# 第ⅩⅥ部

# ＩＲＣの運用状況とデータ解析

# 第16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は、IRC(Internet Relay Chat) に関する研究と、そのためのテストベッドとしての IRC サーバ網の運用を行っている。

2002 年の IRC ワーキンググループの主な活動内容は、これらの IRC サーバの安定運用であった。IRC サーバは他のワーキンググループでの連絡用などにも使われており、そのインフラストラクチャーとしての重要性は高い。

本報告書では、まず最初に IRC と我々 IRC ワーキンググループの活動について簡単に紹介する。次に、2002 年の活動についての報告と、その活動の一環として運用した IRC サーバのログの解析を通じた考察を行う。最後に、2003 年の活動として、2002 年とは少し違う形を検討していることを踏まえ、その研究の方向性について、ここで述べておきたい。

## 第2章　IRC と IRC ワーキンググループ

IRC は、元々、文字ベースのチャットシステムとして開発された。IRC システムには、ユーザとのインターフェースを提供するクライアントと、メッセージの転送を受け持つサーバが存在する。IRC のネットワークは、基本的には、サーバを中心とするスター型のネットワークである。それに加えて、複数のサーバを接続することによって、サーバ群を形成することができる。IRC のネットワークは、これら複数のクライアントと複数のサーバから構成される、IP ネットワーク上に構築されたオーバレイネットワークであり、IRC は、その上での汎用的なユニキャスト及びマルチキャスト通信を提供するシステムである、と言える。

IRC ワーキンググループは、この IRC に関する研究をするために設立された。IRC に関する研究には、大きく 2 種類に分けられる。1 つは、IRC のシステム自体の研究であり、もう 1 つは IRC 上で交わされる人と人のコミュニケーションに関する研究である。

IRC ワーキンググループでは、互いに接続された複数の IRC サーバを運用し研究に利用すると共に、一般のユーザに開放している。運用している IRC サーバは、次の 4 つである。

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

これらのうち、irc6.kyoto.wide.ad.jp は IPv6 によるクライアントからの接続を担当しており、他の IRC サーバは IPv4 を使用している。

IRC は人と人の間で使われるコミュニケーションツールであるため、必然的に、コミュニケーション上のトラブルも発生する。こうした場合に、他人に迷惑をかける目的で、システム自体を攻撃対象にするユーザも存在する。これを防ぐためには、IRC のシステムがこうした攻撃によって攻撃者が利益を得ることのないようになっていることが重要である。つまり、攻撃によって IRC サーバが混乱したり停止したりすることのないようにしなければならない。

## 第3章　サーバの運用

IRC ワーキンググループでは、2002 年の主な活動として、IRC サーバの運用を行った。

IRC サーバそれ自体は、大きな不具合があるわけではなく、それほど管理コストが大きいものではない。しかし、今年は、IRC サーバが DoS 攻撃の対象となることが多く、その対応に時間を費した。

DoS 攻撃によって、IRC サーバそのものやその通信線が利用不能になると、その IRC サーバに接続し

ているクライアントに影響が出るだけでなく、そのIRC サーバが属しているサーバ群全体が不安定な状態に陥いることがある。

2002 年に IRC WG で運用している IRC サーバが受けた DoS 攻撃は、IRC サーバを混乱を陥れるに留まらず、WIDE バックボーンや、さらには、隣接する AS にまで影響を与えるものであった。

そこで、以下のような対策を施した。

1. IRC サーバが使用する IP アドレスの変更
2. WIDE バックボーンでのパケットフィルターの追加
3. 経路情報の広告範囲の制限
4. IRC サーバ網の国際リンクの多様化
5. サーバ間接続へのトンネリング技術の適用
6. ircd への機能追加 (hemp パッチ)
7. ircd の機能修正 (mod_modproxy バグ修正)

これらのうち、前の 3 つの対策は、即効性を期待した IP ネットワークの運用面からの対処方法であり、一般に DoS 攻撃を受けた場合に応用することができる。次の 2 つは、IRC のサーバ網の運用に関する工夫であり、最後の 2 つは、IRC のシステム自体の DoS 攻撃に対する耐性を高めるための変更である。

上に挙げた対策を施した結果、2003 年 1 月現在、IRC システムを狙った DoS 攻撃は問題となる規模では観測されなくなっている。

### 3.1 IRC サーバが使用する IP アドレスの変更

IRC WG では、IRC サーバの使用するアドレスを 192.244.23.0/24 の空間内にまとめる作業を進めてきた。これは、パケットフィルターや経路の制御などを行い易くするためである。

irc.tokyo.wide.ad.jp と irc.kyoto.wide.ad.jp に引き続き、irc.fujisawa.wide.ad.jp についても、2002 年 7 月 26 日に 192.244.23.3 への IP アドレスの変更作業が完了した。なお、irc.tokyo.wide.ad.jp と irc.kyoto.wide.ad.jp については、2002 年の 1 月と 4 月に作業を行っている。これについての詳しい報告は、2002 年 7 月発行の 2001 年度の WIDE 報告書を参照されたい。

### 3.2 WIDE バックボーンでのパケットフィルターの追加

IRC サーバでは、DoS 攻撃に関係する可能性があり、IRC サーバにとって受信できなくても問題ないパケットを、ルータあるいはサーバの OS に備えられたパケットフィルターによって排除している。これによって、IRC サーバにかかる負荷を軽減し、また、攻撃の危険性を回避している。

従来より、途中ルータでの大まかなフィルタリングと、IRC サーバ自体での細かいフィルタリングを行ってきている。この使い分けの理由は、途中ルータにて細かく長いルール設定により負荷が上昇することを避けるため、ならびに、IRC サーバ自体では運用状況により機動的に細かい設定を行えるようにするためである。

一方、昨年度は irc.tokyo.wide.ad.jp が東京 NOC 内に設置されていたが、前者のルータによるフィルタリングがルータの性能を越えたため過負荷になって破綻した。これはルータのフィルタリング性能が低く、1 万パケット/秒程度の攻撃に耐えられない仕様であるためであった。

この問題を解決するために今年の 4 月に irc.tokyo.wide.ad.jp は大手町 NOC 内に移設を行った。同時に、サーバが稼働する PC の性能を上げ、IRC サーバ上のみでフィルタリングをするとともに、攻撃パケットの採取記録をして分析を試みる体制へと移行した。

当初は攻撃に対してパケットの記録なども行うことができ、例えばソース IP アドレスがクラス E やプライベートのものまで来ていることが確認された。しかし、すぐに攻撃の度合いが強まった結果、パケットの採取記録による負荷が大きくなり、IRC サーバの運用自体に問題が出るようになった。つまり、IRC サーバが過負荷になることにより、クライアントだけでなくサーバ間に流れるデータを処理できなくなり、結果として、攻撃側の目的であるサーバ間の切断を招いた。

対応策として、攻撃パケットの記録を徐々に中止していき、最終的に、フィルタリングのみの設定運用になった。しかし、攻撃手法が完全に SYN などの小さいパケット怒涛攻撃に移り、10 万パケット/秒近くの攻撃になった結果、IRC サーバ上のみでのフィルタリングでは、再び過負荷になって IRC サーバの運用自体に影響が生じるようになった。

そこで、WIDE バックボーンの運用を担当する TWO WG と議論の上、2002 年 7 月より、バックボーンのルータ自体にパケットのフィルタリングを

行わせることにした。

現在フィルタリングを行っているルータは、以前とは異なり、10 万パケット/秒級の攻撃にも対応することができている。また、細かなフィルタリング設定は以前と同様に IRC サーバ上で行っている。

