ISSN 0917-3668
2003. 6. 16

KUINSニュース

No. 41

京都大学学術情報メディアセンター
情報サービス部ネットワーク担当
http://www.kuins.kyoto-u.ac.jp/

KUINS 利用講習会 (2003 年 4 月 25 日開催) の模様

目　　次

桂キャンパスネットワーク試験運用開始のお知らせ 510
電子ジャーナル利用にあたっての注意 510
セキュリティに関する各種情報 511
KUINS 講習会を開催 511
ネットワーク機器 (HUB) 利用に関するお願い 512
PPP over SSH 513
mpd を用いた PPTP サーバの構築 514
KUINS 会議日誌 520
お知らせ 520

桂キャンパスネットワーク試験運用開始のお知らせ

本学桂地区で KUINS のネットワークが，2003 年 5 月 9 日 (金) から試験運用を開始しました．現在、ネットワークが利用できる建物の正式名称 (建設期間中の通称) は次のとおりです.

- A1 棟 (D 棟、E 棟)
- A2 棟 (A 棟)
- A3 棟 (B 棟)
- A4 棟 (C 棟)
- A クラスター事務棟 (A クラスター事務室)
- インテックセンター棟 (インテックセンター)
- EM センター棟 (EM センター)

電子ジャーナル利用にあたっての注意

附属図書館

附属図書館では，約 7,000 タイトルの電子ジャーナルを提供機関と契約し，利用に供しています．電子ジャーナルは各研究室等からネットワークを通じて利用することができ，論文のダウンロード及びプリントアウトができます．利用は非常に高く，研究者にとっては必須のものとなっています.

しかし，4 月 25 日に一部利用者の不正利用により，約 2 週間，約 80 タイトルの電子ジャーナルが全学的に利用できなくなり，多くの利用者の学習・研究活動に著しい不利益をもたらす結果となりました．

電子ジャーナルの利用にあたっては，提供機関が使用許諾条件を定めています．どの提供機関においてもおおむね以下の事項は禁止されています.

- **プログラム等による短時間での大量ダウンロードやプリントアウト**
- **他者に複製配布，送信すること**
- **個人利用以外の目的，または研究・教育以外の目的での利用**
- **内容の改編**

本学電子ジャーナルホームページ (`http://ddb.libnet.kulib.kyoto-u.ac.jp/gakunaiej.html`) により各出版社の許諾条件にリンクしておりますので，そちらの方もあわせてご覧ください.

今後，再び今回のような事態が生じた場合，電子ジャーナルの利用停止だけではなく，契約違反による損害賠償訴訟等の本学に対して厳しいペナルティが科せられる可能性があります．電子ジャーナル利用条件の更なる厳守をお願いいたします.

セキュリティに関する各種情報

KUINS-II 機器への攻撃増加

最近，セキュリティ監視装置の発する警報から，本学の機器に対する不正アクセスが急増しているようです．その大半がサーバプログラムのバージョンを確認し，古いものを狙って攻撃するタイプとなっています．特に，昨年末に新規導入された機器の中で，最新のセキュリティパッチを適用していないものが攻撃を受けているように思われます．

この種の攻撃はサーバプログラムのバージョンを確認し，そのバージョンに存在するセキュリティホールを狙って攻撃を仕掛けてきますので，ほぼ 100%の確率で管理者権限を奪われています．また，攻撃者はサーバプログラムがログを記録する前に乗っ取りに成功するよう試みますので，攻撃を受けたにもかかわらず，アクセスあるいはアクセス拒否の記録が全く無い場合は，乗っ取りを防いだのではなく，乗っ取られてしまったと判断されます．

このような攻撃を防ぐため，不要なサーバプログラムは停止し，かつ，セキュリティパッチの適用を頻繁に行うように心がけてください．ほとんど全ての種類の OS では，週に数度，頻繁なときは，毎日セキュリティパッチが公開されているのが現状です．自動アップデート機能を持つ OS であれば，確認の間隔を毎日に，手動で確認する OS であっても日に一度は新たなセキュリティパッチの有無を確認するようにお願いします．

