第XV部

IRCの運用状況とデータ解析

第 15 部
IRC の運用状況とデータ解析

第 1 章　はじめに

WIDE プロジェクト IRC 分科会では、国際的に大規模な IRC (Internet Relay Chat) 網である IRCnet に参加して IRC サーバを複数運用している。そして、以下のような目的をもって複数の活動を行ってきている。

- インターネット上での分散会話環境の長期安定的な提供
- 大規模ユーザ利用サーバの実証的実験
- ユーザの利用データからインターネット利用状況変化などの調査分析
- ユーザの認証や接続制限や分散サーバへのユーザの適切な誘導の試み
- DoS 攻撃などが多い環境を利用した DoS 攻撃などへの対策
- 踏み台ホストを利用して IRC サーバを利用することが多いことに対するそれらの調査

第 2 章では IRC サーバの運用状況とともに、ユーザ利用状況とその分析によって得られた結果を報告する。

第 3 章では IRC サービスに対してなされる DoS 攻撃への対策とネットワーク構成などについて報告する。

第 2 章　IRC の利用状況と分析

2.1 運用状況と全体利用状況

ここでは、WIDE プロジェクトのサーバが接続参加している国際的な大規模 IRC 網である IRCnet に関して、その国内部分の運用状況と利用状況分析を述べる。

図 2.1 は IRCnet の国内ユーザ数の 1997 年からの推移を表わしている。WIDE インターネットを利用した IRC サーバは 1990 年から運用を行ってきているが、この図にない 1996 年くらいまではユーザ数も数百程度で推移していた。図中の上側のグラフが毎日の同時最大接続ユーザ数を示し、下側のグラフが平均接続ユーザ数を示している。1999 年から 2000 年にかけては両者は 3 倍の開きを示しているが、現在では両者の開きは 2 倍にも達しなくなっている。この状況の原因についての詳細は次節以降で述べる。

ここ 2 年の国内の IRCnet のユーザ数については図 2.2 に示すように同時最大接続数は 14000 前後から 18000 前後へと増加してきている。ピークの部分が各月 4 つ程度尖って山ができているのは週末を示しており、この詳細分析については次節以降で述べる。また、図中の黒い部分の底辺を支える部分が閑散時のユーザ同時接続数を示しており、1 年前は 2000 程度であったが現在は 7000 程度へと急上昇していることがわかる。ここで、両年ともにお正月とお盆

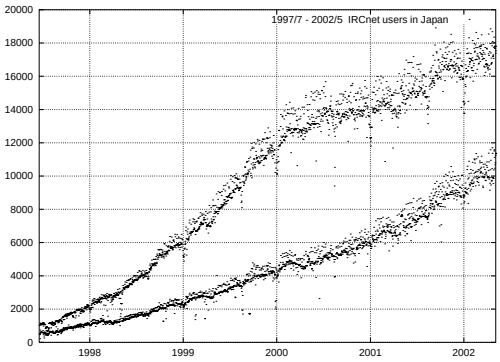

図 2.1.　IRCnet の国内ユーザ数の推移

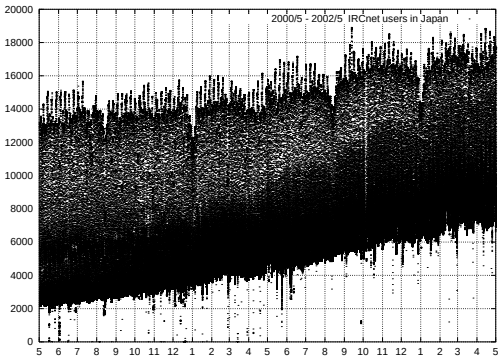

図 2.2.　IRCnet の国内ユーザ数の状況

表 2.1.　IRCnet の日本の国際接続

接続名	サーバ名	ホスト名
∗.stealth.net	ircd.stealth.net	ircd.stealth.net
∗.se	irc.ludd.luth.se	irc.ludd.luth.se
∗.de	tu-muenchen.de	irc.leo.org

表 2.2.　IRCnet の国内のサーバ

サーバ名	開放ポート	備考
irc.dti.ne.jp	6666–6667	6666 は dti 内部のみ
irc.huie.hokudai.ac.jp	6667	
irc.fujisawa.wide.ad.jp	6660–6669	
irc.kyoto.wide.ad.jp	6660–6669	
irc.tokyo.wide.ad.jp	6660–6669	
irc6.kyoto.wide.ad.jp	6667	IPv6 用

の時期にはユーザ数が減少していることが見られる。注意深く見ると 2001 年 9 月のところで一つ抜き出ているが、これはニューヨークでテロのあった日である 2001 年 9 月 11 日であり、前後から推測される 16000 人よりも 3000 多い約 19000 人が同時接続していた。

国内の IRCnet サーバ群は irc.tokyo.wide.ad.jp を介して国外の IRCnet へとつながっている。そのときの現在の接続先サーバを表 2.1 に示す。ここで、接続名とは IRC サーバ同士が接続するときに名乗る接続名であり、こちら側のサーバは ∗.jp と名乗っている。サーバ名は、IRC 網上での各サーバの固有の名前であり、ホスト名は通常の DNS 的意味と同じである。

現在接続されている国内の IRCnet のサーバは表 2.2 のようになっている。このうちサーバ名に wide.ad.jp がつく 4 台を WIDE で運用している。そのうちの irc.kyoto および irc.tokyo の 2 台において、ユーザの接続元アドレスと接続開始時刻、接続持続時間、切断理由を記録しているため、それらの記録を今回解析した。次節以降は、その 2 台のデータの解析結果であり、データは 2001 年 4 月 1 日から 2002 年 4 月 30 日までのものを使用している。以下、サーバ別の評価ではない部分では、2 台のデータを合計した値をもとに分析している。