### 3.3 経路情報の広告範囲の制限

DoS により、WIDE バックボーンと隣接 AS との間の回線だけに留まらず、隣接 AS 内、さらにその向こう側の回線など、広汎な影響が観測されたため、BGP による経路制御を利用した対策を行うことにした。

IRC サーバによって利用されている IP アドレスブロック 192.244.23.0/24 に関する経路情報は BGP によって広告されているが、必要な AS 以外には広告しないようにした。IRC WG で運用している IRC サーバへの到達性が必要な AS は次の 2 種類である。一つは、日本国内で運用されている AS である。これは、IRC WG で運用している IRC サーバは、日本国内からのクライアントの接続を対象にしているためである。もう一つは、海外の AS のうちサーバ間接続に必要な AS である。

これにより、192.244.23.0/24 宛の経路を持っていない AS からは、そもそもパケットが出てこないため、パケットのフィルタリングと似た効果が得られる。

### 3.4 ircd への機能追加 (hemp パッチ)

2002 年 8 月 24 日から IRC サーバを hemp パッチのあてられたものに変更した。hemp パッチの提供する新機能は IRCnet の split detection である。連結された IRC サーバ群全体の Global servers/users があらかじめ設定された閾値を下回ると IRC サーバは split mode に移行する。IRC サーバが split mode 中であると、クライアントは新しい channel を作るときに channel operator 権限を得られない。

国内の IRC サーバはこれまで DDoS に悩まされていた。日本の IRC サーバ を IRCnet から split させるために、IRC サーバやサーバ間接続経路上のルータが DDoS の対象となるのである。IRC サーバが IRCnet から独立すると channel/nick 情報の同期が不能となる。その隙に独立してしまった IRC サーバに接続し channel/nick を乗っ取る、というのがこの DDoS の主な理由であった。hemp パッチは IRC サーバがなんらかの理由で IRCnet から切断状態にあると、channel operator 権限を新規に与えないものであるため、split させる、すなわち DDoS の対象とする意味をなくすものである。そのため、現時点では DDoS 削減に非常に有効な手段であるといえる。本来、海外のユーザは日本の IRC サーバに接続できないが、DDoS が主に海外からである理由のひとつは、日本には踏台となるホストが多く存在しているため国内からの接続のように振舞うことができることである。この点への対策は次節で述べる。

2002 年 8 月現在、海外ではすでに hemp パッチをあてて既に 300 日近く運用され続けているサーバもあった。当時 IRCnet には 120 近くのサーバがあり、実に 80 以上ものサーバで hemp パッチは使われていた。その実績から今回のパッチ導入に踏みきったものである。

### 3.5 ircd の機能修正 (mod_webproxy バグ修正)

現在、IRC WG で運用している IRC サーバでは、mod_webproxy というモジュールを組み込んでいる。このモジュールは、HTTP の CONNECT メソッドを利用した Open Proxy を検出し、それを利用している可能性のあるクライアント接続を排除するものである。Open Proxy は、不正な行為を行おうとするユーザによって、使用されると考えられる。なぜなら、IRC サーバ側からクライアントのユーザを辿ることが難しくなるためである。

また、もともとの mod_webproxy モジュールには複数ポートを検出するよう設定している場合、先に一つでも TCP コネクションを張ることができてしまうと残りのポートを調べに行かないというバグがあったため、これについても修正するとともに、HTTP サーバからの返事を記録するよう拡張を行って運用をしていた。

しかし、このモジュールの利用にもかかわらず、Open Proxy を利用したクライアント接続が行えることが発見されたため、IRC WG で調査を行った。その結果、このモジュールにバグがあることが発見された。このバグを修正した mod_webproxy モジュールを 2002 年 11 月 10 日から運用している。その結果として、1 日あたりの平均 Open Proxy 検出数を比較してみると、修正前の 2002 年 11 月 1 日〜10 日の期間では 55.1 回であるのに対し、修正後の 2002 年 11 月 11 日〜20 日では、467.7 回となった。

なお、IRC WG では、このバグと修正方法を IRCnet のオペレータ用メーリングリストで報告し、IRCnet の他のサーバ運用者にも注意を促した。

同様に Open SOCKS を検出する mod_socks というモジュールもあり、以前に、大きな実装ミスを発見して修正するなどの貢献をしている。

### 3.6 IRC サーバの国際リンクの多様化

日本では欧米との接続以外に、以前にマレーシアとの接続も行っていたが、これはあくまでも*.my というリーフ扱いの接続であった。

一方、DoS 攻撃対策のために、新たに日本と台湾の間での接続が行われた。これは、互いにトランジットを許すことで、例えば、日本側が太平洋越えリンクを利用して国際接続をすることなく、台湾経由で欧米などのサーバとつながるようになり、逆の場合も含めて互いに攻撃による影響を抑えることを実現している。

運用上の注意点としては、日本と台湾が直接つながっているときに、両者が同時に太平洋越えリンクにて欧米側とつながることを避けるため、サーバ間接続の制限機能を利用して互いに注意深く設定をしている。

また、台湾側のサーバでは複数 AS にインタフェースを持つことで、利用可能な経路を使い分けているが、現在、日本と台湾の間のサーバ間接続が通る IP 経路に問題が生じたため、調整が行われる予定である。

### 3.7 サーバ間接続の柔軟化

IRC のサーバ間接続においては、使用される自分の IP アドレスは無指定か、あるいは指定した IRC サーバで利用する IP アドレスの固定になる。また、使用される相手の IP アドレスについては自由に設定できるが、そのアドレスについては一般に公開される形となる。

IRC ワーキンググループでは、DoS 攻撃対策の一貫としても役立つよう、サーバ間接続の別経路化、多重切替、ならびに隠蔽化を実現するために、任意の設定で TCP を中継する tcpbridge という小さなプログラムを用いてサーバ間接続の運用を行っている。これにより、以下の効用を実現している。

- 任意の別経路地点での中継 (通常通らない経路を用いることが可能)
- ローカルで中継することで中継点や相手先の隠蔽 (IRC サーバからは::1 や 127.0.0.1 への接続に見える)
- 複数 IP アドレスを持っている場合の自由な使い分け (WIDE の運用では IRC サーバのアドレスとは別にホスト自体のアドレスもある)
- 複数インタフェースを持っている場合の自由な使い分け (DoS 攻撃が来るクライアント受理用と別のインタフェースを利用できる)
- 両者のローカルで中継することでの利用経路の自由選択 (例えば IPv4 サーバ同士が IPv6 にて接続も可能)
- 中継相手先を複数列挙指定することでの経路の多重切替 (例えば IPv6 でだめなら IPv4 で接続という運用が可能)

以前より開発して用いている tcpbridge は以下の機能を持っている。

- IPv4 と IPv6 の混在指定が可能
- listen するアドレスの複数列挙可能
- accept する相手アドレスの制限が可能
- connect しに行く時の自分のアドレス候補の複数列挙可能
- connect しに行く時の相手のアドレス候補の複数列挙可能

これを用いることで上述のサーバ間接続の柔軟化を実現している。

## 第 4 章　IRC の利用状況と分析

### 4.1 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。

ここ 2 年間の国内の IRCnet のユーザ数の推移を図 4.1 に示す。IRC サーバは時間帯などによりユーザ数が大きく推移するため、グラフの上端が同時最大接続者数を示し、グラフを底辺で支える部分が閑散時の同時接続者数を示す。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いるが、そのユーザ数はこれまでずっと増加傾向にあった。しかし、ここ 1 年間の最大同時接続者数に

