# JANOG6

Yet Another network command/tool/system

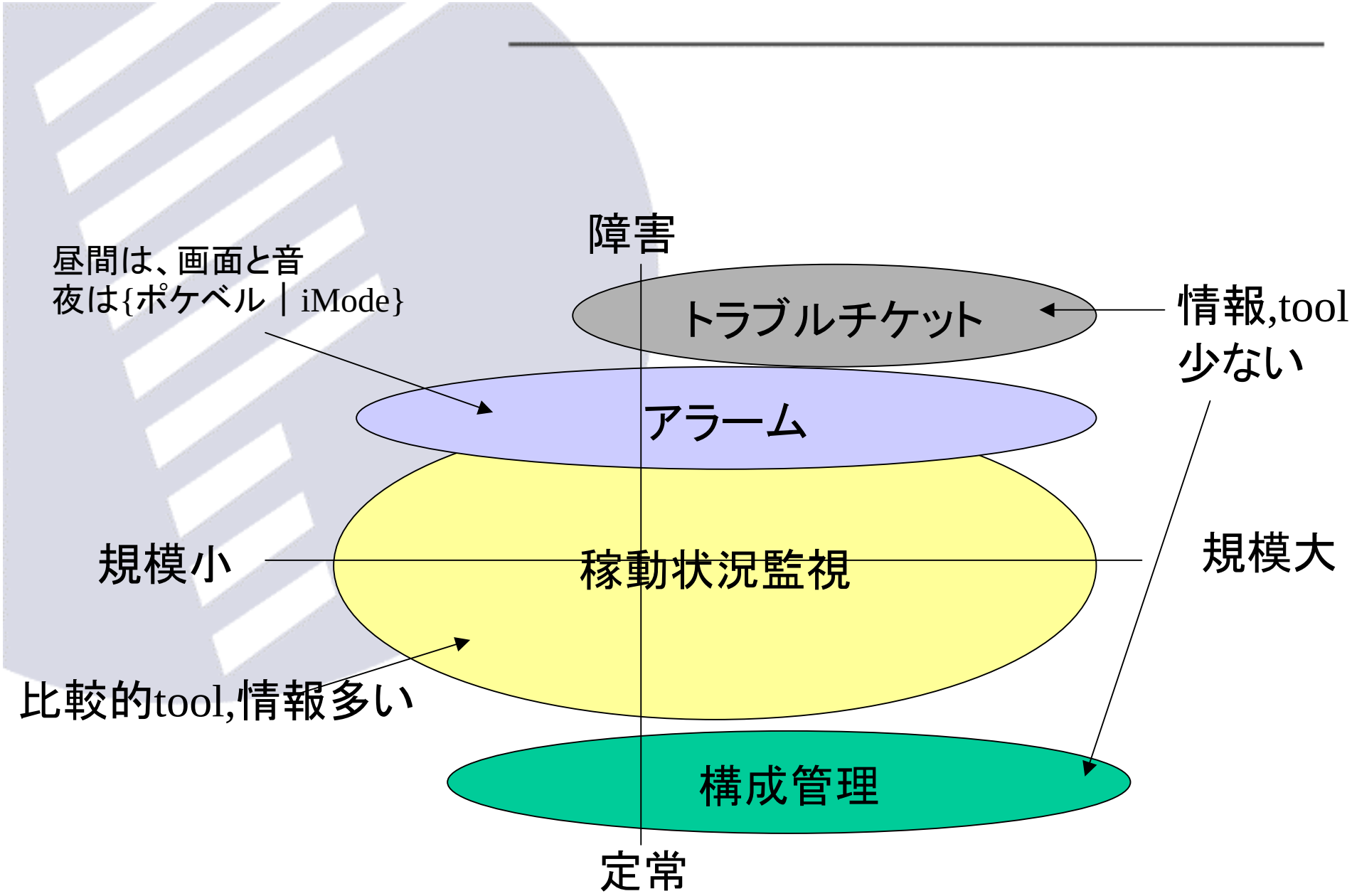
**ファストネット株式会社**

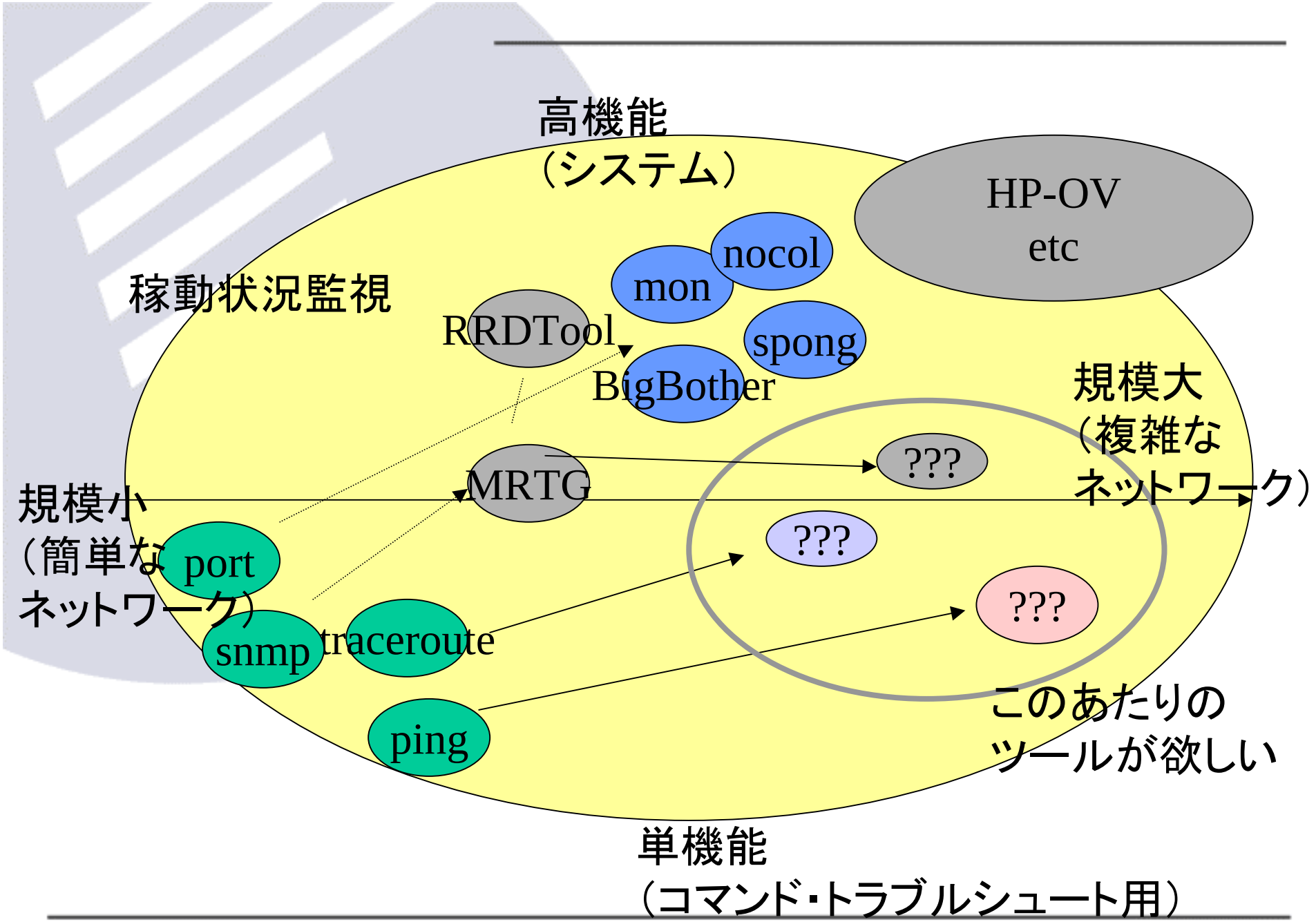
**向阪 正彦**

kosaka@fastnet.co.jp

# 発表内容

1. 概要
2. ping関連のツール
3. traceroute関連のツール
4. Webインターフェースのツール
5. まとめ、付録


障害
昼間は、画面と音
夜は{ポケベル | iMode}
トラブルチケット
情報,tool
少ない
アラーム
規模小
稼動状況監視
規模大
比較的tool,情報多い
構成管理
定常


高機能
（システム）
HP-OV
etc
nocol
mon
稼動状況監視
RRDTool
spong
BigBother
規模大
（複雑な
ネットワーク）
???
MRTG
規模小
（簡単な
ネットワーク）
???
port
???
snmp
traceroute
ping
このあたりの
ツールが欲しい
単機能
（コマンド・トラブルシュート用）

# Ping関連

# 初心に返って...ping

## pingは頻繁に使う

- たまに使うならUnix標準のpingを普通に使うだけでもOK
- intervalは最低でも1秒。
- 100回打つだけでも2分弱かかる。遅い！（Ciscoなら5秒ぐらい）
- -f オプションを使う。（floodオプション）
  - rootでしか使えない
  - 1秒かからない
  - 下手したらDoSになる？

```
bear# time ping -f -c 100 192.168.1.236
PING 192.168.1.236 (192.168.1.236): 56 data bytes
.
--- 192.168.1.236 ping statistics ---
100 packets transmitted, 100 packets received, 0% packet loss
round-trip min/avg/max/stddev = 3.424/3.501/4.010/0.062 ms
0.013u 0.000s 0:00.36 2.7%      168+252k 0+0io 0pf+0w
bear#
```

# ping(cont.)

- pingのプログラム自体でintervalを1秒以下に設定できるように改造

  FreeBSD2.2.8上でpingを改造

  実は、FreeBSD3.xから、-i(インターバルオプション)は、rootでは1秒以下に設定できる!!! ^^;

```
bear# time ping  -i  0.05  -q  -c 100 192.168.1.236
PING 192.168.1.236 (192.168.1.236): 56 data bytes

--- 192.168.1.236 ping statistics ---
100 packets transmitted, 100 packets received, 0% packet loss
round-trip min/avg/max/stddev = 3.418/3.475/3.963/0.063 ms
0.000u 0.010s 0:05.94 0.1%      336+512k 0+0io 0pf+0w
bear#
```

# pingは一度に複数宛先に打ちたい

fping

・FreeBSDのports/packageにある

・1行に1宛先を書いたファイルを読み込み複数宛先にpingを送る

・ICMPは3回しか投げないので Dead or Aliveの確認程度。

・Replyのsrcアドレスが違うものから帰ってくると、unreachableになってしまう。(NATの設定がおかしい場合等）

```
