Vol.2009-IOT-7 No.4
2009/10/9

# TCP コネクション単位でトラフィックの視覚化を行うツールの開発

宇都木　進[†1]　渡邊　晶[†2]

ネットワーク管理者に TCP トラフィックの概要をリアルタイムに提示するためのツール，necosit を開発した．necosit は，各コネクションを帯状に表示する．単位時間あたりのトラフィック量を色のグラデーションによって示し，経過した時間だけ帯をずらし，新しいものを表示することで，アニメーションのように表示する．またコネクションのソート／フィルタ機能を備え，特徴ある通信のみを表示することができる．

# Development of a tool visualizing the traffic by TCP connection unit

Susumu Utsugi[†1] and Akira Watanabe[†2]

We have developed the tool which shows an overview of the TCP traffic in real time, called necosit. Necosit visualizes each connection as a bar and paints the bar the gradation of the color according to the traffic of the connection. Necosit periodically deletes oldest part of each bar, shifts bars to the left, and draws the new part of each bar. Necosit has the sort and filter functions for connections to display specific connections.

## 1. はじめに

ネットワーク管理者は，ネットワークの利用状況の把握や帯域を圧迫する通信などの特定など，ネットワークトラフィックの調査を行うことがしばしばある．RRDtool[1] は，通常 5 分に 1 度，トラフィック量の推移を提示するため，長期間のモニタリングに適している．一方，リアルタイムのトラフィック量の調査や，特定の通信のみを動的に抜き出して監視することはできない．tcpdump[2] は，ネットワークに流れる各パケットの情報を詳細に表示することができるので，リアルタイムにトラフィックの解析を行うことができる．しかしトラフィック量が多くなり，出力される情報が大量になると，管理者は迅速に状況を把握することはできない．我々の開発したツール，necosit は，ネットワークトラフィックを TCP コネクション単位でリアルタイムに視覚化する．視覚化したコネクションのトラフィック情報を並べて表示することで，複数コネクションのトラフィックの推移の比較や，ネットワークに影響を与えるプロセスの調査を迅速に行うことができる．また，コネクションは確立と終了が短時間の間に行われる場合も多く，トラフィック情報のすべてを管理者に提示することはできない．そこで，ソート／フィルタ機能を備え，特徴ある通信のみを表示することを可能とした．本論文では，TCP コネクション単位の視覚化方法と，necosit の実装，特徴ある通信を表示する機能について述べる．

†1 明星大学大学院 情報学研究科 情報学専攻
Department of Information Science, Graduate School of Information Science, Meisei University
†2 明星大学 情報学部 情報学科
Department of Information Science, Meisei University

## 2. 関連研究

前述の RRDtool を含め，ネットワークトラフィックをリアルタイムに視覚化することができる様々なツールが提案されている．

Sven 氏らの研究[3] で開発されたツールは，特定ネットワーク内のホスト（内部ホスト）から送出される各パケットのトラフィック量を送信元 IP アドレスごとに示し，外部ホストから内部ホストへ送出される各パケットのトラフィック量を送信元ポート番号ごとに示す．TNV[4] は，ネットワークに流れるパケットを取得し，宛先と送信元の IP アドレスと，タイムスタンプを参照し，IP アドレスとユーザの定めた時間間隔とのマトリクス表示を行い，色によって時間間隔内のトラフィック量を示す．ユーザの要求によって，あるホストの時間間隔内に送受信されたパケットが，どのホストとやりとりされたものかを視覚的に強調でき，使用された送信元と宛先のポート番号をマッピングできる．これら 2 つのツールは，ネットワークトラフィックをホスト単位に視覚化するものであるため，複数の内部ホストが単一の外部ホストと通信している場合，通信ごとのトラフィックの推移を視覚化することができない．

新川氏らの研究[5] で開発されたツールは，IP アドレスの下位 8bit とポートの下位 8bit の 2 次元マトリクスを用いて，ネットワークトラフィックを二次元平面上に表現する．パケットの宛先の IP アドレスとポート番号か，あるいは送信元の IP アドレスとポート番号