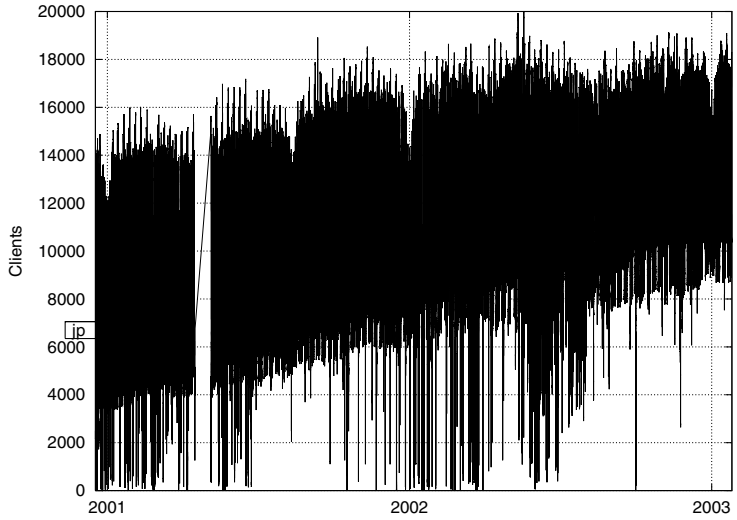


**図 4.1**. IRCnet の国内ユーザ数の状況

変化はなく、その理由には各サーバのユーザ認証を以前より厳しく設定したため、同一ホストから多数のクライアントが接続できなくなったことが考えられる。閑散時のユーザ同時接続数は順調に延びており、2003 年 1 月には常に 8000 人以上が接続している。この傾向から、インターネットの利用に常時接続を用いている IRC ユーザが増加していると考えられる。今年度の最大同時接続ユーザ数は 19979 人であり、2002 年 5 月 19 日の 0 時 34 分に観測された。

**表 4.1**. 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 |
| .tw | irc.nctu.edu.tw | 163.28.64.210 |

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。国外の接続先サーバを表 4.1 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、国外に対して日本側のサーバは*.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。

**表 4.2**. 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 |

現在接続されている国内の IRCnet のサーバは表 4.2 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。そのうちユーザ収容数が多い irc.kyoto、irc.tokyo、irc.fuijsawa の 3 台において、2002 年 4 月から 2003 年 1 月までのユーザ数の推移を解析した。

### 4.2 サーバ毎のクライアント接続数の分析

今年度は、irc.kyoto.wide.ad.jp において 3 分ごとに集計している、国内の各サーバの収容ユーザ数を元に解析を行った。

各サーバにおける一日の最大同時接続者数をグラフ化したのが図 4.2 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 4.2 によると、5 月から 7 月の間 irc.tokyo の利用者が激減しており、その変わりに irc.kyoto に最大 1 万 2000 近くの利用者が集まっていることが分かる。この時期は DoS による攻撃が irc.tokyo に向け

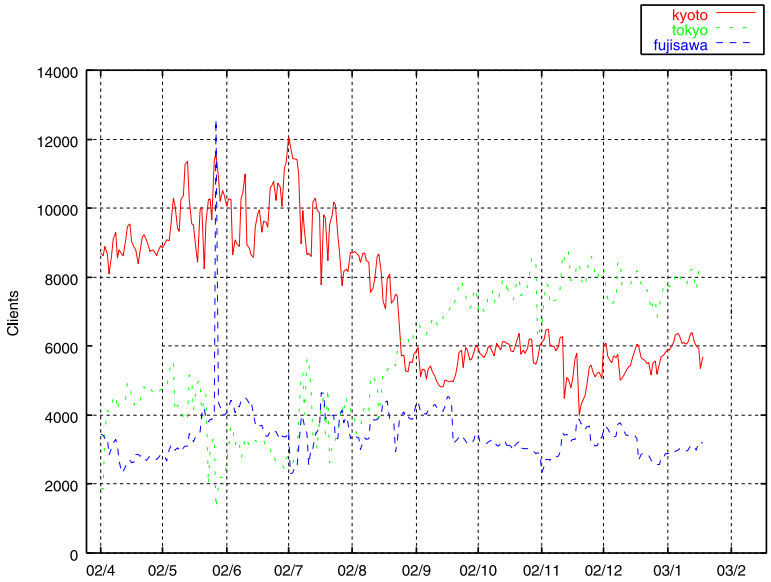


**図 4.2**.　2002 年度のクライアント数の変化

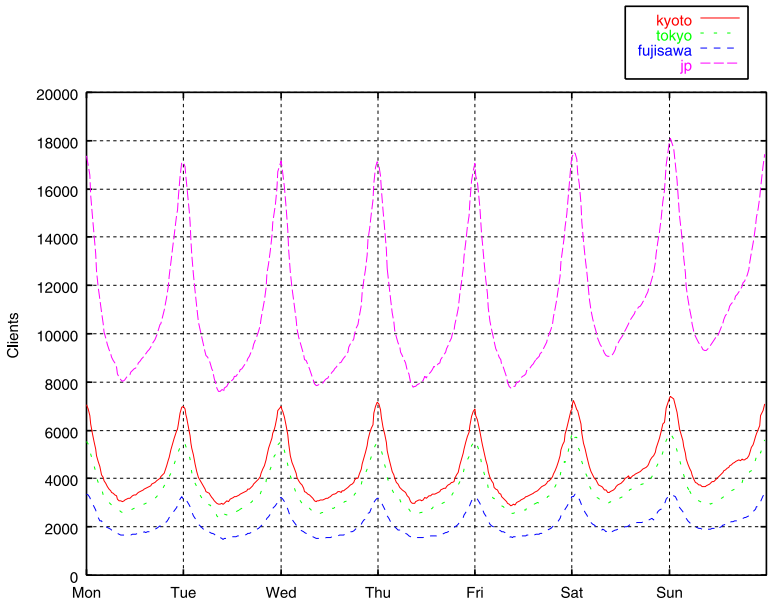


**図 4.3**.　2002 年度の週間のクライアント数の変化

られ、サーバ間のリンクが切れたため、利用者が他の利用者と会話するために同一のサーバ (irc.kyoto) に接続を試みたことが考えられる。逆に、8 月から 9 月の間は irc.kyoto の利用者が激減し、irc.tokyo にユーザが集まっていることが分かる。この時期は DoS 対策のため IRC サーバ間のリンクに現在攻撃を受けずらい IPv6 ネットワークを導入した時期であり、その効果があがったため、それまで irc.kyoto を一時的に利用していたユーザが irc.tokyo につなぎかえた可能性がある。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 irc.tokyo が不安定だったために irc.tokyo へ到達できなくなると irc.kyoto や他のサーバに自動的につなぎかえていたものが、irc.tokyo 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たとも考えられる。irc.fujisawa については年間を通して大きな変化がなく、最大接続時に 3000 程度のユーザを収容している。

