2Y-1

ネットワーク異常検知のための 通信状態可聴化システムの設計と実装

中島　明日香[†]　重松　邦彦[‡]　水谷 正慶[‡]　武田　圭史[†]　村井 純[†]

[†]慶應義塾大学 環境情報学部　[‡]慶應義塾大学大学院 政策・メディア研究科

1　はじめに

本研究では，ネットワーク通信を把握するため，パケットやフロー情報を音で表現することで，異常な通信の発生などの通信状況を知覚できるシステムを実装した．可聴化に際し，長期的に可聴化した通信を聞けるように試みた．そして，HTML 5の audio タグを利用し，通信情報の音をブラウザから配信することを実現した．これによりネットワークの状況を知りたいユーザは，本研究によって通信の大まかな状態を視覚情報無しに直感的に認知することができる．

2　目的

ネットワークの状況や通信の内容を把握するには，ネットワークについて精通していなければ難しい．また，ネットワークに精通していたとしても，Wiresharkなどのツールを使用して，通信状況を把握するには非常に手間と時間がかかる．さらに，なんらかの異常な通信が発生したとしても，ユーザがその画面を見ていなければ，異常を認知する事はできない．

そこで本研究の目的は，ネットワーク通信を可聴化する事により，異常な通信の発生などの通信の状況を簡単に把握できるようにする．通信を音で表現することにより，ネットワークの知識が乏しい人でも，音の変化を聞く事により直感的にネットワークの状態を知ることができるようになる．他にも，大量のパケットを音で抽象的に表現する事により個々のパケットやログを見るよりも，多くの情報を処理できる．それだけではなく，聴覚から情報を取得する事により，ネットワークの状況把握のために，常に画面を見ている必要性から開放する事ができる．このように音を利用する事によって，容易なネットワーク状況の把握が期待できる．

Implementation of Network Sonification System

Asuka Nakajima[†], Shigematu Kunihiko[‡], Masayoshi Mizutani[‡],Keiji Takeda[†]and Jun Murai[†]

[†]Faculty of Environment and Information Studies, Keio University 252-8520, Kanagawa, Japan

[‡]Graduate School of Media and Governance, Keio University,252-8520, Kanagawa, Japan

{asp,sigematu, mizutani, keiji, jun}@sfc.wide.ad.jp

3　関連研究

ネットワーク通信可聴化の研究は今までいくつか行われている [1][2]．しかし，これらの既存のシステムは，ネットワーク管理者のみに焦点を当てており，一般ユーザを対象にしていない．また，特定のソフトウェアなどをインストールする必要があり，一般ユーザが容易にシステムを利用できない問題点があった．そこで本研究では，より聞きやすく，どんなユーザでも容易に使用できるシステムの構築を目指す．

4　機能要件

本研究の目的を満たすために必要な，以下の3つの機能要件を挙げる．

1. **不快を感じない音**

ネットワーク通信の可聴化に際して，ユーザが発生した音を不快に感じないよう考慮する必要がある．また，音の変化による異常検知のために長期的な可聴が必要である事から，本研究では人が不快に感じない音を選び，割り当てた．

2. **汎用性の高いユーザーインターフェース**

ネットワークの状況を把握したいユーザに対して，誰でも特別な環境を用意せずとも，簡単に可聴化された音を聞けるようにする必要性がある．そこで本研究では，どの環境においても標準的にインストールされ，かつ普段からユーザが使用しているブラウザを，音声を聴くインターフェースを利用する．

3. **定常状態と異常状態の差が知覚可能**

ネットワーク通信の定常状態と異常状態との区別を音で知覚できる必要がある．本研究では，定常状態のパケットの情報を記録しておくことで，異常状態を区別する．

5　可聴化手法

この章ではネットワーク通信の情報を音に変換する手法を述べる．を述べる．通信の可聴化に際し，パケットの流量とポート番号の２つの情報を，それぞれ別の楽器音と対応させ，通信の流量の音を主旋律，ポート番号の音を副旋律の音とした．

5.1 パケットの流量

パケットの流量の情報を取得し，ピアノの音（単音）に対応させた．パケットの流量は，ネットワーク上にどれだけのデータが流れたかを示す重要な情報であるから，聞き取りやすく，かつ音の差異が明確なピアノ音を割り当てた．