2.2 サーバ毎のクライアント接続数の分析

接続開始時刻と持続時間を積分し、一日の接続数の最大値をプロットしたのが図 2.3 である。これが各サーバごとの年間のクライアント数の変化となる。

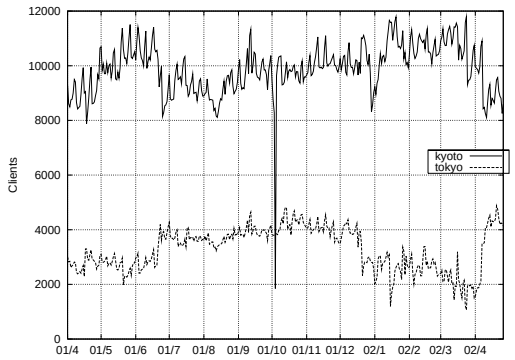

図 2.3.　2001 年度のクライアント数の変化

図 2.3 によると、irc.kyoto.wide.ad.jp は一年をとおして一万程度の接続をさばいている。irc.tokyo.wide.ad.jp は、irc.kyoto.wide.ad.jp より少なく 4000 程度の接続を担当してたが、2001 年 12 月頃から DoS アタックがひどくなったためか、利用者が激減していた。2002 年 4 月上旬に大手町に移設するとともに DoS に強くなって安定したため、京都への過剰集中を回避して負荷分散をするために東京へユーザを誘導したため一気に増加している。また、DoS の被害が大きくて京都につなぎかえていたユーザが東京につなぎかえた可能性もある。さらに、複数のサーバを指定できるクライアントの場合は、従来は東京が不安定だったために東京へ到達できなくなると京都や他のサーバに自動的につなぎかえていたものが、東京が安定したために、一旦東京につながるとそのまま安定して東京への接続時間が増えている可能性も考えられる。

次に、年間を通して週の各時刻ごとの平均をとり、プロットしたものが図 2.4 である。

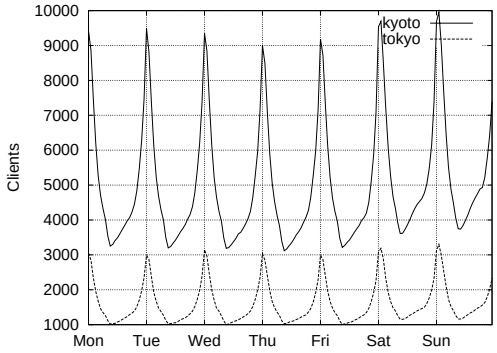

図 2.4. 2001 年度の週間のクライアント数の変化

図 2.4 によると、昨年度と同じくサーバごとの変化のパターンの違いはほとんどなく、相似である。また、曜日ごとの変化は少ないが、どのサーバの場合でも金曜・土曜の夜に平日の夜よりもクライアント数が増えている。また週のなかでは水曜、木曜の夜の利用者数が他の平日よりも若干少ないことがわかる。昼間の谷の部分については、土日が多いことがわかる。

時間ごとの変化をみると、2 台のサーバとも同じ変化を示し、昼間がいちばん少なく、22 時ごろからクライアント数が急増し、テレホーダイ時間帯の 1 時に最大となり、テレホーダイ時間終了とともに減っている。

図 2.5 は接続クライアント数の 24 時間での変化を示している。グラフの形状の性質上、横軸は昼の 12 時から翌日の昼の 12 時までとなっている。なお、縦軸の接続クライアント数はこの図についてのみ、IRCnet 国内のサーバでの総数となっている。

四つの時期においてのそれぞれのグラフを表示しているが、一番下の 2000 年 3 月から 6 月にかけての平均グラフでは 23 時における鋭い立ち上がりがみられ、同時に朝 8 時の落ち込みがあることから、この頃はテレホーダイによる影響は色濃く受けていたことが推測される。この現象は徐々に薄まっていき、一番上の 2001 年 9 月から 12 月にかけての平均グラフでは 23 時の集中的上昇は極軽微となっているとともに、お昼間の時間帯での接続数が大幅に延びていることから、常時接続環境の普及が進んでいることが推測される。

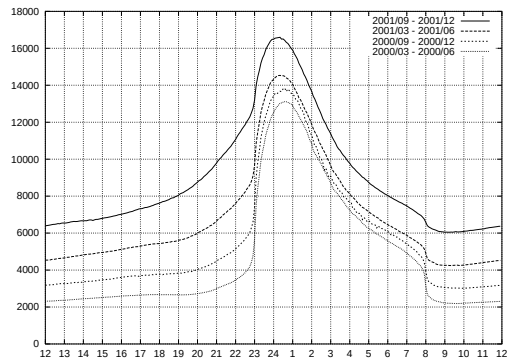

図 2.5. クライアント数の 24 時間での変化

2.3 クライアントの接続・切断頻度の分析

次に、クライアントの接続開始時刻データを分析し、ユーザが接続し始める時刻とユーザが接続を切断する時刻を調べた。そして、毎分に接続を開始したクライアント数と毎分に接続を切断したクライアント数、PingTimeout で切断するクライアント数を求めた。これについては昨年度のデータを併記して比較を行なう。

期間中のデータを各時刻ごとに平均し、一日の変化を図示した。2001 年度を図 2.6 に示し、昨 2000 年度のデータを図 2.7 に示す。グラフ中のクライアント数は、同じスケールにいれる関係で 1/50 して示してある。

