/日)

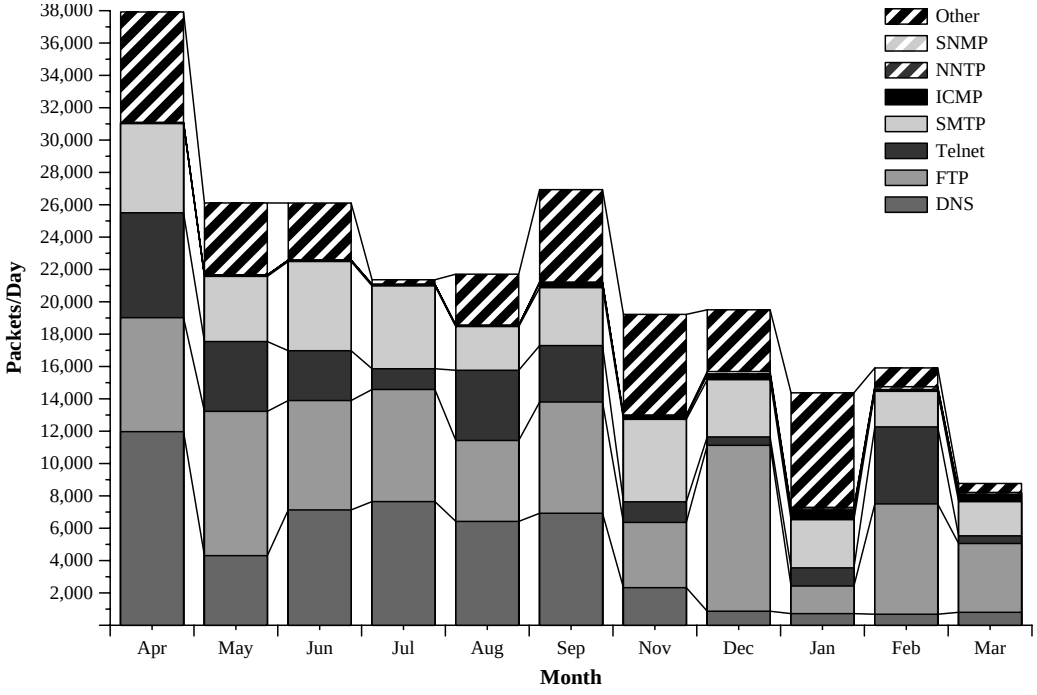

図 3.24: TRAIN-JAIN 間のトラフィック (パケット数/日)

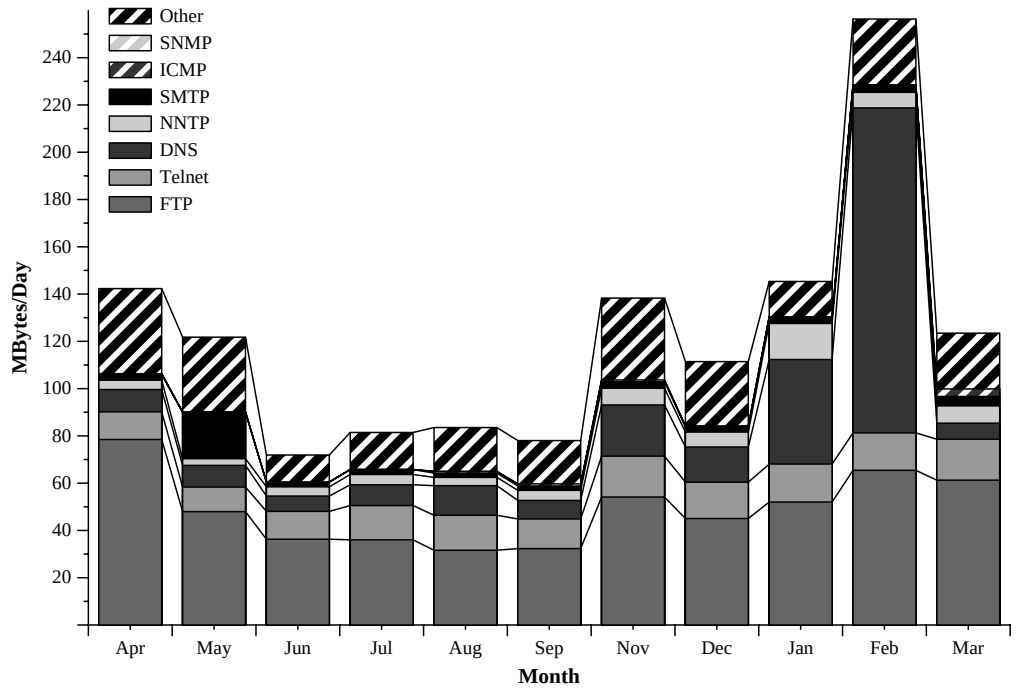

図 3.25: TRAIN-TISN 間のトラフィック (バイト数/日)

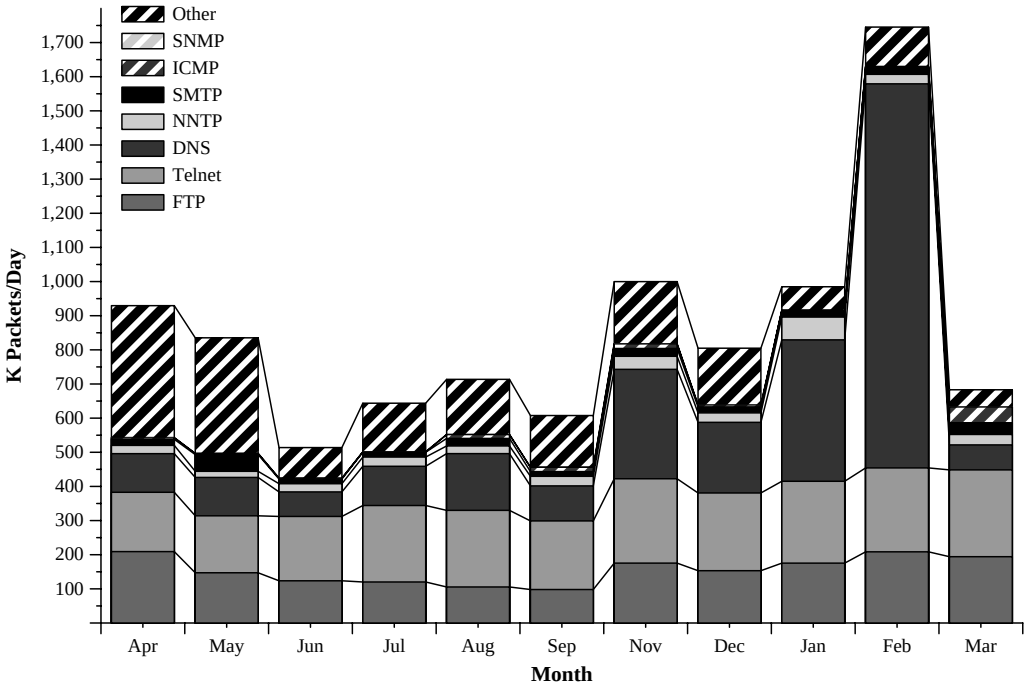

図 3.26: TRAIN-TISN 間のトラフィック (パケット数/日)

