通信トラフィックとネットワーク情報の三次元視覚化ソフトウェアの提案

斉藤 匡人† 金田 裕剛† 青柳 禎矩† 徳田 英幸†,‡

† 慶應義塾大学大学院 政策・メディア研究科
‡ 慶應義塾大学 環境情報学部
E-mail: {masato, ichiriki, sada, hxt}@ht.sfc.keio.ac.jp

現在、携帯電話網や ADSL・FTTH などを経由したインターネット接続が一般家庭にも普及し、社会インフラの重要な部分を閉めている。しかし、複数のコンピュータから構成される「コンピュータネットワーク」は人々にとっては未だ不透明な存在である。ユーザにコンピュータ同士の接続関係であるネットワークを意識させないことは End-to-End 議論の観点からは利に適っているが、不利点としてユーザがネットワーク通信接続トポロジを容易に把握不可能という問題があり、これが近年のコンピュータウィルスやワームの爆発的な流布を許している一因となっている。

そこで本稿では、人々がより直感的にコンピュータネットワークを把握し興味を抱く助けとなることを目的に、単一ホストを基点としたネットワーク通信状態・トポロジの３次元グラフィカル視覚化ソフトウェア (3D-tcpdump) を提案する。本ソフトウェアはユーザが使用する計算機端末上で独立に動作し、その端末におけるネットワーク通信フローと通信相手を含むネットワークトポロジ、フローを発生させているアプリケーション情報をもとに視覚化処理を行う。本ソフトウェアの使用用途には、異常トラフィック視覚化検出やコンピュータウィルス発生源ホストの特定、家庭内ネットワークにおける通信フィルタリング設定補助ツール、ネットワーク・通信プロトコルの教育、などが挙げられる。

1 はじめに

計算機同士の大規模ネットワークであるインターネットなどのコンピュータネットワークは、計算機間通信インタラクションの OSI 7 層モデル通信プロトコル階層化によって、そのユーザに対して長くブラックボックス化されてきた。こういった状況は、ユーザにコンピュータ同士の接続関係であるネットワークを意識させるべきではない、という End-to-End 議論 [10] の観点からは利に適っている。むしろ、通信相手でさえ誰であるかの認識なくインターネットを利用しメールやウェブ閲覧などを行っているケースが一般的である。しかし、近年のコンピュータウィルス増加や、オペレーティングシステム (OS) 脆弱性攻撃型ワームソフトウェアの隆盛により、人々はコンピュータネットワークの存在を意識せざるをえない状況となっている。たとえ、コンピュータプログラムや OS を最新品質に保っていたとしても、膨大な量のサービス拒否攻撃を受ける可能性も存在する。ウィルス対策ソフトウェアなどにとって未知な攻撃は、通常の通信トラフィックとは異なるという意味の異常トラフィックとして検知することが可能であるが、異常であるかの決定は最終的にはその通信を担っているユーザに委ねられる必要がある。これらの攻撃に対処するには、一般ユーザであってもネットワークに関する簡単な知識獲得や攻撃状況目視を行う必要がある。

加えて、近年のユビキタス計算・ネットワーク環境の普及過渡期に見られるように、身の回りに存在するネットワークや計算機端末が増加することにより、一般家庭においても情報家電、小型センサ、無線接続端末などの複数計算機端末によってローカルネットワークを構成することが一般的になると考えられる。センサなどから構成されるネットワークは主に無線接続型であり、物理的にネットワーク配線が見えないため、より一段とその接続関係を視覚化することはネットワーク管理の観点から重要である。

このような状況を踏まえて、本稿では人々がより直感的にネットワークというものを把握し興味を抱く助けとなることを目的に、単一計算機を基点としたネットワーク通信状態・トポロジの三次元グラフィカル視覚化ソフトウェア (3D-tcpdump) を提案する。本ソフトウェアがターゲットとする一般ユーザとは、コンピュータネットワークに関する知識は皆無であるが、メールやウェブなどを利用して計算機を扱っている人々までを指す。本ソフトウェアによって、こういったユーザが自分が扱っている計算機端末が危険な状況にさらされていないかの判断が行える、もしくはネットワーク管理者などに報告が可能になることが 3D-tcpdump プロジェクトの目的である。

