第 XXII 部

IRC の運用状況とデータ解析

第 22 部
IRC の運用状況とデータ解析

第 1 章　はじめに

IRC ワーキンググループでは Internet Relay Chat（以下 IRC）に関する研究と、そのテストベッドとしての IRC サービス網の運用を通じて、大規模サービスの安定運用に関する研究を行っている。また、WIDE プロジェクト内の他のワーキンググループと連携した研究活動も行っている。

IRC とは、人と人とのコミュニケーション手段の 1 つである、文字ベースによるリアルタイムチャットを、インターネットのサービスとして提供するシステムである。これは、1988 年、フィンランドで開発されたシステムであり、日本では 1990 年から利用されてきた。

IRC のシステムは、メッセージ転送を受け持つサーバと、ユーザとのインターフェイスであるクライアントにより構成される。IRC のサービスは、これらをサーバを中心にスター型に接続した IRC ネットワーク上でメッセージを順次バケツリレーの如く転送することにより提供されるもので、広域分散技術にもとづいて構築され世界規模で運用されている。

IRC ワーキンググループでは複数の IRC サーバを運用・接続し、研究に利用するとともに、国内の一般ユーザにも開放している。現在 IRC ワーキンググループが WIDE インターネット上で運用するサーバは以下の 4 台である。

- irc.tokyo.wide.ad.jp
- irc.fujisawa.wide.ad.jp
- irc.nara.wide.ad.jp
- irc6.nara.wide.ad.jp

このうち、irc6.nara.wide.ad.jp は IPv6 によるクライアント接続を受け付けており、他のサーバは IPv4 による接続を担当する。

本報告書では、2006 年の IRC ワーキンググループの研究活動の報告と、WIDE プロジェクトにて運用されている IRC サーバ群の利用状況について報告する。

第 2 章　2006 年の IRC ワーキンググループの活動

IRC ワーキンググループでは、サーバ運用から得られた知見を研究に活かし、同時に研究から得られた成果を運用に活かすことを目標に運用と研究活動を行っている。本年度は、IRC サーバが非常に安定した運用状態になっていたため、研究活動、特に SCTP ワーキンググループと連携した研究活動に多くの時間をかけることが出来た。

2.1 サーバ運用について

2.1.1 サーバの安定運用

IRC サーバは国内に 4 サーバ存在するが、そのうちの 1 つが 1000 日以上の連続稼動という実績を達成した。

通常の運用方法では、電源の法定点検による停電やセキュリティ対策による再起動の必要性などにより、このような 3 年にもわたる連続稼動は困難である。このサーバにおいては安定した電源設備のある場所に設置した上で、同じサーバで稼動しているサービスの数や種類を極小まで減らしている。その上でサービスごとのパッチあてと再起動を行いつつも、サーバの再起動を避けてきた。この期間には本来ならカーネルに対してパッチを適用して再起動を必要とする問題もあったが、これらに対してはサーバの手前に設置されたルータやフィルタの設定により、問題が発生しないように工夫してきた。

このサーバ上で稼動するサービスである IRC デーモンも 700 日以上の連続稼動を達成している。（2.11 系へのバージョンアップ作業以降、IRC サーバは連続稼動していることを意味する。）近日 IRC サーバの再度のバージョンアップを行う予定であるので、その際同時に OS の更新と再起動も行う予定である。今後もサービスの安定稼動のノウハウを蓄積していきたい。

2.1.2 IRC サーバのバージョンアップによる DDoS 対策

これまでの IRC サーバのオペレーションは、DDoS によりサーバやルータを攻撃しサーバ間接続を切ろうとする攻撃者との闘いともいえるものであった。これに対して IRC ワーキンググループでは「サーバ間接続で利用する IP アドレスやインタフェイスを秘密にする」「サーバ間接続でパケットが経由するルータに関する情報を秘密にし、外部から攻撃できないようにする」といった対策を講じてきた。しかしながらサーバの物理構成には自由にならない点があったなど対策が十分ではなく、DDoS による攻撃に一定の効果がある状態であった。

これに対し、DDoS による攻撃に対する耐性が強く、同時に DDoS 攻撃により攻撃者に利益が生じにくいバージョン 2.11 系列が開発された。そこで 2005 年に全世界的に協調しつつサーバをバージョンアップすることで DDoS 対策を行った。この作業以降、WIDE プロジェクトの管理するサーバだけでなく、日本国内にある別のサーバにおいても DDoS の頻度が非常に下がっている。