3.4 サイト間トラフィック解析

前年度までのトラフィック解析は、リンク上にどのようなプロトコルが流れるかを中心に行ってきた。93 年度は、前述の通り測定サイトの増設を行った。これにより WIDE バックボーンを構成する NOC 間の関わりあいを検証する事が可能となった。

本解析では、WIDE バックボーンを構成するリンク、KYO-HIJ, KYO-NAKASU, SFC-KYO, SFC-SND, TYO-SFC, TYO-SPK および国際線上を流れる全データに対し、どのサイト間のトラフィックであるかについて統計をとった。サイトとはある NOC に継っている下位組織を一塊に見たものとする。サイトの区分けは、福岡、広島、京都、奈良、大阪、藤沢、仙台、札幌、東京 NOC とした。また、WIDE バックボーンを構成するゲートウェイ等のノード郡も 1 サイトとした。区分けを行うにあたって、ftp.nic.ad.jp:/pub/inet/wide-config.ps を参照した。解析期間は 1994 年 3 月 20 日から 4 月 19 日までの一ヵ月間である。

グラフ表記は、サイトを FUK、HIJ、KYO、NARA、OSK、SFC、SND、SPK、TYO、WIDE およびそれ以外を * とした。また、グラフ上の数字は、期間中流れた全データに対する各サイト間トラフィックの占める割合である。