本論文は全五節から構成され、次節において 3D-tcpdump ソフトウェアを提案し開発するに至った研

究背景と既存の関連ソフトウェアについて述べ、第三節ではそれらを踏まえた上での 3D-tcpdump の設計・開発方針に関して明記する。第四節において、3D-tcpdump ソフトウェアの実装内容とソフトウェア設定情報、現段階での 3D-tcpdump 実装スクリーンショットを披露し、第五節において本研究のまとめと今後の課題に関して述べる。

2 研究背景

ネットワーク情報の視覚化に関する研究自体は新しいものではなく、情報視覚化の研究となればアニメーションや三次元化などその歴史は長い。既存のネットワーク情報視覚化研究はインターネットや WWW 構造の大規模視覚化が主要であり [9]、インターネット運用の観点からはパケットプローブを利用した大規模ネットワークトポロジ・接続性視覚化 [1] などの研究が主要である。もちろん、これらの研究やツールは、ネットワーク管理者や研究者用途である。

一方、ローカルネットワークや自ホストを対象として、通信トラフィック情報の視覚化を行うツールや研究も多く存在する。いくつか例を挙げれば、ネットワークトラフィック表示ツールとして最も有名な tcpdump [12] やその GUI 操作解析ツールである Ethereal [4]、tcpdump のリアルタイムグラフ表示ツールである ttt [2] などが存在する。また、ネットワーク運用管理を目的としたトラフィック解析製品として Netasyst Sniffer [6] など多くの解析ソフトウェア製品が存在する。しかし、これらのソフトウェアは全てネットワーク管理者と研究者向けのものである。

3D-tcpdump ソフトウェアが対象とするのは、tcpdump などと同じローカルネットワークや自ホストにおける通信トラフィックとネットワークトポロジ情報の視覚化である。既存のネットワーク情報視覚化研究やツールと 3D-tcpdump ソフトウェアとの位置関係を図 1 に示す。縦軸には、コンピュータネットワークに関する習熟度として上側が IT 管理者、下側に一般ユーザ層を位置づけ、3D-tcpdump を含めた関連ソフトウェア群の対象ユーザ層を示している。横軸には、ネットワーク情報として大きく通信トラフィック情報と通信トポロジ情報の二つに大別し、その二つを両端に位置づけた。

3D-tcpdump ソフトウェアは、単一計算機、つまり自分が利用するコンピュータホストで行われているコンピュータ通信と、通信に関わる計算機ネットワーク・トポロジの三次元視覚化を行う。その対象ユーザ層は、ネットワーク管理者やコンピュータ科学研究者などのネットワークに関する知識が既に十分な人々ではなく、コンピュータを利用しているがネットワークというものはよく分からない、もしくは意識したことがないといった人々である。

コンピュータネットワーク視覚化を行うソフトウェアは大きく分けて、通信トラフィック視覚化とネットワークトポロジ視覚化の二つに分類することができる。3D-tcpdump と同じ一般ユーザ層向けであるが、ウェブの HTTP トラフィック視覚化のみに特化した VisitorVille [13] や不正侵入検知に特化したネットワーク視覚化ソフトウェア研究 [14] などが 3D-tcpdump に特に関連するソフトウェアである。しかし、これらのツールは用途が特定化されているために、一般ユーザの日常的なコンピューティング環境での使用には適していない。また、三次元情報視覚化手法を用いたネットワークトポロジ視覚化ツールとして、3d Traceroute [5] ツールが開発されているが、通信トラフィック解析には向いていない。

