パケット通信の可視化

Visualization of packet communication

歌代昂和 ，山﨑浩一

Kowa Utashiro and Koichi Yamazaki

玉川大学工学部ソフトウェアサイエンス学科，　194-8610　東京都町田市玉川学園 6-1-1

Department of Software Science, College of Engineering, Tamagawa University,

6-1-1 Tamagawagakuen, Machida, Tokyo, 194-8610, Japan

Abstract

Because of its convenience, most of users utilize the Internet without awareness of data communication. This situation might make the existence of cyberattacks dilute. That should be avoided for the safe use of the Internet. In this paper, we develop a system to visualize the data communication performed by the user's PC with the Internet. The system would provide users with chances to realize the data communication.

Keywords: packet communication, visualization, Internet Protocol address, cyber attack

1. はじめに

社会基盤として広く普及し，利用率が 80% [1)] を超えたインターネットは日常生活から切り離すことのできない技術となっている．インターネットを支えるデータ通信は，様々な領域で利用され，種々の技術で成り立っている．これらのデータ通信は利便性が極めて高く，利用するために煩雑な手続きを必要とせず，その存在を意識することなく利用できる．このことは，様々な側面においてメリットとなる．一般ユーザにとっては，SNS や Web 検索といった各種サービスにおいて，データ通信を意識することなく，その利用に集中できる．一方で，サイバー攻撃者にとっても，データ通信の希薄化が都合のよい状況を生み出す．サイバー攻撃の存在を薄めるからである．

今後もデータ通信は発展し，より利便性が高まり，身近になっていくことが予想される．データ通信のブロードバンド化や IoT 技術の普及は，利便性を大きく向上させるであろう．しかし，利便性の向上は，認識の希薄化を加速させる懸念がある．現在においても，通信の存在を意識することは稀であろう．また，意識的な通信はもちろん，バックグラウンドで秘密裏に行われる通信も存在している．今後，身近となっていくデータ通信に対し，その認識が伴わない状態は危険といえる．

現在，サイバー攻撃の認識を深めようとする機会は多く存在している．一方で，データ通信そのものに焦点を当て，その認識を深めようとする機会は少ない．当然ながら，ネットワークデバイスは攻撃時以外にも通信している．攻撃時のみに注目するのではなく，それを包括的に認識できるデータ通信そのものに焦点を当てることも有意義であろう．

本研究では，データ通信の内，パケット通信に焦点を当てる．パケット通信の様子をリアルタイムに観測・分析し，可視化するアプリケーションを開発する．利用者は一般的なユーザを想定し，専門的な情報の提示は最大限控える．パケット通

信を可視化することで，その認識を深める機会の提供が期待される．

2. 技術概要

本研究で利用する技術について説明する．

2-1. パケット通信

パケット通信とは，インターネット上の通信で利用される通信方式である．通常，インターネットを介したデータ通信は 4 つのレイヤーを介す．ネットワークインタフェース層，インターネット層，トランスポート層，アプリケーション層である．この 4 層は TCP/IP4 層モデルと呼ばれる [2]．

ネットワークインタフェース層では，物理的なデータの表現方法を決定し，同一ネットワークにおけるデータ通信を実現する．インターネット層では，インターネットを介したデータ通信を実現する．トランスポート層では，通信の信頼性を保証し，アプリケーション層では，アプリケーション間の通信を実現する．

インターネット層におけるデータ形式はパケットと呼ばれ，IP ヘッダとデータ部により構成される．IP ヘッダには，送信元および送信先の IP アドレスが格納されている．IP アドレスとは，インターネット上における住所に相当するものであり，32 ビットの整数値で表現される．一般的には 8 ビットごとにピリオドで区切り，4 ブロックに分けて 10 進数で表記される．