3.4.1 国際線におけるサイト別利用率

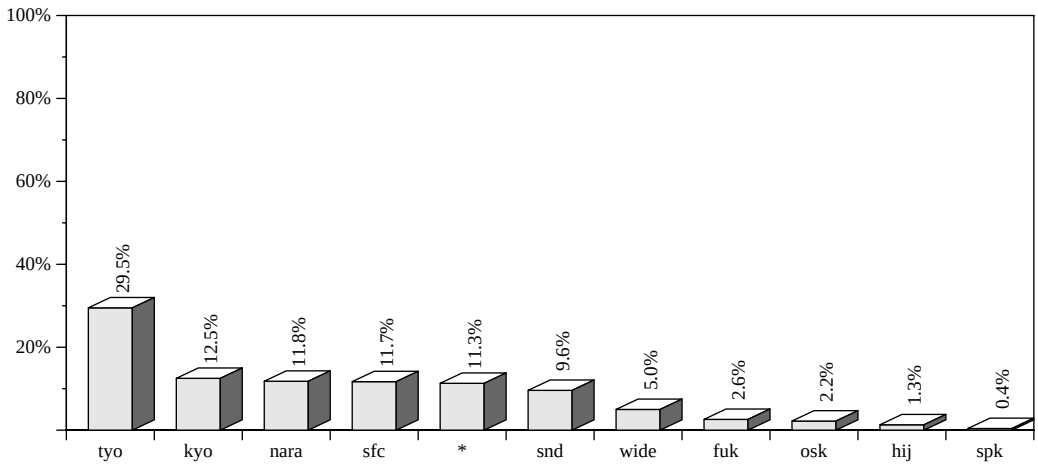

図 3.27: 国際線におけるサイト別利用率

3.4.2　京都、広島間リンクにおけるサイト別利用率

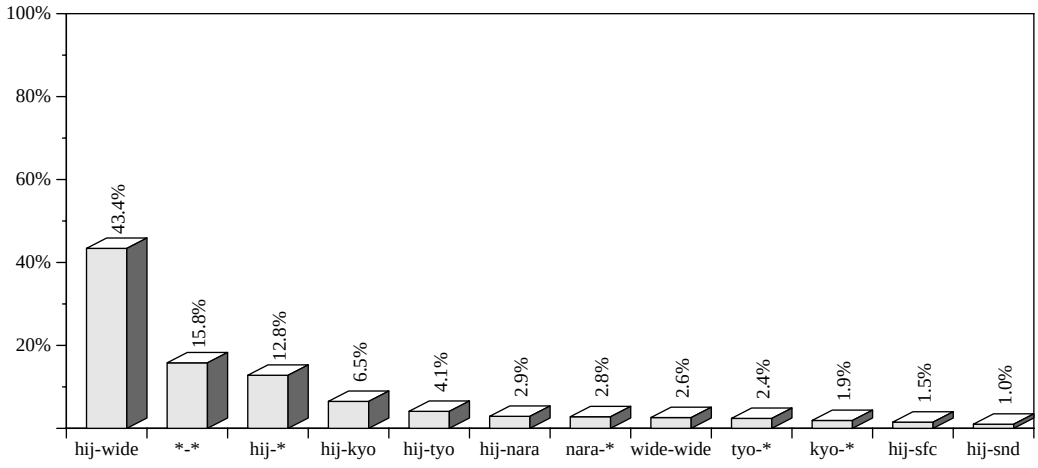

図 3.28: KYO-HIJ 間におけるサイト別利用率

3.4.3　京都、中州間リンクおけるサイト別利用率

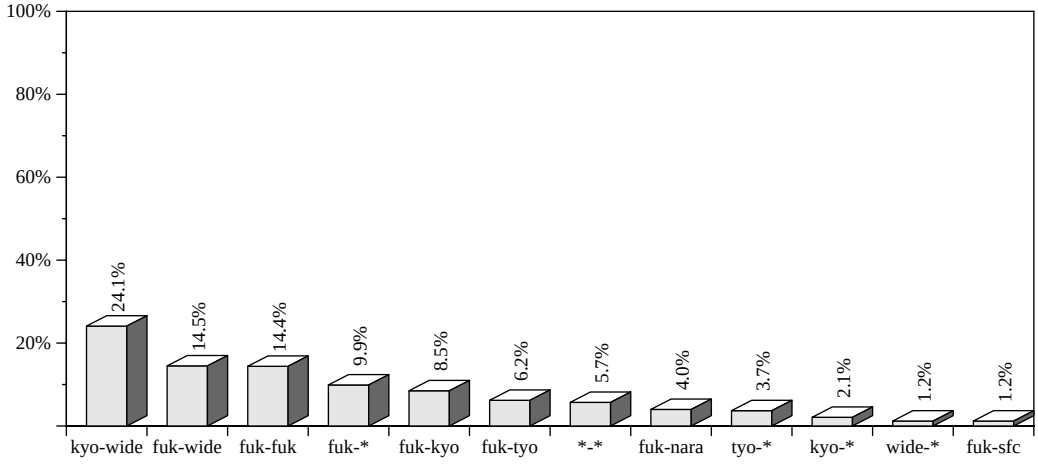

図 3.29: KYO-NAKASU 間におけるサイト別利用率

3.4.4 藤沢、京都間リンクにおけるサイト別利用率

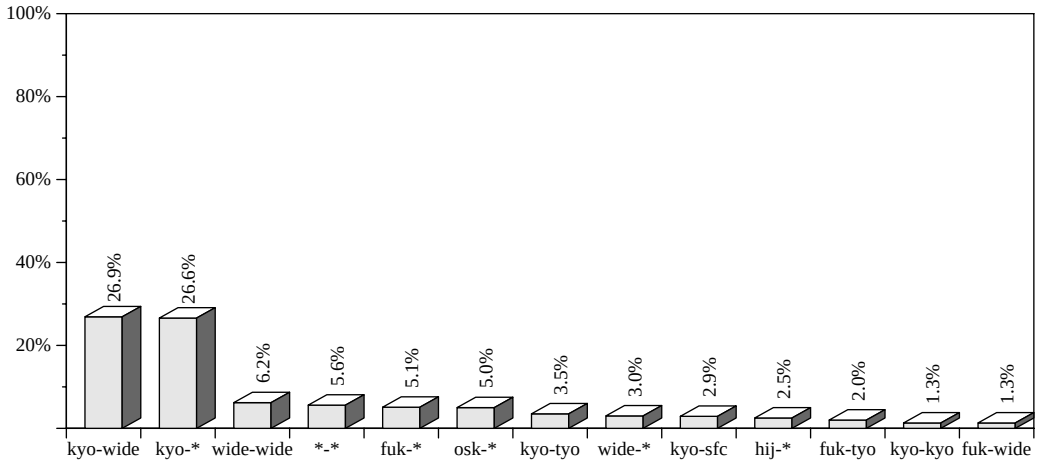

図 3.30: SFC-KYO 間におけるサイト別利用率

3.4.5 藤沢、仙台間リンクにおけるサイト別利用率

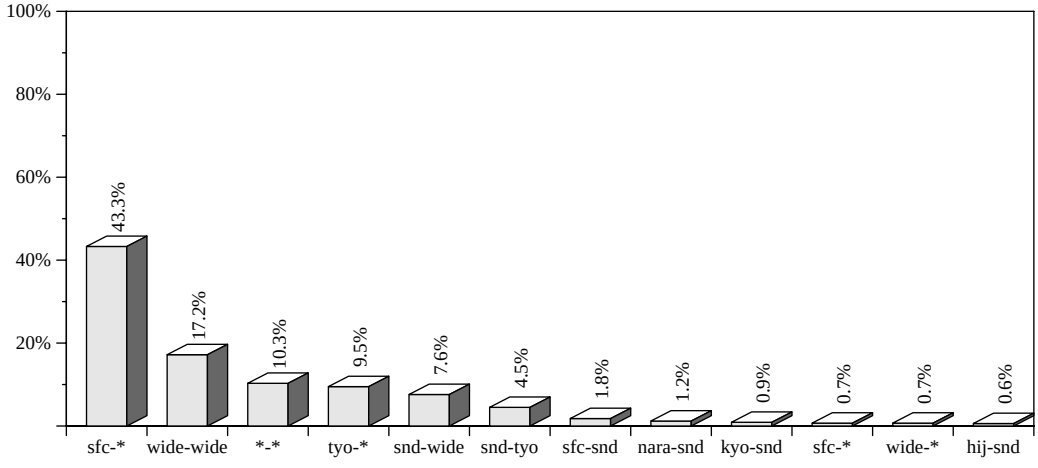

図 3.31: SFC-SND 間におけるサイト別利用率

3.4.6　東京、藤沢間リンクにおけるサイト別利用率

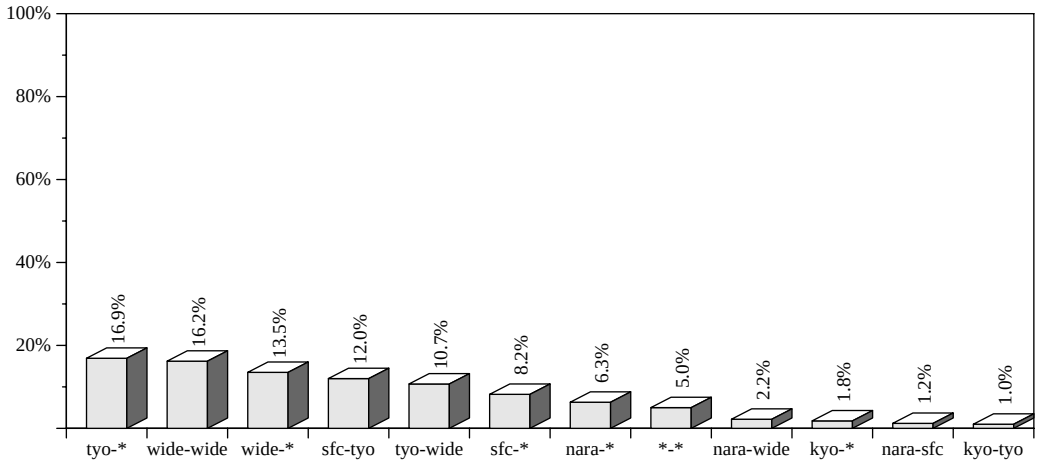

図 3.32: TYO-SFC 間におけるサイト別利用率

3.4.7　東京、札幌間リンクにおけるサイト別利用率

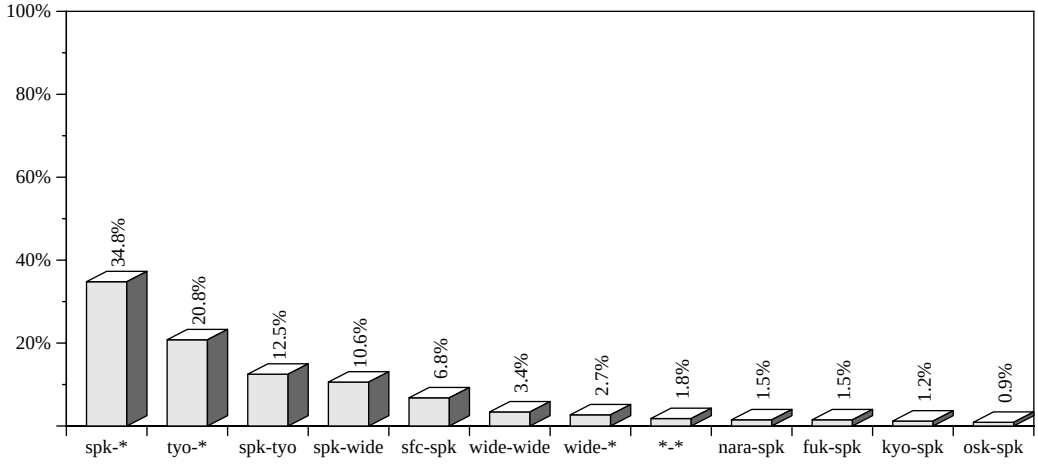

図 3.33: TYO-SPK 間におけるサイト別利用率

3.5 IPIP プロトコルの測定

サイト間のトラフィック解析に加え、新たに IPIP の解析も始めた。これは、近年、マルチキャストの需要が延び始め、トラフィック解析のニーズが増してきたためである。WIDE バックボーン上を流れるマルチキャストパケットの大部分は IPIP プロトコルで占められる。このため、マルチキャストの需要を調査するため、IPIP プロトコルの測定を始めた。

本解析では、一月分のデータを解析し、IP プロトコルのデータ中、IPIP プロトコルが占める割合を示したものである。期間は 1994 年 3 月 20 日から 4 月 19 日までである。表 3.5に、期間中、各リンク上に流れた IPIP, IP の総データ量、IP 中 IPIP の占める割合、および双方向における平均利用量を示す。

表 3.5: 全 IP プロトコル中、存在する IPIP プロトコルの割合

リンク	帯域幅 (Kbps)	IP/IP データ量 (byte)	IP/IP の割合 (%)	全データ量 (byte)	平均利用量 (Kbps)
INTER	192	96,840,414	0.15	62,879,379,158	188
KYO-HIJ	64	0	0.00	10,393,266,923	31
KYO-NAKASU	192	8,143,176,097	22.3	36,445,291,800	109
SFC-KYO	192	8,679,203,211	20.9	41,557,915,494	124
SFC-SND	64	0	0.00	17,005,219,446	51
TYO-SFC	384	18,587,996,555	16.7	111,437,088,949	333
TYO-SPK	64	95,897,996	1.42	6,734,777,887	20

第 4 章

ネットワークモニター情報の自動統計機構

