http://itpro.nikkeibp.co.jp/article/COLUMN/20070403/267311/
Linux でパケットキャプチャするには

```
tcpdump
```

を使うと便利。

オプション

--	--
-f	外部のホストとのやりとりに対しては外部のアドレスのみを表示する。その際に、名前解決を行わずに IP アドレスやポート番号をそのまま表示する。内部のアドレスは名前解決をして、解決した名前で表示する。
-l	標準出力の内容をバッファリングする。出力結果をパイプ（|）で他のプログラムに渡す場合には、このオプションを指定する必要がある。標準出力でキャプチャを監視しながら取得したデータを保存しておきたい場合に有効である。
-n	IP アドレスやポート番号などを名前に変換せずに表示する。IP アドレスなどを表示する際には通常、名前解決を行い解決した名前で表示する。だが、このオプションを指定すると名前解決を行わず、IP アドレスやポート番号をそのまま表示する。
-N	ホスト名のうちのドメイン名の部分を表示しない。例えば、ns.example.com とやりとりする場合、通常は「ns.example.com」と表示するが、このオプションを指定するとドメイン名の部分が省略され「ns」と表示する。「-n」オプションと同時に指定すると、「-n」オプションのほうがが優先され、名前変換しないで表示される。
-S	TCP シーケンス番号を絶対値で表示する。通常、シーケンス番号は必ず「1」から始まるとは限らず、毎回ランダムな値から始まる。tcpdump では通常、このシーケンス番号を「1」から始まる相対値で表示するが、このオプションを指定すると実際にやりとりされているシーケンス番号をそのまま表示する。

-t	時間情報を出力しない。通常はパケット情報出力時に時間情報を表示するが、このオプションを指定すると時間情報は表示しない。
-v	詳細情報を出力する。このオプションを指定すると、通常の情報に加え、TOS（type of service）値、TTL（time to live）値、フラグ情報、サービス情報なども表示する。
-x	リンク・レベル・ヘッダーを除く全てのパケットの内容を、16 進で表示する。snaplen が指定されている場合、パケットのサイズが snaplen より小さければ全てのパケット情報を、パケットサイズが snaplen より大きければ snaplen バイト分のデータを出力する。
-X	16 進で表示する際に、ASCII 文字も表示する。「-x」オプションと同時に指定した場合、16 進と ASCII 文字の両方が表示されることとなる。ただし、パケットの箇所によっては、-x オプションを指定しない場合にも 16 進と ASCII 文字の両方が表示される。
-c パケット数	受信するパケット数を指定する。この「-c」オプションを指定した場合、ここで指定したパケット数を受信した後 tcpdump プログラムを終了する。このオプションを指定しない場合、「Ctrl+Z」を押すまでパケットを取得し続ける。
-i LAN インタフェース名	監視する LAN インタフェースを指定する。複数の LAN インタフェースが存在する場合、インタフェース名で指定したインタフェースを監視する。このオプションを指定しない場合、ループバック・インタフェースを除く LAN インタフェースのリストの中から、最も小さい番号で有効になっている LAN インタフェースを監視する。

-s データ長	取得するパケットのデータ長を指定する。このオプションを指定すると、各パケットから snaplen バイトのデータを取得する。このオプションを指定しない場合、68 バイトのデータを取得する。パケットを取得したいプロトコルによっては、68 バイトのデータでは情報が足りなくなるため、その場合、このオプションで取得するデータ長を指定する。このオプションの制限によりデータが切り詰められたパケットは、出力時に「[| プロトコル名]」の形式で出力し、プロトコル名にはデータの切り捨てが生じたプロトコルの名前を表示する。ただし、データ長を大きく指定し過ぎるとパケットの消失が発生する可能性も出てくるため、必要最小限の大きさを指定するのが望ましい。
-w ファイル名	取得したパケット情報を出力するファイル名を指定する。このオプションを指定すると、取得したパケット情報を解析せずに、指定したファイルに出力する。パケット取得後、「-r」オプションを使って解析した情報を標準出力に表示することもできる。ファイル名に「-」 を指定した場合、取得したパケットは標準出力に出力される。
-r ファイル名	あらかじめ「-w」オプションを使って作成したファイルからパケット情報を読み込む。ファイル名に「-」を指定した場合、取得したパケットは標準入力から読み込まれる。
-F ファイル名	フィルタリングの条件式を、指定したファイルから読み込む。あらかじめファイルに条件式を記述しておき、tcpdump 実行時にこのオプションで指定して読み込んでパケットのフィルタリングを実行することができる。このオプションを指定した場合、コマンド・ラインで指定した条件式があっても無視される。
条件式	パケットをフィルタリングするための条件式を指定する。「-F」オプションを指定している場合、ここで指定した条件式は適用されない。

使用例

■ 80 番ポートのパケットのヘッダを表示

```
tcpdump port 80
```

http://x68000.q-e-d.net/~68user/unix/pickup?tcpdump
ack と seq の表示が相対表示になることに注意。
例えば、３ウェイハンドシェイクのログを見ると

```
localhost.webcache: Flags [S], seq 472302579, win 32752, 省略
localhost.45513: Flags [S.], seq 1197515254, ack 472302580, win 32728, 省略
localhost.webcache: Flags [.], ack 1, win 512, 省略
```

となっていて、最後の ack は 1 になっている。seq や ack が大きいと見にくいので 開始時のシーケンスとの差（相対値）を表示している。
絶対値を表示したい場合は

```
tcpdump port 80 -S
```

とする。

```
localhost.webcache: Flags [S], seq 4180253150, win 32752, 省略
localhost.45514: Flags [S.], seq 1541210937, ack 4180253151, win 32728, 省略
localhost.webcache: Flags [.], ack 1541210938, win 512, 省略
```

■ 80 番ポートのパケットを表示する

```
tcpdump -Xx port 80
```

-Xx で、パケットをバイナリと ASCII の両方を表示する

■インターフェイスを指定する

```
tcpdump -i eth0 -Xx port 80
```

■キャプチャしたデータを解析せずにファイルへ出力

```
tcpdump -i eth0  -w log.txt
```

■キャプチャしたデータを解析せずに標準出力へ

```
tcpdump -i eth0  -w -
```