IP アドレスはネットワーク部とホスト部から構成される．ネットワーク部は該当ホストが属するネットワークの住所を示している．ホスト部はネットワーク内におけるホストの位置を示している．ネットワーク部のビット長は，IP アドレスの後尾にスラッシュを入れて付記される．32 ビットからネットワーク部のビット長を引いた値はホスト部のビット長となる．ホスト部のビットを全て 0 としたアドレスは，ネットワークアドレスと呼ばれる．

IP アドレスには，2 つのバージョンが存在する．先に述べたものはバージョン 4 であり，IPv4 と表記される．もう 1 つのバージョンは IPv6 であり，IPv4 の枯渇に伴って登場したものである．IPv6 のアドレスは 128 ビットで表記され，実用上ほぼ無限に近いアドレス空間をもつ．

IP アドレスの割り当ては，ICANN（The Internet Corporation for Assigned Names and Numbers）により行われる．ICANN は 1998 年設立の非営利法人であり，インターネットにおける一意的な識別子の管理・監督を担っている機関である [3]．IP アドレスの割り当ては，ヨーロッパなどの各地域に点在するレジストリに対して，ネットワークアドレス単位で行われる．その後，各地域のレジストリは国単位でアドレスを割り当てる．さらに，国はインターネットサービスプロバイダにアドレスを割り当てる．この割り当て構造に伴い，ネットワークアドレスは国情報を含む．

本研究では，ユーザが送受信するパケットの IP ヘッダを解析する．IP ヘッダから，通信相手の IP アドレスを取り出し，そのネットワークアドレスを求める．ネットワークアドレスが把握できれば，通信国の特定が可能となる．

2-2. 可視化

可視化とは，人間が直接的に見ることができない事象を認識可能とすること，もしくは，ある事象を整理し，潜在的な事実を把握しやすいようにすることである．いずれの場合においても，人間の認識を促進することが目的となる．

この一例として， Jigsaw 社の Digital Attack Map がある [4]．Digital Attack Map では，DDoS 攻撃の様子をリアルタイムで世界地図上に可視化している．その表示例を図 1 に示す．

図 1 より，世界地図上に描画された 2 点間の曲線を確認できる．この曲線は攻撃元・攻撃先の 2 点を結んでいる．曲線の色は DDoS 攻撃の種類，曲線の太さは攻撃の頻度を表している．

Digital Attack Map では，前述した可視化の主

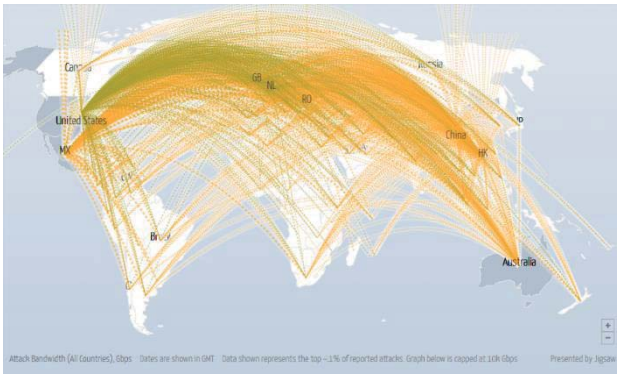

図 1　Digital Attack Map

旨をいずれも体現している．1 点目については，人間が知覚できない事象である DDoS 攻撃を認識可能な形へ変換している点である．2 点目は，攻撃地点や攻撃量の視覚的な理解を促している点である．また可視化は見る人がいることで，その価値が最大化される．このことを踏まえると，誰でも閲覧するできる Web サービスとして提供されている点も重要である．

本研究では，パケット通信が可視化対象となる．サイバー攻撃と比較すると，パケット通信は大きな意味合いを持つ事象ではない．しかし，サイバー攻撃よりも身近な事象であり，またサイバー攻撃の引き金となりえる事象である．このことを考慮しつつ，適した可視化方法を提案する．

2-3. Processing

Processing とは，2001 年，ベン・フライ，ケイシー・リースにより開発されたプログラミング言語および開発環境である [5]．Java ベースの言語であり，ビジュアルな表現に特化している．1 つのプロジェクトはスケッチとして管理され，ソースファイルや画像などの各種データにより構成される．ソースファイルの拡張子は pde（Processing Development Environment）となる．