年間を通して週の各時刻ごとの平均をとり、グラフ化したものが図 4.3 である。

図 4.3 によると、昨年度と同じくサーバごとの変

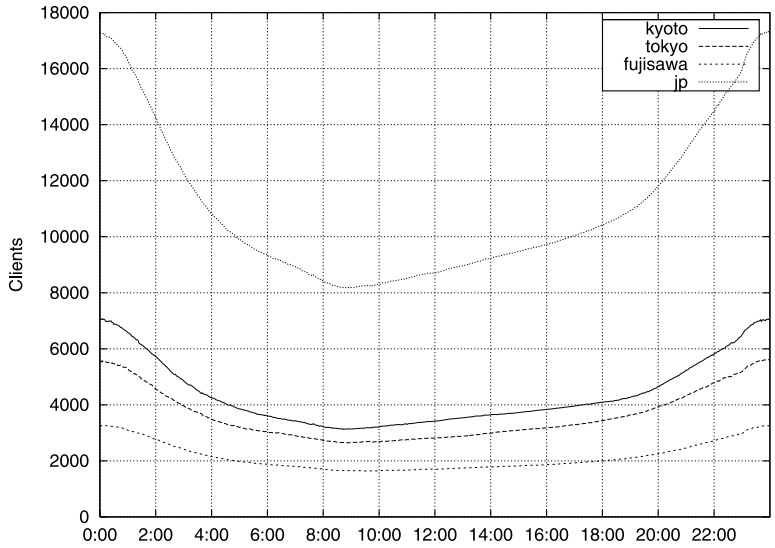


**図 4.4**. クライアント数の 24 時間での変化

化のパターンの違いはほとんどない。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、土曜・日曜の昼間は平日と比べてユーザ数の減少が少ないことが分かる。

年間を通して一日の各時刻ごとの平均をとり、グラフ化したものが図 4.4 である。

時間ごとの変化をみると、全てのサーバで同じ変化を示している。昼間がいちばん少なく、夕方から夜にかけてにユーザ数が増加し、夜 12 時頃を頂点にしてその後序々にユーザ数が減少している。昨年から、テレホーダイ時間 (夜 11 時から朝 8 時まで) の開始時刻・収量時刻付近におけるユーザ数が変化が緩やかになる傾向があったが、今年はその影響がほとんど見られなくなった。

### 4.3 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。2002 年度のデータを図 4.5 に示し、

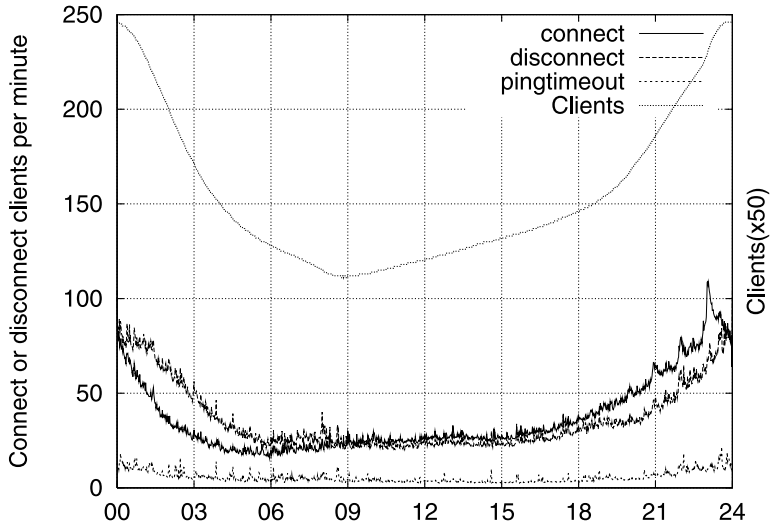


**図 4.5**. IRC 接続数の一日の変化 2001 年度

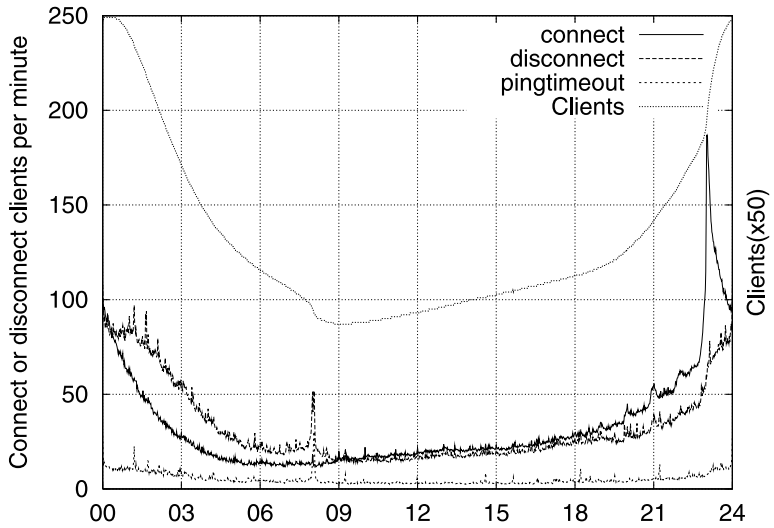


**図 4.6**.　IRC 接続数の一日の変化 2000 年度

昨 2001 年度のデータを図 4.6 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。

昨年度は、それまでに比べ傾向が弱くなっていたものの、Connect 数が 23 時のテレホーダイ開始とともに急激に増加し、朝 8 時のテレホーダイ終了付近に Disconnect・Pingtimeout が増加していた。しかし、今年度はそのような傾向がほとんど見られず、IRC の利用者の接続・切断はテレホーダイとほとんど無関係であることが分かった。

また、図 4.1 に示した通り、ここ一年間の最大同時接続者数はあまり変化していないが、図 4.5 と図 4.6 との比較から平均的な接続者人数は増加していることが分かった。

夕方 18 時頃から利用者数・Connect 数が増加しているのは、常時接続の利用者が帰宅後すぐに IRC に接続しているからと考えられる。また、閑散時の利用者数の減少が昨年度よりも少ないのは、常時接続環境を利用し IRC の接続も維持したままの利用者が増えているからと考えられる。

