Vol.2010-IOT-8 No.29
2010/3/2

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改良

宇都木 進[†1] 渡邊 晶[†2]

我々の開発したツール，necosit は，ネットワークのトラフィックを TCP コネクション単位でリアルタイムに視覚化する．このツールの機能について検討し，特定コネクションのパケットの中身の表示，表示するコネクションの帯の幅の変化によるズーミングなどの改良を行った．また necosit の性能評価を行った．

Improvement of a tool visualizing the traffic by TCP connection unit

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

Necosit shows an overview of the TCP traffic in real time. We added new functions to necosit, which included dumping packets of the specific connection and zooming in and out of the connection list pane. We also evaluated performance of necosit.

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．我々の開発したネットワークのトラフィックを TCP コネクション単位に視覚化するツール，necosit[1)] は，それぞれのコネクションのトラフィック量の推移の比較や，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，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もできる．

我々は，このツールの機能について検討し，実装済みのソート機能とフィルタ機能についての改善，特定コネクションのパケットの中身を表示するダンプ機能の実装，より多くのコネクションを表示できるようにするズーミング機能の実装，ファイルからのモニタリングや，特定コネクションに対する RST パケットの送信機能などを実装した．本論文では，これらの改良と追加を行った機能について述べ，necosit の性能評価を行った結果を示す．

2. 改良前の necosit

図 1 は，改良を行う以前の necosit の実行画面である．necosit は，ネットワークインターフェースから TCP パケットを取得し，コネクションのリストを生成する．そして，ウィンドウの右端を現在時刻として，保持するリストと同じ順番でコネクションを帯状に視覚化する．(a) のラベルには，necosit が保持するコネクションのリスト数と現在時刻，キャプチャパケット数とドロップパケット数が表示される．(d) と (e) の 2 つボタンは，ウィンドウに表示されるコネクションの帯に対して，それぞれ設けられる．(d) がクリックされると非表示となり，(e) がクリックされるとそのコネクションについての詳細情報が別窓に表示される．(f) の切り離された Config メニューからは，トラフィック視覚化の粒度を変更でき，この図の場合，単位時間を 0.05 秒として，過去 7.4 秒のトラフィックをウィンドウに表示しており，1 秒に 1 度のウィンドウの更新を行うことで，トラフィックをアニメーションのように表示する．コネクションの単位時間の bps を IP ヘッダの total-length フィールドから算出し，bps の高いところを，より濃い色として帯を表示する．また，(b) のソートボタンからは，対応する要素でコネクションのリストをソートでき，(f) からは，キャプチャするパケットを選別できるフィルタを入力することができる．

3. 機能の改良と追加

図 2 は，改良を行った necosit の実行画面である．今回の改良に伴い，necosit のメインウィンドウに (g) から (j) のユーザインターフェースを新しく追加した．(i) の Pause ボタンを押下することで，ネットワークインターフェースからパケットパケットを取得しつつ，ウィンドウの更新を停止できるようにした．その他の新しいユーザインターフェースの機能については後述する．(b) から (f) までのインターフェースの表示には変更はなく，(a) のラベルには，necosit が保持するコネクションのリスト数と，ウィンドウに表示しているコ

