エンドユーザ向けリアルタイムトラフィック可視化システムの設計と実装

王　亮 (福井大学大学院)
白井治彦 (福井大学工学部)・黒岩丈介・小高知宏・小倉久和 (福井大学大学院工学研究科)

1　はじめに

近年、情報通信技術の発展に伴って、ネットワーク通信の高速化、大容量化が進んでいる。ADSL や光ブロードバンドという光ケーブルを用いた通信の普及とコンピュータ操作の簡便化により誰でも、いつでも、どこでも通信ネットワークを気軽に利用することが可能となった。しかしネットワーク通信は目に見えなく、実際に行われていることが分かりづらいという問題がある。ネットワーク通信の知識が乏しいエンドユーザは、コンピュータウィルスや不正アクセスなどにより利用中のコンピュータが侵入されてしまうことをよくある。これはネットワーク通信の知識を分からないと理解できないと考えている。

そこで本研究では、ネットワーク知識が乏しいエンドユーザに向け、リアルタイムで利用中のマシンがネットワーク上でどのように通信しているか、パケットがどのように流れているかをはっきり把握させたいため、やり取りするパケットのヘッダ情報を分かりやすい方式で可視化する。それによってネットワーク知識を身に付けさせ、セキュリティを意識向上することを目指している。本稿では、このようなシステムの設計と実装について報告する。

2　トラフィック可視化システムの設計

エンドユーザは Web の閲覧、メール送信などのネットワークアプリケーションを使う時、TCP/IP、ルータ、ハードウェア、ソフトウェアなどいろいろな技術を用いている。始めからネットワーク通信の知識を学ぶときは、まずネットワークの仕組みを理解することが重要だと考えている。ネットワークの知識が乏しいエンドユーザに対しては、通信の状況を出来るだけシンプルに提示する必要がある。そこで、ネットワーク通信で利用するウェルノウンポート（宛先ポート）と、対応するプロトコルと通信量をリアルタイムでエンドユーザに提示するシステムを提案する。

提示する内容と理由については表 1 にて示す。

提示項目	提示理由
宛先ポート	クライアントとサーバ間の通信がポートを介して行われることをエンドユーザに把握させる。
プロトコル名 サービス名	宛先ポート番号のみを示すのはどのプロトコル使用しているか、どのようなサービスが行われているかが分かりづらいと考えたためである。
通信量	通常は目に見えない通信の状況を分かりやすく見ることができる。

表 1

しかしながらポートの数はとても多く、またポート番号と動作の対応内容を理解するのは難しいことである。そしてエンドユーザに行ったネットワークアプリケーションが利用している宛先ポートとプロトコル、対応するサービスをはっきり知らせるため、本研究では Figure1 のようなリアルタイムで 10 秒間当たりの宛先ポートにより通信量の上位 3 位までのポート番号、そのプロトコル名、サービス名、また通信量を分かりやすく提示することとした。つまり、10 秒間一回宛先ポート別の通信量を累計して、上位三位のポート番号、対応するプロトコル名、サービス名と通信量のグラフを表示する。さらに、エンドユーザがプロトコルの知識を詳しく理解できるようにするため、プロトコルの解説機能も付ける。

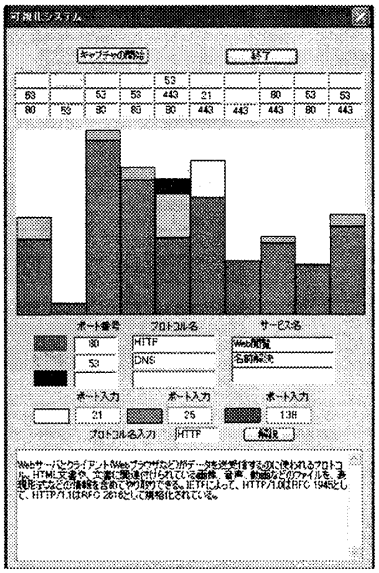

Figure 1: システム画面設計

3　トラフィック可視化システムの実装

以上の要素を組み込んだリアルタイムトラフィック可視化システムは Figure2 にて示すような四つの機構から構成されている。

まずパケット取得機構では、BSD ライセンスにもとづき配布されている Windows 用のパケットドライバである WinPcap を用いて、利用中のマシンがやり取る全てのパケットと取得時刻を取得して、パケット処理機構へ渡す。