ネットワーク上の通信量は，観測するネットワークによって大きく異なる．そのため，流量の閾値を設定して音を割り当てた場合と，ネットワークによっては，同じ音しかならない可能性が考えられる．そこで，どのようなネットワークでも音が偏らず鳴るように音を割り当てた．具体的には，0.5 秒毎に流れたパケットの総流量を調べ，その間に流れたパケットの量の平均を出す．そして，0.5 秒に流れたパケットの総量が，平均よりどれだけ乖離しているかで音を決定する．0.5 秒間のネットワーク流量の総量がその平均と同じであれば，ハ長調で「ド」を鳴らし，平均から 1 割づつ上回って離れて行くごとにハ長調で「ド」から 1 音づつ上の音を鳴らす．反対に，平均から 1 割づつ下回って離れて行く事に，同じくにハ長調で「ド」から 1 音づつ下の音を鳴らす．

このように音を割り当てる事で，どのネットワークでも単調なメロディになる事を防ぎ，さらにネットワークの定常状態の流量との違いを示す事ができるので，音による異常検知が可能となる．

5.2 ポート番号

パケットのポート番号の情報を取得し，各種楽器音を割り当てた．現在は TCP を使用する一部のプロトコルのポート番号のみを対象として音を割り当てている．対象とするポートは，HTTP，SSH である．そして，通信が開始されたタイミングが分かるように，SYN パケットが検知されたら音を出力するようにした．通信の開始を認識することで，DoS 攻撃やポートスキャンなどの異常な通信を音で検知する事が可能になる．

6 実装

実装はパケットキャプチャ部と，音声出力部分に分けた．これにより、監視しているネットワークに繋げたコンピュータ以外でも，可聴化した通信を聞く事を可能にした．

6.1 パケットキャプチャ部

パケットキャプチャ部では、libpcap-1.4.2.11 を利用してネットワーク通信のパケットをキャプチャした．まず，キャプチャしたパケットのヘッダを解析して，第 5 章で述べたアルゴリズムを使用し，対応する音声ファイル名だけを標準出力する．

6.2 音声の出力部

音声の出力部では，まずパケットキャプチャ部で出力された音声ファイル名を標準入力で node.js-0.2.6 に読みこむ．次に，Socket.IO-0.6.8 を使用して，音声

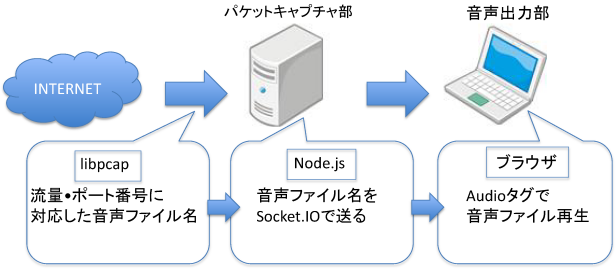

図 1: 実装概要図

ファイル名の情報をブラウザにリアルタイムで送る．ブラウザ側で送られた音声ファイル名を，HTML5 の audio タグを使用してその音声ファイルを再生する．実装の概要図を図 1 に示す．可聴化した通信がブラウザから聴ける事で，難しい設定などをせずとも，ユーザは可聴化した通信が聞けるようになる．本システムは，Firefox-v3 と v4，Safafi-v5 で動作する事を確認した．

7 今後の課題

現状の本システムでは，パケットの流量とポート番号に音を割り当てたのみであり，その他の要素を考慮していない．今後は，他の要素も追加して，通信の状況がより明確に把握できるようする．これを踏まえて，ネットワーク通信可聴化の手法と実装を進める．

8 まとめ

本研究ではネットワーク通信の状況を聴覚によって，音の変化として知覚できるシステムを設計・実装した．ネットワークを可聴化する事によって，容易なネットワーク状況の把握と，長期的に可聴化通信を聞いてもらえる事を目的として，可聴化の手法考案と実装を行った．そして，ネットワーク通信の流量とポート番号に可聴化のアルゴリズムから決められた音を割り当て，ブラウザからその音声出力させた．これにより，ネットワークの状況を知りたいユーザが容易に大まかな通信状況を視覚情報無しに認識できる基本的なシステムを構築した．

参考文献

[1] 成田哲也 大野 浩之. ネットワークトラフィック可聴化システムを遠隔地から利用するためのユーザインタフェース. 第 52 回全国情報処理学会

[2] Cris Chafe,Randel Leistikow Standford University: Levels of temporal resolution in sonification of network performance.International Conference on Auditory,July,2001.

[3] Adrienne Brown, Miguel Vargas Martin,Bill Kapralos, Mark Green Miguel A. Garcia-Ruiz:Towards Music-Assisted Intrusion Detection,IEEE,2009.

[4] 佐藤和哉　丸山一貴　寺田実　電気通信大学. CodeMusician:プログラム実行可聴化の試み. 第 3 回エンターテイメントと認知科学シンポジウム,2009 年 3 月.