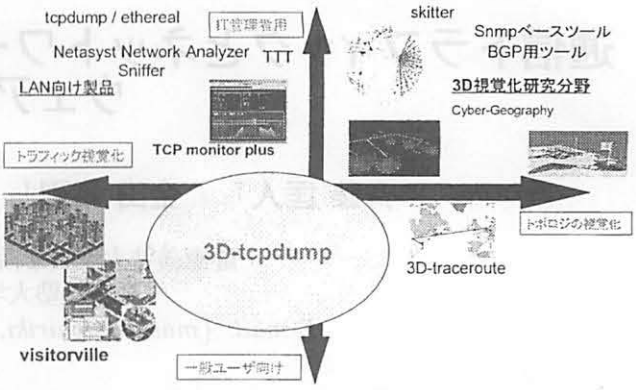


Figure 1: 3D-tcpdump 関連研究俯瞰図

3 設計方針

3D-tcpdump におけるネットワーク情報視覚化では、通信トラフィックフローの視覚化に特に重点を置いている。一般ユーザにとっては、実際に自分が使用しているホストが関わっているトラフィックがどこから来ている、もしくはどこに向かっているのか、ということが最も重要だからである。ネットワークトポロジにおける途中経路ルータを把握する必要性があるのは、ネットワーク管理者や研究者であり、一般ユーザにとっては自分のホストが存在する LAN やホームネットワークにおけるデフォルトルータを把握できれば十分だと考えられる。もちろん、より詳しく Traceroute 機能などの結果を知りたい一般ユーザも存在すると思われるので、ユーザの操作や要望に応じてネットワーク情報を開示していける視覚化ポリシのもとで 3D-tcpdump を構築する。つまり、最初の初期設定におけるネットワーク情報視覚化は自ホストと通信相手ホスト、デフォルトルータのシンプルなトポロジ上での、全ての通信トラフィック視覚化であるが、マウス操作や表示切り替えを行うことでネットワーク管理者の要望まで耐えられるように要求指向で視覚化表示フィルタの粒度を変更していく。

3.1 通信トラフィックの視覚化

3D-tcpdump で視覚化する通信トラフィックはアプリケーションレベルの通信である。つまり、(宛先 IP アドレス、送信元 IP アドレス、宛先ポート番号、送信元ポート番号) の組合わせによるアプリケーショントラフィックを区別する。しかし、ユーザにとって重要なのはそのトラフィックを誰 (どのホスト) が発生させ、どのアプリケーションが関わっているかを把握することが重要である。そのため、ポート番号レベルの細かい区別は、デフォルトの通信トラフィック視覚化設定では行わず、ポート番号からアプリケーションプロトコルが判断されるものに関してホスト単位でグラフィック表示を行っていく。

3.2 ネットワークトポロジの視覚化

ネットワークトポロジ視覚化に関しては、一般的には物理層、MAC 層、ネットワーク層など様々なレベルでネットワークトポロジが存在する。しかし、本研究ではまず一般ユーザ層を想定しているので、ネットワーク層におけるネットワークトポロジに視点を置く。ただし、トラフィック視覚化も行うという点を考慮すると、通信トラフィックの全ての途中経路ルータを表示することは、一般ユーザの視点に立てば冗長であるので、最低限のネットワーク層トポロジとして 3D-tcpdump ではローカルネットワークの視覚化をまず行う。一般ユーザにとって最もネットワークを意識するものは、インターネットサービスプロバイダから配布される ADSL ルータやブロードバンドルータであると考えられ、そこから意識することはあまりないと考えられるからである。これによって、ローカルネットワークの視覚化によってデフォルトルータが視覚表示されない場合は、ローカルネットワーク設定もしくは自ホストのネットワーク設定がおかしいことが判断可能である。

3.3 三次元グラフィカル表示

三次元のオペレーションが非常に柔軟性に富むために、任意の情報や操作に応じて必要な情報を取り出すというポリシのもとで情報視覚化を行う。例えば、三次元表示における高さの軸 (Z 軸) は、通信プロトコル種別や、送信レート、ロスレート、通信遅延などの様々なパラメータで動的変更可能な軸として利用できる。

また、異常トラフィック検知機能として、*/etc/services* などに存在しない通信フローで、かつある閾値以上のレートで流れるフローを異常トラフィックであると判断して、通信エンドホストの両 3D オブジェクトを赤色点滅させる機能を設けた。これにより、一般ユーザに何かおかしなフローが流れているということを通知する。異常トラフィック検知に関しては、将来的にはウィルス対策ソフトなどの検知エンジンなどと連携することでより強固なものになると考えている。