Vol.2009-IOT-7 No.4
2009/10/9

によってマッピングされた位置をトラフィック量に応じて色付けする．このような視覚化方法では，時間経過によるトラフィック量の推移をみることができず，下位 8bit が重複する場合，トラフィック量が同じ位置に表示される．

以上のように既存のツールでは，ネットワーク全体のトラフィック量を提示するためにホストやプロトコルごとにトラフィック量をまとめているか，あるいは特定ホストのみのトラフィックを視覚化するので，ネットワーク全体のトラフィック量を通信ごとに示すことはできない．

## 3. コネクションの視覚化方法

necosit は TCP を対象とし，複数のコネクションのトラフィックの推移を並べて表示するために，図 1 のように帯状にコネクションを視覚化する．帯の色はコネクションの状態を表す．SYN_RECEIVED と SYN_SENT の場合は青で描き，FIN_WAIT_1，FIN_WAIT_2，TIME_WAIT，CLOSE_WAIT，LAST_ACK の場合は橙で描く．また，ESTABLISHED の場合は赤と緑で描く．最初にキャプチャしたパケットの送信側を赤（Foreign 側）とし，受信側を緑（Local 側）とする．赤と緑のグラデーションの濃淡は，4.4 で後述する単位時間あたりのトラフィック量を表す．単位時間内のすべてのパケットの IP ヘッダを参照し，total-length フィールドから bps を算出する．8Kbps までの場合，一番薄い色となり，16Kbps，32Kbps，64Kbps と指数的に増えるごとに黒へグラデーションし，128Mbps 以上は完全に黒となる．このグラデーションは 16 段階となっている．並べられた帯を，一定時間が経過するごとに，経過した時間だけ左へ移動した新しい絵を描画し，それを繰り返すことによってアニメーションのように表示する．

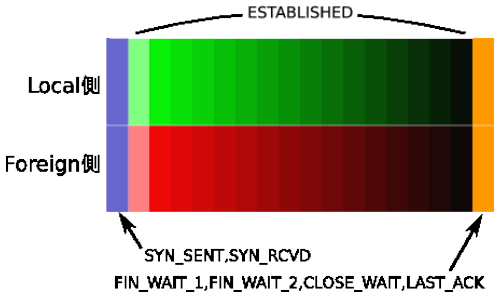


**図 1** コネクションの視覚化モデル
Fig. 1 Visualization model of the TCP connection

## 4. 実　　装

図 2 は，necosit の実行画面である．それぞれのコネクションの帯は縦に並べられる．一番下に表示されたコネクションの下にある時間軸は，右端を現在時刻としている．この図では過去 7.4 秒のトラフィックを視覚化している．各コネクションには，(d) と (e) の 2 つのボタンがそれぞれ設けられる．(d) のボタンには，モニタリングされた順につけられたコネクションの番号が書かれ，(e) のボタンには，Local 側と Foreign 側の IP アドレスとポート番号が書かれる．これらのボタンの機能については後述する．(a) のラベルの情報は，necosit が把握しているコネクションの数と表示している数，モニタリング時の現在時刻，キャプチャしたパケット数とドロップしたパケット数である．


**図 2** necosit のスクリーンショット
Fig. 2 Main window of Necosit

SYN パケットを送出したホストが SYN+ACK パケットを受信することができず，タイムアウトと判断するまでの時間は，TCP の実装によって異なってくるが，本ツールではタイムアウト時間を 3 秒とした．また，TIME_WAIT の時間は，MSL の倍とされているが，この時間も TCP の実装によって異なってくるため，その状態は常に 2pixel で描くこととしている．

### 4.1 データ構造

necosit は，pcap[2] を使用することで，ネットワークインターフェースに到着したパケットをキャプチャすることができる．キャプチャしたパケットの情報から各コネクションの情報のリストを作る．このリストは図 3 のようなデータ構造となっている．コネクションのリストのそれぞれは，Local 側と Foreign 側の単位時間あたりのトラフィック情報をリストとして保持している．新たなコネクションの情報をキャプチャした場合，その情報をコネクションのリストの最後に追加する．古いトラフィック情報をいつまでも保持しておくと，necosit を実行するコンピュータのメモリの空き領域が不足してしまう恐れがあるため，ウィンドウの左端の時間より過去のものとなったコネクションのトラフィック情報を廃棄している．同様に，通信が終了した，すなわち FIN パケット，RST パケットをキャプチャしたか，あるいは SYN_RECEIVED，SYN_SENT の状態からタイムアウトしたコネクションは，最後にキャプチャしたパケットがウィンドウの左端の時間よりも過去のものとなったとき，リストから削除される．