接続クライアント数は、昼間の時間帯が一番少ない

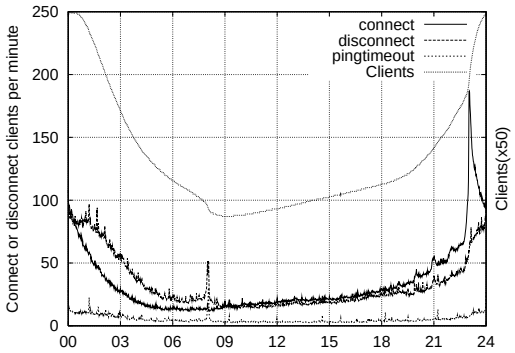

図 2.6. IRC 接続数の一日の変化 2001 年度

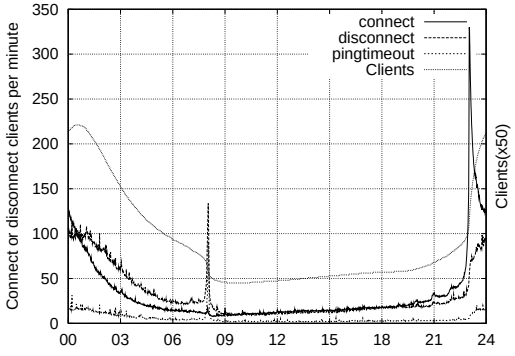

図 2.7. IRC 接続数の一日の変化 2000 年度

が、最低でも 4300 クライアント接続している。1999 年度は 1500 であり、2000 年度は 2200 であったため、東京・京都のサーバの昼間のユーザ数は倍増している。また、夕方から夜にかけて徐々にクライアント数が増加し、23 時のテレホーダイ開始とともに急激に増加し、0 時 40 分ごろに約 12500 クライアントで最大となり、そこから朝にむけて徐々に減少する。そして朝 8 時のテレホーダイ終了とともに激減するが、23 時ほど顕著には減らない。昨年度と比較すると、テレホーダイの影響がかなり減ったことがわかる。

接続開始クライアント数（接続頻度）、切断クライアント数（切断頻度）は昼間 9 時から 18 時ごろまで微増し、23 時前まではわりとなだらかに増加している。昨年度よりも 18 時以降の利用者の増えが大きくなった。これまではテレホーダイのために使うのをがまんしていたひとが常時接続に移行して、夕方帰宅してすぐに接続するようになってきたことが読みとれる。

一日のあいだの接続数の変化をテレホーダイ時間帯の 23 時前後に注目した図を図 2.8 に、昨年度を図 2.9 に示す。これによると、23 時に一分間に 187 クライアント程度の接続が集中し、そのあとなだらかに減っている。23 時に大量に接続要求がきて、最初の一分間に 187 処理し、そのあと数分かけて徐々にさばいているようであるが、昨年度よりは変化がなだらかになっている。昨年度は一分間に 330 もの接続をさばいていたが、今年度は 187 となっている。ここからもテレホーダイから常時接続に移行してきていることがわかる。

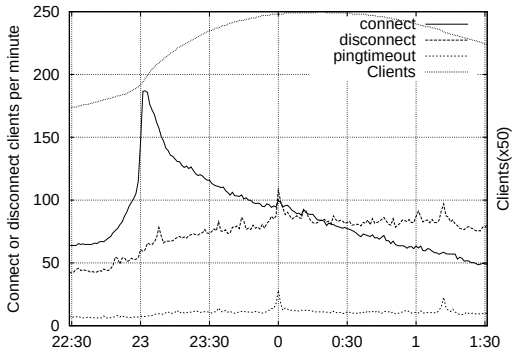

図 2.8.　IRC 接続数の一日の変化 2001 年度（テレホーダイサービス開始時刻付近）

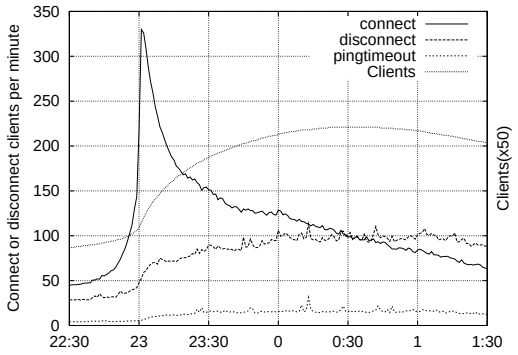

図 2.9.　IRC 接続数の一日の変化 2000 年度（テレホーダイサービス開始時刻付近）

一日のあいだの接続数の変化をテレホーダイ終了の朝 8 時に注目した図を図 2.10 に、昨年度を図 2.11 に示す。

昨年度は 8 時に切断するクライアント数が突出していたが、今年度はそれまでの時刻の倍に増えるだけで、すぐにもとにもどっている。これまで、テレホーダイの時間だけずっと使い続けるといった使い方をしてきたひとの多くが常時接続の回線に切り替えてきていて、つなぎたいときにつなぎ、切りたい時に切るようになってきていることがわかる。

2.4 利用時間分布

クライアントの接続持続時間分布を図 2.12 に示

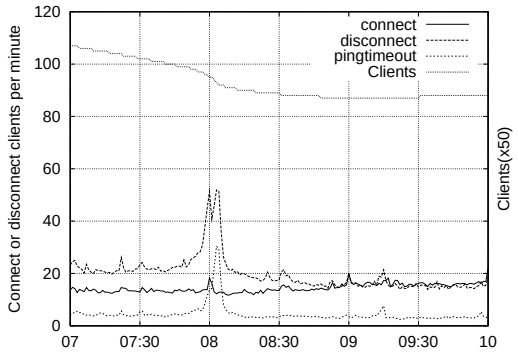

図 2.10.　IRC 接続数の一日の変化 2001 年度（朝）

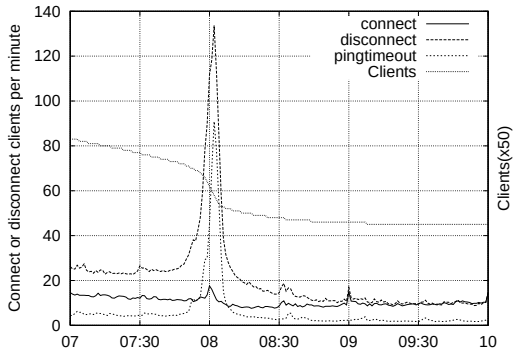

図 2.11.　IRC 接続数の一日の変化 2000 年度（朝）

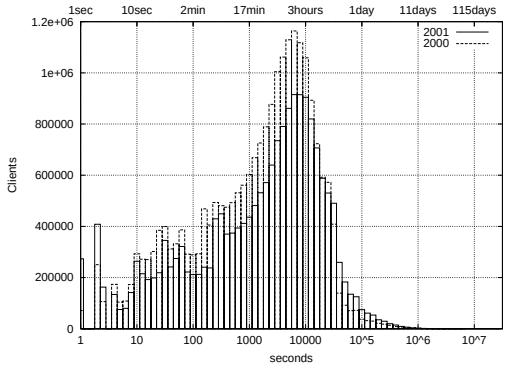

図 2.12. クライアント接続持続時間の分布（クライアント数）

す。2000 年度と 2001 年度を図示し、比較する。横軸は接続秒数を対数でとった。棒の幅は、10 倍を対数で 10 等分した間隔である。たとえば、100 秒の範囲は、100 秒から $100 \times \exp(\log(10)/10)$ 秒（125.9 秒）となる。