一度乗っ取られてしまうと，どこに盗聴プログラムを仕込んだかを調べることは事実上不可能ですので，再インストールが必須となりますので，ご注意ください．

P2P ソフトウェアの利用制限について

現在，総長補佐 (情報基盤担当) の指示により，学術情報メディアセンターでは主な P2P ソフトウェアのディフォルトポートを閉鎖しております．これは，国内外の著作権管理団体より各大学に対し要望がなされたためだけでなく，本学に対し国外の著作権管理団体より抗議があったため，緊急措置として指示されたとのことです．

一方で，P2P ソフトウェアの利用自体は違法ではありませんし，完全な通信遮断も不可能です．しかし，利用者本人は違法なファイル交換を行わない場合でも，そのソフトウェアの仕組みから第三者の違法行為を幇助したと見做される可能性があり，実際に利用者本人に対する訴訟が起きております．ここで言う違法行為には，著作物交換だけでなく，個人情報漏洩なども含みます．

今後，P2P ソフトウェアの扱いについては，何らかの指示があると思われますので，研究等で利用を継続されたい方は，各通知や本センターの web ページをご確認頂くようお願いいたします．

KUINS 講習会を開催

2003 年 4 月 25 日 (金) に学術情報メディアセンター (北館) で，4 月から新規に京都大学に着任した教職員を対象に京都大学学術情報ネットワークシステム (KUINS) の利用に関する講習会を開催しました (参加者 40 名)．

講習内容として，学術情報メディアセンターと KUINS システムに関する概要，KUINS の具体的な利用方法に関する説明を行い，また KUINS におけるセキュリティについて講演を行いました．

今後，KUINS では，セキュリティ関係や利用者講習会なども開催予定です．詳細等はホームページなどでアナウンスいたしますので，皆様のご参加の方をよろしくお願いします．

なお，講習会の資料等は，
　http://www.kuins.kyoto-u.ac.jp/seminar/
でご覧になることができます．

ネットワーク機器 (HUB) 利用に関するお願い

KUINS-III において，Ethernet(10Mbps) インタフェースを持つネットワーク機器 (Shared HUB) の接続による通信障害が発生している情報コンセントが少なからずあるようです．通信障害が長時間継続している場合は，学術情報メディアセンターのネットワーク管理装置で把握できますので，その情報コンセントについて VLAN 管理責任者と連絡担当者にご連絡を差し上げております．

しかし，短時間の場合はどうしても把握漏れが生じます．もし，DHCP による IP アドレスの取得失敗の多発やデータ転送の時間がかかり過ぎると感じられていて，現在 Shared Hub をお使いの方は，衝突 (collision) ランプを確認し，もし頻発に点灯しているようでしたら，Fast Ethernet Switich Hub への交換をご検討ください．一般に，大量ファイルのアクセスがあるサーバがなければ，廉価版の Switching Hub でも大幅な通信状況の改善が図れます．

次に，技術的な説明を述べます．大雑把に言えば，図のように Shared HUB は 10Mbit 毎秒 (Mbps) 流せる 1 本の配線を全てのポートで共有しています．また，Ethernet のコンセント (RJ-45) は 8 ピン (4 組) になっていますが，Shared HUB ではこの内の一組しか利用していません．つまり各ポートでは流入と流出は一組の配線を共有 (半二重) しています．さらに，元々の Ethernet の設計では，同時に複数のコンピュータが送信することは滅多に無いと想定され，運悪く衝突が起きた場合は，衝突したパケットを再送信していました．