また、基本的に 3D-tcpdump ソフトウェアは全ての情報を三次元表示するが、Pcap ライブラリから取得している情報を加工するだけなので、表示領域を小さくしたいという要望に会わせて二次元でのリアルタイムグラフ表示機能も保持している。

3D-tcpdump ソフトウェアの操作体系に関しては、三次元オペレーションの柔軟性をうまく活かすことを考慮して、ウィンドウ画面の縦軸スライドバーをズーミング機能に、横軸スライドバーを三次元視点の自動回転の速度に比例するように機能 (メリーゴーランド機能) を設けている。横軸スライドバーが真ん中にある場合は静止状態であり、ユーザはマウス操作ににより視点を変更する。マウスドラッグにより 360 度の視点自由回転が可能である。ただし、X・Y 平面の真下からネットワーク通信状態を見上げるという操作は意味がない上に、X・Y 平面を軸に 360 度回転してしまうと、ユーザによっては目が回ってしまうなど操作感に悪影響が生じたため、高さにおける回転幅は 180 度で制限している。

4 3D-tcpdump の実装

図 2 に 3D-tcpdump ソフトウェアのモジュール構成を示す。「Pcap ライブラリ」から全パケット情報を取得し、そのパケット情報を「パケット解析モジュール」がプロトコルごとのヘッダ解析を行う。ヘッダ解析されたパケット情報は、「トラフィック推論モジュール」と「トポロジ推論モジュール」に渡され、通信トラフィックのプロトコル情報把握や通信レート計算、通信相手情報をもとにした Traceroute 機能と Ping 機能実行による途中経路、デフォルトルータ把握、相手先ホストへの遅延情報把握が行われる。次いで、「GUI 表示フィルタモジュール」を通して、これらのネットワーク情報結果が「GUI 表示モジュール」において三次元グラフィカル表示される。フィルタモジュールの命令インプットは、3D-tcpdump の初期設定や XML 設定ファイル、マウスやキーボード操作による「インタフェース操作モジュール」から行われる。

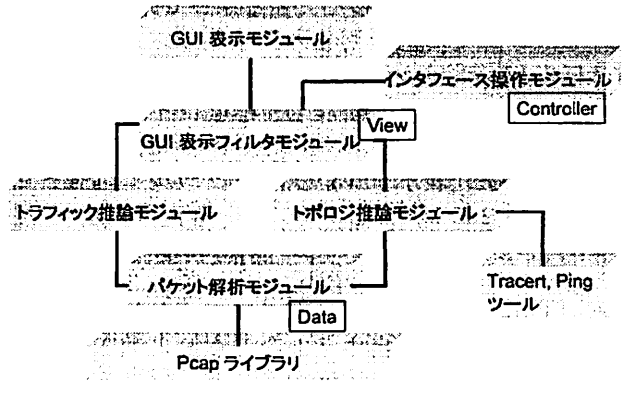


Figure 2: 3D-tcpdump モジュール構成図

4.1 ネットワーク情報視覚化

3D-tcpdump ソフトウェアのプロトタイプ実装には、通信トラフィック取得に *libpcap* 標準ライブラリ [12] を利用し、三次元表示系には Java3D [7] を使用している。*libpcap* 標準ライブラリに関しては、Windows や Linux、FreeBSD などの現在使われている汎用 OS のほとんどにおいて使用可能であるために採用を決定した。三次元表示系で選択した Java3D は、実行プラットフォーム OS に依存しないという Java の利点を享受できるのにくわえ、3D 表示機能が実行マシン上のグラフィックデバイス性能に大きく依存することを避けるためである。個々の OS やグラフィックデバイスへの依存部分を可能な限り、Java3D ライブラリに吸収してもらうという方針である。Java3D の採用はまた、現在の二次元的なコンピュータデスクトップ環境が完全三次元される近未来を想定してのことでもある。既に、UNIX の X ウィンドウ環境で動作する完全三次元デスクトップシステムである、Project Looking Glass [11] が開発されオープンソース化されようとしている。