この一連の事象は、穴のない適切なプロトコルと適切なオペレーションを行うことにより DDoS 攻撃者が利益を得ることがないようにすることで、DDoS のそのものを根絶できる可能性があることを示しているのかもしれない。

2.1.3 BGP オペレーションによる DDoS 対策

IRC ワーキンググループにおいては上記以外の DDoS 対策として、BGP オペレーションにより日本の IRC サーバ群に対する海外からのアクセスを困難にするといった対策も行っている。この処置は「海外からの DDoS を防ぐことが出来る」という効果の反面、「海外にいるユーザ（日本人）が日本の IRC サーバを利用できなくなる」という弊害があった。DDoS の猛威が去った現状において、この対策を見直す時期に来ているのかもしれない。

2.2 海外サーバとの協調について

サーバを 2.11 系列である Version 2.11.0 にするバージョンアップ作業を 2005 年に行ったが、その後マイナーバージョンアップである Version 2.11.1 が公開されている。日本のサーバにおいては日本語対応を行う必要があるなどの特殊事情により海外サーバよりもバージョン更新が遅れがちであるが、早急にこの最新バージョンに移行することが求められている。

2.11.1 のバージョンアップにおける変更点は、サーバのバージョンアップだけでなく、ニックネームやチャンネル名の文字数・文字種制限の緩和なども行われており、利用者への利便性の向上も含まれる。

既にこのバージョンに対応した日本語パッチは作成済みであり、実際のバージョンアップ作業をどのように行うかが次年度の課題となっている。

2.3 Source Address Based Routing によるサーバ運用

2.3.1 複数インターフェイスを持つサーバオペレーション

IRC サーバの運用においては、各サーバに「ユーザからの接続」「サーバ間の接続」「管理用の SSH 接続」の 3 つの種類の接続が張られる。これらの接続はそれぞれ利用の目的を異にするものであり、性質や要求される安定度や重要度がそれぞれ異なる。

まず、ユーザからの接続は利用者に IP アドレスを知らせる必要がある。また、このアドレスに対して DDoS が行われた際にも、サーバ間接続や管理用の SSH 接続に対して影響を及ぼしてはいけない。この DDoS は非常に大規模なものである場合が多く、DDoS が行われている最中にはその DDoS が通過するルータやスイッチ、インターフェイスなどを通る通信の全てが影響を受けてしまう。そのため、IRC サーバのオペレーションにおいては、「ユーザからの接続」を受ける NIC（Network Interface Card）と管理を目的とした接続（「サーバ間の接続」と「管理用の SSH 接続」）を受ける NIC とは、独立別個のものにする必要性がある。

このように TCP によるサービスのオペレーションを行うサーバが複数のインターフェイスを持つ場合において、上述の IRC サーバの例のように NIC ごとに用途が違う場合や Ingress Filtering（端末からプロバイダに流入するパケットに対する Source IP アドレスにもとづくフィルタリング）が行われている際には、サーバに届いたパケットの返りパケットはそれが流入してきたインターフェイスから送り返す必要がある。

このような場合には Default Route にしたがったルーティングをそのまま利用することは出来ないだけでなく、宛先アドレスによるルーティングを利用しても適切なパケット転送を行うことはできない。

そこで、このような複数インターフェイスを持つサーバのオペレーションにおいては、送出しようとするパケットのソースアドレスにもとづいたルーティング、すなわち、Source Address Based Routing が必要となる。

2.3.2 Source Address Based Routing の実現方法

これまでに Source Address Based Routing を実現する手法には、「IPFW 等のパケットフィルタを用いる方法」と「Kernel を Source Address Based Routing 対応に拡張する方法」とが検討できる。

以下の議論においては IRC サーバが FreeBSD 上で動作していることから、FreeBSD における実装に限定した議論とする。

2.3.2.1 ipfw を利用する手法

カーネルに手を加える必要のない手順として、ipfw を用いる手法を試みた。

FreeBSD にはパケットをフィルタすることを目的とした ipfw と呼ばれる機構が存在する。これはインターフェイスを出入りするパケットを監視し、あらかじめ指定された条件に適合するパケットをフィルタしたり転送したりする機構である。

この機構を利用して以下のようなルールを追加することでパケット転送ポリシーを変更する。

- ipfw add 100 allow ip from SRC to NET:NETMASK
- ipfw add 110 fwd GATEWAY ip from SRC