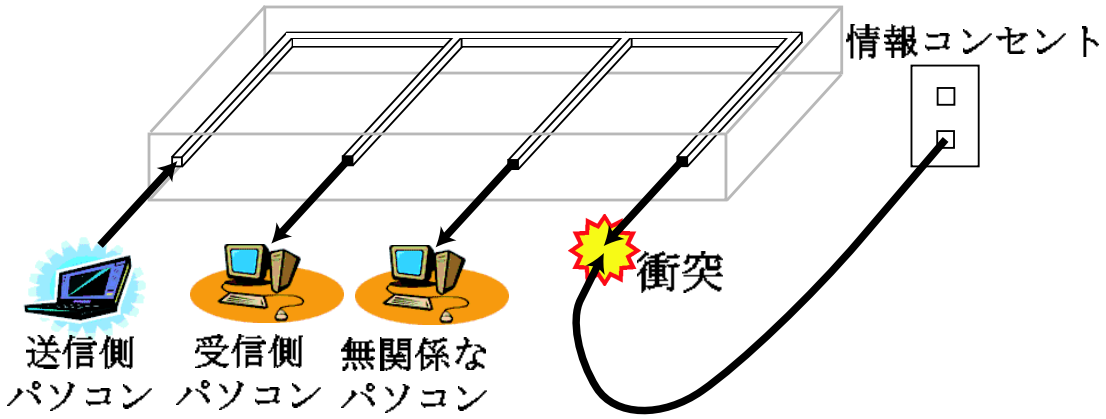

図 1: Shared Hub の概念図

一方で，最近のコンピュータは通常 100Mbps，ノート型でも 1Gbps の入出力能力を持つものもあります．このため，個々のポートでさえ 10 分の 1 以下の流量しか確保できない上に，反対側からの逆流があれば，衝突を起こします．現在は，10Mbps 半二重の環境では，僅か 2〜3 台でも同時送信と衝突が多発し，実質的にはほとんどデータが流せない状態になることがあります．

一方，見た目は同じ形をしていますが，Fast Ethernet 用 Switching Hub は，その内部に 100Mbps を流せる配線を複数備えており，ポート間の接続を適宜切り替える (switch) することで，装置内の衝突を回避しています．また，各ポートでは，流入と流出で違う配線を利用 (全二重) するため，ポートでの衝突も起こりません．なお，Switching Hub の価格には幅がありますが，それは装置内の配線数 (帯域) によって決まります．

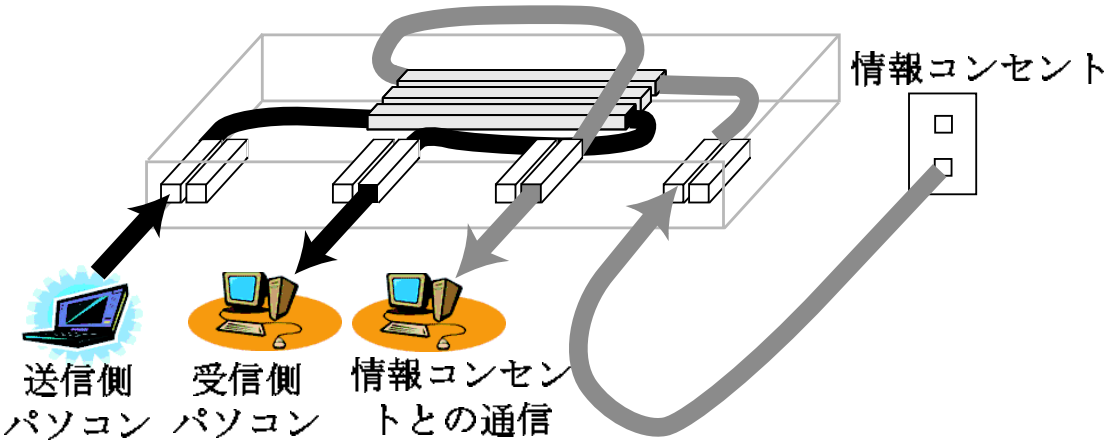

図 2: Switching Hub の概念図

PPP over SSH

京大マイコンクラブ (KMC) もぐらプロジェクト
鵜川 始陽 (foosen@kuis.kyoto-u.ac.jp)

これまで，オープンスペース設定の KUINS-III から各研究室のネットワークに接続するには，研究室に PPTP サーバを用意し，PPTP を使った仮想プライベートネットワーク (VPN) を構築して接続する手段しかありませんでした．

しかし，PPTP は

- PPTP サーバの選択肢として Windows 以外ほとんど考えられず，Windows では詳細な設定をするのが難しい，
- PPTP では NAT しているネットワーク内のクライアントからは接続できないため，KUINS-III と同じ設定では，自宅やフリースポットなど学外から研究室に接続できないことがある

