福井大学 大学院工学研究科 研究報告 第57巻 2009年3月
Mem. Grad. Eng. Univ. Fukui, Vol. 57 (March 2009)

エンドユーザのセキュリティ意識向上を目指したパケットヘッダ可視化システム

王 亮* 白井 治彦† 黒岩 丈介** 小高 知宏* 小倉 久和**

A packet header visualization system for the end-user security education

Liang WANG,* Haruhiko SHIRAI,† Jousuke KUROIWA,**
Tomohiro ODAKA* and Hisakazu OGURA**

(Received February 5, 2009)

To improve security awareness of the end-eser, we designed and implemented the packet header visualization system that visualizes the condition of network communication. We implemented our system using the Microsoft Visual Studio 2005 with the winpcap library. This system capture a packet and visualize the packet header information, the flow of network traffic and protocol and port number of the conection.

Key words : Network, Security, Visualization, Packet Header

1. はじめに

情報化社会の発展とともに、情報入手の手段も広がっている。Internet技術の発展に伴って、ネットワーク通信は現代の生活の一部分として欠かせないものとなっている。

ADSLや光ケーブルの普及により、通信ネットワークの常時接続形態がますます一般化している。そして技術の発展とともに、例えばPLC（Power Line Communications）という電力線を介したネットワーク通信など，新しい技術も普及している。こうした技術のおかげで、いつでも、どこでもネットワーク通信を気軽に利用することができるようになった。しかし通信ネットワークは我々に利便性を与えるとともに、いろいろな危険性ももたらしている。これはすなわちセキュリティの問題である。

近年、ウィルスや不正アクセス被害の報道がよく聞かれるが、これらは企業また個人に大きな損害を与えている。常時接続のネットワーク環境が広く普及し、それぞれのコンピュータでネットワークに接続する時間が長くなるに伴い、通信量が増大し、コンピュータウィルスやワームなどの悪意あるプログラムによる危険性も以前より高くなっている。通信ネットワークの技術の発展により、ウィルスやクラッカーの攻撃手段も変化している。ウィルス対策ソフトを開発している企業は対応技術を更新しているが、ウィルスや不正アクセスなどセキュリティ問題を徹底的に取り除くことは困難である。つまり、セキュリティ対策ソフトだけでは自分のコンピュータを完全に守れることはできないのが現実である。

ウィルスや不正アクセスを根本的に抑えたければ、通信ネットワーク利用者の一人一人がセキュリティについて理解しなければならない。しかしネットワーク上の通信は目に見えなく、実際に存在していることが分かりにくい。色々なネットワーク解析ツールが開発されているが、ネットワークの専門知識を持っていない

*原子力・エネルギー安全工学専攻
**知能システム工学専攻
†技術部
*Nuclear Power and Energy Safety Course, Graduate School of Engineering
**Human and Artificail Intelligence Systems Course, Graduate School of Engineering
†Technical Support Division

と提示されたデータを理解することは困難である。

そこで本研究では、ネットワークの専門知識が乏しいエンドユーザやネットワークの知識を勉強しようとするエンドユーザを対象とし、ユーザが使用しているコンピュータにおけるネットワークの情報を分かりやすく提示するシステムを提案する。本システムはネットワーク通信を利用するユーザのセキュリティ意識向上を目的とする。対象とするユーザが初心者であることを考慮に入れ、分かりやすいインタフェースを持ったシステムであることが重要であると考えた。また、通常は見ることが出来ないネットワークにおけるデータの流れを見えるようにする。つまりパケットの可視化を行うことがセキュリティ意識の向上には必要であると考えた。

本システムは開発環境に Microsoft Visual Studio 2005、開発言語として Visual C++言語を使用した。

本論文の構成として，2 章でトラフィック可視化の重要性と本システムの設計方針について述べる。3 章では、2 章での可視化の重要性を受けてシステムの実装について述べる。4 章では、本システムでの実験について述べる。5 章では、実験の考察、本システムの考察を述べる。6 章では、本研究、本システムの設計、実装に対するまとめと今後の課題について述べる。