libpcap によってネットワークインタフェースに到着する全てのパケット情報が取得可能であるが、現在のプロトタイプ実装では NetBIOS や DHCP [3] などのブロードキャスト通信とマルチキャスト通信を非表示にしている。これはマルチキャスト通信の最も適切な表示方法が考案できていないことにくわえ、主要なソフトウェアターゲットが一般ユーザであるということを考慮すると、マルチキャスト通信のフロー情報はエンドホストにとってそれほど重要ではないと判断したからである。また、現在の実装では OS で提供される */etc/services* 情報を利用して[1]通信フローのトランスポートプロトコル区別を行っているが、これだけの情報では例外フローとして判断されてしまう通信が多くなってしまう。そのため、トランスポートポート番号情報からマッピング可能なアプリケーションをプログラム的に判断し、それをユーザに情報提供してフローが例外であるかの最終判断をユーザに委ねている。アプリケーション情報の取得は、*netstat* や *ps* プログラムなど OS 依存になってしまう面があるために、現在は Windows プラットフォームに依存した実装となっている。OS に依存しない形での汎用的なアプリケーション情報取得機構の試案は今後の課題である。

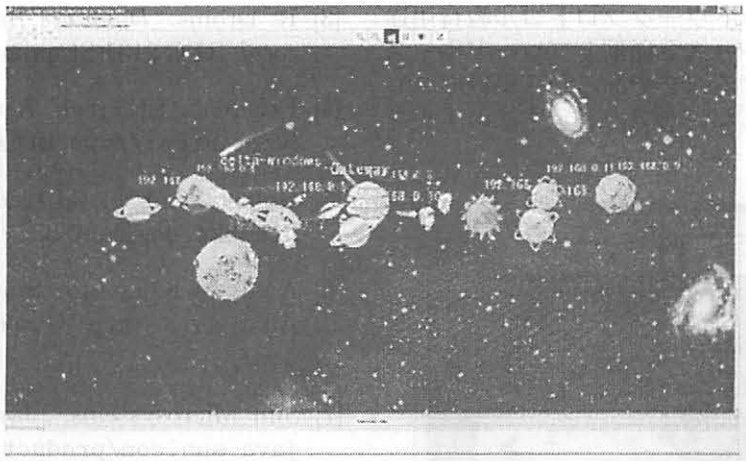
libpcap は C 言語実装の OS 標準ライブラリであるために、Java から Java Native Interface (JNI) を利用して三次元表示 Java3D モジュールに統合させている。図 2 における、「パケット解析モジュール」が JNI 部である。図 3 に 3D-tcpdump のスクリーンショット群を示す。図 3(b) において、通信フローのポート番号区別によって例外フローとして認識された通信端末相手と自ホストを、点滅表示させている。ソフトウェア上では赤色ライトを発光させている。自ホストも赤色点滅させているのは、現在何らかの攻撃もしくはプロトコル検知できない通信が発生しているということをユーザに通知するためである。また、図 3(b) における手前部分の矩形平面は、3D-tcpdump 実行ホストのローカルエリアネットワークを表し、この矩形平面の奥に位置する「Gateway」が実行ホストのデフォルトルータである。

```
<?xml version='1.0' ?>
  <Skin>
    <background>
      <mapping>sphere</mapping>
      <division>60</division>
      <texture>bgC.jpg</texture>
    </background>
    <service>
      <port>80</port>
      <object>desktop.obj</object>
      <size>10.0</size>
      <color>LIGHT_GRAY</color>
      <rotation>180</rotation>
      <mappattern>auto</mappattern>
      <texture>galleon.jpg</texture>
    </service>
    <packet>
      <port>23</port>
      <object>packetC.obj</object>
      <size>10.0</size>
      <color>YELLOW</color>
      <rotation>0.0</rotation>
      <mappattern>auto</mappattern>
      <texture>galleon.jpg</texture>
      <morphslot>0</morphslot>
      <animation>line</animation>
    </packet>
    <sound1>alert1.au</sound1>
  </Skin>
```