### 4.2 プロセスのスレッド化

necosit は，帯の描画とネットワークインターフェースに到着するパケットのキャプチャを同時に行う必要がある．この 2 つの処理をシングルスレッドで行うと，描画中に到着するパケットを処理できず，ドロップする可能性が高くなってしまう．そのため necosit は，モニタリング開始時に新たに 2 つのスレッドを生成する．necosit のスレッドによる並行処理の流れを図 4 に示す．1 つ目のスレッドはネットワークのパケットをキャプチャし，2 つ目のスレッドはコネクションの帯を描画をする．これらのスレッドを生成したメインスレッドは，フィルタや特定の帯の非表示，コネクションのリストのソートなどの，ユーザから要求される後述の機能を処理する．モニタリングを終了するときに，メインスレッドは，生成したスレッドにシグナルを送信し，終了したことを伝える．

### 4.3 詳細情報の表示

リアルタイムでのトラフィックモニタリングを行うために，トラフィックの概要を迅速に把握できる視覚化は有効であるが，ユーザの要求次第でコネクションの詳細な情報を提示

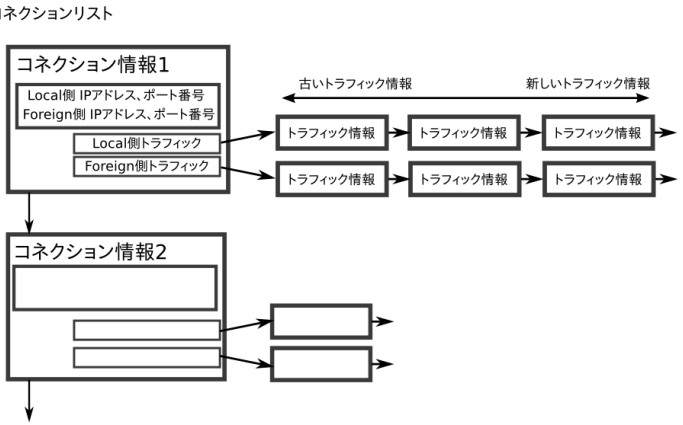


**図 3** コネクションのデータ構造
Fig. 3 Data Structure data for TCP connections

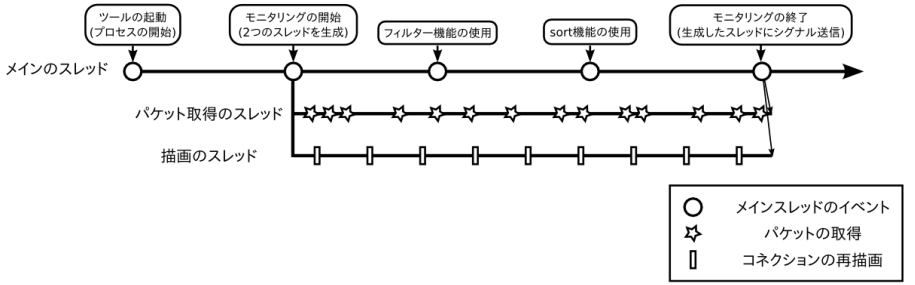


**図 4** マルチスレッドによる並行処理の流れ
Fig. 4 Multithread processing in Necosit

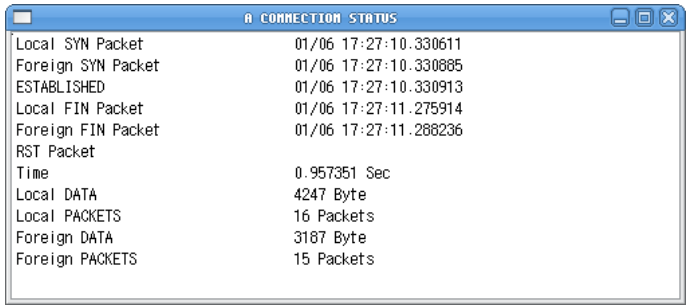


**図 5** 詳細情報の表示ウィンドウ
Fig. 5 Window of detailed TCP information

する機能も必要である．necosit は，コネクションごとに配置された（e）のボタンがクリックされることで，図 5 のように以下のコネクションの情報を別ウィンドウに表示する．