> fping  -e  -f  ip.list
202.228.128.217 is alive (25 msec)
202.228.128.222 is alive (24 msec)
:
:
202.228.128.186 is alive (15 msec)
202.228.128.176 is alive (14 msec)
202.228.128.183 is alive (14 msec)
>
```

# pingは一度に複数宛先に打ちたい(Cont.)

multiping

- ・nocolのパッケージの中
- ・オプションは、nomalのpingに近い。IPを引数で複数指定
- ・-t オプションで結果を表形式で出力

```
wani1# ./multiping -c 10 -n -t -q `cat ~kosaka/ip`
PING 202.228.128.190 (202.228.128.190): 56 data bytes
PING 202.228.128.179 (202.228.128.179): 56 data bytes
        :
        :
PING 202.228.128.176 (202.228.128.176): 56 data bytes
PING 202.228.128.222 (202.228.128.222): 56 data bytes
PING 202.228.128.219 (202.228.128.219): 56 data bytes
PING 202.228.128.217 (202.228.128.217): 56 data bytes

-=-=- PING statistics -=-=-
                          Number of Packets        Round Trip Time
Remote Site                Sent   Rcvd   Rptd  Lost    Min  Avg  Max
--------------------------- ------ ------ ------ ----   ---- ---- ----
202.228.128.190              10     10     0   0%     15   69   302
202.228.128.179              10     10     0   0%     15   16    28
        :
        :
202.228.128.176              10     10     0   0%     15   18    30
202.228.128.222              10     10     0   0%     25   25    29
202.228.128.219              10     10     0   0%     26   30    64
202.228.128.217              10     10     0   0%     26   39   116
--------------------------- ------ ------ ------ ----   ---- ---- ----
TOTALS                      140    140     0   0%     14   23   302
wani1#
```

# あちこちのルータからpingを打って確かめたい

・rsh（ssh)経由でCiscoのpingをたたく

Ciscoのrsh設定 →

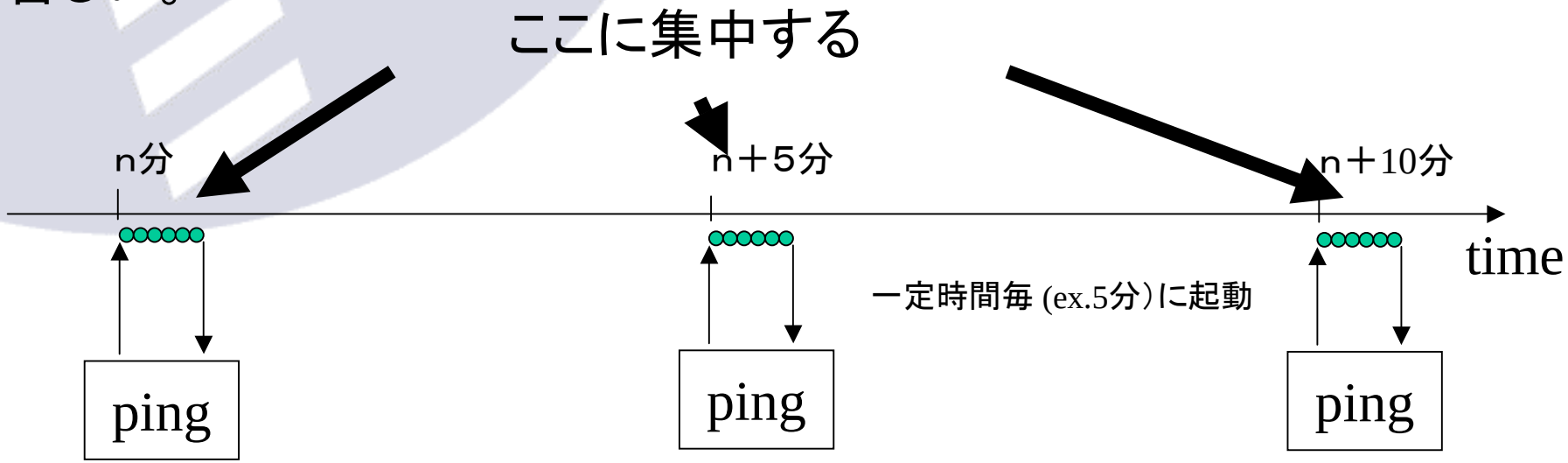
```
  :
ip rcmd rsh-enable
ip rcmd remote-host kousaka 202.228.???.??? kousaka enable
  :
```