ここに、SRC はインターフェイスに割当てられたソースアドレス、NET および NETMASK はインターフェイスの属するサブネットのネットワーク部およびネットマスク、GATEWAY はゲートウェイを表す。（コマンド中の 100 および 110 はルール番号を示し、この番号はインターフェイスごとに異なるようにする）

なお、ipfw において fwd コマンドを利用できるようにするために、カーネルの再設定が必要となる場合がある。（カーネルオプションで IPFIREWALL_FORWARD 及び IPFIREWALL_FORWARD_EXTENDED を有効にする必要がある）

このように設定することで、原則として SRC をソースアドレスとするパケットは GATEWAY に送られることになる。しかし、インターフェイスの数が増えてくると管理が非常に困難であるだけでなく、特殊な事例ながらこの手法が適切に動作しない場合が存在する。詳細を次項において述べる。

2.3.2.1.1 ipfw における M_SKIP_FIREWALL フラグの影響　FreeBSD の ipfw では、パケットが無限に ipfw ルールの中でループすることがないように、fwd ルールや divert ルールにマッチしたパケットは、その後再度 ipfw ルールを通過することがないように、ipfw ルールを一度通過したパケットには M_SKIP_FIREWALL フラグが立てられるように設計されている。

そのため gif トンネルを利用している際には、gif encapslate された状態と外れた状態とでそれぞれ ipfw ルールにより fwd しようとしても機能しない。

2.3.2.1.2 Internally generated Packet の問題
別の問題として、ICMP による Port Unreachable の応答や TCP reset 等の internally generated packet は ipfw を通過しないために Default Route に従ってパケットが送出されてしまうという問題がある。

2.3.2.2 Routing テーブルを拡張する手法

カーネル内におけるルーティングテーブルの検索である rtrequest1 等のコールにおいて、ソースアドレスの情報にもとづいた応答をするように拡張を行った。

まず、アドレス変更情報を抽出するために、routing socket に対するアドレス通知を監視し、その情報を Source Address Based Routing Table（SABR テーブル）に保存するようにした。

次いで、struct route にソースアドレスの情報も含めることが出来るように拡張をした。

```
+++ ./sys/net/route.h Thu Mar 23 12:22:53 2006
@@ -48,6 +48,9 @@
 struct route {
        struct  rtentry *ro_rt;
        struct  sockaddr ro_dst;
+#ifdef SABR
+       struct  sockaddr ro_src;
+#endif
 };
```

また、rtrequest1 等でルーティングエントリーを検索した結果が Default Route にもとづくものであることを示すために、rt_flags に対して RTF_DEFAULT というフラグを追加した。

その上で、rtrequest1 が呼び出された際、その応

答に RTF_DEFAULT フラグが含まれている時には、続いて SABR テーブルを検索して、マッチした際にはその内容を返し、マッチしなかった場合にはもとの応答をそのまま返すようにした。

また、SABR エントリーを一覧表示するためのコマンドとして sabr_ctl というコマンド、及び、route コマンドを拡張し、“route add -sabr SRC GATEWAY” のような手法で手動で SABR エントリーを操作できるようにした。

2.3.3 IRC サーバにおける実験

上述した kernel に対するパッチを irc-new.media.kyoto-u.ac.jp に導入して動作を確認している。このサーバは物理インターフェイスが 6 つある複雑な構成のサーバであるが、現在のところ意図通りに動作している。

2.4 SCTP（Stream Control Transmission Protocol）の利用

複数の IP アドレスを用いて安定した持続的接続を行う目的に適したトランポートプロトコルである SCTP を IRC サーバ間接続および IRC ユーザ接続に利用することにより、これらの接続を安定させることが出来るかどうか調査している。

詳細は `https://member.wide.ad.jp/wide-confidential/memo/wide-memo-irc-sctp-research-02.txt` を参照のこと

SCTP は 1 つの接続において両端のホストがそれぞれ複数のアドレスを用いることが出来、これらのアドレスの変化や経路の障害などに対して冗長性を確保することが出来るようになる。

IRC ワーキンググループはこの 1 年間にわたり SCTP ワーキンググループと協調して開発などを行い、SCTP ワーキンググループの行った実証実験においては持続的な接続を行うアプリケーションの例として IRC が利用された。

その結果、定量的な評価は難しいものの、有線接続から無線接続へ、そして PHS へと接続を維持したまま移行できることは、非常に気分のいいものであると感じられた。

SCTP 側の実装がまだ不十分なのか、時々 SCTP 実装に起因する問題により接続が切れることがあったが、これらの問題が解消し次第日常的に利用したいと考えている。