2. トラフィック可視化の重要性及び可視化システムの設計方針

2.1 トラフィック可視化の重要性

ネットワークインフラの急速な整備によりインターネット環境は飛躍的に発展している。FTTH（光回線）に代表されるインターネットのブロードバンド化だけでなく、携帯電話や PDA 等のモバイル機器による通信でも高速データ通信が徐々に可能になってきている。また、無線通信技術の発展も目ざましく、まさにいつでもどこでもだれでもネットワークを利用することができる。これにより、ユビキタスネットワークの社会がすぐそこまで近づいている。

しかし、このような状況にも関わらずウィルス対策ソフトやファイアウォール等の導入といった防御策を全く行わずにネットワーク通信を利用するユーザが後を絶たないという現状がある．この状況は，ネットワーク環境の改善によりインターネット利用者に対する間口が広がったことに起因すると考える．これにより，専門的な知識がなくても誰でも簡単にネットワーク通信が利用できるようになった．そのため，インターネット初心者はネットワークには危険が多く潜んでいることを知らないままネットワーク通信を利用することになる．

このような一連の流れで不正アクセスに対して無防備なユーザが生み出されているのではないかと考える．ネットワークセキュリティの脅威、防備など知識を身に付けられれば、安全で安心なネットワーク環境が作れると考えられる。

2.2 システムの設計方針

現在の常時接続環境ではセキュリティ対策が必要不可欠であり、それと同時に高いセキュリティの意識を持つことも重要である。しかし、インターネットの利用歴の浅いユーザはネットワークに関する事象の認知度も低いと考えられる。

また、人間は目に見えないもの、もしくは見づらいものに対しては、興味を持つことが難しい。見づらいものの一例として，大規模なデータであるサーバログがあげられる。サーバの管理者が攻撃の可能性などをサーバが出力したログから発見することは、そのログのデータの容量の大きさ、項目数の多様性から大変な作業である。そしてログを読むためには専門的な知識が必要となる。

そのような問題を解決するために，大量のログを可視化することで攻撃の可能性を容易に発見し管理者の負担を軽減するというツールが提案されている [1]。見えないもの、見づらいものは、可視化することによって理解がしやすくなるものと考える。しかし従来のネットワーク可視化ツール [2][3] はネットワーク管理者に対して開発されたものであり、ツール利用の前提となるネットワーク知識に対して要求が高い。例えば、UNIX 系の Tcpdump や Wireshark などパケットアナライザと呼ばれるソフトは、監視するネットワーク上のすべてのパケットを取得し、パケットに含まれるそれぞれの情報を表示する。ネットワーク状況の分析には有利であるが、ネットワーク知識が乏しいエンドユーザに対しては、それらの情報を理解しにくいという問題がある。

そこで、図 1 のように、本システムではネットワーク知識が乏しいエンドユーザを対象とし、セキュリティ意識を向上させ、ネットワークの基礎的な知識を身に付けさせることを目的とする。

エンドユーザは Web やメール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無意識に用いている。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。したがってここでは、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

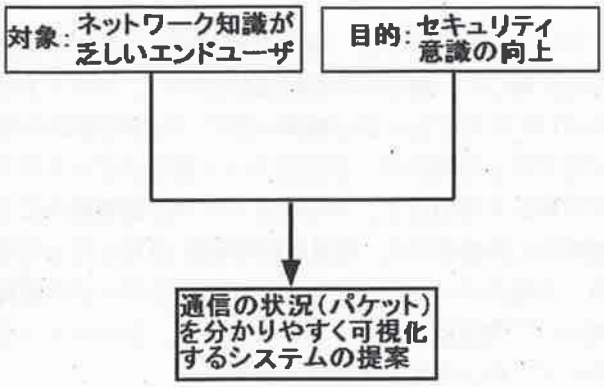

図 1: システムの設計方針

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表 1 に示す。

表 1 システムの提示項目

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でどどのプロトコルを使用しているのか、どのようなサービスが行われているの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。

パケットを可視化するためには、パケットの取得が必要不可欠である。そこで本システムではパケットを取得するために、BSD ライセンスに基づき配布されている WinPcap ライブラリを使用する [4]。WinPcap ライブラリは、Windows 環境においてネットワークアダプタでやりとりされるパケットの取得に関する様々な操作を行うことができるライブラリである。