あとは、perlで →

```
> ./cisco2ping.pl -i 202.228.???.??? -t 202.228.128.188 -r 100 -d 100
Protocol [ip]:
Target IP address: 202.228.128.188
Repeat count [5]: 100
Datagram size [100]:100
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 202.228.128.188, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
.!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 98 percent (98/100), round-trip min/avg/max = 1/4/20 ms
```

# 大規模なサイトのping監視の問題

・一般的にネットワークの監視では、5分に一回程度で、複数宛先にpingを打つ。
・最近は時間がNTPで合っている。
・大規模なネットワーク監視時には、5分おきにICMPがhost,networkとも苦しい。

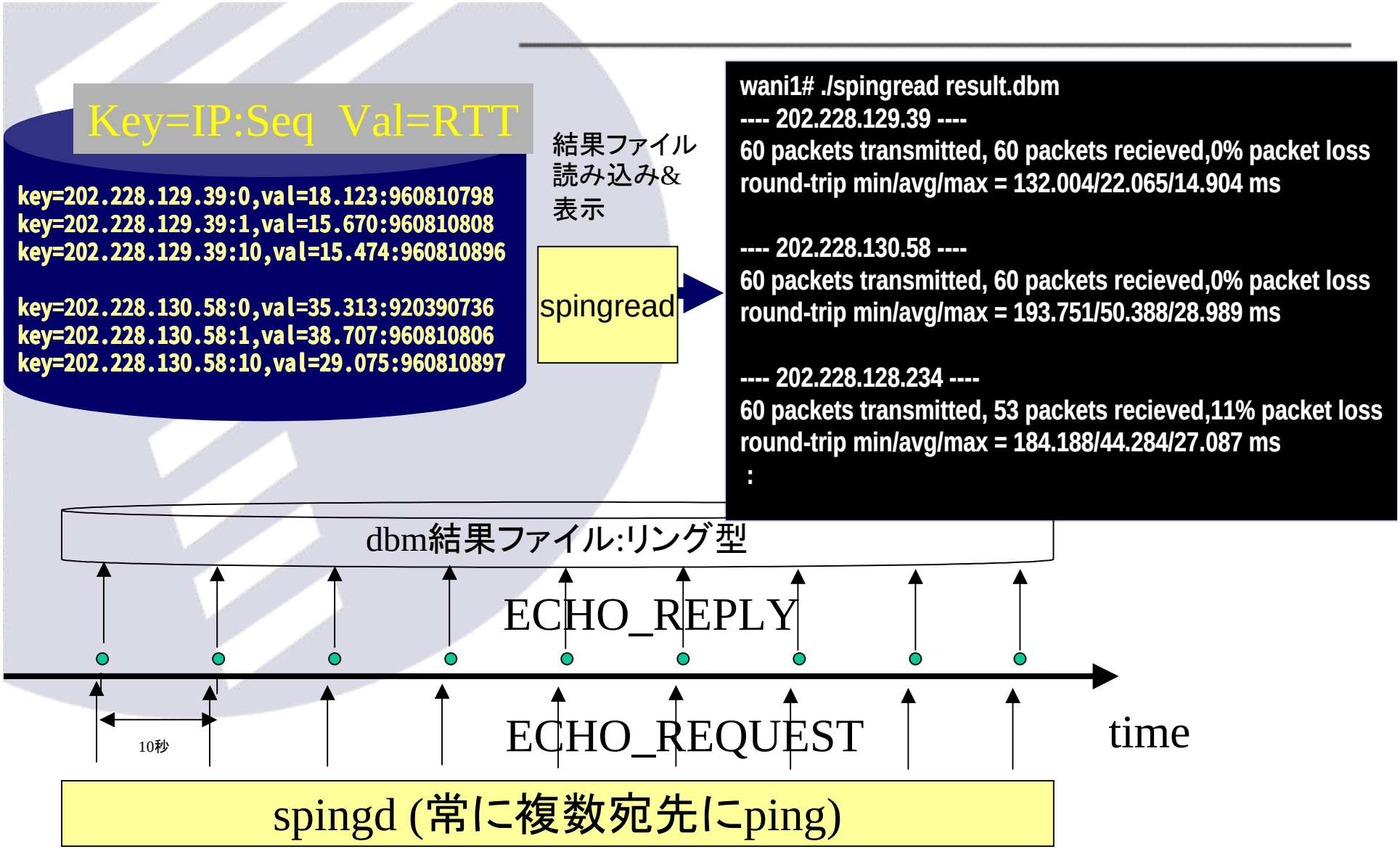


# こんなのはどうなんでしょう

spingd&spingread

- 常に監視している機器に対しては、むしろ、ゆっくりとしたインターバルで常時打ち続ける。
- 常に一定サイズのdbmに書き出す。
- fpingをモディファイして実装。

- 10秒に1回のICMPだと、正確な情報が出ない？
- 10秒おきに2回だといい？
  - 1回目の情報は捨てるとか。


Key=IP:Seq Val=RTT
key=202.228.129.39:0,val=18.123:960810798
key=202.228.129.39:1,val=15.670:960810808
key=202.228.129.39:10,val=15.474:960810896
key=202.228.130.58:0,val=35.313:920390736
key=202.228.130.58:1,val=38.707:960810806
key=202.228.130.58:10,val=29.075:960810897
結果ファイル
読み込み&
表示
spingread
wani1# ./spingread result.dbm
---- 202.228.129.39 ----
60 packets transmitted, 60 packets recieved,0% packet loss
round-trip min/avg/max = 132.004/22.065/14.904 ms
---- 202.228.130.58 ----
60 packets transmitted, 60 packets recieved,0% packet loss
round-trip min/avg/max = 193.751/50.388/28.989 ms
---- 202.228.128.234 ----
60 packets transmitted, 53 packets recieved,11% packet loss
round-trip min/avg/max = 184.188/44.284/27.087 ms
:
dbm結果ファイル:リング型
ECHO_REPLY
ECHO_REQUEST
time
10秒
spingd (常に複数宛先にping)