この実験について詳しくは SCTP ワーキンググループの活動報告を参照して頂きたい。

第 3 章　IRC サーバの利用と分析

IRC ワーキンググループでは運用する各 IRC サーバにおいて IRC クライアントの接続状況などを記録している。ここではそれらのうち、IRC クライアントの同時接続数からみた利用状況を分析し、それらを通して見たインターネット利用状況とその変化について、得られた分析結果を報告する。

3.1 IRC クライアントの同時接続数

IRC クライアントの同時接続数とは、各 IRC サーバまたは IRC サーバ網へ、ある時刻において同時にいくつのクライアントが接続されているかを示す。メールやウェブなどの利用とは異なり、IRC では一つの TCP コネクションを張り続けたままメッセージのやり取りを行ない、サーバとクライアントが再起動しなければ 1 年以上も接続されたままという状況も見られる。したがって、IRC の利用状況の推移を観察するにはこの同時接続数が適している。

利用時間帯によって同時接続数の変動が大きいため、ある期間内の最大同時接続数と平均同時接続数の二つの数値が重要となる。また、時間帯別の分析を行なう場合は、ある時刻の同時接続数を例えば 365 日分といった一定期間分だけ集めたものの平均値という意味で、その時刻の平均同時接続数と定義する。

尚、今回の報告においては、特にサーバ別の同時接続数と明示していない限り、IRCnet-JP 全体への同時接続数について扱う。

3.2 最大同時接続数と平均同時接続数の推移

現在までの大きな流れ全体を見るために、各週における最大同時接続数と平均同時接続数の推移を示したのが図 3.1 である。

ところどころ大きく垂れ下がっている部分のうち、毎年の年末年始と八月のお盆にあたるものは季節的要因である。詳しくは、3.4 節の特殊な時期の最大同時接続数の分析のところで述べる。

2000 年前後では最大同時接続数と平均同時接続数

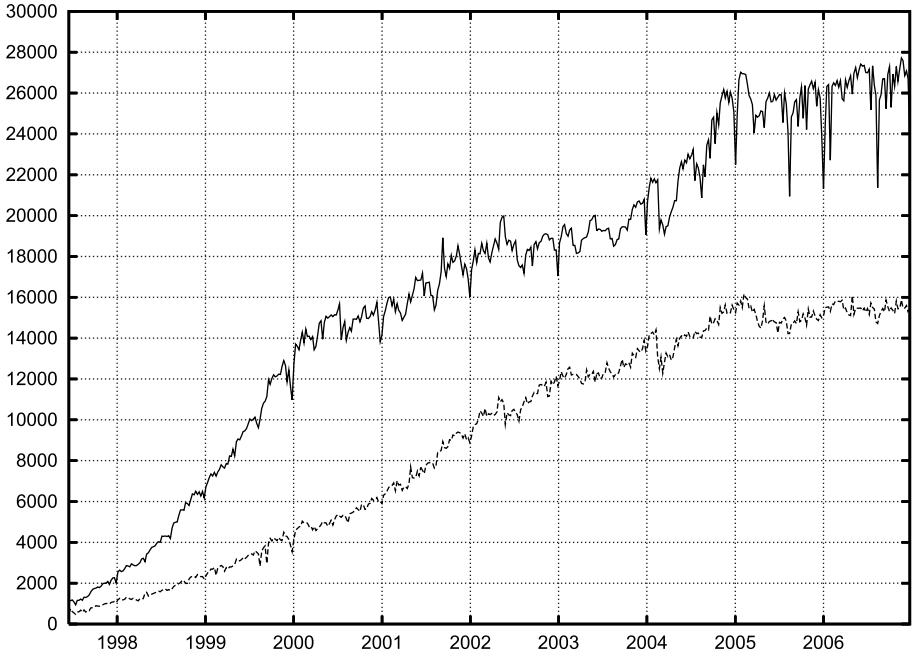

図 3.1. 同時接続数の各週最大値と平均の推移

の差が 3 倍前後と大きく開いており、これは当時のインターネット利用形態に起因する。詳しくは、3.5 節の各時刻における平均同時接続数の変動のところで分析する。

最大同時接続数も平均同時接続数も右肩上がりに伸びてきたが、ここ 2 年は平均同時接続数が伸び悩む中で最大同時接続数のみ伸びている。詳しくは、3.6 節の各曜日における時間別同時接続数の変動のところで分析する。

