メモ

■ tcpdump マニュアル

・http://www.linux.or.jp/JM/html/tcpdump/man1/tcpdump.1.html
・ローカルホスト以外が関わる TCP 通信の TCP スタートとエンドのパケット (SYN と FIN のパケット) を表示する :

```
tcpdump 'tcp[13] & 3 != 0 and not src and dst net localnet'
```

・ゲートウェイ snup を通過する 576 バイト以上の IP パケットを表示する :

```
tcpdump 'gateway snup and ip[2:2] > 576'
```

・パケットのサイズ指定が指定できる。
・SYN/FIN などの TCP パケットの種類が指定できる。