†1 明星大学大学院 情報学研究科 情報学専攻
Meisei University
†2 明星大学 情報学部 情報学科
Meisei University

図 1 改良前の necosit の実行画面
Fig. 1 Main window of Necosit before improvement

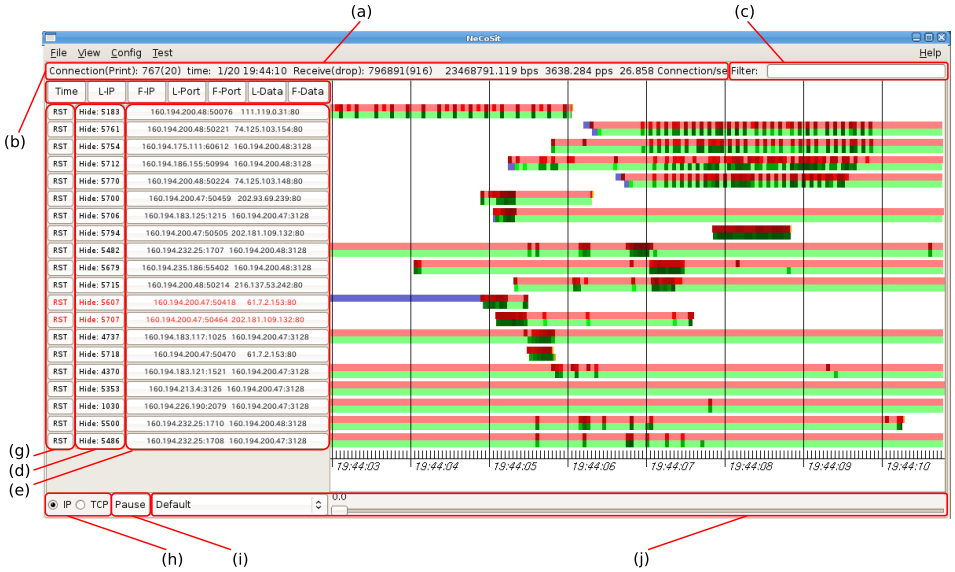

図 2 改良後の necosit の実行画面
Fig. 2 Main window of Necosit after improvement

ネクション数，現在時刻，取得したパケット数，ドロップしたパケット数，pps，bps，秒あたりの平均コネクション確立数を表示し，ユーザに提供する情報を追加した．

3.1 ソート機能の改良

necosit は，図 2 の（b）のボタンをクリックすることで，その要素ごとにソートすることができる．改良前の necosit のソート機能は，ボタンをクリックしたときのコネクションリストをソートするために，それよりあとにコネクションリストに追加されたものに関してはリストの最後に追加する仕様となっていた．しかし，新たに検知したコネクションのモニタリングや，データの転送量のもっとも多いコネクションの表示を常に行い場合は，ユーザが常にソートを行う必要がある．そこで，リアルタイムモニタリング時に行われる定期的な画面の更新に伴い，定期的にコネクションのリストをソートすることで，コネクションの表示順を常にソートできるようにした．

3.2 フィルタ機能の改良

necosit は，ネットワークのトラフィックを取得するために pcap[2] を使用している．necosit は pcap のフィルタ機能を使用し，図 2 の（c）からパケット単位のフィルタリング行うことができる．しかし，これはフィルタリングを実行したあとに到着するパケットをフィルタするものであるため，それ以前にリストに追加したトラフィックの情報は，フィルタリングの対象とはならず，リストに情報が残ってしまう．pcap の柔軟なパケットフィルタリングを実現しつつ，この問題を解消するために，フィルタリングが実行されたとき，フィルタの対象になるかどうかにかかわらず，リストのすべてのコネクションを非表示とし，フィルタリング実行後にパケットを取得したコネクションのみを表示するようにした．

3.3 機能の追加

3.3.1 パケットダンプ機能

ネットワークトラフィックを necosit でモニタリングする場合，コネクション別にトラフィック量の推移を確認できるが，パケットの内容を確認することはできない．また，necosit で不審なコネクションを発見してからでは，ネットワークトラフィックをパケット単位でダンプできるツールを用いて内容を確認することが困難な場合がある．そこで，necosit に選択

されたコネクションのパケットをダンプする機能を追加した．図 2 の（f）のボタンを Shift キーを押しながらクリックすることで，図 3 のように別ウィンドウに以下の情報を表示する．

- パケットのキャプチャ時刻
- TCP のフラグ
- IP-Length
- TCP-Length
- シーケンス番号
- ACK 番号
- ウィンドウサイズ
- TCP ヘッダのオプション

このリストに表示される文字の色は，そのコネクションの最初にキャプチャしたパケットのパケットの送信元を緑とし，宛先を赤として表示を行う．リアルタイムモニタリング時は，1 秒ごとに表示が更新され，右上のチェックボックスがチェックされている場合，縦のスクロールバーが常に最下にある状態となる．また，左下のチェックボックスがチェックされている場合，ホスト名が IP アドレスとして表示される．