3.3 サーバ別の最大同時接続数の推移

2006 年の各サーバ別の最大同時接続数の推移を示したのが図 3.2 である。一部の例外を除くと年間を通しての大きな変化はあまり見られないが、どのサーバにおいても常に一週間のサイクルで変動している。詳しくは、3.6 節の各曜日における時間別同時接続数の変動のところで分析する。

例外的な動きのほとんどは理由を説明することができる。その一つはサーバ所在地の計画停電によるサーバの一時的停止が挙げられる。まず、10 月 22 日の奈良先端科学技術大学院大学（NAIST）の計画停電により、irc.nara.wide.ad.jp の利用者が、irc.tokyo.wide.ad.jp などの他のサーバへと接続する先を移動したであろうことが読み取れる。また、12 月 2〜3 日と二日間にわたり慶應義塾大学湘南藤沢キャンパス（SFC）にて計画停電が行われたため、irc.fujisawa.wide.ad.jp の利用者が急激に減っている。さらに、12 月 23 日にも NAIST が計画停電となって同様に減少している。もう一つの例外的な動きとしては、1 月初めや 8 月半ばに見られるように、全ての IRC サーバにおいて同時に接続数が大きく減少しているのが見られる。詳しくは、3.4 節の特殊な時期の最大同時接続数の分析のところで述べる。

3.4 特殊な時期の最大同時接続数の分析

ここでは、2006 年の図 3.2 で見られるサーバ一斉での例外的な接続数の激減が、例年発生しているかどうかを調べるために、さらに詳細に分析する。まず、5 年分の年末年始における最大同時接続数の推移を示したのが図 3.3 である。

このような形で焦点を当てると一目瞭然となるように、年末年始の接続数の激減は毎年発生していることがわかる。また、5 年分の 8 月のお盆における最大同時接続数の推移を示したのが図 3.4 である。こちらも同様に各年ともに落ち込んでいることが判明した。これらの点は、3.6 節で述べる日曜日の利用増加とは対照的な結果となっている。ところで、8 月 14 日に東京方面で送電線の切断による大規模停電が発生した。この停電はかなり影響範囲の大きなものであったが、偶然にもお盆と時期が重なっておりも