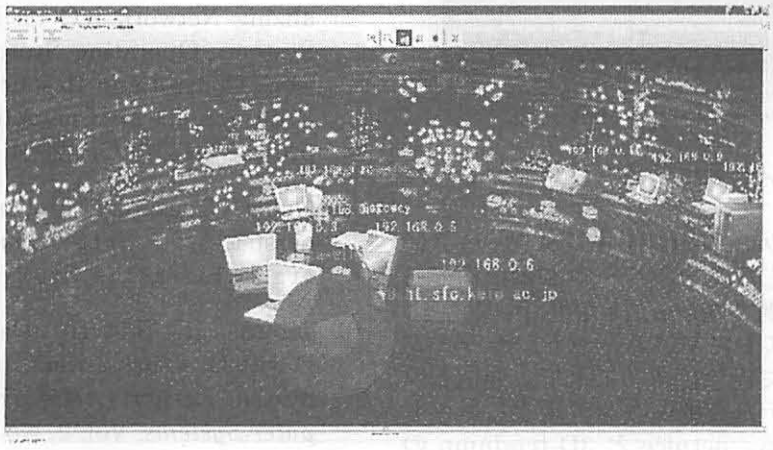
Figure 4: 3D オブジェクト表示 XML 設定ファイル抜粋

視覚化の実装ポリシとして、デフォルトの初期設定では 3D-tcpdump 実行ホストである自ホストと通信における一ホップ目のデフォルトルータ、宛先群のコンピュータオブジェクトのみを表示している。このような大胆なネットワーク情報の枝がりによって分かりやすさを実現し、設定ファイルやマウス操作などにより、詳細な情報が見えるよう表示系を制御している。これは三次元のオペレーションが非常に柔軟性に富むために、任意の情報や操作に応じて必要な情報を取り出すことが可能であるからである。三次元表示における高さの軸は、通信プロトコル種別や、送信レート、ロスレート、通信遅延などの様々なパラメータで動的変更可能である。

1. Windows 系 OS にも /etc/services ファイルは存在する。



(a) 遠景スクリーンショット



(b) セキュリティアラート例 I

Figure 3: **3D-tcpdump ソフトウェア・スクリーンショット群**

4.2 三次元グラフィカル表示

通信相手ホストや自ホスト、パケット、背景などの三次元グラフィカル表示に関しては、3D-tcpdump ソフトウェアを使用するユーザが自由に 3D オブジェクトやテクスチャ画像を変更できるように全て XML 設定ファイルによって変更可能である。現在の 3D-tcpdump 初期設定では、プロトコル番号ごとに 3D 表示オブジェクトを統一しているため、HTTP や SSH などのアプリケーション通信ごとに相手先オブジェクトの表示が統一されている。三次元表示オブジェクトなどに関する XML 設定ファイルの一部を図 4 に抜粋する。

5 まとめと今後の課題

本稿では、人々がより直感的にコンピュータネットワークを把握し興味を抱く助けとなることを目的に、単一ホストを基点としたネットワーク通信状態・トポロジの 3 次元グラフィカル視覚化ソフトウェアを開発した。本ソフトウェアはユーザが使用する計算機端末上で独立に動作し、その端末におけるネットワーク通信フローと通信相手を含むネットワークトポロジ、フローを発生させているアプリケーション情報をもとに視覚化処理を行う。本ソフトウェアの使用用途には、DoS 攻撃視覚化検出やコンピュータウィルス発生源ホストの特定、家庭内ネットワークにおける通信フィルタリング設定補助ツール、ネットワーク・通信プロトコルの教育、などが挙げられる。

今後の課題には、*libpcap* から取得したネットワーク通信情報を常時保存して、時間軸を変化可能にすることでの四次元ネットワーク情報表示や、ソフトウェア全体の処理性能を軽くすることによる壁紙プログラムやスクリーンセーバソフトウェアとしての常駐化、通信セッションのフィルタリングやパーソナルファイアオール機能への操作インタフェースとしての連携機能強化などが挙げられる。三次元グラフィックスの表示系デザインに関しては、XML 設定ファイルによる表示スキンセットの変更が可能であるために、通信端末やパケット、背景などを海に存在する貝や魚によって抽象化した「海スキンモデル」の開発が進行中である。(図 5 を参照。) また、ネッ