### 4.4 利用時間分布

クライアントの接続持続時間分布を図 4.7 に示した。2001 年度と 2002 年度を図示し、比較する。横

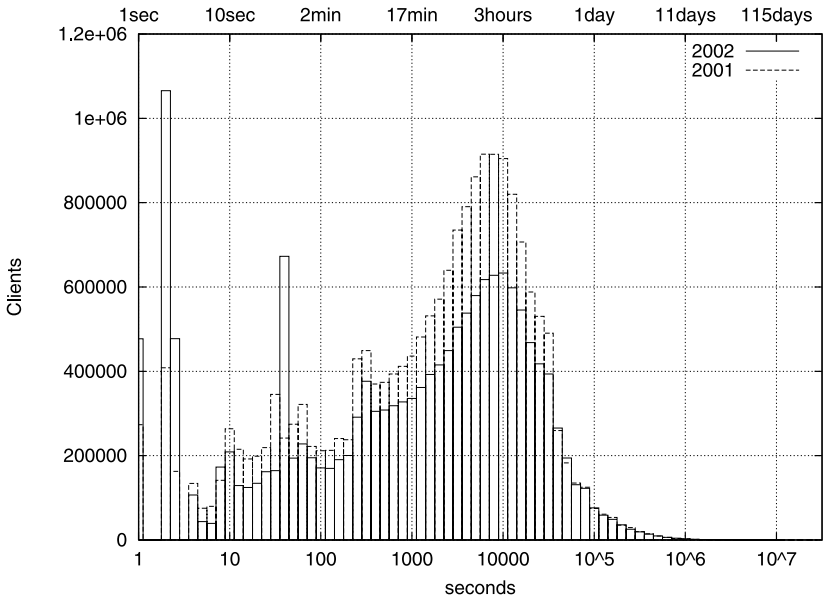


**図 4.7**.　クライアント接続持続時間の分布 (クライアント数)

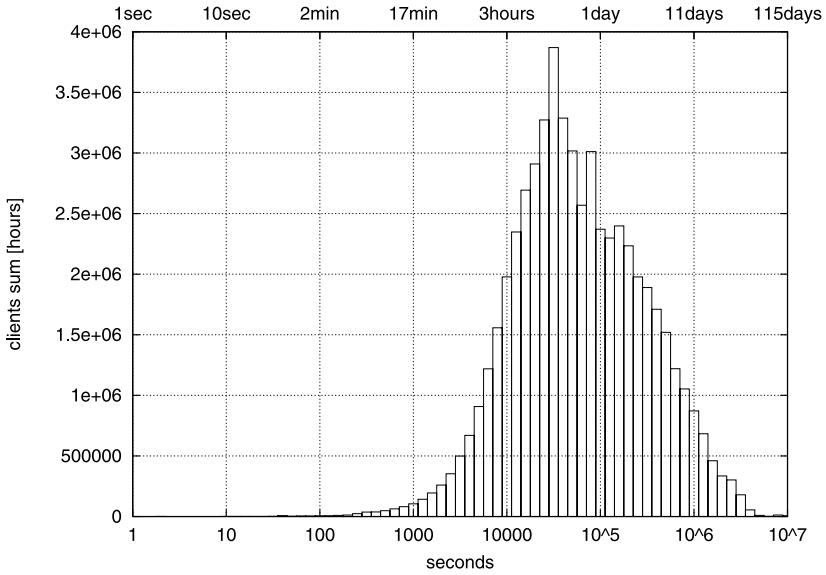


**図 4.8**. クライアント接続持続時間の分布 (クライアント数)

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 $100 * \exp(\log(10)/10)$ 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。特に 3 秒付近て突出しているクライアント数は、この影響が強いと考えられる。

また、数時間接続するクライアント数と一日以上の長期間接続し続けるクライアント数の差が縮小していることがわかる。昨年度よりもクライアント数が少ないのは、本データを集計しているサーバのうち irc.tokyo が今年度の春から夏にかけて利用が少なくなっていたこと、他のサーバに利用者が分散したことによると考えられる。

次に、さきほどと同じ段階で切り、2002 年度の各

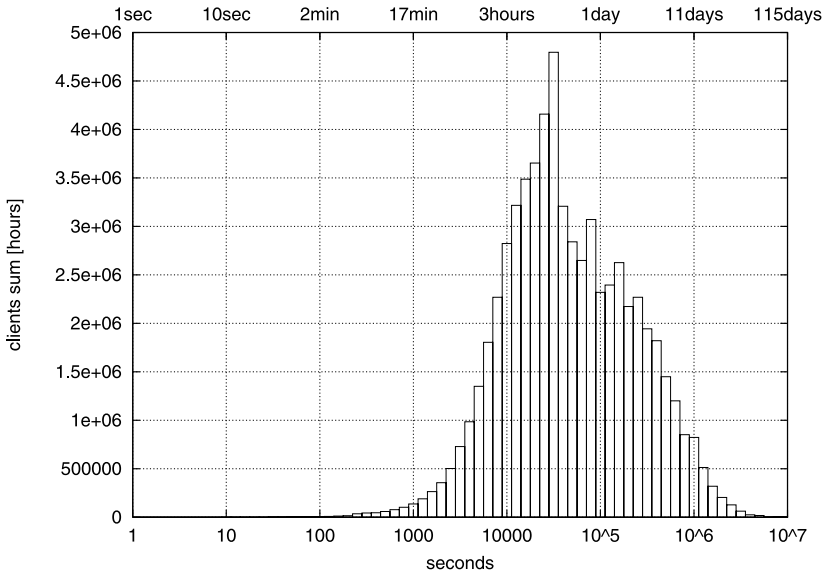


**図 4.9**. クライアント接続持続時間ごとの IRC サーバ接続時間 2001 年度

**表 4.3**.　2002 年度の時間ごとのクライアント接続元の変化

| hour | 0 時 | | | 1 時 | | | 2 時 | | | 3 時 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | AS | clients | | AS | clients | | AS | clients | | AS | clients | |
| 1 | OCN | 978 | 10.88 | OCN | 846 | 10.82 | OCN | 726 | 10.87 | OCN | 642 | 10.96 |
| 2 | ODN | 926 | 10.30 | ODN | 795 | 10.17 | ODN | 667 | 9.99 | ODN | 573 | 9.79 |
| 3 | NTTPC | 875 | 9.74 | NTTPC | 763 | 9.75 | NTTPC | 651 | 9.76 | NTTPC | 570 | 9.73 |
| 4 | INFOWEB | 634 | 7.05 | INFOWEB | 543 | 6.94 | INFOWEB | 458 | 6.87 | INFOWEB | 400 | 6.83 |
| 5 | SO-NET | 504 | 5.61 | SO-NET | 429 | 5.49 | SO-NET | 353 | 5.30 | SO-NET | 301 | 5.15 |
| 6 | ATHOME | 402 | 4.47 | ATHOME | 351 | 4.48 | ATHOME | 296 | 4.45 | ATHOME | 255 | 4.36 |
| 7 | DION | 365 | 4.06 | DION | 315 | 4.03 | DION | 265 | 3.97 | DION | 228 | 3.90 |
| 8 | MESH | 344 | 3.83 | MESH | 289 | 3.70 | IIJ | 246 | 3.70 | IIJ | 219 | 3.75 |
| 9 | IIJ | 319 | 3.55 | IIJ | 284 | 3.63 | MESH | 235 | 3.53 | MESH | 198 | 3.39 |
| 10 | ZAQ | 260 | 2.89 | ZAQ | 221 | 2.83 | ZAQ | 182 | 2.73 | DTI | 158 | 2.70 |
| 全クライアント数 | | 8996 | | | 7828 | | | 6680 | | | 5861 | |

| 時刻 | 4 時 | | | 5 時 | | | 6 時 | | | 7 時 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | AS | clients | | AS | clients | | AS | clients | | AS | clients | |
| 1 | OCN | 588 | 11.04 | OCN | 556 | 11.12 | OCN | 530 | 11.13 | OCN | 499 | 11.12 |
| 2 | NTTPC | 515 | 9.68 | NTTPC | 481 | 9.64 | NTTPC | 456 | 9.59 | NTTPC | 430 | 9.58 |
| 3 | ODN | 512 | 9.62 | ODN | 476 | 9.52 | ODN | 448 | 9.42 | ODN | 415 | 9.26 |
| 4 | INFOWEB | 363 | 6.82 | INFOWEB | 340 | 6.80 | INFOWEB | 323 | 6.79 | INFOWEB | 300 | 6.69 |
| 5 | SO-NET | 268 | 5.05 | SO-NET | 248 | 4.96 | SO-NET | 233 | 4.89 | SO-NET | 214 | 4.78 |
| 6 | ATHOME | 230 | 4.33 | ATHOME | 215 | 4.30 | ATHOME | 204 | 4.28 | ATHOME | 194 | 4.32 |
| 7 | DION | 204 | 3.83 | DION | 189 | 3.79 | IIJ | 179 | 3.76 | IIJ | 168 | 3.76 |
| 8 | IIJ | 200 | 3.77 | IIJ | 188 | 3.76 | DION | 177 | 3.73 | DION | 164 | 3.66 |
| 9 | MESH | 176 | 3.32 | MESH | 164 | 3.28 | MESH | 154 | 3.24 | MESH | 143 | 3.19 |
| 10 | DTI | 143 | 2.70 | DTI | 134 | 2.69 | DTI | 127 | 2.69 | DTI | 120 | 2.67 |
| 全クライアント数 | | 5327 | | | 5001 | | | 4762 | | | 4490 | |