プログラムは大きく分けて setup メソッドと draw メソッドから成る．setup メソッドはプログラム起動時に 1 度のみ実行されるメソッドであり，画面サイズやフレームレートといったパラメータの設定が行われる．draw メソッドは描画用の関数であり，setup メソッドの終了時に呼び出される．draw メソッドは，指定したフレームレートに従い，繰り返し実行される．1 回の実行が 1 フレームの描画に相当する．

実行したプログラムは Java コードに変換され，Java プログラムとして実行される [6]．アプリケーションとしてエクスポートする場合も同様である．各種プラットフォームに向けた Java アプリケーションとしてコンパイルされる．

本研究では，パケット通信の解析結果を可視化するために Processing を利用する．1 フレーム単位の解析結果を draw メソッドに引き渡し，その内容をもとに可視化を行う．

2-4. Pcap4J

Pcap4J とは，パケットキャプチャやパケットの送受信を可能とする Java ライブラリである．パケットはオブジェクトとして取得され，各種データへアクセスできる．Ethernet, IPv4 や IPv6, TCP や UDP といった多様なプロトコルがサポートされている．

システム要件として，UNIX 系であれば libpcap, Windows であれば WinPcap が必要となる．これらのソフトウェアは，オペレーティングシステム内のパケット情報へアクセス機能を提供する．Pcap4J は管理者権限で実行する必要がある．

Pcap4J を利用したパケットのキャプチャ結果の一部を図 2 に示す．また，図 2 のキャプチャ実行環境における IP アドレス情報を図 3 に示す．

図 2 より，IPv4 ヘッダの内容を確認できる．送信元アドレスは 150.100.16.111 であり，送信先アドレスは 192.168.11.2 である．

図 3 より，キャプチャ実行環境における IPv4 アドレスを確認できる．該当のアドレスは 192.168.11.2 である．図 2 で述べた通り，このアドレスは送信先として指定されている．図 2, 3 より，このパケットは，150.100.16.111 のホストか

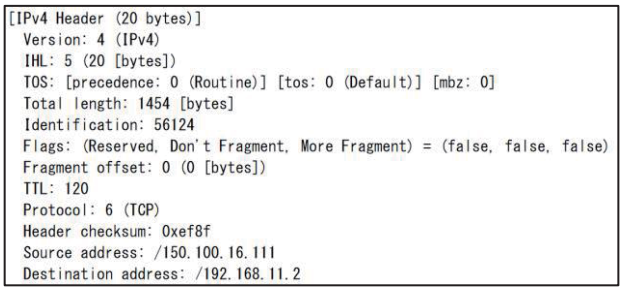

図 2　パケットキャプチャ結果

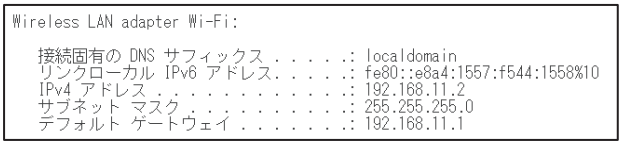

図 3　IP アドレス情報

ら送信されてきたものだと判断できる．

本研究では，上記のようなユーザがやり取りしたパケットの IP ヘッダを取得する．IP ヘッダから IP アドレスを取得し，通信相手のアドレスを把握する．続いて，該当アドレスを解析し，通信国を特定する．上記の例では 150.100.16.111 を解析することになる．このアドレスは日本が保有するアドレスである．

3. 本研究について

本研究の目的は，パケット通信を再認識する機会の提供である．パケット通信をリアルタイムかつ自動的に可視化するアプリケーションを開発する．対象のユーザは，パケット通信に関する専門知識を持たない一般ユーザとする．可視化では，パケットの通信量および通信国に焦点を当てる．プロトコルなどの専門的な情報の提示を避けることで，一般ユーザの理解を促すことが期待される．