- 最初の SYN パケットを取得した時刻
- 最初の FIN パケットを取得した時刻
- 最初の RST パケットを取得した時刻
- ESTABLISHED の開始時刻（最初の ACK パケットを取得した時刻）
- コネクションを確認してからの通信時間
- コネクションがやり取りしたパケット数
- コネクションがやり取りした総バイト数

SYN パケットをキャプチャしていない（通信の途中からモニタリングした）ものと，FIN パケットをキャプチャしていない（まだ通信が終了していない）ものの時刻の情報は Unkown と表示する．また，RST パケットをキャプチャした場合は，Local 側と Foreign 側のいずれが送出したかとキャプチャした時刻を表示する．

### 4.4 視覚化の粒度

（f）の小さなウィンドウは，切り離した Config メニューである．Config メニューからは，コネクションのトラフィック視覚化の粒度を変えることができる．このメニューには以下の項目がある．

- Refresh Rate
  1 秒間に画面の表示を何度更新するかを決定できる．1 秒間あたりの更新回数を多くすれば，necosit を実行するコンピュータへの負荷は多くなるが，アニメーションようにコネクションのトラフィックを見ることができる．
- Sec per Unit
  図 2 の実行画面において，時間軸から一定間隔ごとに引かれている縦の線がある．Sec per Unit は，この縦の線の間の時間が何秒かということを変更できる．これをより長い時間に変更することで，表示は大まかなものとなるが，さらに過去のトラフィックも視覚化できる．
- Pixels per Unit
  Sec per Unit に割り当てられる pixel 数を変更する．この pixel 数を大きくすることで，表示するコネクションの横幅を調整することができる．
- Stat per Unit
  Sec per Unit あたりの統計情報の更新時間を変更する．この更新時間は，トラフィック量を表示する単位時間となる．単位時間を調整することで，トラフィックの表示の概略の度合いを変更することができる．

Stat per Unit と Sec per Unit から算出される単位時間より短い間隔に Refresh Rate を指定しても，画面を更新するごとに新しいトラフィック情報を示すことができないため，単位時間以上の間隔に Refresh Rate を設定するべきである．

### 4.5 特徴あるコネクションの表示

necosit の視覚化方法では，表示できるコネクションの数には限りがある．コネクションの表示順は，そのコネクションのリストの順と同じであり，通信の開始時刻が古いものからとなる．図 2 では，17 本のコネクションのみ表示しているが，ツールが把握しているコネクション数は 147 本である．necosit にはスクロールバーを設けていない．その代わり，表示するコネクションを選択する機能をいくつか実装した．この節ではそれらの機能について述べる．

#### 4.5.1 ソート機能

（b）のボタンは，ソートボタンである．ボタンは左から，コネクションの通信時間，Local 側 IP アドレス，Local 側ポート番号，Foreign 側 IP アドレス，Foreign 側ポート番号，Foreign 側総トラフィック量，Local 側総トラフィック量を表している．ソートボタンをクリックするとコネクションのリストを，その要素によって昇順にソートする．続けて同じボタンをクリックすると，降順にソートする．ソート後に新たに検知したコネクションの情報は，ソートせずリストの最後に追加する仕様となっている．

#### 4.5.2 フィルタ機能

（c）のテキストエントリからは，pcap 形式のフィルタを入力することができる．例えば IP アドレスやポート番号など，選び出したいコネクションの特徴があらかじめ分かっているならば，これにより，視覚化するコネクションの情報をパケット単位で選択することができる．しかし，これはフィルタの実行後にキャプチャするパケットを選別するものなので，それより前にリストに追加したトラフィックの情報はフィルタの対象とはならず，リストに情報が残ってしまう．メニューからリストの情報をすべて廃棄することができるので，フィルタリングの対象外となるトラフィック情報を廃棄するためには，リストを初期化する必要がある．