パケットを解析するためには、パケットの構造が分からなければならない。取得対象のパケットは図 2 のような構造をしている。Ethernet フレーム、IP パケット、TCP セグメントのそれぞれにヘッダ部とデータ部が存在する [5]。Ethernet フレームのデータ部に IP パケットのヘッダ部とデータ部が含まれており、同様に IP パケットのデータ部に TCP セグメントのヘッダ部とデータ部が含まれている。すなわち、一つのパケットにおける純粋なデータは TCP セグメントにおけるデータ部のみであり、残りの部分は通信に必要な情報が占めていることになる。本システムでは WinPcap ライブラリを用いて、これらのパケットのヘッダ部の情報をデータとして取得する。

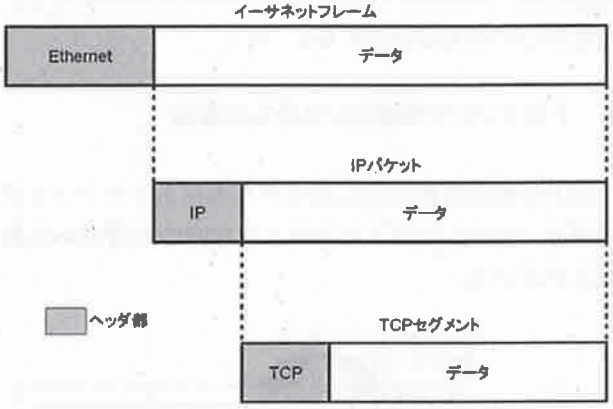

図 2: パケットの構造

しかし、パケットに含まれる数字と文字をそのまま表示するだけでは、ネットワークの仕組みやパケットの流れなどを理解することはできない。また、ポートの種類はとても多く、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。そこでエンドユーザの使用している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エンドユーザに対して明確に知らせる。ネットワーク通信の流れは簡単に言うと、サーバで保存しているデータをパケットで伝送し、クライアント側で伝送されてきたデータを組み合わせて表示することである。こういうイメージを考えた上で、本研究では、指定される倉庫（サーバ）から指定されるトラック（パケット）で注文した品物（データ）を指定される場所（ネットワークアプリケーション）まで走っていくアニメーションをエンドユーザに提示することとした。つまり、ポート——プロトコル——サービスという形でエンドユーザに提示する。これによって、サーバで保存しているデータを特定のプロトコルを介して、パケットによってクライアントまで伝送するというネットワーク通信の流れを直観的に理解できる。

また、セキュリティ意識を身に付けるためには、通信状況の分析をしなければならない、そこで本システムでは、10 秒間当たりの通信量上位 3 位までのポート番号と通信量をリアルタイムにグラフ化し、エンドユーザに提示することとした。

以上で提示されたポート番号と通信量が、具体的にサーバと通信している結果なのかをエンドユーザに把握させるため、ネットワークサービスを提供しているサーバのドメイン名及び通信量をエンドユーザに提示する。

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、プロトコルの検索機能も用意した。具体的には知りたいプロトコル名を入力すると詳しい説明を提示する。

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図 3 に示すような四つの機構から構成されている。

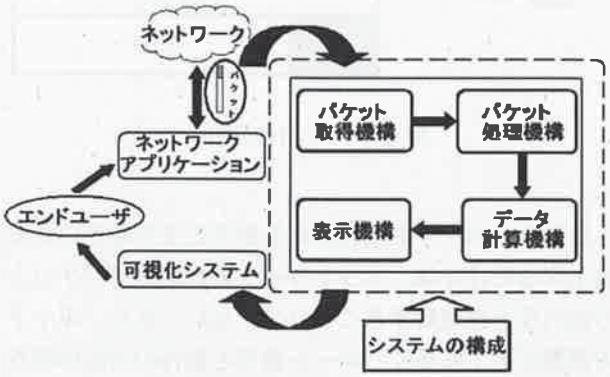

図 3: システムの構成

3.1 システムの実装

前章で述べた設計方針に基づき，開発環境として Microsoft Visual Studio 2005 を用いてシステムを実装した．開発言語は Visual C++を使用した。以下に，システムにおける各々の機構の詳細について示す。