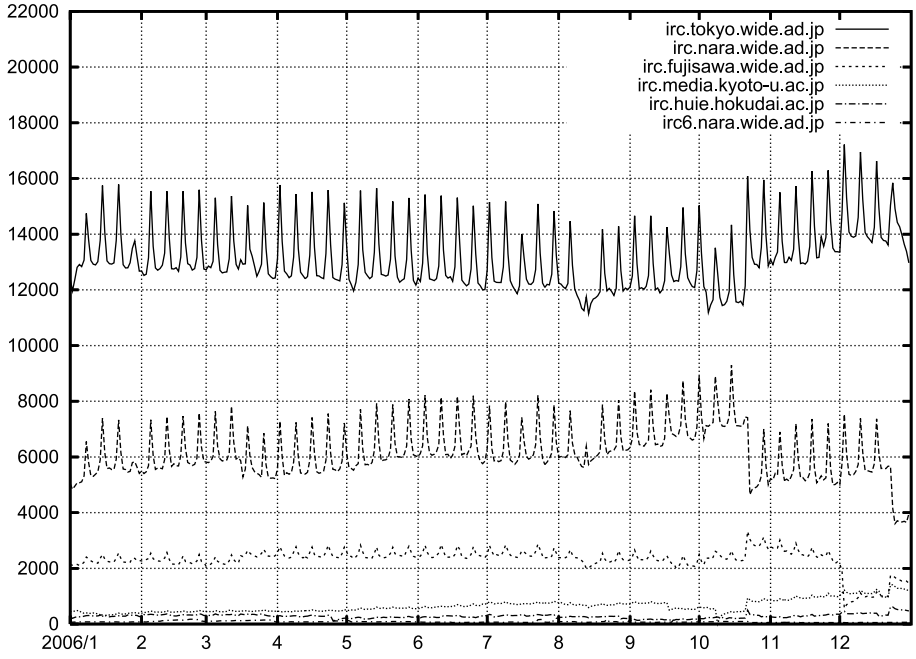

図 3.2.　サーバ別の最大同時接続数の推移

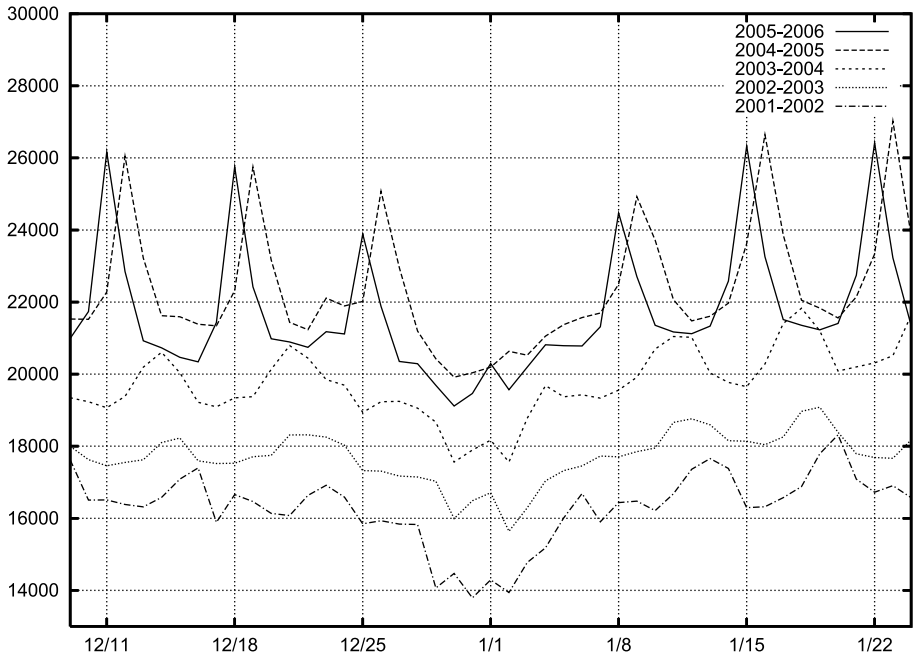

図 3.3.　年末年始の最大同時接続数の分析

ともと利用者が減少する傾向にある時期であったためか、記録の上では特に大きな変動としては現れていない。

3.5 各時刻における平均同時接続数の変動

2000 年から 2006 年までの各年において、各時刻ごとの年間を通した平均同時接続数の一日の変動を示したのが図 3.5 である。見やすく表示するため、横軸の始点と終点を正午としている。

2000 年と 2001 年においては 23 時を境に急激に接続数が増えており、日が変わって 0 時から 1 時の間でピークを迎え、朝 8 時には落ち込みが見られることから、当時の利用者は固定料金で利用できるテレホーダイの影響を強く受けていたことがわかる。こ