4.1 はじめに

コンピューターネットワークをモニターし、その情報を集計して何らかの統計を取ることは、ネットワークを運用維持していく上で必ず必要とされることである。どのような情報をモニターし、どのような統計を取るかは、そのネットワークの運用管理の方針によって異なるであろう。しかし、一度それが決定されたならば、ある一定の期間継続して、その方針に従った統計が取られることになる。

WIDE インターネットでは、すでに、そのようにして統計が取られているのである。しかし、ネットワークをモニターする機構と、統計を取る機構がリンクしていないために、統計処理のために大きな労力を要することがしばしばあった。そこで、これらをリンクさせ、ある程度自動的に統計情報を作成するソフトウェアを設計実装した。現在、これを実験的に運用している。ここでは、このソフトウェアの設計仕様について述べる。実験運用の結果、あるいは評価については、来年度の報告書で述べられるであろう。

このソフトウエアは、ネットワーク管理システム IPANeMa として、IPA からリリースされているソフトウエアの一部である。IPANeMa は、IPA と WIDE プロジェクトが共同開発したものである。

4.1.1 概要

このソフトウエアは、特定ネットワーク上で観察できるホスト間の通信状態、またはネットワーク間の通信状態に関する統計情報を生成する。生成された統計情報はファイルに格納する。

統計情報として得られるものは以下の通りである。

- ホスト間またはネットワーク間で送受信された総パケット数、バイト長
- ホスト間またはネットワーク間で送受信された平均パケット数、バイト長 (1 秒当たりの値)
- ホスト間またはネットワーク間で送受信された最大パケット数、バイト長 (時刻とともに)

このソフトウエアは、ネットワークモニタリングデーモン、ロギングデーモン、スタットデーモンから成る。

- ネットワークモニタリングデーモン (NMD)

  nit デバイスを用いて、イーサネットを流れるパケットをモニターする。

- ロギングデーモン (LOGD)

  ネットワークモニタリングデーモンからモニタリングデータを取得して１次レベルの統計処理を行い、その結果をスタットデーモンに渡す。１次レベルの統計処理とは、指定された単位時間分のモニタリングデータを統計することである。

- スタットデーモン (STATD)

  ロギングデーモンから、１次レベルの統計情報を受取り、それをファイルに落とす。さらに、２次レベル以上の統計処理を行う。これは、単位時間分の統計ファイルが、ある時間分に達したら、その時間分の統計ファイルを作成するものである。１次レベルの統計ファイル、あるいは、低次レベルの統計ファイルを読み込んで、より大きな時間分の統計ファイルを作成する。

スタットデーモン、ロギングデーモン、および、ネットワークモニタリングデーモンの関係を図 4.1 に示す。図 4.1 では、ロギングデーモンとスタットデーモンは、異なる W/S 上で動作しているが、同一の W/S 上で動作することも可能である。

ロギングデーモンとスタットデーモン間の通信は、SUN XDR/RPC で実現されている。スタットデーモンが起動されるに、新たなロギングデーモンが一つ起動され、さらに、新たなネットワークモニタリングデーモンが一つ起動される。スタットデーモンの終了と同時に、ロギングデーモン、ネットワークモニタリングデーモンも終了する。