3.1.1 パケットヘッダ取得機構

まずパケット取得機構では、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りす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。

3.1.2 パケットヘッダ処理機構

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 アドレスによるフィルタリングを行うことで、ユーザが利用中のコンピュータから送出される IP パケットのみを選別する。そしてその 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データ計算機構へ渡す。

3.1.3 データ計算機構

データ計算機構では、取得時刻と現在の時刻との差分を計算して、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的に計測を行う。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。

3.1.4 表示機構

表示機構では、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を色で区別し、注目する宛先ポートに、特定の色を付けられるようにする。

4. 比較実験

本システムの提示内容や表示方式について、一般的なパケット解析ツールと比較するための実験を行った。実験に使用したコンピュータのネットワーク環境を表 2 に示す。

表 2　実験環境

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

4.1 操作を行わない場合の表示

まず何も操作を行わない状況では、本システムは何も表示しない。これに対して、Wireshark はパケットの解析結果を出力する。その原因は，本システムではシステムの導入されたマシンだけを表示対象とするのに対して、Wireshark は図 4 のように同じネットワーク上のすべてのマシンを監視するためである。

例えば No.6、No.10、No.11 の出力の結果で、システムを起動してから数秒経過した後に、マシンの IP アドレス、サーバの IP アドレス、プロトコルと簡略なデータ情報を表示している。しかし実験で使用したマシンの IP アドレスを手がかりに調べると No.6、No.10、No.11 で提示された情報は別のマシンが利用した情報である。

このため、どのパケットがエンドユーザの操作と関係があるのかが分からない可能性が高い。

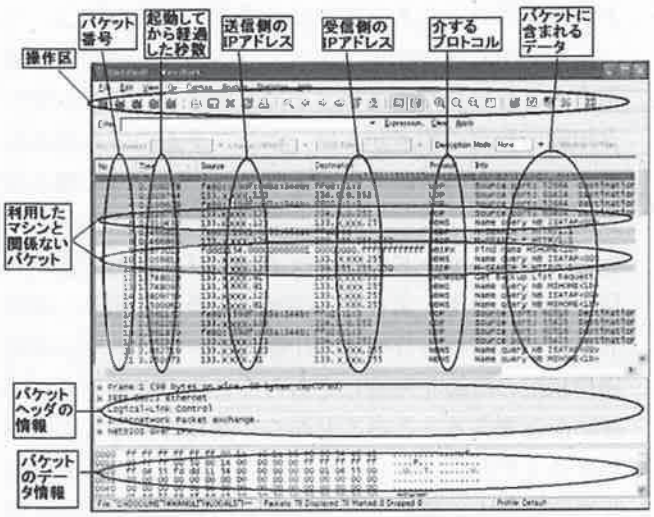

図 4: 無操作の表示（wireshark）

4.2 Web ブラウザの表示

ブラウザを起動し、Yahoo ホームページの閲覧を行う際の出力を比較した。図 5 の Wireshark は一つ一つのパケットを解析し、表示するので、画面は非常に頻繁に更新されている。

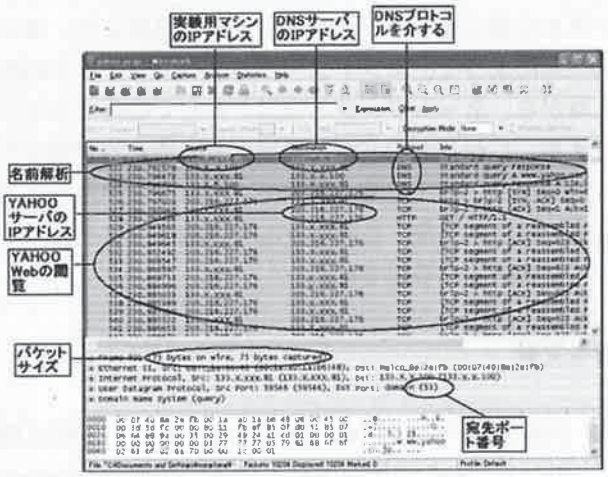

図 5: Web ブラウザの表示 (wireshark)