本研究は 3 つの手順から構成される．パケットの解析に必要となる参照データの作成，パケットの取得および解析，解析結果の可視化である．

いずれの手順も Java で開発する．以降，順を追って詳細を説明する．

3-1. 参照データの作成

本手順では，ネットワークアドレスと国を関連付ける参照データを作成する．参照データの作成に当たり，MaxMind 社が提供しているオープンデータを利用する [7]．このデータには，ネットワークアドレスと国の対応関係などに関するデータが記載されている．データ例を表 1 に示す．

表 1 より，ネットワークアドレスと国の対応関係を確認できる．network は IPv4 のネットワークアドレスであり，country_name は国名である．このデータを以降の IP アドレスの解析に適した形式に加工する．加工内容は 2 点ある．1 点目はネットワークアドレスの未使用領域を挿入することである．2 点目は，同一の国において連続したネットワークアドレスを取る場合，それらを 1 つにまとめることである．

1 点目は，IP アドレスの解析を行う上で必須となる．解析では，参照データ内にあるアドレス空間を二分割していき，解析対象の IP アドレスを含むネットワークアドレスを特定する．このとき，アドレス空間に空きがあると，IP アドレスを正しく探索することができない．未使用領域を埋めることで，アドレス空間を全て網羅する．2 点目は，参照データのデータサイズを削減するためである．MaxMind 社のデータは 280 万件近くある．これは，州や都市といった国よりも小さいレベルでデータが細分化されていること，また，ネットワークアドレス単位でデータが記載されていることに依拠する．これらをまとめていき，データ件数の削減を図る．

上記の加工を実現するためには，ネットワークアドレスの範囲を求める必要がある．表 1 に対応

表 1 ネットワークアドレスと国

network	country_name
137.34.0.0/16	スイス連邦
137.36.0.0/14	アメリカ合衆国
137.40.0.0/15	アメリカ合衆国
137.42.0.0/16	アメリカ合衆国
137.43.0.0/16	アイルランド

するネットワークアドレスの範囲を表 2 に示す.

表 2 より，スイス連邦とアメリカ合衆国の間にアドレス空間の空きがあり，またアメリカ合衆国は連続したアドレス空間となっていることを確認できる．これらの点に対し，前述した加工を適用する．加工結果を表 3 に示す.

表 3 より，スイス連邦とアメリカ合衆国の間に未使用領域が挿入されていることを確認できる．これにより，スイス連邦が持つアドレス情報を確保しつつ，未使用領域を明示できる．また，アメリカ合衆国のアドレス空間を統合し，データ件数を 2 件削除している.

この処理を 280 万件全てのデータに対し適用する．その結果，データ件数は 18 万件程度にまで軽減される．検索効率，データサイズともに，大きく改善できる.

キャプチャにおいて，137.40.1.1 というアドレスが取得されたとする．このとき，表 3 を参照することで，該当する国の判断が可能である．該当のアドレスが, 137.36.0.0 以上（アメリカ合衆国）であり，かつ 137.43.0.0 未満（アイルランド）であることから，アメリカ合衆国のものであると判断できる.

作成した参照データはアプリケーション起動時に読み込まれる.

3-2. パケットのキャプチャ・解析

表 2 ネットワークアドレスの範囲

network	country_name	ネットワークアドレスの範囲
137.34.0.0/16	スイス連邦	137.34.0.0 ～ 137.34.255.255
137.36.0.0/14	アメリカ合衆国	137.36.0.0 ～ 137.39.255.255
137.40.0.0/15	アメリカ合衆国	137.40.0.0 ～ 137.41.255.255
137.42.0.0/16	アメリカ合衆国	137.42.0.0 ～ 137.42.255.255
137.43.0.0/16	アイルランド	137.43.0.0 ～ 137.43.255.256

表 3 加工結果

network	country_name
137.34.0.0	スイス連邦
137.35.0.0	（未使用）
137.36.0.0	アメリカ合衆国
137.43.0.0	アイルランド

本手順では，ユーザが送受信するパケットを取得し，解析する．パケットの取得には，前述した Pcap4J を利用する．パケットをオブジェクトとして操作することができる.