などの問題がありました．

もぐらプロジェクト (`http://www.kmc.gr.jp/proj/vpn/`) では，IPA の 14 年度未踏ソフトウェア創造事業の援助を受けて，PPP over SSH を使った VPN を Windows 上から利用するためのツールを開発し配布していますので，紹介させていただきます．これを使えば，たとえ NAT をしていても，SSH で接続することさえできれば PPTP と同様の VPN を構築し，外部から安全に組織内のネットワークに接続することができます．サーバには一般的な UNIX 系 OS とツール群が利用できるため，既存の UNIX サーバを流用でき，また Windows の PPTP サーバより柔軟な設定が可能です．

ソフトウェアは下記プロジェクトの Web ページから自由にダウンロードして使うことができます．今後 VPN を導入する際の選択肢の 1 つとして考えていただければと思います．

プロジェクトの Web ページ： `http://www.kmc.gr.jp/proj/vpn/`
問い合わせ先: `mogura-info@kmc.gr.jp`

mpd を用いた PPTP サーバの構築

小塚真啓 (法学部)

1. はじめに

KUINS-III ホストはセキュリティ確保のため，外部ネットワークから接続できない仕組みとなっています．しかし，KUINS-III に接続されたホストに外部からアクセスを行いたい場合もあるでしょう．このような場合，KUINS-II と KUINS-III 双方に接続されたマシンを用意し，KUINS-III の IP アドレスを配る KUINS-II 側の IP アドレスで PPTP サーバを立ち上げる方法や，SSH ポートフォワーディングを利用する方法が考えられますが，ここでは，より汎用性の高い前者の PPTP サーバの構築方法を紹介します．なお，構築には OS に FreeBSD 4.8-RELEASE，PPTP サーバとして **mpd** を利用します．OS のインストール，ネットワークの設定もすでに完了していると仮定します．

2. mpd とは?

mpd は netgraph を利用した PPP 実装です．最大の特徴は netgraph を使っている点にあります．この機能によって PPP の処理をカーネル内で行うことになるため，スケジューリングによるパフォーマンス低下が少ないなどのメリットが得られます．なお，netgraph に関してはこちらの Daemon News の記事[1]で開発者による詳細な解説がされています．

3. インストール

mpd は FreeBSD のベースシステムには含まれていません．もっとも **mpd** は ports とパッケージを両方で用意されていますので，いずれかを利用すれば簡単にインストールすることができます．ここではより容易なパッケージを使ったインストールの方法を紹介します．(なお，本稿執筆時での **mpd** の最新バージョンは 3.13 です)

```
# pkg_add ftp://ftp.jp.freebsd.org/pub/FreeBSD/ports/packages/net/mpd-3.13.tgz
```

これで，**mpd** のバイナリ，マニュアル一式が/usr/local/{sbin/,man/,share/doc/mpd/} の下にインストールされ，同時に設定のサンプルが，/usr/local/etc/mpd/ の元に生成されます．

- **mpd.conf** - **mpd** の設定ファイル．**mpd** がどのような動作をするかを記述します．
- **mpd.links** - 同じく **mpd** の設定ファイル．**mpd** でどのようなプロトコルを利用するか，を記述します．
- **mpd.secret** - 認証に用いるユーザ名とパスワードを記述します．

4. mpd の設定

続いて **mpd** の設定を行います．なお，以後 PPTP サーバに割り当てられたの IP アドレスなどネットワークの設定は以下のようになっていると仮定します．