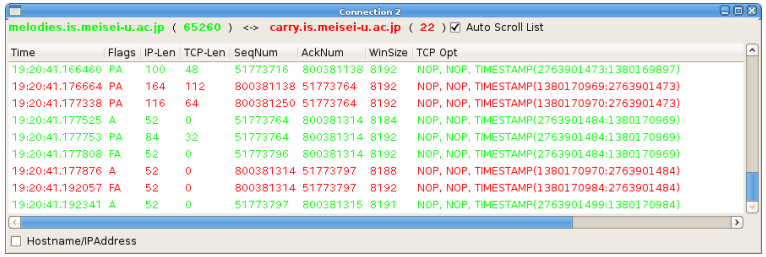

図 3 特定コネクションのパケットダンプ
Fig. 3 Packet list window

3.3.2 ズーミング機能

改良前の necosit は，1920x1200 のモニタでツールのウィンドウを最大化して実行した場合，41 本のコネクションを表示できた．しかし，ソート機能やフィルタリングなどを用いて，特徴あるコネクションのみを選択したとしても，そのすべてを 1 つのウィンドウに表示できない場合がある．より多くのコネクションを視覚化し，トラフィック量の推移を比較できるようにするため，視覚化されたコネクションのそれぞれの帯の縦幅を広くしたり，狭くしたりするズーミング機能を実装した．ウィンドウ上でマウスホイールをスクロールすることによって，ズーム量の大小を調節することが可能である．この機能によりコネクションの帯の幅が狭くなると，それにともなってそれぞれのボタンとその文字も小さくなる使用となるため，多くのコネクションを視覚化しようとすると，図 4 のように，どのホストのコネクションがどのようなサービスを使用して通信しているかは分からなくなる．この機能により，1920x1200 のモニタならば，最大で 123 本のコネクションを表示することができ，IP アドレスとポート番号を確認できる程度にズーミングを行った場合ならば，55 本のコネクションを表示できるようになった．

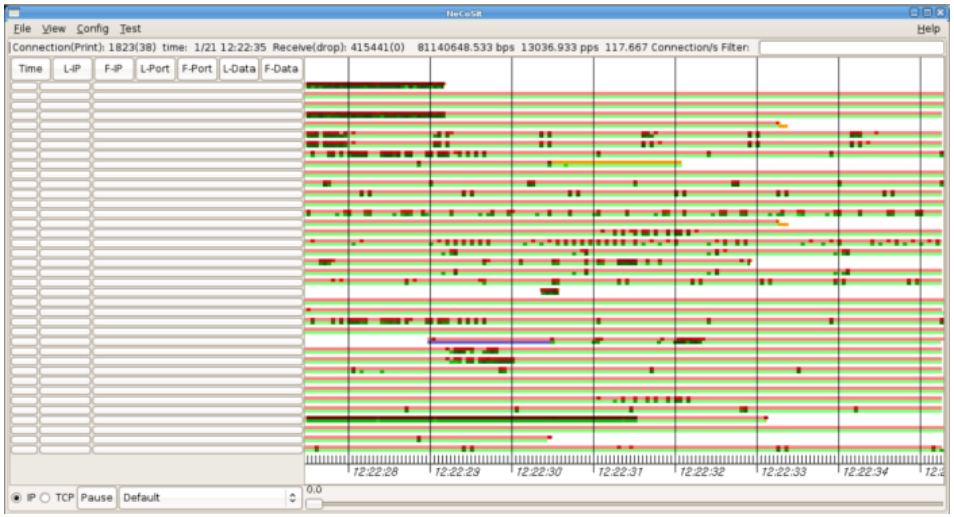

図 4 ズーミングを行ったときの表示
Fig. 4 Zooming out of the connection list pane

3.3.3 ファイルからのモニタリング

我々は，necosit がログファイルからモニタリングできるならば有用だと考え，tcpdump などのツールにより作成できる pcap 形式のファイルからモニタリングできる機能を実装した．図 5 は，ファイルからのモニタリングを行ったときのウィンドウである．リアルタイムモニタリングの場合，定期的なウィンドウの更新に時間をかけると，更新中に到着するパ

ケットを処理できず，ドロップする可能性が高くなるため，表示するコネクション数はウィンドウの大きさに依存する．一方，ファイルからのモニタリングの場合，パケットをドロップすることがないため，図 5 のように，スクロールバーを付け，すべてのコネクションをウィンドウに表示する．