# traceroute関連

# traceroute

・ASを表示

IRRの情報を参照

URL　ftp://ftp.nikhef.nl/pub/network/traceroute.tar.Z

FreeBSDのportsのtraceroute

```
> /usr/local/sbin/traceroute -A -h whois.ra.net www.infoseek.com
traceroute to www.infoseek.com (204.162.96.173): 1-30 hops, 38 byte packets
 1  YOKO-R471-E0.fine.ad.jp (202.228.128.222) [AS4678 - FINE-CIDR-BLK FASTNET, INC.]  0.586 ms  0.633 ms  0.493ms
 2  OOTE-R722-S1-2.fine.ad.jp (202.228.130.81) [AS4678 - FINE-CIDR-BLK FASTNET,INC.]  14.1 ms  21.3 ms  11.3 ms
 3  158.205.226.201 (158.205.226.201) [AS4694 - C&W IDC]  21.8 ms  260 ms  13.9ms
 4  POS0-3.tokg1.idc.ad.jp (158.205.224.149) [AS4694 - C&W IDC]  21.9 ms  13.1 ms  13.1 ms
 5  POS0-0.patg1.idc.ad.jp (158.205.224.38) [AS4694 - C&W IDC]  119 ms  116 ms116 ms
 6  *  *  *
 7  159.ATM2-0.XR1.PAO1.ALTER.NET (152.63.49.162) [AS701 - UUNET, An MCI Worldcom Company]  121 ms  123 ms  116
ms
 8  189.ATM9-0-0.GW2.PAO1.ALTER.NET (146.188.147.225) [AS702 - UUNET, An MCI Worldcom Company]  117 ms  118 ms
120 ms
 9  infoseek-gw.customer.ALTER.NET (157.130.192.102) [AS701 - UUNET, An MCI Worldcom Company]  130 ms (ttl=243!)  133
ms (ttl=243!)  152 ms (ttl=243!)
10  maps.infoseek.com (204.162.96.173) [AS7266 - Infoseek, Inc.]  137 ms (ttl=240!)  135 ms (ttl=240!)  133 ms (ttl=240!)
```

・MTR

traceroutとPingを同時に実行。

いろいろな、出力形式がある。

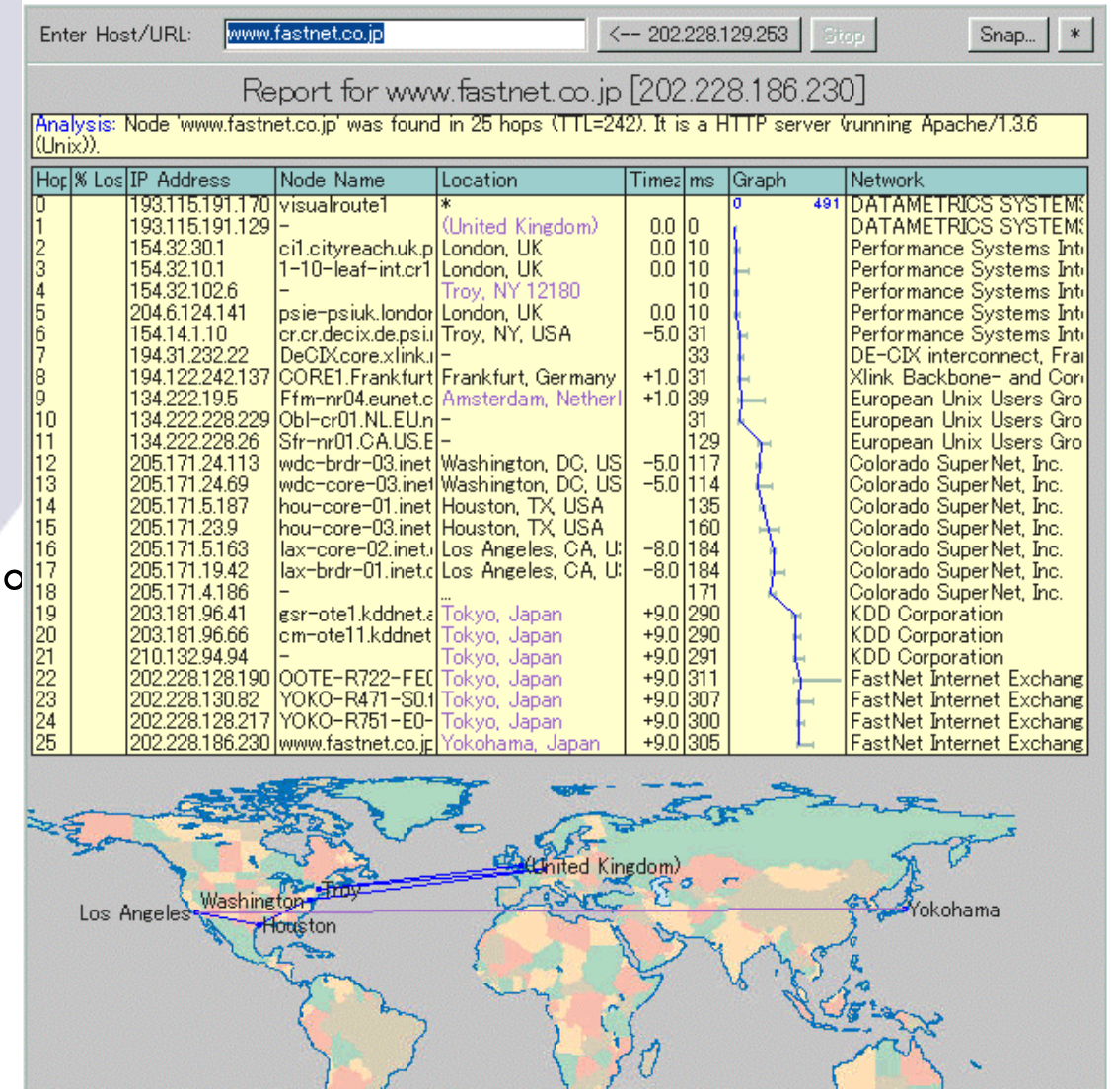
```
 Matt's traceroute  [v0.42]
bear.fine.ad.jp                                          Thu Jun 15 11:39:24 2000
Keys:  D - Display mode    R - Restart statistics    Q - Quit
                                        Packets               Pings
Hostname                              %Loss  Rcv  Snt  Last Best  Avg  Worst
 1. 192.168.2.254                       0%   10   10     1    1    1      2
 2. 202.228.129.254                     0%   10   10     5    5    5      5
 3. 202.228.130.165                     0%   10   10    16   16   16     16
 4. 202.228.128.190                     0%   10   10    15   15   15     16
 5. 202.249.2.11                        0%   10   10    15   15   15     16
 6. 203.183.255.4                       0%   10   10    16   16   16     17
 7. 210.140.200.9                       0%   10   10    16   15   16     16
```