KUINS-II 側のアドレス： 130.54.xx.254
KUINS-III 側のアドレス: 10.xx.yy.254/24

[1] http://www.daemonnews.org/200003/netgraph.html

4.1 mpd.conf の記述

```
# default セクション．セクションを指定せずに mpd を
# 起動した場合に読み込まれる設定です．
default:
 load pptp0
# どのような IP アドレスを割り当てるかを記述するセクション
# 受け付ける最大 PPTP セッションの数を用意します．
# 例えば，10 接続受け付ける場合は，pptp1，pptp2，....pptp9 と 10 個必要です．
pptp0:
# LOCAL 側と REMOTE 側のリンクを指定します．リンクの設定は mpd.links で行います．
 new -i ng0 pptp_link pptp_link
# 割り当てる IP アドレスを指定します．ここでは 10.xx.yy.1 を割り当てることにします．
 set ipcp ranges 0.0.0.0 10.xx.yy.1/32
# PPTP セッションすべてに共通する設定を読み込みます．
 load pptp_common
# PPTP セッションすべてに共通する設定を記述
pptp_common:
# Proxy ARP を行います．行わないと KUINS-III の IP アドレスを
# 配っても他の KUINS-III に接続されたホストと通信できません．
 set iface enable proxy-arp
 set iface idle 1800
 set link keep-alive 10 60
# Address and control field compression と
# Protocol field compression を有効にします．
 set link yes acfcomp protocomp
# 認証方式として CHAP のみを使うようにします．
 set link no pap chap
 set link enable chap
# PPP パケットを GRE に埋め込んだ際，フラグメント化されないような
# 数値に MTU を設定します．
 set link mtu 1460
# Van Jacobson TCP header compression を有効にします．
 set ipcp yes vjcomp
# 研究室の KUINS-III ネットワークにおける DNS サーバを指定します．
 set ipcp dns 10.xx.yy.254
# MS-CHAP2 を使うための設定を記述します．
 set bundle enable compression
 set ccp yes mppc
 set ccp yes mpp-e40
 set ccp yes mpp-e128
 set ccp yes mpp-stateless
```

4.2 mpd.links の記述

```
# PPTP 用のリンクを定義します.
pptp_link:
 set link type pptp
 set pptp self 130.54.xx.254
 set pptp disable originate
 set pptp enable incoming
```

4.3 mpd.secret の記述

記述の例を以下に示します.

```
# ユーザ名 スペース "パスワード" スペース そのユーザに貸与する IP アドレス
# という形式で記述します.
# 最後の要素はユーザごとに固定の IP アドレスを振らない場合は不要です.
 kozuka "kozuka"
 masahiro "masahiro" 10.xx.yy.1
```

なお，このように **mpd.secret** は平文でパスワードが保存されますので

```
# chown root:wheel usr/local/etc/mpd/mpd.secret
# chmod 400 usr/local/etc/mpd/mpd.secret
```

として，管理者以外見ることができないようにしておく必要があります.

4.4 mpd の起動

以上で **mpd** の設定は終わりです．まずフォアグラウンドで起動し，正常に動くかどうかチェックします.

```
# /usr/local/sbin/mpd
  Multi-link PPP for FreeBSD, by Archie L. Cobbs.
  Based on iij-ppp, by Toshiharu OHNO.
  mpd:  pid 973, version 3.13 (root@freebsd.org 11:25 19-Apr-2003)
  [gre] ppp node is "mpd973-gre0"
  mpd:  local IP address for PPTP is 130.54.xx.254
```

以上のようなメッセージがでた後，PPTP で接続を受け付けることができるようになります.

4.5 Windows からの接続

サーバのアドレスに 130.54.xx.254，ユーザ名，パスワードは **mpd.secret** に記述したものを利用します．PPTP クライアントの設定方法は省略します．なお，クライアントを設定する際に以下の点に注意してください．

セキュリティの設定
カスタム設定
データの暗号化 -> 暗号化が必要
Microsoft CHAP Version 2 (この設定にチェックボックスをチェックすることを忘れないようにする)

この設定を忘れた場合，PPP パケットが暗号化されないまま流れることになります．接続すると，PPTP サーバ側で以下のようなインターフェースが作成され，どのような IP アドレスが割り当てられたか知ることができます．

```
# ifconfig ng0
  ng0:  flags=88d1<UP,POINTOPOINT,RUNNING,NOARP,SIMPLEX,MULTICAST> mtu 1400
  inet 10.xx.yy.254 --> 10.xx.yy.1 netmask 0xffffffff
  inet6 fe80::250:56ff:fe40:ad
```

4.6 自動起動の設定

/etc/rc.local に

```
/usr/local/sbin/mpd -b
```

という行を追加してします (なお，-b はバックグラウンドで起動するという意味です)．この設定によって，起動時に **mpd** が勝手に立ち上がり，PPTP 接続を受け付けるようになります．