| 時刻 | 8 時 | | | 9 時 | | | 10 時 | | | 11 時 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | AS | clients | | AS | clients | | AS | clients | | AS | clients | |
| 1 | OCN | 488 | 11.23 | OCN | 506 | 11.39 | OCN | 519 | 11.37 | OCN | 531 | 11.32 |
| 2 | NTTPC | 413 | 9.51 | NTTPC | 419 | 9.43 | NTTPC | 427 | 9.36 | NTTPC | 438 | 9.34 |
| 3 | ODN | 397 | 9.15 | ODN | 403 | 9.07 | ODN | 414 | 9.06 | ODN | 426 | 9.06 |
| 4 | INFOWEB | 292 | 6.73 | INFOWEB | 295 | 6.65 | INFOWEB | 301 | 6.60 | INFOWEB | 307 | 6.55 |
| 5 | SO-NET | 202 | 4.65 | SO-NET | 204 | 4.59 | SO-NET | 208 | 4.56 | SO-NET | 214 | 4.57 |
| 6 | ATHOME | 186 | 4.30 | ATHOME | 188 | 4.24 | ATHOME | 193 | 4.24 | ATHOME | 199 | 4.25 |
| 7 | IIJ | 162 | 3.74 | IIJ | 165 | 3.71 | DION | 171 | 3.75 | DION | 177 | 3.77 |
| 8 | DION | 158 | 3.64 | DION | 164 | 3.70 | IIJ | 169 | 3.71 | IIJ | 172 | 3.68 |
| 9 | MESH | 134 | 3.10 | MESH | 137 | 3.08 | MESH | 141 | 3.09 | MESH | 146 | 3.12 |
| 10 | DTI | 113 | 2.61 | ASAHI-NET | 115 | 2.59 | ZAQ | 117 | 2.58 | ZAQ | 122 | 2.60 |
| 全クライアント数 | | 4351 | | | 4445 | | | 4571 | | | 4700 | |

| 時刻 | 12 時 | | | 13 時 | | | 14 時 | | | 15 時 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | AS | clients | | AS | clients | | AS | clients | | AS | clients | |
| 1 | OCN | 546 | 11.30 | OCN | 564 | 11.29 | OCN | 580 | 11.29 | OCN | 598 | 11.32 |
| 2 | NTTPC | 448 | 9.27 | NTTPC | 462 | 9.26 | NTTPC | 475 | 9.26 | NTTPC | 490 | 9.29 |
| 3 | ODN | 439 | 9.09 | ODN | 454 | 9.09 | ODN | 468 | 9.11 | ODN | 483 | 9.15 |
| 4 | INFOWEB | 316 | 6.53 | INFOWEB | 324 | 6.49 | INFOWEB | 331 | 6.45 | INFOWEB | 340 | 6.44 |
| 5 | SO-NET | 221 | 4.58 | SO-NET | 229 | 4.58 | SO-NET | 236 | 4.60 | SO-NET | 243 | 4.60 |
| 6 | ATHOME | 205 | 4.24 | ATHOME | 213 | 4.28 | ATHOME | 220 | 4.29 | ATHOME | 227 | 4.30 |
| 7 | DION | 182 | 3.76 | DION | 187 | 3.75 | DION | 193 | 3.76 | DION | 199 | 3.77 |
| 8 | IIJ | 177 | 3.66 | IIJ | 182 | 3.64 | IIJ | 187 | 3.64 | IIJ | 191 | 3.63 |
| 9 | MESH | 151 | 3.14 | MESH | 158 | 3.16 | MESH | 164 | 3.20 | MESH | 170 | 3.23 |
| 10 | ZAQ | 126 | 2.62 | ZAQ | 132 | 2.64 | ZAQ | 137 | 2.67 | ZAQ | 142 | 2.70 |
| 全クライアント数 | | 4837 | | | 5001 | | | 5139 | | | 5285 | |

| 時刻 | 16 時 | | | 17 時 | | | 18 時 | | | 19 時 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | AS | clients | | AS | clients | | AS | clients | | AS | clients | |
| 1 | OCN | 624 | 11.41 | OCN | 653 | 11.46 | OCN | 688 | 11.51 | OCN | 748 | 11.54 |
| 2 | NTTPC | 509 | 9.31 | NTTPC | 534 | 9.37 | ODN | 567 | 9.50 | ODN | 628 | 9.69 |
| 3 | ODN | 502 | 9.19 | ODN | 531 | 9.32 | NTTPC | 567 | 9.50 | NTTPC | 621 | 9.59 |
| 4 | INFOWEB | 352 | 6.43 | INFOWEB | 367 | 6.45 | INFOWEB | 389 | 6.51 | INFOWEB | 428 | 6.61 |
| 5 | SO-NET | 253 | 4.63 | SO-NET | 266 | 4.68 | SO-NET | 285 | 4.78 | SO-NET | 316 | 4.88 |
| 6 | ATHOME | 236 | 4.33 | ATHOME | 249 | 4.39 | ATHOME | 266 | 4.45 | ATHOME | 294 | 4.53 |
| 7 | DION | 207 | 3.80 | DION | 216 | 3.79 | DION | 225 | 3.78 | DION | 249 | 3.84 |
| 8 | IIJ | 197 | 3.62 | IIJ | 205 | 3.60 | IIJ | 213 | 3.57 | MESH | 231 | 3.56 |
| 9 | MESH | 179 | 3.28 | MESH | 192 | 3.37 | MESH | 206 | 3.46 | IIJ | 229 | 3.54 |
| 10 | ZAQ | 149 | 2.74 | ZAQ | 158 | 2.78 | ZAQ | 168 | 2.83 | ZAQ | 186 | 2.88 |
| 全クライアント数 | | 5471 | | | 5697 | | | 5979 | | | 6486 | |

| 時刻 | 20 時 | | | 21 時 | | | 22 時 | | | 23 時 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | AS | clients | | AS | clients | | AS | clients | | AS | clients | |
| 1 | OCN | 829 | 11.48 | OCN | 912 | 11.39 | OCN | 999 | 11.29 | OCN | 1061 | 11.10 |
| 2 | ODN | 714 | 9.88 | ODN | 802 | 10.02 | ODN | 898 | 10.15 | ODN | 986 | 10.32 |
| 3 | NTTPC | 703 | 9.73 | NTTPC | 791 | 9.88 | NTTPC | 876 | 9.91 | NTTPC | 931 | 9.74 |
| 4 | INFOWEB | 489 | 6.77 | INFOWEB | 553 | 6.91 | INFOWEB | 622 | 7.03 | INFOWEB | 679 | 7.11 |
| 5 | SO-NET | 364 | 5.05 | SO-NET | 415 | 5.18 | SO-NET | 474 | 5.36 | SO-NET | 532 | 5.57 |
| 6 | ATHOME | 330 | 4.58 | ATHOME | 365 | 4.57 | ATHOME | 402 | 4.55 | ATHOME | 424 | 4.44 |
| 7 | DION | 282 | 3.91 | DION | 319 | 3.99 | DION | 354 | 4.00 | DION | 390 | 4.09 |
| 8 | MESH | 264 | 3.65 | MESH | 299 | 3.74 | MESH | 337 | 3.81 | MESH | 371 | 3.88 |
| 9 | IIJ | 254 | 3.52 | IIJ | 280 | 3.50 | IIJ | 307 | 3.48 | IIJ | 334 | 3.49 |
| 10 | ZAQ | 213 | 2.95 | ZAQ | 240 | 3.01 | ZAQ | 269 | 3.05 | ZAQ | 282 | 2.96 |
| 全クライアント数 | | 7228 | | | 8013 | | | 8852 | | | 9559 | |