図中、各パケットは Yahoo のホームページを閲覧したことでやり取りしたパケットの解析結果である。パケット No.521 から No.524 のパケットはユーザによって入力された Yahoo のドメイン名から DNS サーバで Yahoo サーバの IP アドレスの変換を行う過程のパケット群である。次の No.525 パケットからは Yahoo サーバと通信して Web データを取得した過程である。しかしネットワーク知識が乏しいエンドユーザがこの過程を見るとさまざまな疑問を持つと思われる。まずユーザは、ただ Yahoo ホームページを閲覧するだけなのに、なぜ DNS プロトコルを介して、特定のアドレスのコンピュータと通信するのか、また、Yahoo サーバとの通信における ACK などは何のかがよく分からない可能性が高い。また、表示されるデータ量が多すぎるため、ポートを介して、どのぐらいの通信量が発生したのかを理解するのは困難である。

本システムでの表示では図 6 のように、53 番倉庫から DNS と標記されたトラックがクライアントの名前解析サービスのところまで走っていき、80 番倉庫から HTTP と標記しているトラックがクライアントの Web 閲覧サービスのところまで走っていくアニメーションを表示する。それを見ると、Yahoo のホームページを閲覧する場合、まず 53 番ポートを介して、DNS サーバで名前解析をしてから、80 番ポートを介して通信サーバと通信することが直観的に理解できる。

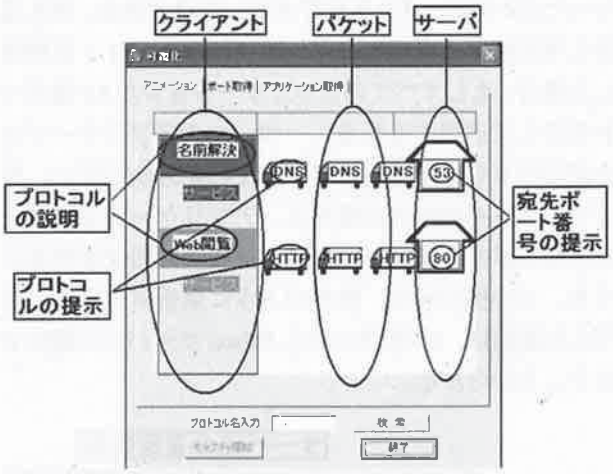

図 6: 本システムの表示 (アニメーション)

同時に、エンドユーザにネットワークの通信状況を把握させるため、図 7 のようにポート取得の表示部にて、単位時間の通信量と対応のポート番号をグラフで提示する。グラフは 10 秒間に一回の割合で表示されるので、この画面では 100 秒間の通信状況を観測できる。一番左のグラフは Yahoo のホームページを閲覧した時発生したポート別の通信量である。これによって、通信の変化状況を直観的に理解できると考えられる。また、異常な通信量や通常は利用しないようなポートが使われたらすぐ発見できる。

