卒業論文　　2012年度（平成24年度）

異常検知のための
ネットワーク通信可聴化システムの設計と実装

慶應義塾大学 環境情報学部

氏名：中島 明日香

担当教員

慶應義塾大学 環境情報学部

村井 純

徳田 英幸

楠本 博之

中村 修

高汐 一紀

Rodney D. Van Meter III

植原 啓介

三次 仁

中澤 仁

武田 圭史

平成25年1月22日

卒業論文要旨 - 2012 年度 (平成 24 年度)

異常検知のための
ネットワーク通信可聴化システムの設計と実装

インターネットの発展に伴い，ネットワーク上に流れる通信量は増加の一途を辿っている．さらに，ネットワークに接続される機器数の増加や，仮想化技術を駆使したシステムによりネットワークはより複雑かつ大規模になっている．ネットワークに異常やセキュリティインシデントが発生すると業務の滞りや会社の信用低下が起こるため，事前の万全の対策とともに，ネットワークの異常を早期に発見，対策することが重要である．しかしネットワークの大規模化・複雑化の結果，ネットワーク上の異常発見の遅れや，異常に対処する早さの低下，監視コストの肥大化が問題となっている．ネットワーク監視や，ネットワークの異常検知のためのソフトウェアはあるが，セキュリティの知識や，ソフトウェアの使用方法の習得など，事前知識が必要なものが多く，必ずしも全てのネットワーク・システム運用者が使いこなせているわけではない．

本研究では，通信の情報を主に音の要素 (音高・音量・音色) に変換することで、音の変化により通信状態の変化を直感的に理解できるネットワーク異常検知手法を実現した．既存の音による異常検知システムは，パケット情報やフロー情報に対して特定の楽器音や自然音に割り当てていたため，使用者は事前に音の割当を学ばなければならず直感的に使用できなかった．本手法の提案に伴い、本手法を実現するシステムを設計・実装し，手法の検証と評価を行った．その結果，事前知識が無くとも，音の変化のみでネットワーク異常検知が行えることを実証した．本研究により、ネットワークの知識やネットワーク異常検知のソフトウェアの利用経験がない者でも直感的な異常検知が可能となり，また，ネットワーク監視画面を凝視し続ける必要がなくなった．これにより，ネットワークの総合的な監視コストが軽減された．

キーワード:
1. 異常検知, 2. ネットワーク通信, 3. セキュリティ, 4. 可聴化,

慶應義塾大学 環境情報学部

中島　明日香

Abstract of Bachelor's Thesis - Academic Year 2012

Design and Implementation of a Netowork Traffic Sonification System for Anomaly Detection

In recent years, computer networks have become larger and more complicated because of virtualization technology and the increase in the number of devices. Once network anomalies occur in a company, the business will stall and trust in the company will be decrease. Therefore, it is important for companies to detect network anomalies. However, because of the complexity and largescale of computer networks, detection speeds decrease and the network monitoring costs increase. In order to facilitate network monitoring, engineers use a network monitoring tool such as Nagios, tcpdump or IDS. However, even though engineers use such tools, to understand the computer network state and especially to detect abnormal network traffic, engineers have had to be familiar with network protocols and the behavior of application programs. In addition, engineers can't detect anomaly traffic, if they don't watch tracking display. Therefore, the purpose of this study is to facilitate the understanding of the network state, including detection of abnormal traffic, by representing network state as sound.

In this research, the author proposes a network anomaly detection method which sonificates netwok flow data, mapping it to elements of sound. By this method the user can understand network state changes and detect network anomalies intuitively based on the changes of sound. There have been several network sonification systems for anomaly detection in the past. However, all the system allocated packet and network flow data to a particular instrument sound or a particular natural sound. Therefore to use an existing system, the user should memorize the match between data and sound in advance. Based on this proposal, the author designed and implemented the newtork sonification system and evaluated the system. As the result of this research, the user can detect abnormal network traffic intuitively, without preliminary knowledge about network and network monitoring tool. Also, using this system, the user need not always watch the display for monitoring network traffic. As a result this research contributed to reducing total costs of network security monitoring.