パケットの取得に際し，キャプチャ対象となるネットワークインタフェースを指定する必要がある．本研究では，ユーザが現在使用しているインタフェースとなる．インタフェースの指定には, IP アドレスなどの専門的な知識が必要となる. そのため，インタフェースの指定の自動化を図り，ユーザの負担を軽減する．ユーザが使用しているインタフェースを自動的に特定し，それがキャプチャ対象として指定されるようにする.

インタフェースの特定は，2 つのプロセスにより実現する．まず，PC 上に存在する全てのネットワークインタフェースの情報を取得する．PC には有線や無線など，複数のインタフェースが存在することがほとんどである．これらのインタフェースが持つIPアドレスなどの情報を取得する.

次に，Inet4Address クラス の getLocalHost メソッドを利用し，PC が主に利用している IPv4 アドレスを取得する. 取得した IPv4 アドレスと，前述した全インタフェースの情報を照らし合わせ，一致する IPv4 アドレスを持つインタフェースを見つけ出す．一致したものが存在した場合，そのインタフェースをキャプチャ対象とする.

一方で, IPv6 を主に利用している場合，上記の方法ではインタフェースの特定ができない．PC のインタフェース一覧情報を取得した際，得られるアドレスは，そのインタフェースが主に利用しているアドレスとなる．IPv6 を主に利用している場合，IPv6 アドレスが取得される．しかし，getLocalHost メソッドでは，取得されるアドレスが IPv4 に限定される．そのため，一致するインタフェースを探し出すことができない．この場合，取得した全インタフェースに対し，並行したパケットキャプチャを開始する．その中で，最も通信頻度の高いインタフェースをキャプチャ対

象とする．キャプチャ対象が決定後，該当のインタフェースに対して，キャプチャを開始する．また，キャプチャ開始後も，定期的にインタフェースを監視することで，キャプチャ対象の変更を検出し，キャプチャ対象の切り替えを行う．

パケットが取得された場合，IP ヘッダから IP アドレスを取り出す．取り出した送信元と送信先のアドレスの内，自分自身でない，かつグローバルであるアドレスを解析対象とする．ここで，送信元アドレスが解析対象となった場合，該当パケットはユーザが受信したものとなる．逆に，送信先アドレスが解析対象となった場合，ユーザから送信されたパケットと判断される．なお，ブロードキャストなどのローカルな通信の場合，該当のパケットは解析対象としない．

IP アドレスの解析は，3-1 節で作成した参照データを二分探索し，対応する国を特定する．特定後，該当の国とパケットの送受信が行われたことを通信ログに記録する．記録されるデータは，送信パケット数，受信パケット数，やり取りした IP アドレスなどである．通信ログは，可視化において参照するデータとなる．

解析結果は検索ログにも保存される．パケット通信は，同一の IP アドレスと複数回通信することがほとんどである．一度解析を終えた IP アドレスについては，次回以降，検索ログから解析がかかるような形とする．

IP アドレスの解析は，参照データの二分探索により実現している．IPv4 であれば，約 18 万件の参照データの中から，目的の項目を探索する．二分探索における計算量は次式で表される．

$$\log_2 n \tag{1}$$

ここで，n はデータ量である．本研究では $n = 1.8 \times 10^5$ となる．したがって計算量は次の通りとなる．

$$\log_2(1.8 \times 10^5) \approx 17.5 \tag{2}$$

17.5 以上で最も小さい整数が必要となる計算量となるため，計算量は18 となる．

一方で，検索ログからの特定は計算量が実質的に 1 となる．その理由は，該当の IP アドレスをもとにしたランダムアクセスを実現しているためである．検索ログには，HashMap クラスを利用している．HashMap クラスでは，キーと値を関連付けて管理する．キーを指定することで，対応する値を一意的に取得することが可能である．