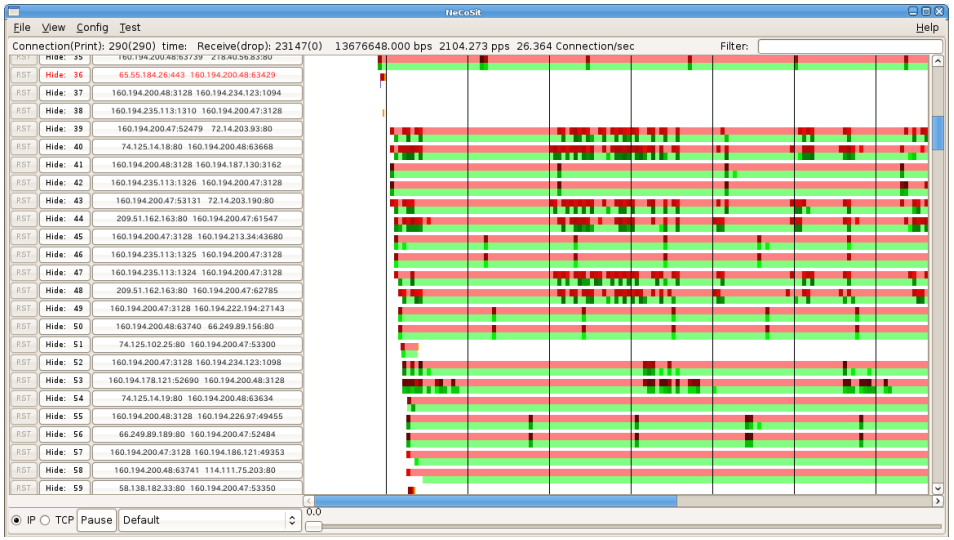

図 5 ファイルからのモニタリング
Fig. 5 Monitoring connection from a file

3.3.4 リセットパケットの送信

ネットワークへ負荷を与えるようなコネクションや不審なコネクションを見つけたとき，そのコネクションを確立しているコンピュータを直接操作し，コネクションを切断しなければならない場合があるが，いつでもそのコンピュータを直接操作できるとは限らない．そこで我々は，necosit に RST パケットを送信する機能を追加した．図 2 の（d）のボタンをクリックすると，そのコネクションを確立している両方のエンドホストに対してリセットパケットを送信する．この機能によってリセットパケットを送信したが，実際はコネクションが切断されていなかった場合，necosit の表示はリセットが送信されたことになるが，送信後にそのコネクションの新たなパケットをキャプチャすると，表示は正しく更新される．

3.3.5 その他の追加機能

トラフィック情報の保持時間

改良前の necosit は，ウィンドウの左端の時刻よりも過去のトラフィック情報を廃棄していた．1920x1200 のモニタならば，約 15 秒分のトラフィックを表示できるが，コネクションの確立と終了が短時間の間に行われる場合も多く，モニタリングされずにリストから廃棄されてしまうコネクションが出てくる．そのようなコネクションをモニタリングするために，トラフィック情報をいつまで保持するかを変更できる機能を追加した．図 2 の（i）のコンボボックスから，トラフィックの保持時間を変更することができ，図 2 の（i）のシークバーを左にスライドすることによって，過去のコネクション情報を表示できる．この機能により，通信が開始されてある程度時間が経過したコネクションについても，そのコネクションの確立時刻や通信開始時のトラフィック推移なども調べることができる．

タブウィンドウ

1 つのウィンドウで複数のモニタリングを可能とするために，タブウィンドウを実装した．図 6 のようにタブには，ネットワークインターフェースからのモニタリングの場合，モニタリングしているホスト名とインターフェース名を表示し，ファイルからのモニタリングの場合，そのファイルをそのパスとともに表示する．このタブウィンドウの機能を使用することにより，特定のインターフェースに到着するパケットに対してそれぞれタブウィンドウで異なったフィルタリングを行ったり，ファイルからのモニタリングとネットワークインターフェースからのモニタリングを同時に行ったりすることができるようになった．

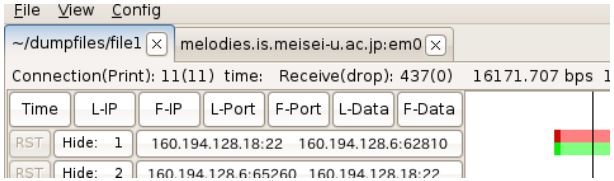

図 6 タブの表示
Fig. 6 Tabed interface

再送パケットの表示

TCP はパケットの順序制御を行うストリーム型の通信であり，相手ホストにパケットが到着しなかったと判断した場合，パケットの再送を行う．我々は，この再送パケットを表示す