4.7 アクセス記録の保存

-b オプションをつけるとバックグラウンドで動くようになりますが，この場合はフォアグラウンドではシェル上に表示されていたメッセージが syslog に daemon facility されるようになります．/etc/syslog.conf に次のような記述をすることで，誰が，どこから，いつ PPTP を利用したかを知るための情報を/var/log/mpd.log に保存するようになります．

```
!mpd
daemon.*                        /var/log/mpd.log
```

5. NAT の設定

ここまでの設定で外部ネットワークから PPTP を通じて KUINS-III へアクセスできるようになります．しかし，KUINS-III の IP アドレスでは外部ネットワークと直接通信することができないため，クライアントの default gateway を PPTP で割り当てられたアドレスに変更してしまうと外部ネットワークに接続されたホストと通信できなくなってしまいます．

この問題を回避するためには，クライアントの default gateway を PPTP で割り当てられたアドレスに変更

しない方法と PPTP サーバで NAT を行い，外部ネットワークと通信する場合は KUINS-II アドレスに変換する方法があります．前者は PPTP サーバには特別な設定は必要はありません．しかし，クライアント側で毎回 route コマンドを使い，適切な経路を設定するといった煩雑な作業が必要となります．後者の場合は，クライアントが外部ネットワークへ接続する際，NAT で送信元アドレスが PPTP サーバの持つアドレスに変換されて出て行くことになるため，適切なログを残す必要がありますが，クライアント側では特に何も設定する必要がありません．今回は利用者の利便を考え後者を採用することにします．ただ，NAT を行うことはそれなりのリスクを伴いますので[2]，場合によっては前者を採用する方が好ましい場合もあるでしょう．

5.1 IPFW の設定

FreeBSD では，**ipfw** の DIVERT 機能と **natd** というプログラムを利用して NAT を行います．まず，**ipfw** が DIVERT 機能が有効になった状態で組み込まれているかを確認します．これは，FreeBSD の起動時にコンソールに表示されるメッセージに以下の内容が含まれているかどうかで判断できます．なお，すでにサーバを起動している場合は，`/var/run/dmesg.boot` に起動時にコンソールに表示されたメッセージが保存されているのでそちらを参照してください．

ipfw が DIVERT 機能つきで組み込まれている場合は以下のような内容が含まれています．

```
IP packet filtering initialized, divert enabled, rule-based forwarding enabled,default to
accept, logging limited to 500 packets/entry by default
```

ipfw が組み込まれているが，divert は入っていない場合は以下のような内容になります．

```
IP packet filtering initialized, divert disabled, rule-based forwarding enabled,default to
accept, logging limited to 500 packets/entry by default
```

ipfw がカーネルに組み込まれていない場合や，含まれていても DIVERT が有効になっていない場合はカーネルを再構築する必要があります．設定ファイルに次のオプションを追加します．なお，カーネルの再構築の方法がわからない場合は FreeBSD ハンドブック[3]に記述がありますのでそちらを参照してください．

```
options IPFIREWALL                      # ipfw をカーネルに組み込む
options IPFIREWALL_VERBOSE              # ログを取る
options IPFIREWALL_FORWARD              # パケット転送を有効化
options IPFIREWALL_VERBOSE_LIMIT=500    # ログの最大数
options IPFIREWALL_DEFAULT_TO_ACCEPT    # 安全のために指定
```

5.2 natd の設定

`/etc/rc.conf` に以下の内容を追加します．

```
firewall_enable="YES"
firewall_type="OPEN"
natd="YES"
natd_flags="-a 130.54.xx.254"
```

[2] http://www.kuins.kyoto-u.ac.jp/news/37/provider-kuins.html
[3] http://www.jp.freebsd.org/www.FreeBSD.org/ja/handbook/

ここで PPTP サーバを再起動します．これによって，NAT 機能有効になります．

5.3 NAT のログを記録する

VPN で KUINS-III へ接続してきたユーザに KUINS-II の IP アドレスで外部にアクセスさせるわけですから立派なプロバイダの行為といえます [2]．よって，VPN 利用者が外で悪さを働き，被害者に情報開示を求められた場合，上述の情報を提供しなければならないということになります．というわけで,「誰が，どの IP アドレスで，どこへ，いつ攻撃を行ったか」を残さなくてはなりません．