# traceroute（Cont.）

・visualroute

http://www.visualroute.com/

pingとtraceroute、DNS情報を表示。
さらに地図上で可視化。



# Webインターフェースのツール

# Webをインターフェースに

LookingGlass：WANのトラブルシュートには必須

http://www.traceroute.org/

http://www.merit.edu/ipma/tools/lookingglass.html

http://www.geektools.com/traceroute.html

サイトにより、リアルタイムで
見れるもの見れない物がある。

# Webをインターフェースに(cont.)

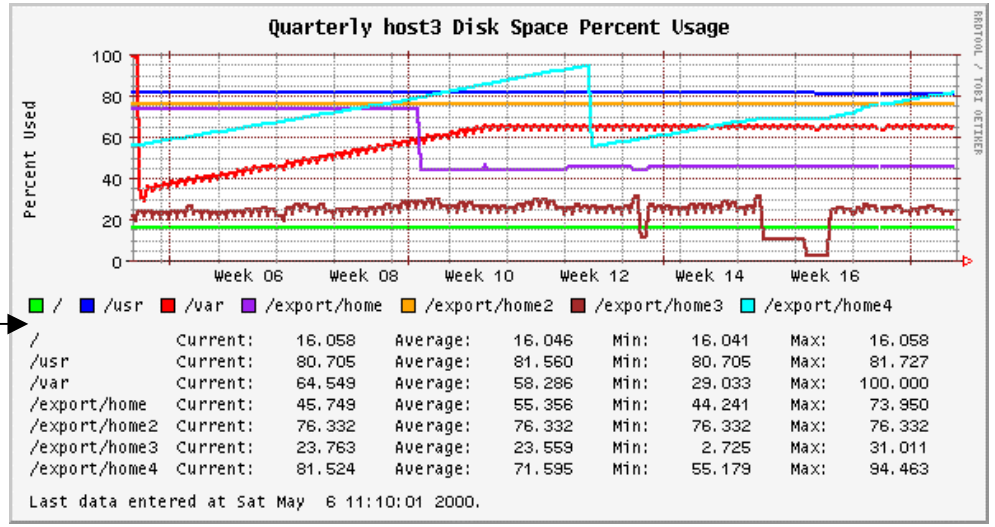
- MRTG

  MRTGは2値しかとれない。traffic以外でも、扱いが楽。

- RRDtool

  まだ、扱いがちょっと難しい。
  どのフロントエンドがいいの？

  このぐらいのデータを
  簡単に表示できるフロント
  エンドが欲しい。

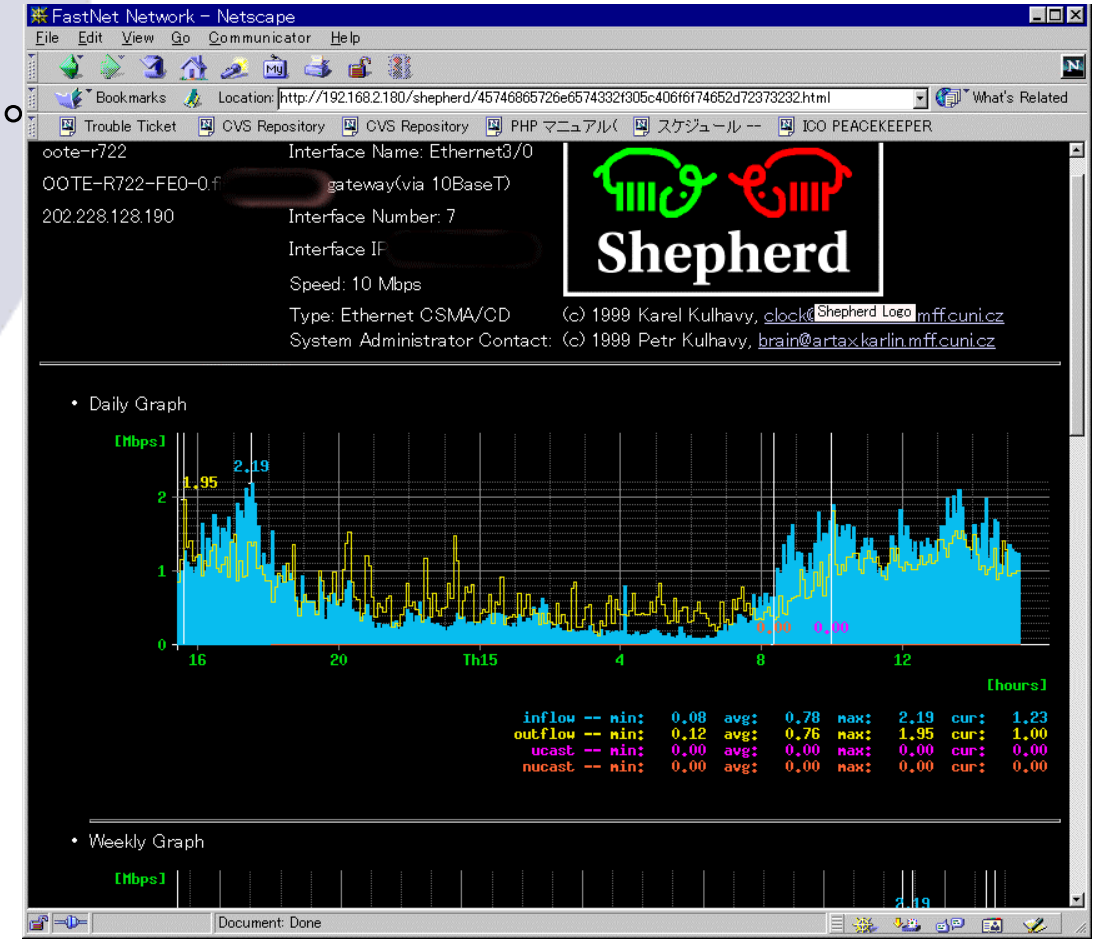


# shepherd

- MRTGの代替となりうる。
- バイナリ形式のログ
- データ収集は高効率。
- 2値以上をハンドリング

欠点：

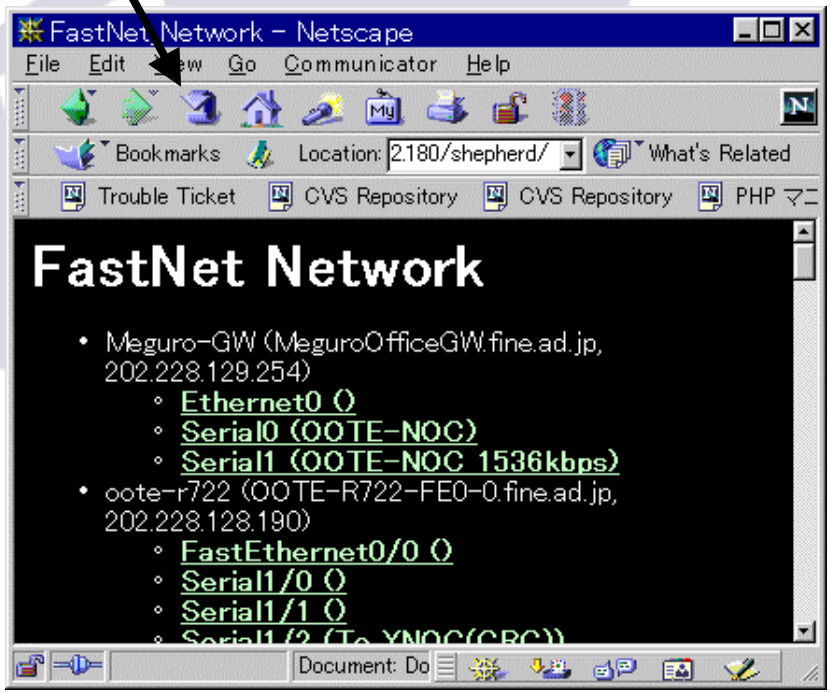
- 十分な情報がない。
- configがわかりにくい。



# 使い方の概略

- shepherd.cfgを作成