トワーク管理者やネットワークプロトコル教育用途においては、マルチキャスト通信とブロードキャスト通信も適切に表示するべきであるが、単独のユニキャスト通信に干渉しない形での表示方法の工夫を考える必要がある。

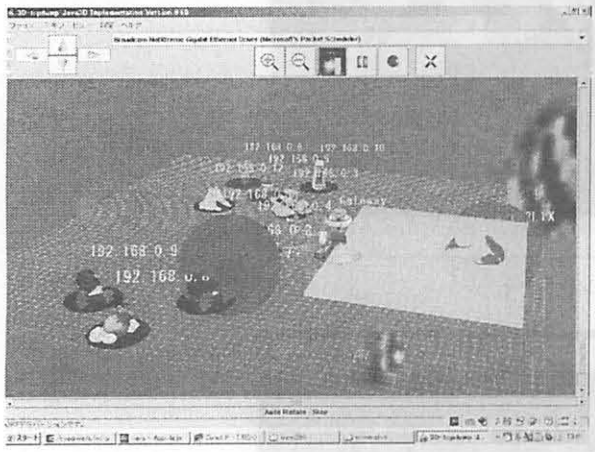


Figure 5: 海スキンモデルのスクリーンショット

通信フィルタリングの 3D GUI インタフェースに関しては、現在、新しいネットワーク制御機構である netnice [8] との連携プロジェクトが進行中である。netnice はエンドホストにおけるネットワークインタフェースを階層的に仮想化することで、通信トラフィック制御とシステム資源保護を実現するネットワーク制御機構である。netnice と 3D-tcpdump の具体的な連携例としては、3D-tcpdump 上で表示される通信フローをクリックしてフィルター設定を選択することによって、netnice へとコマンド命令が発行されて、該当する通信フローがオペレーティングシステムにおいてフィルタリングされる。ADSL や FTTH 経由のインタネットサービスを提供するプロバイダなどが、こういった GUI フィルタリングソフトウェアを顧客に配布し使用してもらうことでより円滑なネットワーク管理、顧客対応が可能になると考えられる。

謝辞

本研究は、独立行政法人情報処理推進機構「未踏ソフトウェア創造事業」、総務省「ユビキタスネットワーク制御・管理技術の研究開発 (ubila プロジェクト)」の支援のもとに行われています。

References

[1] CAIDA. skitter. http://www.caida.org/tools/measurement/skitter/.

[2] Kenjiro Cho. TTT: Tele Traffic Tapper. http://www.csl.sony.co.jp/person/kjc/kjc/software.html#ttt.

[3] R. Droms. *Dynamic Host Configuration Protocol.* RFC 2131 Standards Track, March 1997.

[4] Ethereal. Ethereal: A network protocol analyzer. http://www.ethereal.com/.

[5] Holger Lembke. 3d traceroute. http://www.hlembke.de/prod/3dtraceroute/.

[6] Analyser Sales Ltd. Sniffer Netasyst Network Analyser. http://www.sniffer-netasyst.com/.

[7] Sun Microsystems. Java 3D API. http://java.sun.com/products/java-media/3D/.

[8] Takashi Okumura and Daniel Mosse. Virtualizing Network I/O on End-Host Operating System: Operating System Support for Network Control and Resource Protection. *IEEE Transactions on Computers*, Vol. 53, No. 10, pp. 1303–1316, Oct 2004.

[9] Cyber-Geography Research. Atlas of Cyberspaces. http://www.cybergeography.org/atlas/atlas.html.

[10] Jerome H. Saltzer, David P. Reed, and David D. Clark. End-To-End Arguments In System Design. *ACM Transactions on Computer Systems*, Vol. 2, No. 4, pp. 277–288, Nov 1984.

[11] Sun Microsystems. Project Looking Glass. http://www.sun.com/software/looking_glass/.

[12] tcpdump. tcpdump/libpcap. http://www.tcpdump.org/.

[13] VisitorVille. Website traffic statistics visualization software. http://www.visitorville.com/.

[14] 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. 32–35, 2000.