4.1.2 統計処理パラメータ

以下のようなパラメータがある。これらのパラメータは、スタットデーモンの起動時のパラメータおよびコンフィグファイルで指定する。

(1) 時間パラメータ

統計処理の対象となるデータを集める時間や、処理終了までの時間を指定する。

(2) プロトコルパラメータ

処理対象とするレイヤやプロトコルを指定する。

データリンク層 (イーサネット) を指定した場合には、任意の上位プロトコルごと (タイプごと) の統計情報を生成する。

ネットワーク層を指定した場合には、ネットワークプロトコルとして IP(TCP/IP) または IDP(XNS) のいずれかの任意の上位プロトコルごとの統計情報を生成する。

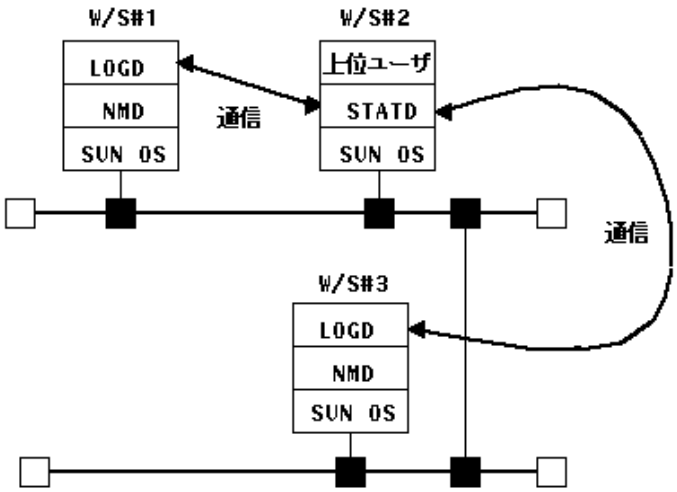

図 4.1: デーモンどうしの関係

なお、ネットワークプロトコルとして IP を指定し、かつ上位プロトコルとして TCP または UDP を指定した場合には、更に任意のポート番号ごとの統計情報を生成する。

(3) アドレスパラメータ

処理対象とするアドレスについての情報を指定する。パラメータには、アドレスタイプとアドレス値を指定する。

- アドレスタイプ　(必須)
  イーサネットアドレス、インターネットアドレスまたはネットワークアドレス。
- アドレス値　(任意)
  アドレスタイプに応じた値。イーサネットアドレス値、インターネットアドレス値またはネットワークアドレス値。複数個の指定が可能。

4.1.3　統計情報

スタットデーモンは、統計情報をアドレスファイルと統計ファイルの二種類に分けて格納する。

(1) アドレスファイル

指定された各パラメータと、モニター結果として得られたアドレス情報を格納する。アドレス情報は、原則として出現順に格納する。本ファイルは、スタットデーモンの起動ごとに一つだけ生成される。

(2) 統計ファイル

ホスト間またはネットワーク間での統計データを格納する。本ファイルは、指定された単位時間ごとに一つ生成される。また、ある時間に達したら、それまでのいくつかの統計ファイルをまとめて、より長い時間分の統計ファイルが生成される。

4.2 スタットデーモン

スタットデーモンは、ユーザが作成したパラメータの定義ファイル (コンフィグファイル) に従った統計処理を行い統計情報を生成する。生成した統計情報は、一定時間ごとにファイルに格納する。また、このように生成された複数のファイルに対して更に統計処理を行い、より上位レベルの統計情報を生成する。この処理をレベルアップ処理と呼ぶ。

レベルアップ処理では、スタットデーモンが自動的に処理を行う場合と、ユーザが手動で処理を行う場合の二種類がある。

スタットデーモン起動の方法は、即時開始と指定時刻開始の二種類がある。開始時刻は、月、日、時などで指定が可能である (at コマンドの表記に従う)。

スタットデーモンの提供する機能は、以下の四つに分けられる。

- 統計処理パラメータの取得 (コンフィグファイルの読み込み)
- ロギングデーモンの制御
- 統計情報のファイル生成
- 統計レベルアップ処理

4.2.1 統計処理パラメータの取得

時間パラメータのみ起動時のコマンド引数として与えられ、それ以外のパラメータはコンフィグファイルによって与えられる。

(1) 時間パラメータ

スタットタイム	統計情報を生成する単位時間 (秒)
スタットピリオド	統計処理の開始から、終了までの時間 (秒) (スタット・タイムより大きな値)

レベルアップ処理を指定した場合、スタットタイムの値は、その値より大きなレベルアップ周期の約数でなければならない。ただし、最大のレベルアップ時間 (24 時間) 以上の値の場合には任意の値が指定できる。レベルアップ処理を指定しない場合には、スタットタイムは任意の値を指定できる。

(2) プロトコルパラメータ

統計処理の対象とするレイヤおよびプロトコルを指定する。

(3) アドレスパラメータ

収集するホスト情報として、アドレスのタイプおよびアドレス値を指定する。

ここでアドレスを指定すると、そのアドレスを送受信先とするパケットのみが統計処理の対象となる。また、この時、アドレスファイルには、ここで指定された順番にアドレスが書き込まれる。

(4) レベルアップ処理パラメータ

レベルアップ処理を実施するかどうかを指定する。

4.2.2　ロギングデーモンの制御

指定されたパラメータに従って、ロギングデーモンを起動、あるいは、終了する。

スタットピリオドの指定が ”無限” の場合には、ユーザからの停止要求を受けるまで処理を続ける。

(1) コネクション制御

ロギングデーモンとの間にコネクションの確立および解放を行う。一定時間 (サービスタイムアウト時間) の間、ロギングデーモンのインタフェースが使用されない場合、確立されたコネクションはロギングデーモンによって解放される。

(2) サービス制御

サービスの開始、停止および属性の読み出しを行う。サービスとは、ロギングデーモンとの通信サービスである。

(3) ロギング制御

上記サービスを用いて、ロギングの開始、停止、属性の操作および統計情報の読み出しを行う。

4.2.3　統計情報のファイル生成

リモートまたはローカルホスト上で動作するロギングデーモンから、統計情報を取得して統計ファイルを生成する。統計ファイルは、スタットタイムで指定された時間ごとに生成される。

この統計ファイルとは別に、アドレスファイルが生成される。アドレスファイルは、スタットデーモン１個につき、ひとつ生成される。コンフィグファイルのアドレスパラメータでアドレスが指定されていない限り、モニターしたアドレスが出現順に書き込まれる。