Keywords :
1. Anomaly Detection, 2.Network Traffic, 3.Internet Security, 4.Sonification

Keio University, Faculty of Environment and Information Studies

Asuka Nakajima

目 次

第 1 章　序論 **1**
1.1 背景 1
1.2 本研究の目的 2
1.3 本論文の構成 2

第 2 章　背景技術 **4**
2.1 ネットワーク異常と対策技術 4
2.1.1 異常 4
2.1.2 異常の種類 4
2.1.3 ネットワーク上の異常 6
2.1.4 ネットワーク異常の対策 8
2.1.5 ネットワーク監視ツール 9
2.2 聴覚ディスプレイ 11
2.2.1 聴覚ディスプレイの特徴 12
2.2.2 聴覚ディスプレイの種類 12
2.2.3 聴覚ディスプレイの利用形態 14
2.2.4 可聴化 14
2.2.5 可聴化の用途 15
2.2.6 可聴化の手法 15
2.2.7 可聴化に使用される音 16
2.3 まとめ 17

第 3 章　関連研究 **18**
3.1 ログの可聴化 18
3.1.1 WebMelody 18
3.1.2 Peep 18
3.1.3 既存のログ可聴化の問題点 19
3.2 ネットワーク通信の可聴化 19
3.2.1 Stetho 19
3.2.2 Sound-Assisted IDS 19
3.2.3 既存のネットワーク可聴化の問題点 20
3.3 まとめ 20

第 4 章　音によるネットワーク異常検知手法の提案　21
4.1 提案手法 . . . 21
4.1.1 既存研究との違い . . . 21
4.1.2 音を使用する利点 . . . 21
4.2 提案手法によるネットワーク異常検知の戦略 . . . 22
4.3 想定される利用例 . . . 22
4.4 要求事項 . . . 22
4.4.1 不快を感じさせない音 . . . 23
4.4.2 通信状態変化の明確性 . . . 23
4.4.3 インターフェースの柔軟性 . . . 23
4.5 まとめ . . . 23

第 5 章　音の設計　24
5.1 音とは . . . 24
5.1.1 音の三要素 . . . 24
5.2 音楽とは . . . 26
5.2.1 音楽の三要素 . . . 26
5.3 不快を感じさせない音の設計 . . . 27
5.3.1 音高の設計 . . . 27
5.3.2 音量の設計 . . . 27
5.3.3 音色の設計 . . . 28
5.3.4 リズムの設計 . . . 28
5.3.5 ハーモニーの設計 . . . 28
5.4 通信の要素と音の要素のひも付け . . . 29
5.4.1 可聴化する通信情報の要件 . . . 29
5.4.2 可聴化方法 . . . 30
5.5 まとめ . . . 31

第 6 章　実装　32
6.1 設計 . . . 32
6.1.1 設計要件 . . . 33
6.2 実装したシステムの構成 . . . 34
6.2.1 パケットキャプチャ部 . . . 35
6.2.2 情報加工部 . . . 36
6.2.3 音声変換部 . . . 37
6.2.4 実行 . . . 39
6.3 まとめ . . . 40

第 7 章　検証・評価 **41**
7.1 検証 41
7.1.1 検証実験概要 41
7.1.2 検証実験の構成 42
7.1.3 実験結果 44
7.1.4 考察 50
7.2 評価 51
7.2.1 評価実験概要 51
7.2.2 評価実験の構成 53
7.2.3 システムの評価 54
7.2.4 音の評価 57
7.3 全体の考察 62
7.4 まとめ 62

第 8 章　結論 **63**
8.1 まとめ 63
8.2 今後の展望 64
8.2.1 ネットワーク異常発生時の認識の向上 64
8.2.2 使用者に負担がかからない音 64

謝辞 **65**

付録 A アンケート調査用紙 **70**

付録 B アンケート調査結果 **74**

付録 C ポスター発表資料 **75**

付録 D ポスター発表資料 **76**

図 目 次

2.1 Point Anomalies 5
2.2 Contextual Anomalies 5
2.3 Collective Anomalies 6
2.4 Icinga によるサーバ監視画面 10
2.5 Wireshark 上で表示したネットワーク通信 10
2.6 snort 用に書かれたスキャンを検知するシグネチャの実例 11