これを見ると、一時間から三時間程度の利用者が一番多いことや、15 分以下の利用者も比較的多くいることがわかる。また 2 分以下の利用者もいるが、短時間ではまともな会話は困難であるので、攻撃のための調査や、DoS などの障害のために短時間しかつながらなかった場合であると考えられる。

また、一日以上の長期間接続しっぱなしのクライアントが有意な数あることと、それが増えていることもわかる。

次に、さきほどと同じ段階で切り、2001 年度の各ステップの IRC サーバ利用時間の総和を図 2.13 に示した。多くの CPU を使っている利用者ほど大きな値となる。これが接続持続時間ごとの IRC サーバの利用時間となる。

図 2.13 によると、10 時間以上接続しているクライアントによる利用時間が IRC サーバ利用時間の半分を占めている。また 11 日以上連続して接続するクライアントによる利用も多いことがわかる。

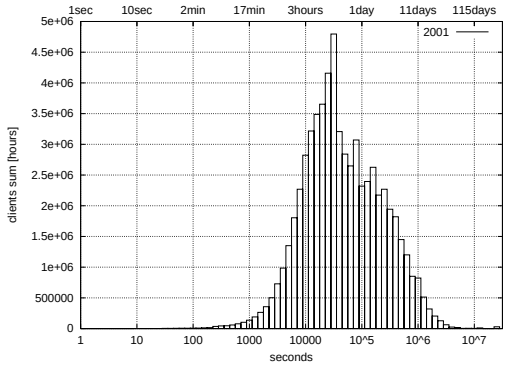

図 2.13. クライアント接続持続時間ごとの IRC サーバ接続時間 2001 年度

2.5 クライアントの接続元の分析

IRC サーバへの接続元 IP アドレスから AS 番号を得て各 AS からの接続時間を積算し、一年間の平均をとって、一日の各時刻ごとの上位 10 AS を調べたのが表 2.3 である。図 2.4 にて利用が最小になる昼間には、昨年度までは大学系の SINET や、daemon を動かせるシェルサービスを提供している RIM などがあらわれて、夜にはダイヤルアップユーザの多い ISP があらわれていたが、今年度についてはそのような傾向がみられない。どの時間帯でもおなじような順位となっている。昼間の利用者についても、一般の常時接続による利用者のほうが顕著になってきていることがわかる。

IRC サーバごとのユーザの接続元 AS を調べ、表 2.4 に示した。これは、一年間の接続データをサーバごとに積算し、AS ごとのユーザ数の平均値を求めたものであるため、常時接続者の傾向が強めにでる。この表により、どの AS からの利用者がどのサーバを好んで使うかをみることができるが、表によると、きわだった差はないようである。昨年と同様に irc.kyoto.wide.ad.jp に OMP のユーザが多い傾向はみられるが、昨年と違い、30 位までには NCA5 や SINET などの研究教育系なネットワークがでてこない。

表 2.3.　2001 年度の時間ごとのクライアント接続元の変化

時刻	0 時			1 時			2 時			3 時		
	AS	clients		AS	clients		AS	clients		AS	clients	
1	OCN	1201	9.83	OCN	1025	9.78	OCN	858	9.85	OCN	733	9.94
2	INFOWEB	857	7.01	INFOWEB	710	6.78	INFOWEB	569	6.53	INFOWEB	468	6.36
3	IIJ	634	5.19	IIJ	555	5.30	IIJ	473	5.43	IIJ	407	5.53
4	NTTPC	607	4.97	NTTPC	522	4.99	NTTPC	437	5.02	NTTPC	372	5.05
5	DION	548	4.49	DION	459	4.38	DION	371	4.26	DION	306	4.15
6	SONET	544	4.45	SONET	455	4.34	SONET	362	4.16	SONET	290	3.94
7	MESH	449	3.67	ATHOMEJP	378	3.61	ATHOMEJP	313	3.60	ATHOMEJP	262	3.56
8	ATHOMEJP	440	3.60	MESH	372	3.55	ODN	293	3.37	ODN	247	3.36
9	DTI	433	3.55	DTI	359	3.43	MESH	292	3.36	DTI	237	3.23
10	ODN	425	3.48	ODN	357	3.41	DTI	289	3.32	MESH	233	3.17
全クライアント数		12229			10485			8712			7376	

時刻	4 時			5 時			6 時			7 時		
	AS	clients		AS	clients		AS	clients		AS	clients	
1	OCN	650	10.03	OCN	592	10.06	OCN	554	10.14	OCN	506	10.40
2	INFOWEB	405	6.24	INFOWEB	363	6.16	INFOWEB	332	6.09	INFOWEB	284	5.85
3	IIJ	361	5.58	IIJ	329	5.58	IIJ	304	5.57	IIJ	271	5.59
4	NTTPC	327	5.06	NTTPC	298	5.07	NTTPC	277	5.08	NTTPC	250	5.14
5	DION	264	4.08	DION	237	4.04	DION	216	3.95	DION	181	3.72
6	SONET	244	3.77	SONET	214	3.64	ATHOMEJP	194	3.56	ATHOMEJP	180	3.71
7	ATHOMEJP	229	3.54	ATHOMEJP	208	3.54	SONET	192	3.53	ODN	163	3.37
8	ODN	218	3.36	ODN	199	3.38	ODN	185	3.39	SONET	163	3.36
9	DTI	203	3.14	DTI	181	3.08	DTI	165	3.03	ZAQ	143	2.95
10	MESH	196	3.03	MESH	173	2.94	MESH	155	2.85	XEPHION	140	2.90
全クライアント数		6487			5895			5466			4863	