(1) アドレスファイル名

生成されるファイルは、起動時に指定された文字列に以下の文字列を付け足したものである。

ファイル拡張子: sadr

例えば、ユーザが指定した文字列が ”log ”である場合、log.sadr となる。

(2) 統計ファイル名

生成されるファイルは、起動時に指定された文字列に以下の文字列を付け足したものである。

西暦年月日、時分秒 (YYMMDD_HHMMSS)
統計レベル (_u または_l1 から_l4)
ファイル拡張子: sadr

例えば、ユーザが指定した文字列が ”log ”である場合、スタットタイムごとに生成される統計データファイル名は、log940102_034500_u.sdat のようになる。

4.2.4 統計レベルアップ処理

複数の統計ファイルをまとめて、上位の統計ファイルを生成する。統計レベルアップ処理の対象となるファイルは、共通のアドレスファイルを持つ統計ファイルでなければならない。

上位の統計ファイルは、下位の統計ファイルの各項目を合計した合計ファイルと、下位の統計ファイルの各項目をくし刺しにして最大値をまとめた最大ファイルの二通りである。合計ファイルは、単位時間ごとの統計ファイルと同じデータ構造である。これらのファイルのデータ構造については、後に説明する。

(1) レベルアップ周期

原則として以下の周期でレベルアップを行なう。

1 分
10 分
1 時間
1 日

(2) ファイル名

合計ファイルの拡張子は、統計データファイルと同様 ”.sdat ”である。
最大ファイルの拡張子は、”.smax ”である。

4.2.5　プロセス構成

スタットデーモンは、スタットプロセスと、レベルアッププロセスから成っている。スタットプロセスは、スタットデーモン起動によって起動される。

レベルアップ処理の指定がある場合には、スタットタイム分のロギングデータの取得が終わった時点でレベルアップ周期に、スタットプロセスによって、レベルアッププロセスが必要な個数だけ起動される。

スタットプロセスが 1 次統計ファイルを生成し、レベルアッププロセスが、上位統計ファイル、すなわち、合計ファイルと最大ファイルを生成する。

4.2.6　モジュール構成

スタットデーモンのモジュール構成を以下に示す。

```
スタットデーモン  - start_stat  - get_statpram（統計パラメータ取得）
                                - mkstatadrf（アドレスファイルの生成）
                                - apstatadrf（アドレスデータ取得）
                                - statdataf（統計データ取得）
                                - levelup（統計レベルアップ）    - nssum
                                                                 - nsmax
                  - stop_stat
                  - ps_stat
                  - at_stat
                  - atq_stat
                  - atrm_stat
                  - nssum
                  - nsmax
```

(1) start_stat

スタットデーモンを起動するコマンドである。

```
% start_stat host stat-time stat-period string config-file

host            :ロギングデーモンの動作しているホスト名
stat-time       :スタットタイム (秒)
stat-period     :統計処理の終了までの時間 (秒)  (0: 無限指定)
string          :アドレスファイル、統計ファイルの識別名
config-file     :コンフィギュレーションファイルの名前
```

(2) stop_stat

スタットデーモンを停止させるコマンドである。

```
% stop_stat process-id

process-id      :スタットデーモンのプロセス ID
```

(3) ps_stat

既に起動されているスタットデーモンを表示するコマンドである。

```
% ps_stat [process-id]

process-id      :スタットデーモンのプロセス ID
```

(4) at_stat

時刻を指定してスタットプロセスを起動するコマンドである。at コマンドのジョブキューとして z を使用する。

```
% at_stat  time host stat-time stat-period string config-file

time            :at コマンドに使用可能な時刻パラメータ
host            :ロギングデーモンの動作しているホスト名
stat-time       :スタットタイム (秒)
stat-period     :統計処理の終了間での時間 (秒)  (0: 無限指定)
```

```
string          :アドレスファイル、統計ファイルの識別名
config-file     :コンフィギュレーションファイルの名前
```

(5) atrm_stat

at_stat コマンドで起動予約したスタットデーモンの起動を取り消すコマンドである。

```
% atrm_stat  job-id

job-id          :atq_stat によって表示されるジョブ ID
```

(6) atq_stat

スタットデーモンの予約状況を表示するコマンドである。未起動のジョブのみが表示される。すでに起動されたジョブは、ps_stat コマンドによって表示される。

```
% atq_stat  [job-id]

job-id          :予約されているスタットデーモンのジョブ ID
```

(7) nssum

複数の統計ファイルから、合計ファイルを作成する、すなわち統計レベルアップを行なうコマンドである。

各統計ファイルは、アドレスファイルを共有し、かつ同じスタットタイムで作成されたものでなければならない。

```
% nssum  [-w] in-files -o out-file

[-w]            :入力ファイルが生成されるまで待ち合わせを行う。(無限)
in-file         :入力統計データファイル (一つ以上)
out-file        :出力ファイル
```

(8) nsmax

複数の統計ファイルから、最大ファイルを作成する、すなわち統計レベルアップを行なうコマンドである。

各統計ファイルは、アドレスファイルを共有し、かつ同じスタットタイムで作成されたものでなければならない。

```
% nsmax  [-w] in-files -o out-file

[-w]            :入力ファイルが生成されるまで待ち合わせを行う。(無限)
in-file         :入力統計データファイル (一つ以上)
out-file        :出力ファイル
```

4.2.7 コンフィグファイル

コンフィグファイルでは、表 4.1 のようなパラメータを指定することができる。

各行はキーワード、等号、数値または文字列 (予約語) からなる。各々はスペースまたはタブで区切られていなければならない。なお、空行または行の最初にシャープ記号のある行は無視する。

以下に、コンフィグファイルの例を示す。

```
#
#       -- Configuration File --
#

#level-up      = YES NO

#filter = DL_ETHER NW_XNS NW_IP
#
#       << for ethernet >>
#upper-filter   = 0x0600 0x0800 0x0806 0xffff
#       << for xns      >>
#upper-filter   = 1 4 5
#        << for ip       >>
#upper-filter   = 1 6 17
#option-filter    = 20 23 25
```

```
#
#address-type   = ETHERNET INTERNET NETWORK
#
#address        =
#       << for ethernet >>
#address        = 0x0800200ad2a1
#       << for xns      >>
#address        = 0x00000080/0x08003700dcb1
#       -- network
#address        = 0x00000082
#       << for ip       >>
#address        = 131.221.64.80
#       -- network
#address        = 131.221.64.0
#netmask        = 255.255.64.0
#       ---------------------------------------------

level-up        = YES

filter          = NW_IP

#      ICMP, TCP, UDP

upper-filter    = 1
upper-filter    = 6
option-filter    = 23
option-filter    = 20
option-filter    = 21
option-filter    = 25
option-filter    = 43
option-filter    = 53
option-filter    = 119
option-filter    = 123

#       UDP
upper-filter    = 17
option-filter    = 53
option-filter    = 69
option-filter    = 517
```

```
option-filter    = 2049         #nfs
option-filter    = 520

address-type     = INTERNET
```