しかし、違うアプリケーションが同じポートを介して通信することが多いので、ポート別の通信量を表示するだけでは、どのアプリケーションがどんな通信を

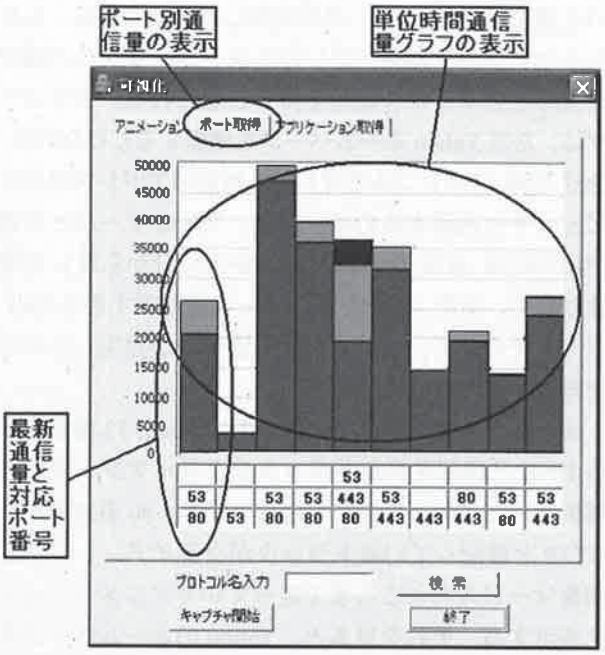

図 7: ポート別の通信表示

行ったのかをはっきり区別できない場合がある。例えば同じ単位時間内で複数の同一アプリケーションを利用した場合、もしすべてのアプリケーションが 80 番ポートを介して通信するなら、一つ一つのアプリケーションがどのぐらいの通信量であったのか分からない。そこで，サーバ別の表示部では、アプリケーションサービスを提供するサーバのドメイン名別の通信量を表示する。この例の場合、図 8 のように最新単位時間に発生した通信は、DNS サーバと Yahoo サーバとの通信であることが分かる。

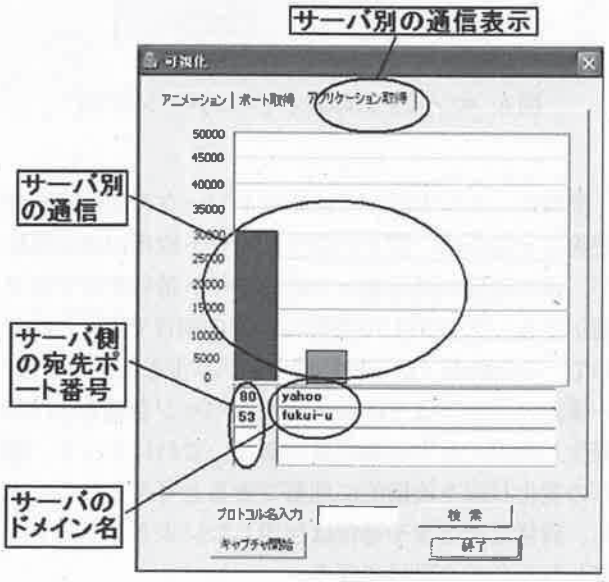

図 8: サーバ別の通信表示

5. 考察

比較実験では、同じ状況下において、既存のパケット解析システムと本システムの機能を比較した。

比較動作実験の結果について、システムの操作性、表示方式と分かりやすさなどを比較すると，ネットワーク知識の教育の観点からは，本システムのほうがエンドユーザに有効であると考えられる。例えば，図 5 のアニメーション表示と図 6 のポート別通信状況の表示などにより、エンドユーザはネットワークの変動が一目で理解できる。よって，提案システムにより，エンドユーザにネットワークの仕組みや、ネットワークの通信状況の概観を理解してもらうことができるのではないかと考える。このことから，例えばウィルスやスパイウェアといったマルウェアに感染した場合の劇的な通信量増大に際して，本システムを利用することでいち早く異常に気づく等の対応が可能になるのではないかと考える。

以上より，提案した本システムはユーザのセキュリティ意識向上に有効であると考える。

6. 今後の課題

今回実装したシステムはネットワークの知識が乏しいエンドユーザを対象として開発した。エンドユーザの教育を効果的に行うために、基本的な情報だけをシンプルに提示するシステムを設計し、実装した。本システムによって、エンドユーザがネットワークを利用しながら、ネットワークの知識を楽しく勉強できると考える。しかしエンドユーザがさらに進んで学習を行うためには、提示情報の増加や表示方式の改良などが必要である。今後、このような発展的なシステムについても検討する予定である。

参考文献

[1] 小池英樹、高田哲司. 視覚表現による不正侵入検知システムの提案と実装.Cyber Security Magazine, Vol.1,No.1,pp. 32 ー 35, 2000.

[2] wireshark http://www.wireshark.org/

[3] tcpdump http://www.tcpdump.org/

[4] WinPcap: The Packet capture and network monitoring library for windows, http://www.winpcap.org/.

[5] 小高知宏. 基礎からわかる TCP/IP アナライザ作成とパケット解析 Linux/FreeBSD 対応. オーム社, 2001.