時刻	8 時			9 時			10 時			11 時		
	AS	clients		AS	clients		AS	clients		AS	clients	
1	OCN	478	10.76	OCN	492	10.98	OCN	510	11.07	OCN	525	11.08
2	INFOWEB	251	5.66	INFOWEB	251	5.60	INFOWEB	256	5.56	INFOWEB	261	5.52
3	IIJ	248	5.57	IIJ	248	5.53	IIJ	254	5.51	IIJ	259	5.48
4	NTTPC	233	5.24	NTTPC	233	5.20	NTTPC	239	5.20	NTTPC	246	5.19
5	ATHOMEJP	169	3.81	ATHOMEJP	167	3.74	DION	176	3.83	DION	183	3.87
6	DION	159	3.59	DION	167	3.73	ATHOMEJP	171	3.71	ATHOMEJP	175	3.71
7	ODN	150	3.38	ODN	150	3.36	ODN	152	3.32	ODN	156	3.30
8	SONET	143	3.23	SONET	141	3.16	SONET	143	3.12	SONET	147	3.12
9	ZAQ	136	3.06	ZAQ	137	3.07	ZAQ	141	3.06	ZAQ	145	3.07
10	XEPHION	132	2.99	XEPHION	131	2.93	XEPHION	133	2.90	XEPHION	137	2.91
全クライアント数		4451			4488			4608			4740	

時刻	12 時			13 時			14 時			15 時		
	AS	clients		AS	clients		AS	clients		AS	clients	
1	OCN	541	11.07	OCN	559	11.04	OCN	575	11.03	OCN	592	11.01
2	INFOWEB	270	5.52	INFOWEB	280	5.54	INFOWEB	288	5.52	INFOWEB	298	5.55
3	IIJ	267	5.47	IIJ	276	5.45	IIJ	285	5.47	IIJ	293	5.46
4	NTTPC	252	5.15	NTTPC	260	5.13	NTTPC	267	5.12	NTTPC	274	5.11
5	DION	190	3.90	DION	196	3.87	DION	201	3.87	DION	208	3.87
6	ATHOMEJP	181	3.72	ATHOMEJP	189	3.74	ATHOMEJP	197	3.78	ATHOMEJP	205	3.81
7	ODN	161	3.30	ODN	165	3.27	ODN	169	3.26	ODN	173	3.23
8	SONET	153	3.14	ZAQ	160	3.16	SONET	166	3.19	SONET	173	3.23
9	ZAQ	152	3.11	SONET	159	3.15	ZAQ	165	3.17	ZAQ	172	3.20
10	XEPHION	141	2.89	XEPHION	145	2.87	XEPHION	149	2.87	XEPHION	154	2.88
全クライアント数		4895			5070			5217			5380	

時刻	16 時			17 時			18 時			19 時		
	AS	clients		AS	clients		AS	clients		AS	clients	
1	OCN	613	11.05	OCN	628	10.99	OCN	652	10.96	OCN	698	10.88
2	INFOWEB	310	5.59	INFOWEB	325	5.70	INFOWEB	347	5.84	INFOWEB	388	6.06
3	IIJ	303	5.47	IIJ	315	5.51	IIJ	330	5.55	IIJ	360	5.62
4	NTTPC	283	5.10	NTTPC	293	5.14	NTTPC	307	5.16	NTTPC	333	5.20
5	DION	214	3.87	ATHOMEJP	225	3.94	ATHOMEJP	239	4.02	ATHOMEJP	263	4.10
6	ATHOMEJP	213	3.85	DION	220	3.85	DION	225	3.79	DION	239	3.74
7	SONET	181	3.26	SONET	190	3.33	SONET	203	3.42	SONET	225	3.52
8	ZAQ	180	3.26	ZAQ	190	3.33	ZAQ	200	3.36	ZAQ	218	3.41
9	ODN	179	3.24	ODN	188	3.29	ODN	196	3.30	ODN	214	3.35
10	XEPHION	160	2.88	XEPHION	166	2.91	XEPHION	175	2.95	XEPHION	190	2.97
全クライアント数		5548			5721			5956			6415	

時刻	20 時			21 時			22 時			23 時		
	AS	clients		AS	clients		AS	clients		AS	clients	
1	OCN	772	10.73	OCN	869	10.61	OCN	1009	10.42	OCN	1264	10.04
2	INFOWEB	456	6.34	INFOWEB	538	6.57	INFOWEB	653	6.75	INFOWEB	891	7.08
3	IIJ	408	5.68	IIJ	468	5.72	IIJ	543	5.61	IIJ	657	5.22
4	NTTPC	376	5.23	NTTPC	428	5.23	NTTPC	505	5.22	NTTPC	626	4.97
5	ATHOMEJP	301	4.18	ATHOMEJP	345	4.22	ATHOMEJP	399	4.12	DION	567	4.51
6	DION	273	3.79	SONET	317	3.88	SONET	394	4.07	SONET	554	4.41
7	SONET	264	3.67	DION	316	3.86	DION	389	4.02	MESH	457	3.63
8	ZAQ	249	3.47	ZAQ	289	3.54	ZAQ	340	3.52	ATHOMEJP	455	3.62
9	ODN	244	3.40	ODN	280	3.42	ODN	334	3.46	DTI	450	3.58
10	DTI	221	3.08	DTI	264	3.23	DTI	331	3.42	ODN	445	3.53
全クライアント数		7201			8192			9689			12597	