5.1 音が伝わる仕組み 24
5.2 音の三要素 25
5.3 音楽の三要素 26
5.4 平均律の音律に対応している音階 27
5.5 ドを根音とした時の長三和音 (ピアノ) 29

6.1 設計概要図 32
6.2 本システムの実行想定環境例 33
6.3 実装概要図 34
6.4 パケットヘッダを保存する構造体 36
6.5 情報加工例 36
6.6 音声変換部の概要 37
6.7 マルチプロセスによって生成される和音 38
6.8 実行例 39
6.9 本システムから出力される音 40

7.1 検証実験概要 41
7.2 検証実験内容 42
7.3 可聴化した通信の波形図 43
7.4 検証実験用サイト 44
7.5 音 1 に対して異常を感じた瞬間 45
7.6 音 1 のヒストグラム 46
7.7 音 2 に対して異常を感じた瞬間 47
7.8 音 2 のヒストグラム 48
7.9 評価実験概要図 51
7.10 事前調査アンケート 52

7.11 評価実験の様子 52
7.12 評価実験構成図 53
7.13 監視対象サーバの通信内容 54
7.14 Nagios へのアクセス時間 55
7.15 監視サーバへのログイン時間 56
7.16 唾液アミラーゼモニター 58
7.17 唾液アミラーゼ値の変化 58
7.18 SD 法によるアンケート 60
7.19 5 段階アンケート評価 61

表 目 次

2.1 ネットワーク異常対策の種類と対策内容・具体例 8
2.2 聴覚と視覚の特徴の比較表 12
2.3 可聴化に使用される音の種類と例 16

6.1 実装環境 35
6.2 コマンドラインフラグ一覧 39

7.1 各音に対するボタンが押された回数 49
7.2 t 検定の結果 50
7.3 ストレス値の目安 59

第1章　序論

本章ではまずネットワーク異常の背景にある，ネットワーク通信の増加やシステムの高度化についての現状を述べる．その後，現状の異常検知技術を挙げ，ネットワーク異常監視の際の問題点について述べる．そして，それらの問題点を踏まえ，本研究の概要と目的について記述する．最後に本論文の構成を記す．

1.1　背景

ネットワーク上の通信の増大に伴い，セキュリティの面において様々な問題が発生している．それに伴いネットワーク監視コストも増大している．総務省総合通信基盤局の試算 [1] によれば，日本のインターネットトラフィックは 2011 年 11 月時点において，1696Gbps であり，2008 年 11 月時点より 80.6 %の増加が見られた．通信量の増加は日本だけでなく世界的な傾向で，その原因としては，インターネットユーザの増加，ネットワークに接続されるデバイス数の増加，ブロードバンドの高速化，ビデオトラフィックの増加，Wi-Fi の拡大の 5 つの要因が挙げられる [2]．さらに，ネットワークトラフィックの増大だけでなく，IPv6 化やクラウド化がネットワークをより大規模かつ複雑にしている．これらの要因に伴い，セキュリティインシデントの数も増大している．情報化白書によると [3]，JPCERT/CC に報告されたインシデント (フィッシングサイト，Web サイト改ざん，スキャン，マルウェアサイト，DoS(Denial of Service)/DDoS(Distributed Denial of Service)，その他) の件数は，2008 年時点では 3058 件だったものが，2010 年では 9865 件と 3 倍に伸びている．

上記の背景に加え，セキュリティインシデントやネットワーク異常が起きると，業務の滞りや社会的信用の低下が起こることから，ネットワーク監視やセキュリティ対策に関する重要性は概ねどの組織でも認識されている．また経済産業省が行った調査 [4] によると 90 %近くの企業がなんらかの情報セキュリティ対策を行っているとの統計がある．しかし，情報セキュリティに対する重要性は認識されているにも関わらず，マルウェア感染の不安やシステム運用・管理人材の不足などが半数近くの会社で問題として挙がっているのが現状である．これに加え，セキュリティ対策に対する費用や人材コストも問題になっている [5]．情報セキュリティ対策にかかるコストは年々上昇しており [4]，2010 年度における企業のセキュリティ対策費用は平均して 1070 万円であった．また，システムやネットワークの運用・管理の人材不足から，運用管理者一人に対する負担も年々上昇しているのが現状である．