- ./shepherdを起動。
- ./make_indexでインデックス作成

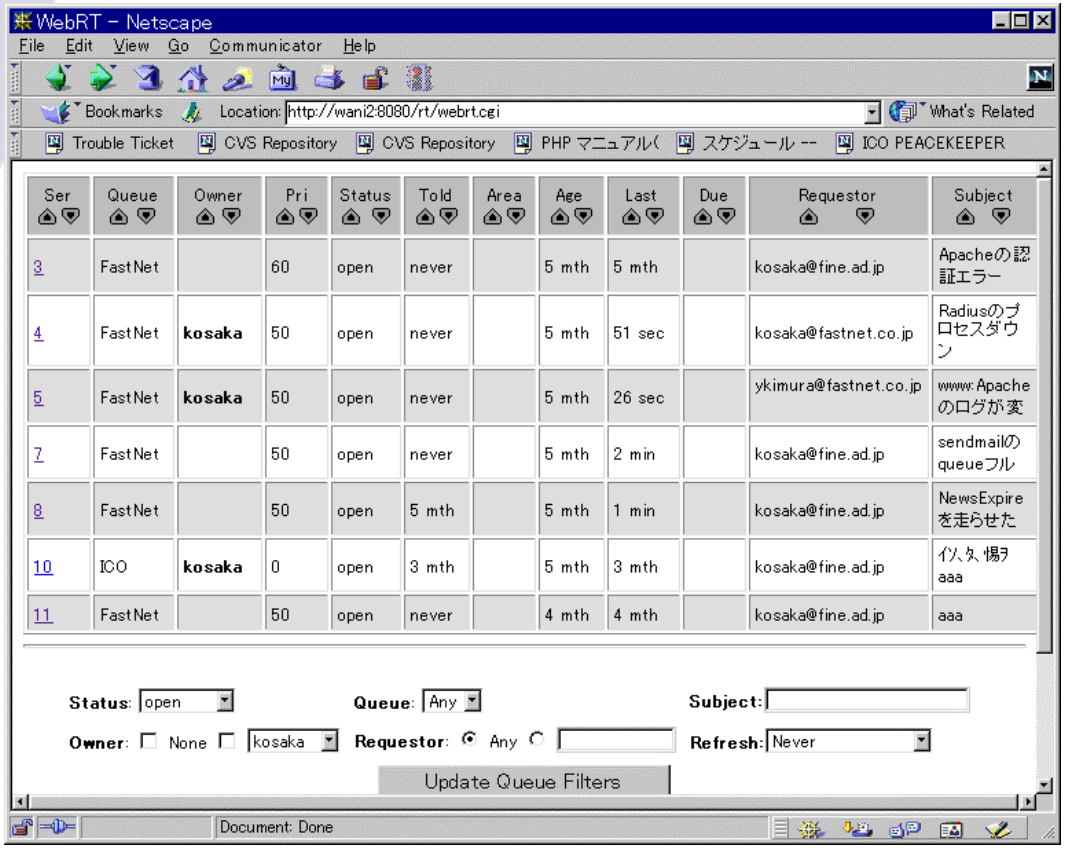
```
====== shepherd.cfg======
type 2 int
type 65 customint
type 67 timeticks

qty 1.3.6.1.2.1.2.2.1.10 customint inflow
qty 1.3.6.1.2.1.2.2.1.16 customint outflow
#    :
# 略
ip 202.228.129.254 Meguro-GW
ip 202.228.128.190 oote-r722
#   :

{
 max_rotundity 128
 max_afloat 16
 packet_timeout 5
 try_expire_time 10
 start 0
 period 300
 test_period 300
 n_tries 3
 {
  community なんとか
  rset Meguro-GW oote-r722 ......
  {
   iset  all
   qset inflow outflow ucast nucast
  }
 }
```



# Webをインターフェースに(トラブルチケット)

RT

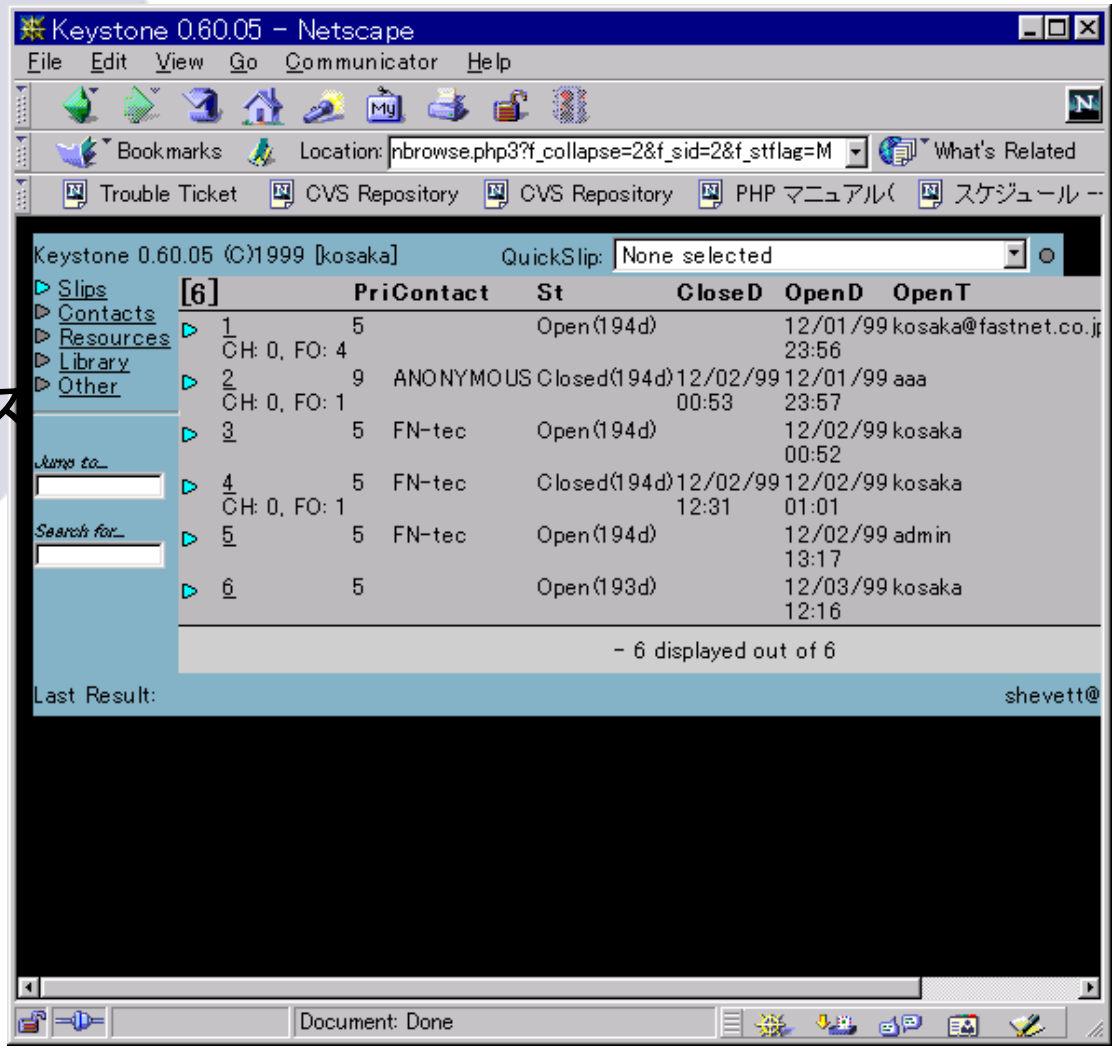
- MySQL＋CGIで構成されている。
- 比較的分かりやすい
- 最低条件は満たしている。
- baseはコマンドラインI/Fの Req
- mailのI/Fもあり。