しかし，オリジナルの **natd** では，いつ，どのパケットのどのアドレスを変換したのかを一切記録しません．そこでそれらの情報を記録するようにするためのパッチ[4] を作成しました．このパッチを wget などでローカルディスクに保存した後，FreeBSD のソースコードツリー (/usr/src) にパッチをあてて，**natd** を作り直します．また，システムをアップグレードした際，上書きされてしまわないように，/usr/local/sbin/に別途保存し，こちらを利用するようにします．

```
# cd /usr/src
# patch -p1 <  /natd-access.log.patch
# cd /usr/src/lib/libalias
# make obj
# make depend
# make
# make install
# cd /usr/src/sbin/natd
# make obj
# make depend
# make
# make install
# cp /sbin/natd /usr/local/sbin/natd
```

/usr/local/sbin/natd を NAT プログラムとして利用するには，/etc/rc.conf に以下の内容を追加します．

```
natd_program="/usr/local/sbin/natd"
```

これによって再起動すれば，/var/log/alias.log に以下のようなログが記録されるようになります．

```
Sat Jun 14 04:37:30 JST 2003:  10.xx.yy.1 => 130.54.xx.254
([ICMP:1536] From:10.xx.yy.1 To:210.81.150.5)
Sat Jun 14 04:37:32 JST 2003:  10.xx.yy.1 => 130.54.xx.254
([TCP]From:10.xx.yy.1:3059 To:210.81.150.5:80)
```

ログはパケットごとにどのアドレスをどれに書き換えたかを記録するのではなく，natd がどのようなアドレス変換テーブルを作成したかを基準にしています．例えば，同じホストのペアで連続して ICMP echo reply が 100 発やり取りされた場合でもこのように 1 行だけのログとなります．TCP のセッションや，UDP についても同様です．なお，上記のログは，www.yahoo.co.jp に ping を打った場合と，http で見に行ったときのものです．

[4] http://www.kozuka.jp/patch/natd-accesslog.patch

6. ログのロテート

mpd，NAT のログ共にそれなりの分量となるため，見易さ，ディスク容量の節約の観点から，古くなったログを別のファイルに避けるようにしたほうが便利です．FreeBSD では newsyslog というプログラムでこれを行うことができます．/etc/newsyslog.conf に以下の記述をすることで，**mpd**，NAT のログでロテートを行うことができます．

```
/var/log/alias.log                600   99999  *   @T00  Z  /var/log/natd.pid
/var/log/mpd.log                  600   99999  *   @T00  Z
```

毎日午前 0 時に，その日のログが mpd.log.0.gz，元々mpd.log.0.gz だったファイルは mpd.log.1.gz と退避したファイルの数が 99999 に達するまで保存します．

KUINS 会議日誌

平成 15 年 3 月 15 日〜平成 15 年 6 月 15 日

KUINS 運用委員会

平成 15 年 3 月 24 日 (第 13 回)
- KUINS 負担金状況報告
- KUINS-III パンフレットについて
- 講習会開催について
- サブドメインの申請について
- その他

平成 15 年 4 月 10 日 (第 14 回)
- KUINS 負担金状況報告
- KUINS データベース利用アカウントについて
- サブドメインの申請について
- その他

平成 15 年 4 月 22 日 (第 15 回)
- KUINS 負担金状況報告
- KUINS データベースについて
- 広報関係について
- その他

平成 15 年 5 月 6 日 (第 16 回)
- KUINS 負担金状況報告
- 桂キャンパスネットワークについて
- KUINS-III での WWW サーバ設置について
- その他

平成 15 年 5 月 29 日 (第 17 回)
- KUINS 負担金状況報告
- KUINS データベースについて
- KUINS ニュース No.41 の発行について
- その他

お知らせ

KUINS ニュースへの寄稿を歓迎します．詳細は

kuins-news@kuins.kyoto-u.ac.jp

または下記までお問い合わせください．

問い合わせ先

学術情報メディアセンター 情報サービス部ネットワーク担当 ((075) 753-7841)
（学術情報メディアセンター等ネットワーク掛 ((075) 753-7432)）