表 2.4. 2001 年度の IRC サーバごとのクライアント接続元

サーバ	tokyo			kyoto		
	AS	接続時間	%	AS	接続時間	%
1	OCN	1744534	11.51	OCN	4835649	10.11
2	INFOWEB	1008934	6.66	INFOWEB	2920577	6.10
3	IIJ	856931	5.65	IIJ	2594637	5.42
4	NTTPC	771142	5.09	NTTPC	2448175	5.12
5	ATHOMEJP	732470	4.83	DION	1918276	4.01
6	DION	627160	4.14	SONET	1792423	3.75
7	SONET	561953	3.71	ODN	1698310	3.55
8	MESH	493058	3.25	ATHOMEJP	1647224	3.44
9	ZAQ	442638	2.92	ZAQ	1528689	3.19
10	ODN	429805	2.84	DTI	1519062	3.17
11	DTI	409854	2.70	MESH	1395781	2.92
12	XEPHION	408052	2.69	XEPHION	1334411	2.79
13	ASAHI-NET	328320	2.17	ASAHI-NET	1116014	2.33
14	SPIN	326290	2.15	TTNET	880584	1.84
15	TTNET	308889	2.04	GIGAINFRA	781466	1.63
16	METALLIC	263009	1.74	OMP	731904	1.53
17	RIM	189063	1.25	METALLIC	681237	1.42
18	MEX	187726	1.24	DOLPHIN	629529	1.32
19	DOLPHIN	186433	1.23	INTERVIA	494578	1.03
20	INTERVIA	165998	1.10	HIGHWAY	470351	0.98
21	GIGAINFRA	159124	1.05	RIM	464283	0.97
22	HIGHWAY	117241	0.77	WIDE	360172	0.75
23	OMP	110722	0.73	ALPHA-NET	344529	0.72
24	ALPHA-NET	93476	0.62	INTERQ	306991	0.64
25	IDC	86631	0.57	IDC	287371	0.60
26	INTERQ	80451	0.53	MEX	241060	0.50
27	CTC	74189	0.49	CTC	236206	0.49
28	ALTERNET	72551	0.48	ALTERNET	228892	0.48
29	SAKURA	71939	0.47	SANNET	227553	0.48
30	KCOM	69670	0.46	PANANET	213969	0.45
全接続時間		15155099			47851969	

第 3 章　IRC における DoS 対策とネットワーク構成の変更

3.1 IRC サーバ関連の DoS

今年度も two に報告が上がるぐらいの DoS が何度かあったので順に記録する。以下、各ホスト名の wide.ad.jp を省略する。packet per second を pps と書き、1000 pps を 1 kpps と書く。

- 2001/5/21 00:50–02:00 Korea Telecom 方面から KDDI 経由で irc.tokyo 宛の DoS がきて KDDI にて SLA アラーム検知。数万 pps。大手町ルータのフィルタを直して東京 NOC を救った。
  UUnet から KDDI America LA へ 65 Mbps irc.tokyo 宛。ソースアドレスが少なかったため、UUnet にてフィルタ。
  これに関して、KDDI や LAX を通る irc.tokyo 宛通信に関してはサーバ間接続のみ許可してあとは禁止してもよいと提案した。
- 5/25 APAN 方面から最大 35 Mbps 95 kpps の DoS
  APAN からの DoS パケットをフィルタして WIDE 内を守った。
- 7/23 cisco1.lax へ irc.tokyo 宛パケットが多数届く。
  cisco1.lax にて irc.tokyo 宛を rate limit して解決。
- 10/14 cisco5.otemachi 向け TCP の DoS により KDDI の海外線に 100 Mbps もの traffic が流れたため、KDDI から WIDE 向けの BGP 接続を落とされた。
  KDDI、その上流にて該当アドレス宛 TCP のフィルタを書いてもらい、BGP の接続を復活した
- 10/17 08:36 cisco5.otemachi、cisco2.otemachi、foundry2.otemachi 向けの UDP DoS により、KDDI の海外線があふれて BGP 接続を切られた。
  KDDI、その上流にて該当アドレス宛パケットすべてを落とすフィルタを書いてもらい、BGP の接続を復活した。
  10/17 時点での KDDI でのフィルタは、cisco5.otemachi、cisco2.oteamchi、foundry2.otemachi のアドレス向けパケットをすべて禁止とするものである。
- 10/19 08:54–10:49、11:16–11:24、12:16–13:06、10/22 23:15 10/23 00:55、02:05-06:00 irc.tokyo 宛の ICMP を用いた DoS
- 11/14 irc.tokyo 向け DoS
- 12/9 0500- irc.tokyo 向け KDDI 経由の DDoS
- 12/14 irc.tokyo 向け複数ホストからのポートスキャン
- 12/15 irc.tokyo 向け複数ホストからの icmp echo request
- 12/16 irc.tokyo 向け、一つのホストからの大きな icmp echo request
- 12/21
  KDDI や LAX 経由の DoS が激しいため、IRC サーバで使うアドレスを WIDE バックボーンのアドレスとは違うアドレスに変更し、BGP での経路広報やフィルタの制御をしやすくする提案がなされた。これについては 3.2 節で説明する。
- 12/27 irc.tokyo 向け DoS
- 2002/1/7 UUNET POS に 150 Mbps の DoS
- 1/15 1542 16〜23 kpps DoS
- 1/16 KDDI にて irc.tokyo 宛の DoS を検知したため ICMP をフィルタ
  この時点で KDDI にて irc.tokyo、irc.kyoto アドレス宛 ICMP をフィルタしている。
- 3/10 irc.fujisawa 宛の DoS
  KDDI にて irc.fujisawa 宛の icmp をフィルタした。
- 3/20 irc.tokyo 新アドレス宛 DoS TCP SYN アタック
- 3/23 irc.tokyo 向け TCP SYN アタック
  3.3 節で説明するがネットワーク構成を変更して対応した。
- 2002/4/8 に以下の内容のフィルタを KDDI にで設定してもらった。
  - IRC サーバへの ICMP echo-reply 禁止
  - IRC サーバで使っているサーバ間接続の UDP を許可（7667）
  - それ以外の IRC サーバ向け UDP 禁止
  - DoS 対象となった cisco2.otemachi、cisco5.otemachi、foundry2.otemachi 宛のパケット