表 4.1: コンフィグファイルで指定するパラメータ

キーワード	説明
level-up	レベルアップするかしないか (YES / NO)
filter	レイヤ、プロトコルの指定 (DE_Ether / NET_IP / NET_XNS)
upper-filter	上位プロトコル番号 (filter = NET_IP の場合は、 TCP, UDP, ICMP 等のプロトコル番号)
option-filter	ポート番号 (filter = NET_IP の場合のみ有効)
address-type	収集するアドレスのタイプ (ETHERNET / INTERNET / NETWORK)
address	プロトコルに準じた論理アドレス これを指定すると、そのアドレスへの送受信 パケットのみが統計の対象となる。
netmask	address-type = NETWORK で、filter = NET_IP のとき、address を指定する場合は必ず、 ネットマスクも指定しなければならない。

4.2.8 統計ファイルのデータ構造

以下に、アドレスファイルと、1 次レベル統計ファイル / 合計ファイルを読み込んだ表の例と、合計ファイルを読み込んだ表の例を、それぞれ 表 4.2、表 4.3 に示す。それぞれの統計ファイルはバイナリで書かれている。

4.3 ロギングデーモン

ロギングデーモンは、スタットデーモンからの要求に応じて、ネットワークをモニターし、その情報を指定された時間分だけロギングする。ロギングしながら、一次レベルの統計処理を行ない、その結果をスタットデーモンに渡す。これらの処理は全てメモリー上で行なわれ、、ファイルにデータが出力されることはない。

表 4.2: １次レベル統計データ / 合計データの表

src / dst		addr#1		addr#n		OTHERS		合計		平均	
		pkts	len	pkts	len	pkts	len	pkts	len	pkts	len
addr#1	TCP	0	0	10	100	0	0	10	100	1	10
	(ftp)	0	0	5	50	0	0	5	50	0.5	5
	(smtp)	0	0	5	50	0	0	5	50	0.5	5
	UDP	0	0	10	100	0	0	10	100	1	10
	ICMP	0	0	0	0	0	0	0	0	0	0
	Others	0	0	0	0	0	0	0	0	0	0
	Total	0	0	20	200	0	0	20	200	2	20
addr#n	TCP	0	0	10	100	0	0	10	100	1	10
	(ftp)	0	0	5	50	0	0	5	50	0.5	5
	(smtp)	0	0	5	50	0	0	5	50	0.5	5
	UDP	0	0	10	100	0	0	10	100	1	10
	ICMP	0	0	0	0	0	0	0	0	0	0
	Others	0	0	0	0	0	0	0	0	0	0
	Total	0	0	20	200	0	0	20	200	2	20
OTHERS	TCP	0	0	0	0	0	0	0	0	0	0
	(ftp)	0	0	0	0	0	0	0	0	0	0
	(smtp)	0	0	0	0	0	0	0	0	0	0
	UDP	0	0	0	0	0	0	0	0	0	0
	ICMP	0	0	0	0	0	0	0	0	0	0
	Others	0	0	0	0	0	0	0	0	0	0
	Total	0	0	0	0	0	0	0	0	0	0
合計	TCP	0	0	20	200	0	0	20	200		
	(ftp)	0	0	10	100	0	0	10	100		
	(smtp)	0	0	10	100	0	0	10	100		
	UDP	0	0	20	200	0	0	20	200		
	ICMP	0	0	0	0	0	0	0	0		
	Others	0	0	0	0	0	0	0	0		
	Total	0	0	40	400	0	0	40	400		
平均	TCP	0	0	2	20	0	0			2	20
	(ftp)	0	0	1	10	0	0			1	10
	(smtp)	0	0	1	10	0	0			1	10
	UDP	0	0	20	200	0	0			2	20
	ICMP	0	0	0	0	0	0			0	0
	Others	0	0	0	0	0	0			0	0
	Total	0	0	4	40	0	0			4	40

表 4.3: 最大データの表

src / dst		addr#1				...	合計の最大			
		時刻	pkts	時刻	len		時刻	pkts	時刻	len
addr#1	TCP	10:20:30	10	10:20:30	100		10:20:30	10	10:20:30	100
	(ftp)	10:20:30	5	10:20:30	50		10:20:30	5	10:20:30	50
	(smtp)	10:20:30	5	10:20:30	50		10:20:30	5	10:20:30	50
	UDP	10:20:30	10	10:20:30	100		10:20:30	10	10:20:30	100
	ICMP		0		0			0		0
	Others		0		0			0		0
	Total	10:20:30	20	10:20:30	200		10:20:30	20	10:20:30	200
...										
合計の最大	TCP	10:20:30	10	10:20:30	100		10:20:30	10	10:20:30	100
	(ftp)	10:20:30	5	10:20:30	50		10:20:30	5	10:20:30	50
	(smtp)	10:20:30	5	10:20:30	50		10:20:30	5	10:20:30	50
	UDP	10:20:30	10	10:20:30	100		10:20:30	10	10:20:30	100
	ICMP		0		0			0		0
	Others		0		0			0		0
	Total	10:20:30	20	10:20:30	200		10:20:30	20	10:20:30	200

ロギングデーモンは複数のスタットデーモンからの要求を、同時に受け付けることができる。ただし、ネットワークモニタリングデーモンの設定によって、その数は制限される。

ロギングデーモンの提供する機能は以下の三種類に分けられる。

- コネクション制御
- サービス制御
- ロギング制御

4.3.1　コネクション制御

ロギングデーモン、および、ネットワークモニタリングデーモンは、inetd に登録して使用する。従って、ロギングデーモンとスタットデーモンとの間のコネクションの確立は inetd によって行われる。

スタットデーモンからの要求に応じてスタットデーモンとの間に確立されたコネクションの解放を行う。ただし、ロギングデーモン内でサービスタイムアウトが発生した場合、またはエラーを検出した場合にはロギングデーモンが能動的にコネクションの解放を行う。

4.3.2　サービス制御

(1) サービスの開始

スタットデーモンからの要求に応じて、ロギングサービスの使用権をスタットデーモンに与える。ただし、既に最大サービス数に達している場合にはエラーを通知する。なお、本サービスはタイムアウト値を持つ。一定時間スタットデーモンとロギングデーモンとの間でアイドル状態が継続するとロギングデーモンはスタットデーモンに与えたサービス使用権を無効とすると同時にコネクションの解放も行う。