# Webをインターフェースに(トラブルチケット)

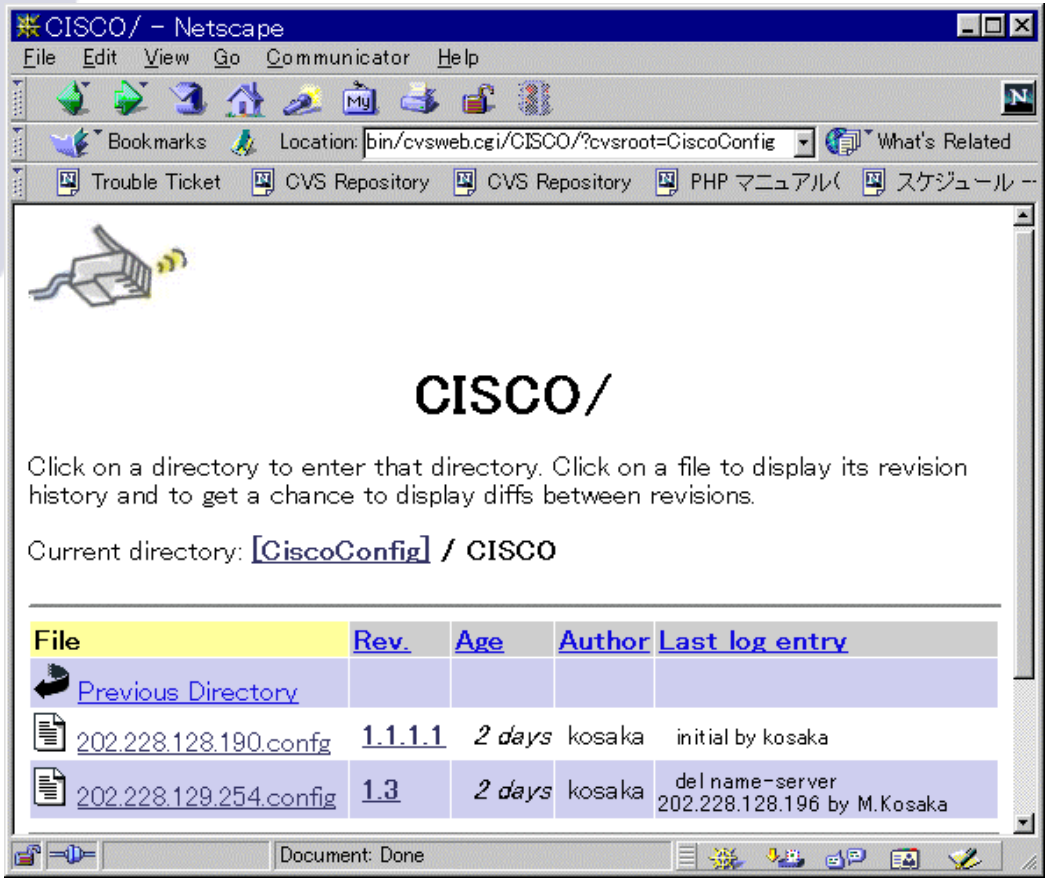
こんなのもあります。

KeyStone
・PHP 高機能だがわかりにくい。
・利用形態によりライセンスが必要。



# Webをインターフェースに(構成管理)

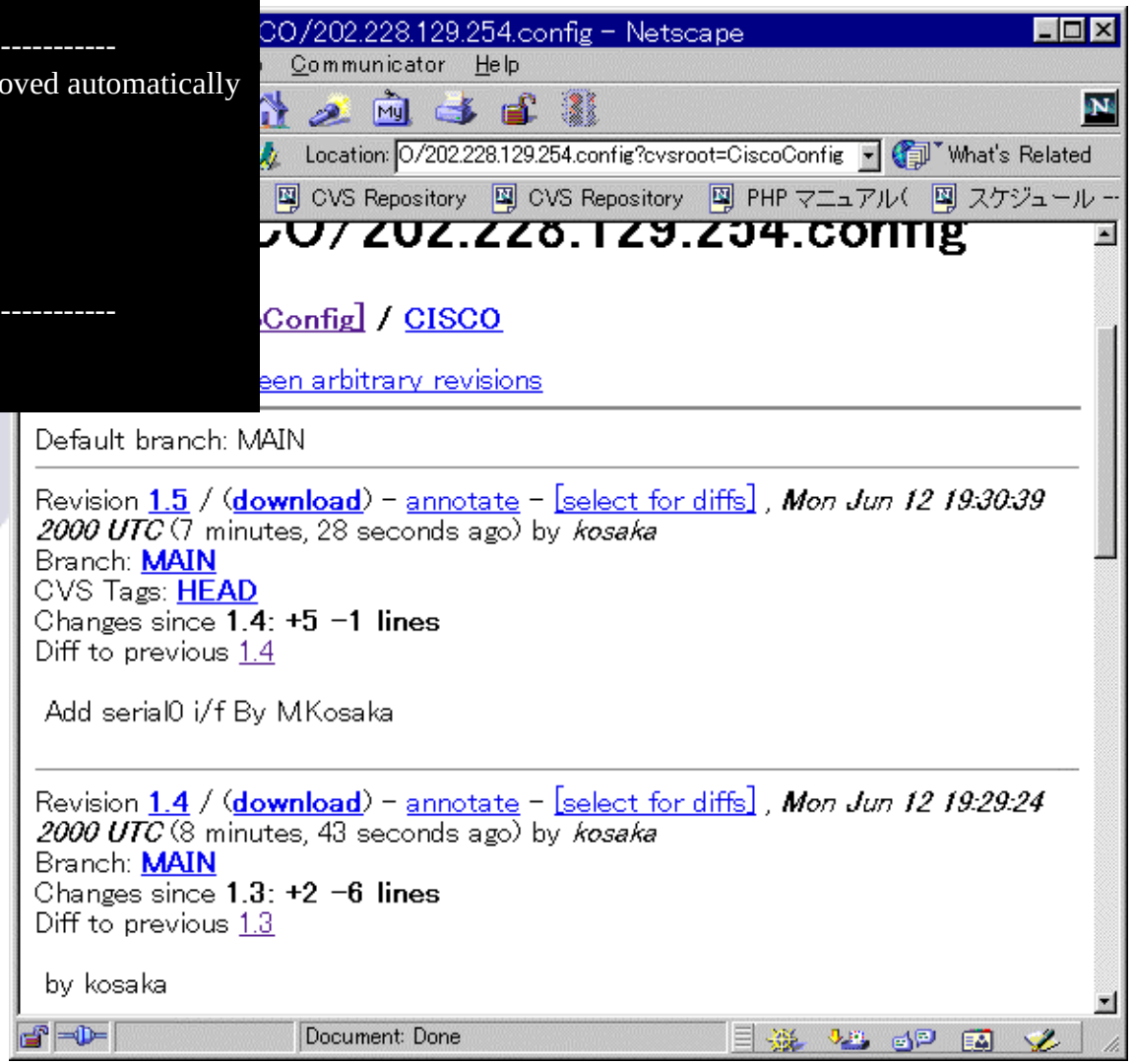
・CVSを
構成管理用 DBに応用。
  ・cvsweb.cgi というツール
  ・ソフト開発者だけが使うのでは、もったいない！
  ・ciscoのconfigの履歴管理に
  ・DNSの設定情報の履歴管理etc....