を禁止

これらの DoS と、それに対するフィルタ記述、3.2 節にて説明する IP アドレスの変更、3.3 節にて説明する大手町への移設により、IRC 網そのものが DoS に強くなり、安定するようになった。また東京 NOC は DoS の影響を受けなくなった。

3.2 IRC サーバのアドレス変更

従来は IRC サーバの IP アドレスとして WIDE-BB のアドレスを用いていた。ところが、対外的に DoS 攻撃発生源方面への一時的経路広報停止やフィルタ設定をお願いするときに、WIDE-BB 内の現在の IP アドレスでは機動性がよくない。そこで、IRC サーバの IP アドレスを 192.244.23.0/24 へ移行した。

この変更を行うことで、KDDI などの ISP へのフィルタ設定依頼をホスト単位ではなくネットワーク単位でできるようになり、また BGP での経路広報を停止することも簡単にできるようになった。

IRC サーバの IP アドレスの移行であるが、以下のような手順で行った。それぞれのステップにおいて、動作確認を行う。

1. IRC サーバに新 IP アドレスをつけ、経路情報が各方面に伝わるのを確認
   今回のつけかえでは、新アドレスが APAN/Abilene 方面にアナウンスされるまで切り替えを待った。
2. 新アドレスの逆引きを設定（irc.tokyo.wide.ad.jp）
3. アクセス制御を行っているルータにて新アドレスへのフィルタを追加する
4. IRC サーバで新アドレスでもサービスを受けられるようにする
5. 新旧二つの IP アドレスを irc.tokyo.wide.ad.jp に DNS 登録する
6. DNS 情報が伝搬するのを待つ
   この時点で両アドレスとも使用可能
   両方のアドレスへ DoS 攻撃が来ることが確認された
7. IRC サーバ間接続のアドレスを新アドレスへ変更（サーバ再起動）
8. irc.tokyo.wide.ad.jp への DNS 登録を新アドレスのみに変更
   アドレスが伝搬するまで待つ
9. IRC サーバでの旧アドレスの受け付け（listen）をやめる。

現在は irc.tokyo.wide.ad.jp と irc.kyoto.wide.ad.jp のみ移行を完了しているが、irc.fujisawa.wide.ad.jp と irc.nara.wide.ad.jp も移行する必要がある。

3.3 irc.tokyo.wide.ad.jp のネットワーク構成

本節では、IRC サーバへの DoS の影響で NOC の機能がよく停止していた東京 NOC での DoS の影響を減らすためのネットワーク構成の変更を説明する。

もともとのネットワーク構成を図 3.1 に示す。このころは外から DoS アタックがくると cisco19 と cisco13 が重くなっていたが IRC サーバ以外から外へは全く通信できなくなることはなかった。

2001 年 4 月 16 日、東京 NOC の再構築を行い、IRC サーバ周辺のネットワーク構成を図 3.2 のように変更した。これは DoS 対策とは関係ない。

以前は cisco7000 と cisco4500 で分担していた処理を cisco1 (cisco3640) 一台に集中させ、そこにすべてが依存するようになった。cisco1 にて ATM を受け、IRC 関連のアクセス制限処理を行う。

このような状況で、頻繁に IRC サーバへ DoS アタックがきた。10 Mbps 程度の DoS が多いが、20 kpps となり、経路途中の cisco1 (cisco3640) の処理能力（アクセス制限処理時で数千 pps）を越えていた。SNMP によりパケット数と CPU 使用率を測定すると相関が見られた。

東京 NOC の場合は NOC 間接続ルータである cisco1 の CPU 利用率が 100%に張りつき、ルータが無反応となり、パケット転送をしなくなり、下流組織への接続性までなくなり、孤立した。

代替経路も用意してあったが、経路が切り替わるたびにそちらに DoS パケットが到達するためにそちらのルータもあふれ、頻繁に経路が切り替わり、どちらも使用できない状態となった。

東京 NOC のルータが弱いので上流の大手町のルータでフィルタしていたが、最近の 10 kpps を越える攻撃では大手町のルータの能力も限界に近づいていた。

そこで、2002 年 1 月 18 日に、従来からほとんど使っていなかった大手町との間の FDDI 線を IRC 専用に使うことにし、IRC 以外のサービスは IRC サーバへの DoS の影響をうけないように図 3.3 の構成に変更した。この段階では、IRC サーバ行きパケットのみ cisco15 FDDI 線を通り、IRC サーバからの戻りパケットは cisco1 ATM 線を通るようにしてあっ