検索ログでは，IP アドレスのハッシュ値をキーにして，該当の国情報を値とする．IP アドレスのハッシュ化には，hashCode のメソッドを利用する．この仕組みにより，ある IP アドレスがキャプチャされた場合，そのハッシュ値に対応する国の有無を確認することで検索済みかどうかを判断できる．検索済みの場合，対応する国を一意的に特定できる．検索済みでない場合，対応する国が存在しないため，参照データへ検索をかけ，その結果を検索ログに保存する．この手順を繰り返し，ユーザがやり取りしている IP アドレスおよび，その国を網羅していく．

二分探索とハッシュによる探索，双方の探索時間を計測した結果を示す．100 万回の検索を 1 セットとし，100 セットの平均実行時間を計測した．その結果，二分探索は 72.8 [ms]，ハッシュによる探索は 20.8 [ms]であった．ハッシュによる探索は，二分探索の 28.6 % の時間であり，効率がよいことを確認できる．

また，通信ログについても，HashMap クラスを利用している．国情報をキーにして，各国の通信情報を管理している．

上記の処理をキャプチャされたパケットに対し，適用し続ける．

3-3. 可視化

本手順では，3-2 節の解析結果を通信国と通信量に注目し可視化する．可視化に当たり，Processing を利用する．可視化では，フレームレートに従い，1 フレーム単位で通信ログへアクセスする．本研究では，毎秒 8 フレームとしている

ため, 125 [ms] 毎に通信ログを参照する. 参照の度，通信ログを初期化し，通信ログが 1 フレーム単位のデータとなるようにする.

通信国は，各国に対応した色を割り振ることで表現する．色の割り振りは，国名をもとにした乱数により決定する.

通信量は 2 つの方向性から可視化する．1 つは国別の通信量に注目したものであり，もう 1 つは通信量の推移に注目したものである.

1 つ目は円グラフにより表現する．キャプチャされたパケットの総通信量を 100%とし，各国との通信量の割合を視覚的に提示する．また，円グラフと合わせて，国別の通信量ランキングを提示する．ランキングでは国名，その対応色，通信量を合わせて提示する．国と対応色の関係性，また通信量を文字ベースで表示する.

2 つ目は通信量の推移であり，円グラフの中にヒストグラム状の図形として表現する．棒グラフは，1 秒毎の通信量である．棒グラフの総数は，約 90 個であり，直近 1 分半の通信量となる．連続的な通信量を提示することで，通信量のピークなどを把握しやすくなる.

3 つの手順の関係性を図 4 に示す．図 4 より，パケットの取得から解析，可視化までの流れを確認できる.

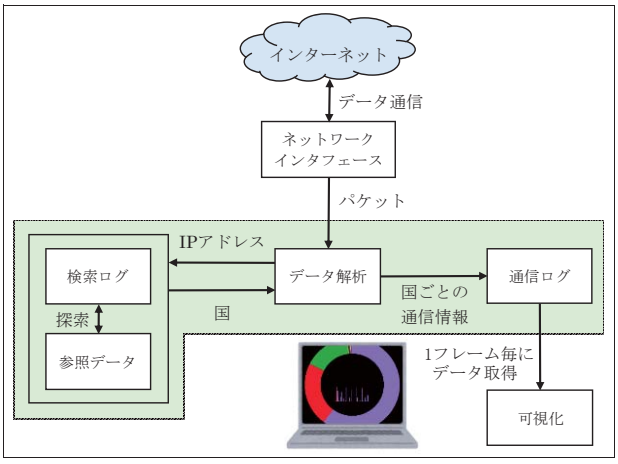

図 4　各手順の関係性

4. 結果・検討

本研究では，パケット通信を認識できるアプリケーションを作成した．本アプリケーションは，キーボード左右矢印キーにより表示する情報を切り替えることができる．一方は，毎回の起動時からもの，もう一方は，初回の起動時からのものである．両者の違いはデータ蓄積期間にある．前者は毎回の起動時が起点であり，後者は初回の起動時が起点である．ヒストグラム状の図形については，いずれの場合も，毎回の起動時からのものを提示する．前者の結果を図 5，後者の結果を図 6 に示す．なお，キャプチャ対象は著者の PC であり，実行時には YouTube にて動画を再生している．キャプチャ期間は，図 5 が約 1 時間，図 6 が約 1 ヶ月である.