(2) サービスの停止

スタットデーモンからの要求に応じて、ロギングサービスの使用権を無効とする。すなわち、既に開始されているサービスを停止する。サービスが開始されていない場合にはエラーを通知する。

(3) サービス属性の通知

スタットデーモンからの要求に応じて、サービスの属性を通知する。ロギングデーモンが提供するサービス属性には以下のものがある。なお、サービス属性に対するスタットデーモンの操作は読み出しのみを許す。

属性	説明

現ステータス	サービスの状態
空サービス数	使用可能なサービス数
タイムアウト値	サービスのタイムアウト値

4.3.3 ロギング制御

ロギングは以下のロギング属性に従って行われる。

属性	説明
時間パラメータ	どのくらいの間ロギングするか、その時間
プロトコルパラメータ	レイヤ（データリンク層 または ネットワーク層） ネットワーク層の場合、IP または XNS
上位プロトコルパラメータ	上位プロトコル番号 プロトコルパラメータが IP の場合は、 TCP, UDP, ICMP 等のプロトコル番号
オプションパラメータ	ポート番号 プロトコルパラメータが IP の場合のみ有効 さらに、上位プロトコルパラメータが TCP または UDP である場合に限り、これを指定できる。
アドレスパラメータ	ロギングの対象とするアドレスタイプ、および アドレス。アドレスはアドレスタイプに従った 値でなければならない。

アドレスタイプとして、以下の３通りがある。

アドレスタイプ	プロトコル	備考
イーサネットアドレス	-	6 バイト
インターネットアドレス	IP	4 バイト
	XNS	10 バイト
ネットワークアドレス	IP	8 バイト (netmask & netnumber)
	XNS	4 バイト

(1) ロギング属性の読みだし

スタットデーモンからの要求に応じて、現在設定されているロギング属性の値を通知する。

(2) ロギング属性の変更

スタットデーモンからの要求に応じて、ロギング属性の値を変更する。なお、この要求はロギングが開始されていない状態でのみ受け付ける。ロギングが開始されている場合には、処理を行わずにエラーを通知する。

(3) ロギング開始

スタットデーモンからの要求を受け付けてロギングを開始する。スタットデーモンによって指定されたロギング属性、またはデフォルトに従った統計処理を開始する。既に開始されている場合には処理を行わずにエラーを通知する。　ロギングされたアドレスデータと統計データは、スタットデーモンからの統計データの読み取り要求が到達するまで、ロギングデーモン内部に保持する。

(4) アドレスデータ通知

ロギングデータの収集、統計処理の対象となったアドレスを通知する。スタットデーモンからの要求時点でまだ通知していないアドレスデータのみを通知する。

(5) ロギングデータ通知

スタットデーモンからの要求を受け付け、スタットタイム当たりのロギングデータを転送する。ロギングデータは、データのサイズに応じて、一回以上の要求により全てのデータを転送する。ロギングデータとは、ネットワークモニタリングデーモンから得たモニタリング情報をロギング属性に従って統計処理した結果である。

通信の負荷を軽くするため、統計結果が 0 の項目は転送しない。

(6) ロギング停止

スタットデーモンからの要求に応じて、ロギング処理を停止する。既に停止されている場合には処理を行わずにエラーを通知する。

4.3.4　プロセス構成

ロギングデーモンは、スタットデーモンからの要求で、inetd から起動される。そして、コネクションが終了すると同時に終了する。ロギングデーモンは、ネットワークモニタリングデーモンと、SUN XDR/RPC で通信することにより、モニタリングデータを取得する。ロギングデーモンは、取得したモニタリングデータを統計処理して、スタットデーモンに渡す。

ロギングデーモンは、同一ホスト上で複数が同時に動作できる。

4.3.5　モジュール構成

ロギングデーモンのモジュール構成を以下に示す。

ロギングデーモン
- get_service_props （サービス属性の通知）
- logon （サービス開始）
- get_stat_props （統計属性の通知）
- change_stat_props （統計属性の変更）
- start_stat （ロギング開始）
- get_stat_addr （アドレスデータの通知）
- get_stat_data （統計データの通知）
- stop_stat （ロギング停止）
- logoff （サービス停止）
- discon_service （コネクション開放）

4.4 おわりに

現在、統計ファイルを読み込んで、表とグラフを表示するユーザーインタフェース、および、スタットデーモンをコントロールするユーザーインタフェースを開発中である。これらは、ネットワーク管理システム IPANeMa に組み込まれる。

この自動統計機構によって、ネットワークのトラフィックを定常的に監視し、より効率的にネットワークを運用するための、高度の統計情報の提供をめざす。

第 5 章

まとめと今後の課題

本報告では、93 年度に行ったデータの収集および解析結果に基づき、WIDE インターネット上のトラフィックについての考察を行った．とくに、WIDE バックボーンにおける、各 NOC 間のトラフィックにも注目し、各 NOC 間のデータのやりとりがバックボーンの各リンクに与える負荷についても分析した。

また、統計データの収集解析と言う観点から、現在用いている NNStat によるデータ収集・解析方法のみではなく、新しいデータ収集および統計解析のためのツールに関する考察も行った。

93 年度における測定サイトの拡大により、WIDE バックボーンの 2/3 をカバーすることができた。しかしながら、NARA サイトに継るリンクを中心に大量のトラフィックがながれていると予想されるリンクが測定されていない。これは、NARA サイトを繋ぐルータが CISCO で構成され、トラフィック収集に利用しているソフトウェア NNStat が CISCO 上では作動しないことが大きな要因となっている。94 年度は、本年度に考察した新しいツールの利用などを通じて、これらの問題をどのように解決していくかを検討し、実現を目指す。

また、測定内容に関しても、緊急時や、様々な解析に対処できるように、比較的細かい時間間隔でのデータを収集するようにしている。しかしながら、測定対象、測定サイトが増加したため、収集されるデータ量も一月に 2.2G と莫大なものとなっている。測定サイトの拡大とともにアーカイブ技術の研究も進めていく事が今後は不可欠である。

94 年度はこれらの成果をもとに更に効率の良いデータ収集・解析・アーカイブの環境の実現を目指すとともに、解析の結果得られるグラフなどのデータをビジュアルな形で提供していく手法についての考察も行う予定である。