#### 4.5.3 選択されたコネクションの非表示

図 2 の（d）は非表示ボタンである．これをクリックすると，それに対応するコネクションは非表示となる．非表示となったコネクションは，リストから削除するわけではなく，トラフィック情報の更新は行われる．また，メニューから非表示となったすべてのコネクションを再表示することができる．これにより，ソート機能やフィルタ機能よりも，表示するコネクションを柔軟に選ぶことができる．

## 5. 評　　価

necosit の性能を評価するために簡単なテストを行った．このテストでは，明星大学日野校の HTTPproxy サーバに流れるトラフィックをモニタリングした．この proxy サーバのトラフィック量は，最大で約 50Mbps，約 7000pps で，コネクション数は最大で約 2000 本である．Refresh Rate を 1，Sec per Unit を 1，Pixels per Unit を 100，Stat per Unit を 20 に設定し，1680x1050 のモニタで，ツールのウィンドウを最大化して実行した．表示の秒間更新回数は 1 回であり，32 本のコネクションの過去 13.12 秒分のトラフィックを視覚化できる．モニタリングしたコンピュータの情報を表 1 に示す．この環境で 2 時間程度モニタリングした結果，パケットのドロップ率は 0.0025%程度であり，約 4000pps を越えない場合はパケットをドロップすることなくモニタリングできるだろうということが分かった．

**表 1**　コンピュータの情報
Table 1　Computer Specifications

| 名称 | 情報 |
|---|---|
| CPU(クロック) | AMD Athlon 64 X2 6000+(3.0GHlz) |
| メモリ | 2GByte |
| グラフィックボード | NVIDIA XFX 8500GT |
| ネットワークインターフェース | Intel 82572EI |
| OS | FreeBSD 8.0-CURRENT(2008 年 2 月 28 日，CVS Checkout のソース) |
| X サーバのバージョン | xorg-server 1.6.0 |
| デスクトップマネージャ | GNOME 2.20.3 |
| GTK のバージョン | GTK2 2.12.8 |
| pcap のバージョン | libpcap-0.9.8 |

## 6. おわりに

ネットワークトラフィックの概要を TCP コネクション単位でリアルタイムに提示するツール，necosit の開発を行った．ネットワークに流れるパケットからのコネクションのモニタリングを可能とし，単位時間ごとのトラフィックや，状態遷移を色により表示した．ソートや pcap 形式のフィルタ，コネクションの非表示による，表示コネクションの選別をできるようにした．このツールを使うことにより，コネクション毎のトラフィック量の推移や開始時間，その状態遷移を視覚的に確認できるようになった．今後，ツールの評価をさらに行い、表示するコネクションの順序を常にソートされた状態にする機能や、既にリストにあるコネクション情報に対するフィルタリングなど，機能の追加をする予定である．

## 参 考 文 献

1) Oetiker, T.: RRD-Tool(Round-Robin Database tool), http://oss.oetiker.ch/rrdtool/.
2) VanJacobson, C.L. and McCanne, S.: tcpdump/libpcap, http://www.tcpdump.org/.
3) Krasser, S., Conti, I.G., Grizzard, I.J., Gribschaw, J., Owen, I.H. and Member, S.: Real-time and forensic network data analysis using animated and coordinated visualization, *In Proceedings of the 6th IEEE Information Assurance Workshop*, IEEE Press, pp.42–49 (2005).
4) Goodall, J.R., Lutters, W.G., Rheingans, P. and Komlodi, A.: Preserving the Big Picture: Visual Network Traffic Analysis with TN, *Visualization for Computer Security, IEEE Workshops on*, Vol.0, p.6 (2005).
5) 拓也新川，卓山之上：IP アドレスとポートによる二次元平面を用いた通信トラフィックの可視化について (第 3 セッション)，情報処理学会研究報告. DSM, [分散システム/インターネット運用技術]， Vol.2006, No.97, pp.31–36 (20060915).