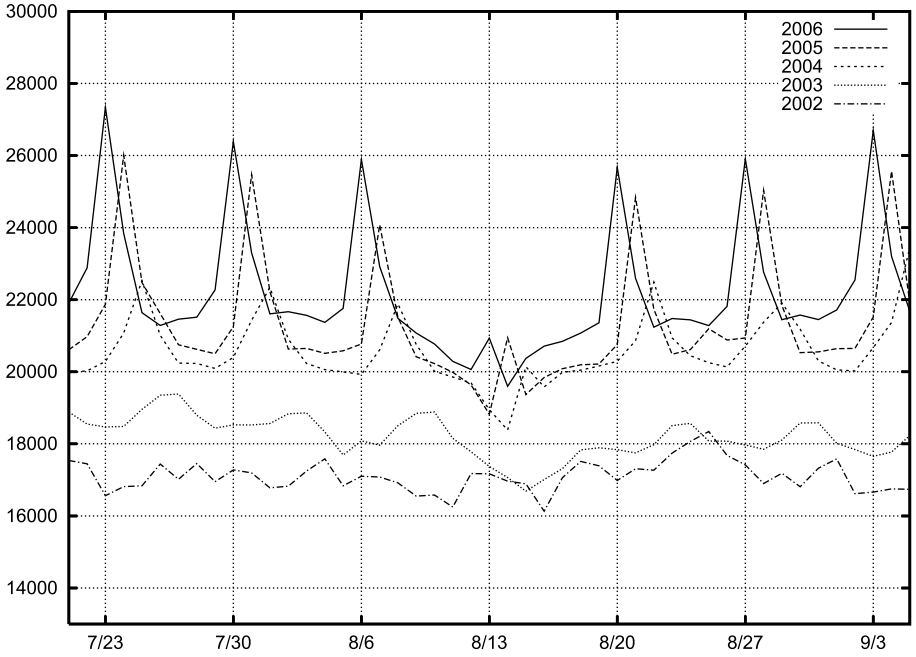

図 3.4. 8 月のお盆の最大同時接続数の分析

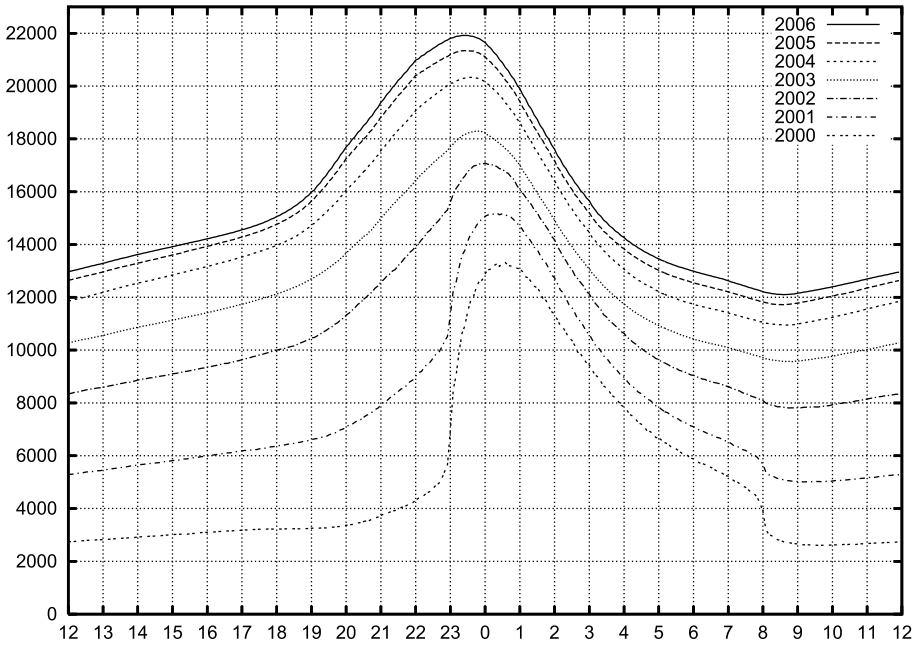

図 3.5. 年別の平均同時接続数の一日の変動

のため、2000 年は一日のピークと日中では同時接続数に 5 倍もの開きが生じていた。

一方、2002 年以降は ADSL 等の常時接続回線が普及し、時間を気にせず利用出来るようになったため、時間帯による差異が減っていった。また、利用のピークが 1 時（25 時）から 23 時へと徐々に移動してきたことも読み取れる。

3.6 各曜日における平均同時接続数の変動

各時刻ごとの 2006 年の年間を通した平均同時接続数を各曜日別に一日の変動を示したのが図 3.6 である。平日はほぼ同じ軌跡を取るため、Weekday として表示している。