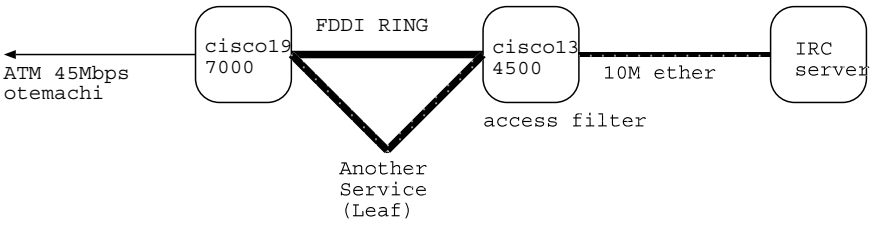

図 3.1.　2001 年 4 月以前の東京 NOC IRC サーバ接続図

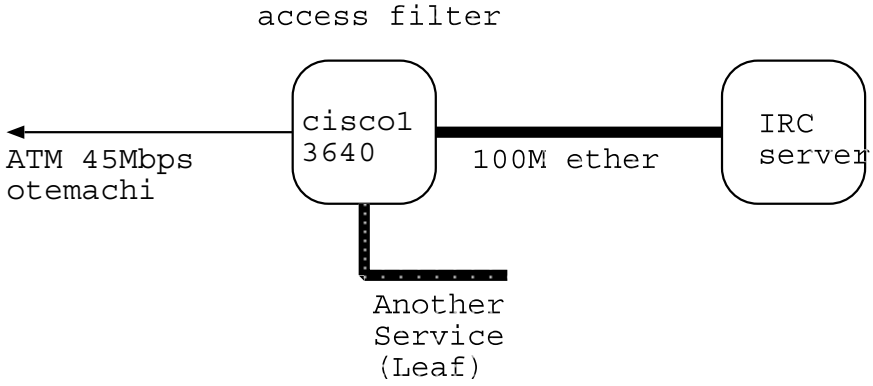

図 3.2.　東京 NOC IRC サーバ接続図（2001 年 4 月 16 日〜2002 年 1 月 18 日）

た。そうしておけば、管理用アドレスへの login については双方向同じ経路（ATM 線）を通るようにできる。

この段階では大手町のルータの負荷と、IRC サービスの耐久性については改善されていない。

これで、IRC サーバ宛の DoS は FDDI 線から IRC サーバへいくだけで、ATM 線には流れなくなった。今回は大量のパケットがきても IRC のみ影響を受け、他は影響を受けないはずであった。

ところが、次の DoS アタックは TCP SYN アタックであった。IRC サーバあてに TCP SYN アタックがくると、IRC サーバは同じ数の SYNACK をソースアドレスに送る。大手町のルータや cisco15 はこのアタックに耐え、IRC サーバも SYN ACK をもどしたせいで cisco1 がダウンしてしまい、東京 NOC がダウンしてしまった。そこで、2002 年 3 月 24 日に、IRC サーバに関しては図 3.4 のように、双方向とも FDDI 線を通すこととした。

この状態では、IRC サーバへの DoS 攻撃で IRC サーバのみ影響をうけ、東京 NOC の他の機能には影響がなくなったが、頻繁にくる DoS アタックのせいで IRC サービスは頻繁に影響をうけてしまっていた。

これまでの対応では、東京 NOC の機能への影響を減らしただけで、IRC サーバが攻撃により使用不能になることの対応ができていなかった。また、攻撃がきても、それを正確に記録することができなかった。そこで、途中ルータでフィルタすることをやめて DoS 攻撃解析を行うためにネットワーク的によい場所に移設し、記録するに足る能力を持つ PC を用

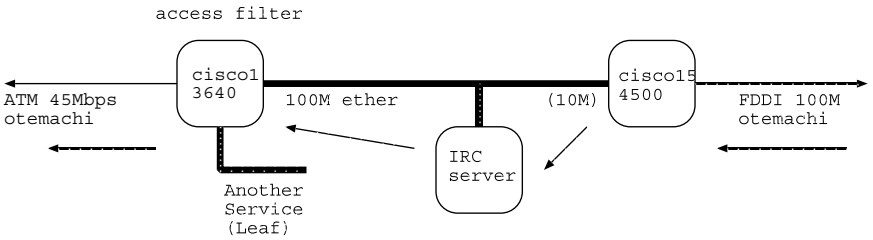

図 3.3.　IRC を分離したネットワーク構成 (1)

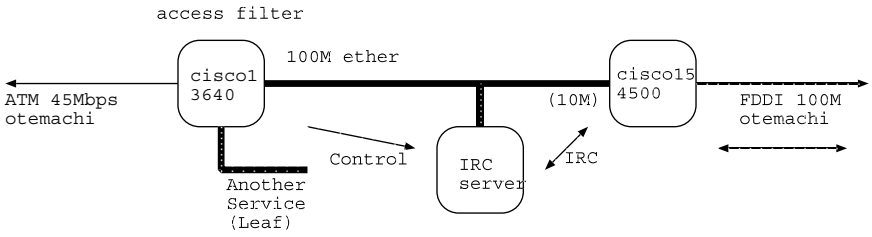

図 3.4. IRC を分離したネットワーク構成 (2)

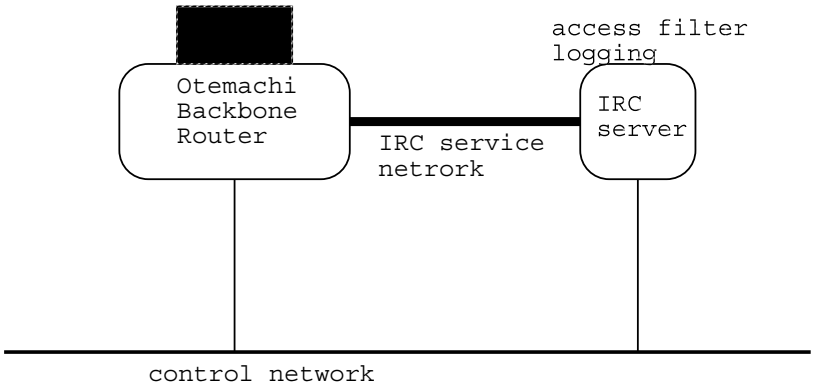

図 3.5. 大手町移設

意する必要があった。

そこで、機材の手配ができ、準備の整った 2002 年 4 月上旬に大手町への移設を行った。大手町では基幹 L3 スイッチに直結し、また攻撃時の制御用に別のサブネットにも接続した。最新の PentiumIII を Dual 構成で使用することで IRC サービスと DoS の記録を行なえるようになった。その結果、かなり強い DoS アタックがきてもほとんど影響を受けなくなった。現在のネットワーク接続図を図 3.5 に示す。

現行 PC のスペックについて記録する。

ラックマウントシャーシ、1U、CPU: Dual PentiumIII 1133 MHz, Memory: 512 MB マザーボード Supermicro 6011H（fxp 2 個と Adaptec U160 SCSI つき)、ディスク 36 G SCSI3

従来の irc.tokyo の CPU は PentiumII-400 であったのでかなり能力が高くなった。