**表 4.4**. 2002 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 | 133037 | 11.13 | OCN | 391265 | 11.13 |
| 2 | ODN | 114891 | 9.61 | ODN | 367836 | 10.47 |
| 3 | NTTPC | 106216 | 8.88 | NTTPC | 309513 | 8.81 |
| 4 | INFOWEB | 74659 | 6.24 | INFOWEB | 224468 | 6.39 |
| 5 | IIJ | 57002 | 4.77 | SO-NET | 158638 | 4.51 |
| 6 | SO-NET | 51319 | 4.29 | IIJ | 158057 | 4.50 |
| 7 | ATHOME | 45364 | 3.79 | ATHOME | 128593 | 3.66 |
| 8 | DION | 41004 | 3.43 | DION | 113969 | 3.24 |
| 9 | MESH | 36198 | 3.03 | DTI | 113860 | 3.24 |
| 10 | DTI | 27038 | 2.26 | ZAQ | 113033 | 3.22 |
| 11 | ASAHI-NET | 25719 | 2.15 | MESH | 107236 | 3.05 |
| 12 | SINET | 25283 | 2.11 | ASAHI-NET | 91049 | 2.59 |
| 13 | ZAQ | 24727 | 2.07 | AT&T | 66610 | 1.90 |
| 14 | TTNET | 24058 | 2.01 | SINET | 55510 | 1.58 |
| 15 | AT&T | 19314 | 1.62 | TTNET | 53319 | 1.52 |
| 16 | DOLPHIN | 17500 | 1.46 | METALLIC | 41702 | 1.19 |
| 17 | RIM | 15239 | 1.27 | DOLPHIN | 36626 | 1.04 |
| 18 | OMP | 13080 | 1.09 | MEX | 34616 | 0.99 |
| 19 | METALLIC | 12865 | 1.08 | CTC | 32157 | 0.92 |
| 20 | WIDE | 12530 | 1.05 | PSI-NET | 30764 | 0.88 |
| 21 | TELEWAY | 12395 | 1.04 | WIDE | 29451 | 0.84 |
| 22 | CTC | 10781 | 0.90 | HIGHWAY | 28045 | 0.80 |
| 23 | PSI-NET | 10030 | 0.84 | RIM | 27909 | 0.79 |
| 24 | HIGHWAY | 9452 | 0.79 | OMP | 24705 | 0.70 |
| 25 | MEX | 9340 | 0.78 | INTERVIA | 19279 | 0.55 |
| 26 | INTERVIA | 8535 | 0.71 | ALPHA-NET | 19227 | |
| 27 | IDC | 8201 | 0.69 | HANSHIN | 18522 | 0.53 |
| 28 | ALPHA-NET | 7404 | 0.62 | TELEWAY | 17685 | 0.50 |
| 29 | PANANET | 7346 | 0.61 | NCA5 | 17675 | 0.50 |
| 30 | SANNET | 5973 | 0.50 | PANANET | 16029 | 0.46 |
| 全接続時間 | | 1195797 | | | 3514276 | |

ステップの IRC サーバ利用時間の総和を図 4.8 に示した。また前年度の同じグラフを図 4.9 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 4.8 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。また、図 4.8 と図 4.9 の比較から、長時間接続する利用者数と利用者あたりの平均接続持続時間が着実に増加していることがわかる。

### 4.5 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 4.3 である。

図 4.3 及び図 4.4 にて利用が最小になる昼間には、2000 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、昨年度に続き今年度も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 4.4 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、リストされている AS のほとんどが全国にユーザを持っているため、AS ごとにきわだった差はないようである。昨年度と違い、各 AS 間の開きが縮小しているのが特徴である。また、今年は SINET や NCA5 など研究教育系のネットワークが見られ、この点は 2000 年度までの傾向に戻ったと言える。

## 第 5 章　今後の研究について

IRC サーバーの管理と運用、そしてそのサーバー網を利用する中には、いくつもの研究テーマが含まれている。ここでは、研究テーマを次の 4 種類に分類してみることにする。

- 基本となるプロトコルとサーバの改良
- コミュニケーションツールとしての利用
- オーバレイネットワークとしての利用
- IRC サーバ運用で得られる情報の活用

本章においては、今後の研究テーマについて、そのそれぞれの方向性について示しておきたい。

### 5.1 基本となるプロトコルとサーバの改良

IRC システムは、IRC プロトコルによって互いに通信する複数のサーバと大量のクライアントによって構成されている。当 IRC ワーキンググループでも、複数の IRC サーバーを管理・運用している。IRC に関連した研究テーマには IRC サーバーを管理していなければ出来ないものが数多く存在する。これらのテーマに対してワーキンググループとして積極的に取り組んでいくことはある意味責務であるともいえる。以下に今後のテーマとして取り上げられるべきものを列挙する。

### 5.2 IRC プロトコルの改良

IRC プロトコルは RFC 1459 として 1993 年に定義されて以降、本質的には大きな変更をされることなく現在に至っている。この間におけるインターネットの普及やセキュリティーへの意識の変化などから、従来のプロトコルのまま運用することは徐々に厳しいものとなってきている。ワーキンググループとして、次世代の IRC プロトコルについて検討をすることは重要なテーマである。

#### 5.2.1 疎結合な Cluster Server 対応

現在の IRC プロトコルでは、ユーザーは IRC 網に接続するためには、複数あるサーバーのうちどれか一つを選択し、会話を続けるためにはそのサーバーに接続をし続ける必要がある。このような設計のままでは、携帯端末の普及など共にクライアント側がマルチホーム化したような状況において、複数のサーバーを任意のタイミングで切り替えながら利用を継続することが出来ないことを意味する。また、クライアントから複数のサーバーへの接続を許すことが出来るようになると、サーバーの負荷分散にも有効ではないかと考えられる。これは IRC 網の携帯端末を含めた普及に備えて検討しておくべき課題であろう。

#### 5.2.2 Secure IRC net

現在の IRC プロトコルでは、ユーザーが送受信するメッセージは暗号化されることなく流されている。それだけではなく、サーバー間接続をする際に相互認証するパスワードも暗号化されていない。また、利用者認証を行うしかけも存在しない。このような IRC 網では機密度の高い会話を行ったり、パスワードの伝達を行ったりという用途に利用することは出来ない。この現状を踏まえて、IRC プロトコルやサーバーの実装といったものを拡張していくことは研究するべき課題である。

- サーバー間コネクションを SSL などを用いて暗号化する。
- サーバークライアント間コネクションに個人認証（パスワード認証・SSL 個人証明書など）を

導入する。

- チャンネル毎に違う暗号化鍵を利用することは出来るか?