る機能を追加した．TCP ヘッダには順序制御を行うためにシーケンス番号が格納されており，再送されずにデータパケットが転送されている場合には，パケットごとに番号が増加する．necosit は，コネクションの最新のシーケンス番号と新しく取得したパケットのシーケンス番号を比較し，その番号が前後していた場合，再送が発生したと判断する．再送パケットと判断した場合，図 7 のように，そのパケットを含む単位時間の帯の幅が半分となる．この機能により，再送が多く行われているコネクションを視覚的に判断できるようになった．

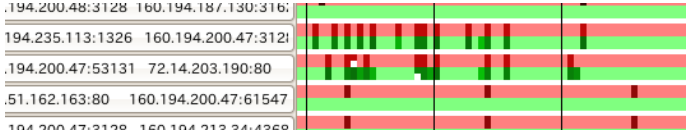

図 7 再送パケットの表示
Fig. 7 Display retransmission TCP packets

リセットパケットの表示

TCP コネクションのステートを色によって示していたが，コネクションの終了は，ほとんどの場合，短時間の間に行われるため，コネクションの終了が FIN パケットによるものなのか，RST パケットによるものなのか，判断できないことがある．RST パケットによる終了は実質的に強制切断であるため，コネクションの異常終了を検知するために RST パケットが送信されたコネクションを表示できる機能が必要だと考え，実装した．RST パケットによって終了した場合，そのコネクションの表示に付加されるボタンの文字の色を，赤に変更して表示する．

トラフィック量の表示のレベル

改良前の necosit は，bps の算出方法に IP ヘッダの total length フィールドを使用していた．そのため，単位時間に TCP の ACK のみのパケットが 1 つでも転送された場合であっても，データのやりとりがされたと見なしていた．しかし，ACK のみのパケットは TCP のレベルで考えると，データを転送していないことと同じである．そこで，TCP コネクションのトラフィック量の表示を TCP レベルで行い，アプリケーションの転送データ量を表示できるようにした．TCP レベルでのトラフィック量の表示では，パケットのシーケンス番号からバイト数を決定し，bps を計算する．necosit の図 2 の（g）のラジオボタンを IP とすると，IP レベルでのトラフィック視覚化となり，TCP とすると，IP レベルでのトラフィック視覚化となる．

4. 性能評価

necosit の性能評価を行った．この評価では，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 サーバに流れるトラフィック量の平均は，約 80Mbps，約 13000pps，コネクション数の平均は約 2000 本であった．ウィンドウの秒間更新回数は 1 回とし，最大で 24 本のコネクションの過去 7.4 秒のトラフィックを視覚化できる設定とした．表 1 は実験に使用したコンピュータのハードウェアとソフトウェアの情報である．この環境において 40 分のモニタリングを行い，ウィンドウの更新に合わせて，necosit の保持するコネクションのリスト数とパケットの受信数，ドロップ数を取得した．図 8 は necosit の保持するコネクションのリスト数とパケットドロップ数の時間による推移を示したグラフである．リスト数が約 2500 を越えないあいだは，トラフィックを正しくモニタリングできたが，リスト数が約 2500 を越えると，著しくパケットをドロップし始め，ウィンドウの更新を 1 秒に 1 度，行うことができなくなった．その後，パケットのドロップ率が徐々に上がっていき，保持するコネクションのリスト数は 20000 を越えた．図 9 は，保持するコネクションのリスト数とパケットの受信数をパケットドロップ数と対比したグラフである．パケット受信数が多くなるにつれてパケットドロップ数が増加している部分は，ツールがパケットの処理に間に合わなくなり，1 秒に 1 度のウィンドウの更新を行えなくなったときのものであり，図 8 における最後の約 10 分と対応するため，パケットをドロップした原因とは関係がない．それ以外の部分では，パケットドロップ数とパケット受信数はあまり関係なく，保持するリスト数が多くなるにしたがって，パケットをドロップしている．necosit は，ネットワークインターフェースに到着したパケットに対応するコネクションを検索するため，宛先と送信元の IP アドレスとポート番号をコネクションのリストのそれぞれと比較する．そのため necosit のパケットドロップ率は，necosit が保持するコネクションのリスト数に比例すると考えられる．また，パケットドロップ率が増加すると，FIN パケットや RST パケット，すなわちコネクションの終了を示すパケットをドロップする可能性も高くなり，実際には終了したコネクションについてリストを保持しつづけてしまう．つまり，necosit が新たなパケットを処理しきれないリスト数になると，ドロップが発生し，リスト数も増加するという，悪循環になっているのではないかと考えられる．