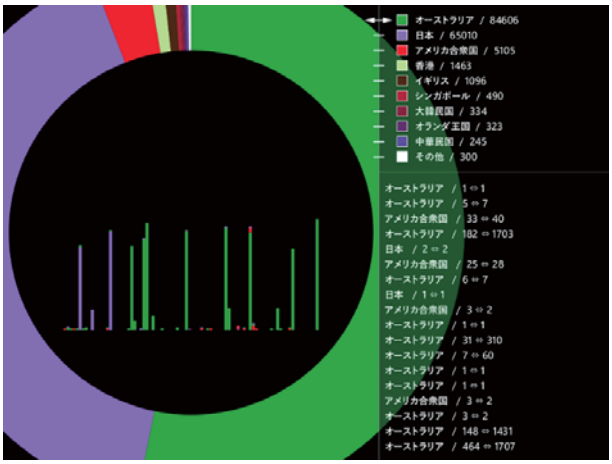

図 5　実行画面

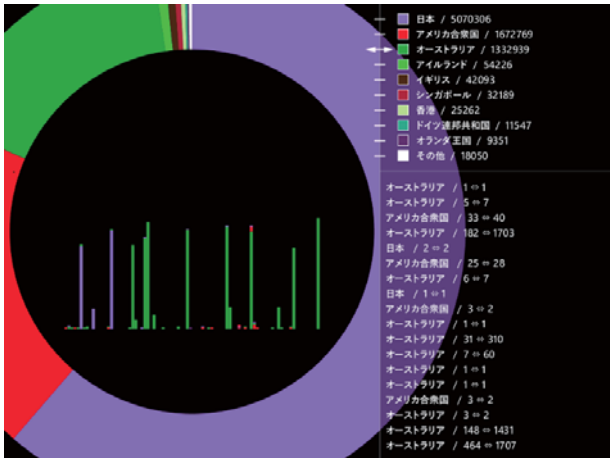

図 6　実行画面（初回起動時以降）

図 5 より，通信量ランキングおよびヒストグラム状の図形を確認できる．通信量ランキングは，オーストラリアが 1 位，日本が 2 位，アメリカ合衆国が 3 位である．その割合は上から 54.7%，40.0%，3.1%である．ヒストグラム状の図形に着目すると，定期的にピークを記録していることを確認できる．これは動画を再生する上で，まとまったデータを定期的にロードしているためであると考えられる．

図 6 では，日本が 1 位，アメリカ合衆国が 2 位，オーストラリアが 3 位となっている．その割合は日本が 61.3%，アメリカ合衆国が 20.1%，オーストラリアが 16.1%である．

上位 2 件については，予想通りの結果といえる．一方で 3 位のオーストラリアは予想外であった．オーストラリアとの通信は IPv6 を利用したものがほとんどであった．該当のアドレスを調査すると，Google 社のものであった．Google 社が広大な IPv6 のアドレス空間をオーストラリアに保有しており，そこと頻繁に通信することによるものであった．

通信ランキングの国名をクリックすることでより詳細な情報を表示できる．オーストラリアをクリックしたときの例を図 7 に示す．

図 7 より，オーストラリア項目の詳細情報を確認できる．ランキング順位，総通信量に対する通信量の割合などが表示されている．また，オーストラリアの通信量の内，送信量と受信量を確認できる．受信量が，送信量の約 3.3 倍となっている．