#### 5.2.3 安全なサーバー構築技術の研究

IRC ワーキンググループでは、IRC サーバを運用していく上でさまざまなサーバに対する攻撃を経験している。セキュリティーホールに対する攻撃はもちろん、DoS 攻撃も受けることが多い。攻撃対象も、IRC サーバだけではなく、途中経路のルータも攻撃されることがある。これらの攻撃は、IRC サーバを攻撃するために特化された攻撃もあるが、一般のインターネット上のホストに対しても通用する攻撃も多い。IRC ワーキンググループが、これらの攻撃に対して対処してきたさまざまな対策は、一般化することによってサーバの構築技術としてまとめていきたいと考えている。

### 5.3 コミュニケーションツールとしての利用

IRC クライアントのアプリケーションは数多く存在するが、現在のところその多くは IRC 網をその本来の目的である「チャット」をするためのものである。すなわち「チャット」をするために便利に作られている。しかしながら、人と人のコミュニケーションの形は、いわゆる「チャット」に限定したものではない。IRC もまた、それらに応じたさまざまな利用法を想定し、そのそれぞれに対して適切なクライアントを研究する必要がある。以下に IRC の利用法のいくつかを示し、その用途において期待されているクライアント像を示す。

#### 5.3.1 遠隔ミーティング

現在存在する IRC クライアントにおいて遠隔ミーティングを行った場合には、往々にして議論が発散しやすく、また会話のログもそのままでは議事録としての役割として使えるレベルには達していない。これらは「任意の参加者が任意のタイミングでの発言が出来るので、単にログを収集しただけでは議論の流れを追うことが困難」「議長のようなものを設定し、発言の機会を制限し、議論の発散を防ぐ」といったところに原因があるものと考えられる。この問題に対しては適切な IRC クライアントを用意することで、IRC を利用した遠隔ミーティングを支援していけるのではないかと考える。

#### 5.3.2 ネットワーク運用支援

複数の管理者がネットワーク管理業務を行うに際して、IRC を介してコミュニケーションをとりながら行うことが多い。これは遠隔地にいる管理者間でチャットを行うのに便利であるからであるが、ここに適切なクライアントを用意することで、さらに IRC の特徴を活かした管理業務が行えるものと考える。IRC のサーバー間コネクションは TCP によるコネクションを常時張り続け、IRC のデータは常にこの 1 本のコネクション上を流れることになる。そのためこのコネクションには、「非常に長時間安定して張り続けることが出来る必要がある」「大量のデータが流れ続ける」「遅延に対して敏感である」といった特徴がある。そのためこのコネクションが切れた場合の影響が大きく、検知が非常に容易である。これはサーバーのおかれた 2 点間で常時 ping や traceroute を継続して行っているようなものだと言える。この特長を生かし、IRC 網の安定度を観測し、サーバー間接続に利用しているネットワークのオペレーションに対して問題点などをフィードバックすることが出来るものと思われる。さらには管理者が IRC を介して管理情報の交換を行っているような場合にはこの会話に対して自動的に情報を提供するようなクライアントを作成することも有用だと考える。さらには syslog などを介して提供される情報を管理者が会話を行っている場所に提供することも検討できる。

#### 5.3.3 利用状況の分析

IRC の利用範囲を広げていくためには、様々なコミュニケーションの形において、IRC がどのように利用されているのかについて、調べる手法を確立する必要がある。

この調査をするためには、プライバシーに対する配慮も必要であるため、慎重に調査項目を選び、ユーザへの協力の要請をすることが欠かせない。まず、これらのポリシーや手順を確立し、IRC 上での利用状況の分析のための基礎データを収集する基盤を確立することを目指す。

### 5.4 IRC 網を利用して何が出来るか

IRC 網は、そこに接続しているクライアント同士の間で任意のメッセージを交換できることから、これは Overray Network としての側面を持っている

ともいえる。また、双方のクライアントがサーバー網に接続してくる形態であるため、TCP コネクションの向きにおいても特徴的な部分がある。これらの特徴を活かした利用法を検討してみたい。

#### 5.4.1 データの転送・共有のための利用

現在でも、IRC では、ファイルの転送のために、DCC(Direct Client Connection) という仕組みが利用されている。しかし、この仕組みは、NAPT と相性が悪いことや、機能がデータの転送だけに限られていることから、あまり使い勝手の良いものではない。そこで、DCC や CTCP を拡張して、データの転送や共有に便利な仕組みを作り、コミュニケーションの支援に使うことを考えている。

#### 5.4.2 マルチキャスト通信の利用

IRC ネットワークのマルチキャスト通信な性質は、複数のホスト上にあるプログラムが協調動作をする仕組みのインフラストラクチャーとして使うことができる。実際、IRC に対して DoS 攻撃を仕掛けるプログラムのいくつかは、IRC ネットワーク自体をその協調動作のインフラストラクチャーとして利用している。

これらの利用法を一般のプログラムに広げ、かつ、その負荷に対応できる IRC サーバの技術を確立することによって、一般のプログラマが、手軽にマルチキャスト通信の性質を利用できる通信環境を手に入れることができると考えている。

### 5.5 IRC サーバ運用で得られる情報の活用

IRC サーバを運用していること自体により、直接ならびに間接に多くの情報が入手することができる。これらの情報の種類として、サーバへ接続しに来るユーザの情報、iauth でのユーザ側へ接続しにいくときに得られる情報、サーバ上でユーザが利用することによる情報、の 3 つに大きく分けられる。

サーバへ接続しに来るユーザの情報としては、その接続や切断の時間、ユーザの IP アドレス、ならびにそこから得られるホスト名とドメイン名や、AS の情報などがあり、これは別の章にて統計を報告する。

iauth のモジュールによってサーバからユーザ側へ接続しにいくときに得られる情報としては、ident, socks, http などそれぞれのモジュールに応じて、各プロトコルで得られる情報がある。

最後にサーバ上でユーザが利用することによる情報としては、ユーザのニック名、ユーザが入るチャネル名、ユーザがつけるトピック名、チャネルで行われる会話、などが挙げられるが、現時点ではプライバシとの関係が未整理であるため、記録を残したり情報を活用したりなどはしていない。

それを除いた前者二つの情報によっても色々な活用方法が考えられる。

#### 5.5.1 踏み台ホストなどの実態調査

DoS 攻撃と表裏一体となっている踏み台ホストなどからの不正利用による IRC サーバへの接続は、その踏み台ホスト側の情報を分析することで、対策の一助となるとともに、セキュリティ的な実態調査をすることができる。

例えば、Open HTTP Proxy を検査している mod_webproxy において、現在記録している情報を分析、あるいは、Open と判明したものへさらに情報を取りに行くことで、問題のある HTTP サーバの種類や version などの動向をとらえることが可能になる。

また、IRC サーバへ接続しに来る TCP コネクションの情報も加えて、TCP fingerprint などを調査することで、問題のある踏み台ホストの OS などの情報も判明する可能性もある。WIDE では、IRC サーバを運用しているメリットを生かして、これらの実態調査についても行おうと考えている。

#### 5.5.2 IRC サーバ利用者の動向

毎年の報告書で分析結果を報告しているように、IRC サーバの利用者の動向については色々と興味深いデータが得られている。DoS 攻撃による切断での大きな変動などの要因を除くと十分なユーザのサンプル数のため、各個人の行動によって影響されないほどの全体としての安定した動向変化のデータが得られている。

例えば、テレホーダイ利用者の減少と常時接続者の増加による影響は、各シーズン毎の分析比較によって見事に移行状況が見受けられた。このようなインターネット上の社会的な動向なども観測可能であり、今後も継続してデータを取得するとともに分析を続けようと考えている。