パケット処理機構では、渡されたパケットから自分のコンピュータにおいて設定された送信元 IP アドレスによ

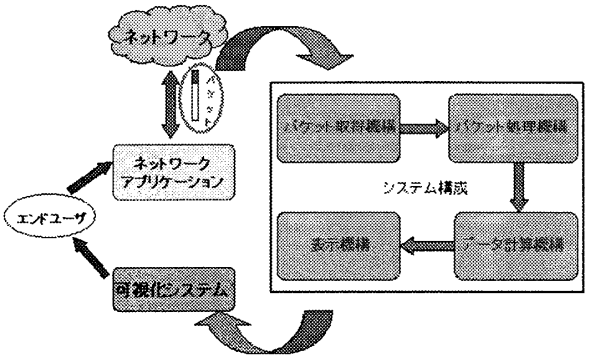

Figure 2: システムの構成

るフィルタリングを行うことで、IP パケットのみを選別して、その IP パケットヘッダに含まれている宛先ポートとパケットサイズを取得して取得時刻と一緒に計算機構へ渡す。

データ計算機構では、取得時刻と現在の時刻との差分を算出して、そこで獲得した情報 (宛先ポート、パケットサイズ) を 10 秒ごとに表示機構へ渡す。取得時間が 10 秒以内であった場合は、各宛先ポート別にパケットサイズの累計を算出して、そのままデータ計算機構内にて継続計測を行う。累計取得時間が 10 秒になった場合、各宛先ポートとパケットサイズ量をデータ計算機構内にて情報量が大きい順にソートし、そのパケットサイズ上位 3 位を表示機構へ渡す。

最後、10 秒間当たり上位 3 位の宛先ポート番号、対応するプロトコル名、サービス名と通信量を分かりやすいインタフェースで表示する。さらに宛先ポート別の通信量グラフは色で区別するので、気になる宛先ポートがあれば、特定の色を付けられる。そのポートが動作すれば、指定された色のグラフを出てきて、ユーザに提示する。

4 実験

作成したシステムを ADSL 経由でインターネット網に接続された実験用 PC 上で稼動させる実験を行った。

ネットワーク	ISP:ぷらら　回線：ADSL 50Mbps
コンピュータ	DELL DIMENSION E521 AMD Athlon(tm)64x2 Dual Core Processor 3600+ 1.90GHz メモリ：1024MByte
実験時間	１０分間

本システムを動作させて最後の 10 秒間で Yahoo のホームページを閲覧することをした。Figure3 で示されるように、この 10 秒間で取得した宛先ポート番号を（53、DNS、名前解決）, (80,HTTP,Web 閲覧) という形で示されていた。通信量グラフは当時の宛先ポート別の通信が色を付けて表示されていた。

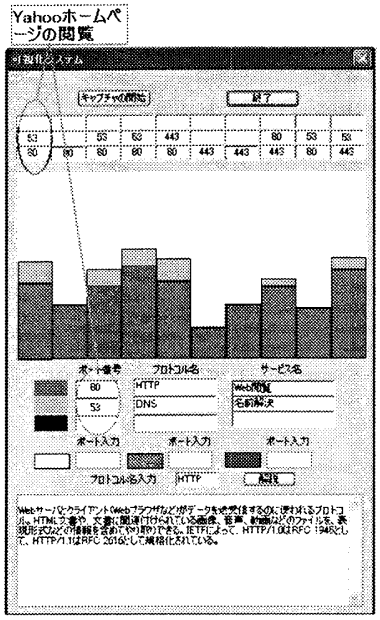

Figure 3: 実験例

5 考察とまとめ

本システムはネットワーク専門知識が浅いエンドユーザー教育を対象に開発した。“目に見えないもの、理解しにくいもの”と考えられていた抽象的な Network という存在がエンドユーザーにいかに分かりやすく、可視化することに成功した。また、エンドユーザーに Port 番号、プロトコル名、サービス名を表記することにより、エンドユーザーが更なる Network への関心をもつ可能性を含めてみた。今後の展開として、エンドユーザーに提示する更なる Network 情報量、そしてエンドユーザーがつねに成長することができるような育成型のシステムへの改良などが課題として考えられる。

References

[1] 小高知宏著「基礎からわかる TCP/IP アナライザ作成とパケット解析」オーム社 (2001)

[2] WinPcap. The packet capture and network monitoring library for windows. http://www.winpcap.org/.

[3] 荒井正之　田村尚也　渡辺博芳　小木曽千秋　武井恵雄. TCP/IP プロトコル学習ツールの開発と評価. 情報処理学会論文誌、Vol.44,No.12,pp.3242-3251,2003.