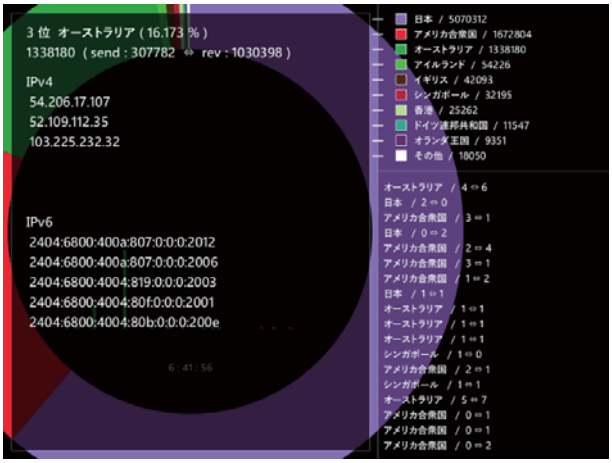

図 7　詳細画面

IPv4 と IPv6 の項目は，オーストラリアにおいて，解析が行われた最新の 5 件のアドレスを表示している．IP アドレスは時として，企業のレベルまで特定が可能な場合があり，それを調査する Web サービスは多く存在している．ここで得られた IP アドレスを提示することで，ユーザのさらなる解析体験につなげられることが期待される．

この他にも，多くのことが判明した．例えば，Windows タスクバー左下のテキストボックスをクリックしただけでパケット通信は行われる．また，Chrome は検索をしなくともブラウザを開いただけでも通信が生じる．YouTube は同一の動画であっても通信国が変化する．そして，学内のネットワークは IPv6 ベースであることも判明した．

何もしていないのにも関わらず，大容量のデータを読み込んでいることがあった．この原因は，PC のシャットダウン時に明らかとなる．更新プログラムの適用が始まったのである．つまり，バックグラウンドで更新データを読み込んでいたことになる．このようなバックグラウンドで生じるパケット通信を見ることも可能である．

5. おわりに

本研究では，パケット通信を可視化するアプリケーションを作成した．これにより，パケット通信をリアルタイムに認識できるようになった．身近ながらも，その認識が困難であるパケット通信を可視化したことは，一定の意義があると考えられる．今後も身近となっていくパケット通信に対し，それを認識する機会となることが期待される．

本アプリケーションは，起動するだけで利用可能な状態とした．専門的な情報の提示も可能な限り控えた．これらはひとえに，専門的な知識を持たずとも利用できるようにするためである．

本アプリケーションは，パケット通信の可視化

以外の機能も有する．パケット通信を解析し，そのデータを蓄積する．そのため，本アプリケーションを見ていなくとも，起動しているだけで，データ収集アプリケーションとしても機能する．

今後の発展として，より専門的な情報に焦点を当て可視化することが考えられる．プロトコルや時間軸上での詳細な分析などである．またスマートフォンを対象とした場合について検討することも 1 つの案である．この他には，パケット通信以外のデータ通信を取り上げることも意義があると考えられる．

参考文献

1） 総務省｜平成 30 年版 情報通信白書｜インターネットの利用状況, http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/html/nd252120.html.

2） 村山公保 : 基礎からわかる TCP/IP ネットワークコンピューティング入門 第 2 版, 121-126, オーム社 (2007).

3） ICANN の役割 - ICANN, https://www.icann.org/resources/pages/what-2012-02-25-ja.

4） Digital Attack Map, http://www.digitalattackmap.com.

5） Overview / Processing.org, https://processing.org/overview/.

6） ベン・フライ, ケイシー・リース（中西泰人訳）: Processing ビジュアルデザイナーとアーティストのためのプログラミング入門, 613, ビー・エヌ・エヌ新社 (2015).

7） GeoLite2 Free Downloadable Databases « MaxMind Developer Site, https://dev.maxmind.com/geoip/geoip2/geolite2/.

2019 年 2 月 28 日原稿受付，2019 年 3 月 15 日採録決定
Received, February 28, 2019; accepted, March 15, 2019