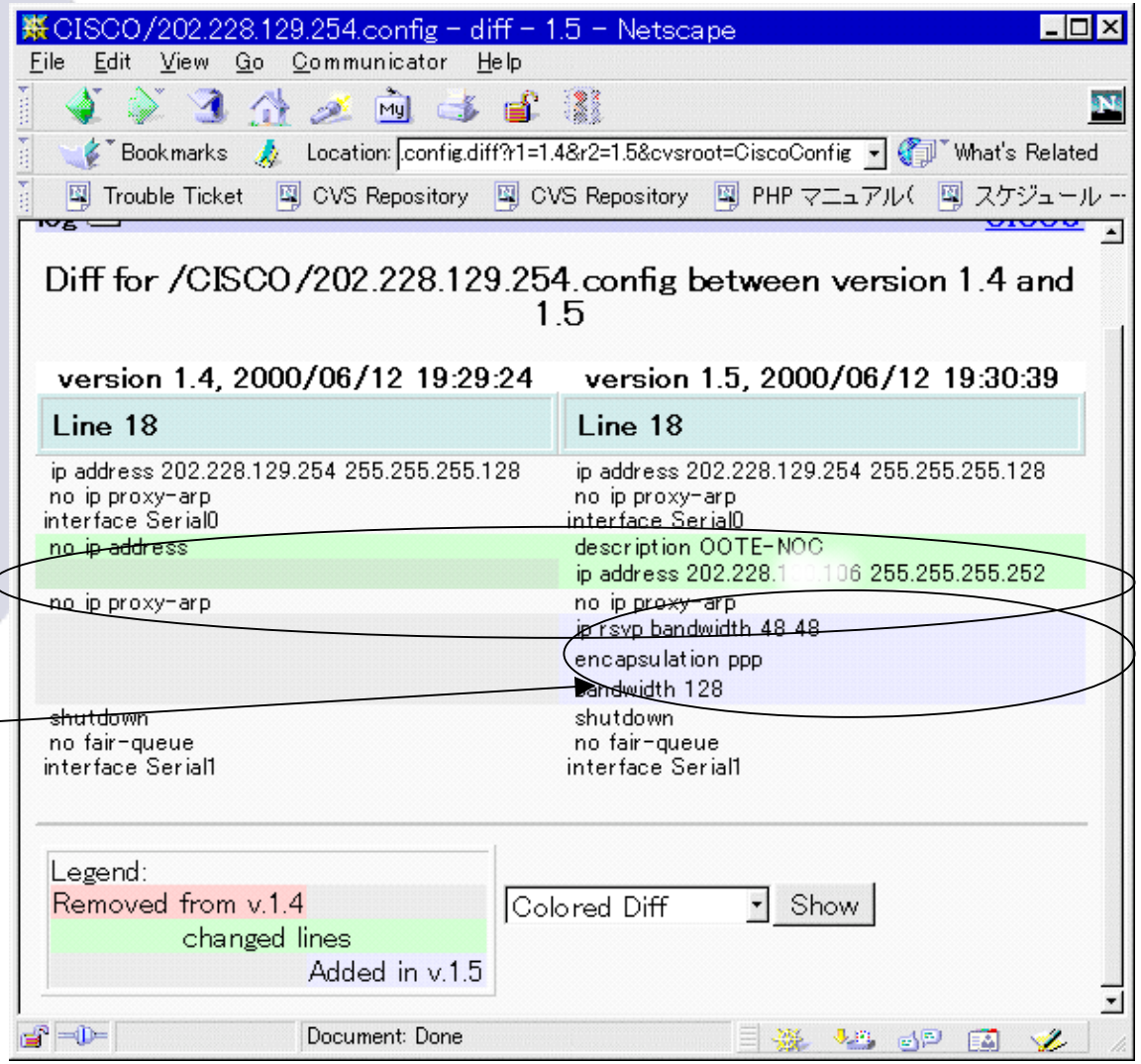
```
>./ciscoconfcvs 202.228.129.254


 Add serial0 i/f By M.Kosaka
CVS: ----------------------------------------------------------------------
CVS: Enter Log.  Lines beginning with `CVS:' are removed automatically
CVS:
CVS: Committing in .
CVS:
CVS: Modified Files:
CVS:    202.228.129.254.config
CVS: ----------------------------------------------------------------------
```

コマンドを打つとコメントを聞いてくる。

コメントも含め、履歴として残る



diffをとって
変更点が
色で分けで表示
される。



# まとめ、付録

・便利な物はいろいろある。
・使い方とか、カスタマイズの余地はいっぱいある。

今後
・さらにいろいろ、OpenSourceのソフトを評価する。
・使い方、使い勝手等をカテゴライズして公開していきたい。

リファレンス

====ping,traceroute====

traceroute-990522: FreeBSDの/ports

fping:FreeBSDの/ports

multiping：http://www.netplex-tech.com/software/nocol

MTR：http://www.bitwizard.nl/mtr/

visualroute：http://www.visualroute.com/index.html

===監視システム====

BigBrother:http://maclawran.ca/~sean/bb-dnld/index.html

spong:http://spong.sourceforge.net/nocol:http://www.netplex-tech.com/software/nocol

mon:http://ftp.kernel.org/software/mon/

===traffic監視====

mrtg/RRDTool：http://ee-staff.ethz.ch/~oetiker/webtools/

shepherd：http://atrey.karlin.mff.cuni.cz/~clock/shepherd/

====cvsweb,trouble ticket====

RT：http://www.fsck.com/projects/rt

KeyStone：http://www.stonekeep.com/

cvsweb：http://www.freebsd.org/~fenner/cvsweb/

http://linux.stud.fh-heilbronn.de/~zeller/cgi/cvsweb.cgi/

ご静聴ありがとうございました。