5. 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

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（2009 年 3 月 4 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

ル，necosit の機能の改善と追加を行った．実装済みであったソート機能とフィルタの機能について改善を行い，特定コネクションのパケットのダンプによって，より詳細に調査を行えるようにし，ズーミング機能によって，表示の範囲を変更できるようにした．tcpdump などのツールにより保存した pcap 形式のファイルからモニタリングできるようにした．コネクションを確立するホストに対して RST パケットを送信する機能を実装し，そのホストを直接操作することなくコネクションを切断できるようにした．性能評価を行い，necosit が保持するコネクションのリスト数が多くなるとパケットドロップ率が高くなることと，処理が追いつかなくなることが分かった．今後，ユーザが使用しやすくなるよう，メニューやボタンなどのユーザインターフェースの改善を行う．また，コネクションのリストのデータ構造を見直すことと，実際には終了したコネクションについて対処できるようにすることで，性能の向上を測る．

参 考 文 献

1) 宇都木進，渡邊　晶：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，情報処理学会研究報告. インターネットと運用技術（IOT），Vol.2009-IOT-7, No.4 (20091009).
2) VanJacobson, C.L. and McCanne, S.: tcpdump/libpcap, http://www.tcpdump.org/.

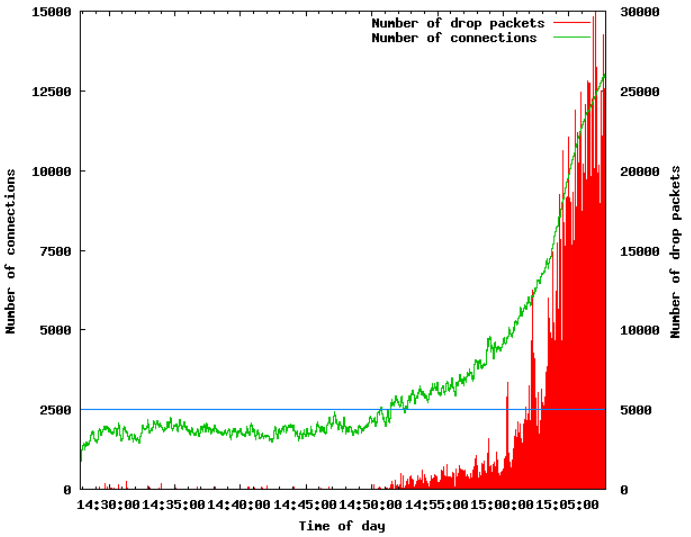

図 8 パケットドロップ数の推移
Fig. 8 Transition of number of drop packets

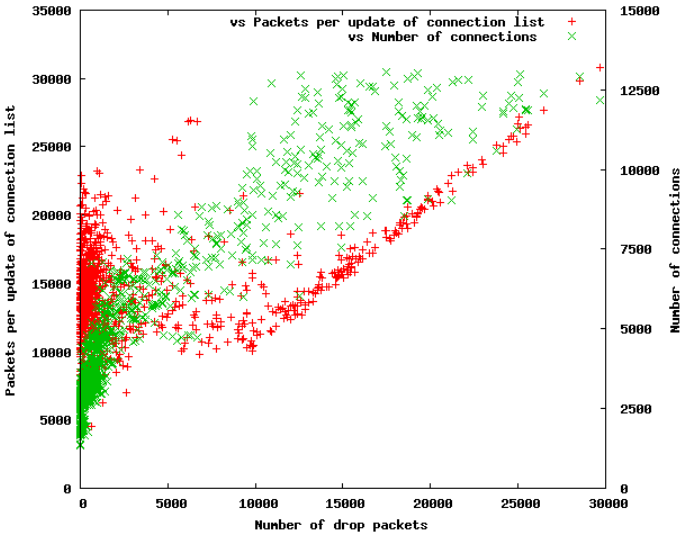

図 9 パケットドロップ数に対する受信パケット数とコネクション数の比較
Fig. 9 Number of drop packets vs Number of receive packets and Number of Connections