図において最も高い位置のものが日曜日であり、

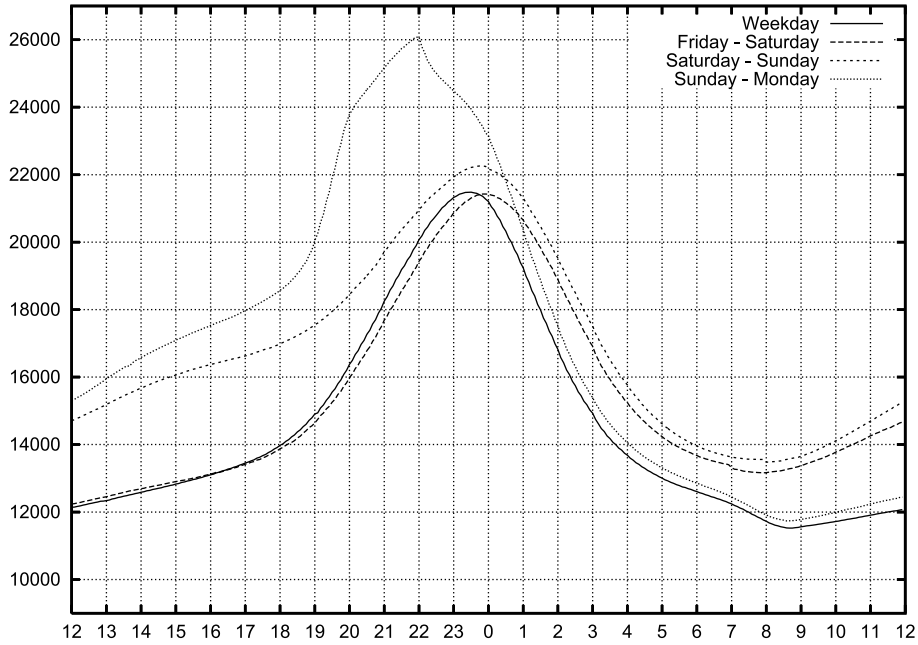

図 3.6.　曜日別の平均同時接続数の一日の変動

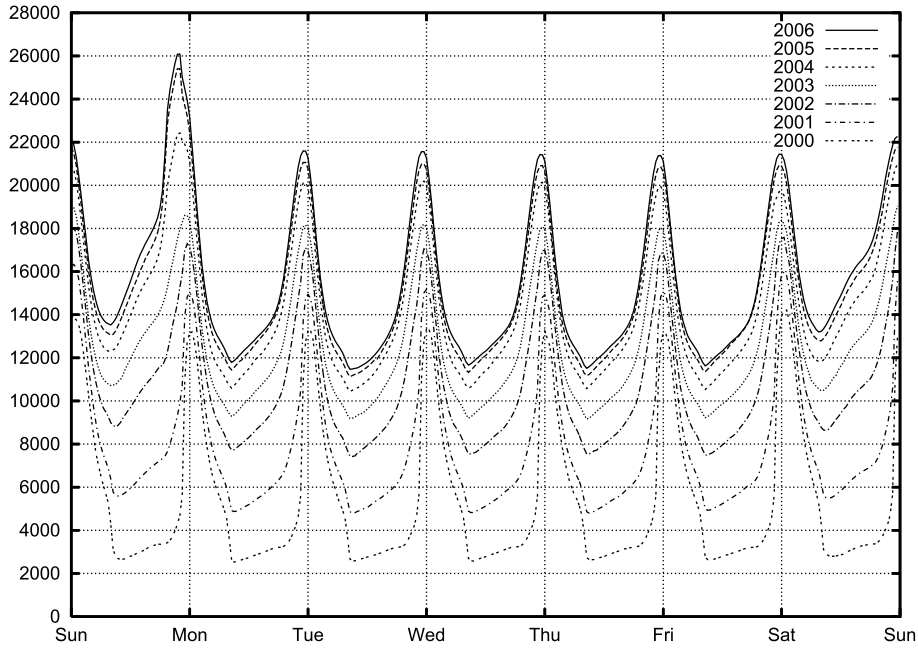

図 3.7.　年別の平均同時接続数の一週間の変動

次が土曜日となっている。金曜の夜は他の平日と比べるとわずかに接続数が少ないが、日が変わって土曜日になると同時に平日より大きく上回るようになる。そして、土曜から日曜にかけて更に上回って順調に推移したあと、日曜の夕方以降は急激に上昇していって日曜の 22 時にピークを迎える。そして急激に接続数が減っていき、日が変わって月曜になると再び平日とほぼ同様の動きへと戻っている。つまり、利用者全体の傾向としては日曜は早めに切り上げる生活サイクルが見られる。

土日は平日よりも接続数が多くて特に日曜が飛び抜けて乖離している状況は、2006 年のみの現象なのかどうかを調査するために、2000 年から 2006 年までの各年において、曜日別で各時刻ごとの平均同時

接続数の一週間の変動を示したのが図 3.7 である。

2004 年以降は特に日曜日が突出した形で乖離していっていることが判明した。そして、このことが図 3.1 における最大同時接続数だけが伸びている要因であり、また、図 3.2 における顕著な一週間サイクルを引き起こしている要因でもある。

第 4 章　まとめ

運用という側面では安定期に入った IRC ワーキンググループではあるが、研究課題という観点ではまだまだ開拓の余地がある。

一例をあげると、Lingr 等の Web アクセスを利用したコミュニケーションツールが近年注目を集めているが、これらは「IRC のような」サービスを目指しつつも、プロトコル上の制約により十分に満足のいくものとはなっていないように思える。同時に IRC を Web から利用するサービスアプリケーションも多数開発されてはいるが、いずれも非同期・リアルタイムなコミュニケーションサービスを提供するにはいたっていない。

今後も研究と運用の相補的な発展を目指していきたい。