ネットワーク・システム管理者のための，セキュリティ対策を含めたネットワーク運用監視を補助するソフトウェアは存在する．本研究ではセキュリティ対策の中でも特にネットワーク異常検出の部分に着目するため，ネットワークの状況把握や異常検知するソフトウェアを挙げる．ネットワーク状況をモニタリングするツールとしては，Nagios[6] や Icinga[7] が挙げられる．また，ネットワークの異常やインシデントを発見し，警告を通知するツールとしては，侵入検知システム (Intrusion Detection System,IDS) である Snort[8] が挙げられる．そして，ネットワーク通信そのものを見て，通信の内容を把握するツールとしては，TCPDUMP[9] や Wireshark[10] が挙げられる．

上記に挙げたような様々なツールは存在するが，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という問題がある．また，ネットワークに精通していたとしても，TCPDUMP や IDS などのツールを使用して，通信状況を把握するには，時間や手間などのコストがかかる．さらに，なんらかの異常な通信が発生したとしても，ネットワーク管理者がその画面を見ていなければ，異常を認知することはできない．異常の認識が遅れると，異常に対して対処するまでの時間も遅れ，システムに対する被害も拡大する．そこで本研究ではこれらの問題を解決するため，音の特性を利用した，ネットワーク通信状況の変化を把握できるシステムを提案する．

1.2 本研究の目的

本研究では，ネットワーク通信を可聴化することにより，異常な通信の発生を含む通信状況の変化を音で直感的に把握出来るようにすることを目的とする．そして通信の状況を直感的に把握可能にすることにより，ネットワーク監視コストの軽減を目指す．

本研究における可聴化とは，通信の情報を音に変換して表現することを指す．通信を音で表現することで，ネットワークの知識が乏しい人でも，音の変化を聞くことにより直感的にネットワーク状態の把握が可能になる．他にも，大量のパケットを音で抽象的に表現することにより，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を無くすことができる．また本研究では，特定の通信の情報を特定の音に割り当てるのではなく，通信の要素に対して音の要素 (音色，音高，音量) を割り当てた．特定の情報に特定の音を割り当てると，ユーザは事前に，なんの情報がどの音に割り当てられているか把握する必要があり，直感的ではない．ただ音を使用するだけでなく，通信の要素に音の要素を割り当てることでより直感的なネットワーク状況の変化の把握を目指す．

1.3 本論文の構成

本論文は全 8 章から構成される．第 2 章では，まず本研究の背景にある技術や概念について説明する．まず，異常とは何かについて述べ，ネットワーク上の異常について取り上げる．そして，ネットワーク異常に対する対策技術について述べる．その後，音声イン

ターフェース技術である，聴覚ディスプレイについて言及する．聴覚ディスプレイの定義や種類を挙げ，聴覚ディスプレイを使用するメリットを述べる．第 3 章では，音によるネットワーク異常検知を行っている研究を挙げ，その内容について言及し，そしてその問題点を指摘する．第 4 章では，第 3 章で言及した問題点を踏まえ，音によるネットワーク異常検知の手法の提案を行う．第 5 章では，実際にネットワークを可聴化する際の手法と，その手法を選んだ理由を述べる．第 6 章では，第 5 章で述べた手法を設計・実装を行う．そして第 7 章では，実装したシステムに関しての評価と考察を行う．最後に第 8 章で本論文の結論と，本研究の今後の展望を述べる．

第2章　背景技術

本論文では，ネットワーク上で発生する異常を検出する手段として，人間の聴覚を利用した直感的なネットワークの状況把握を可能としたシステムについて論じる．そこで，本章では，まず異常とは何であるかについて述べ，異常の種類を挙げる．また，ネットワーク上での具体的な異常の種類と，その対策について挙げる．そして，ネットワーク異常の検出に使用されるツールを挙げ，その具体的な内容を述べる．

2.1　ネットワーク異常と対策技術

本節では，まず異常とは何であるかについて述べ，異常の種類を挙げると共に，ネットワーク上での具体的な異常の種類と，その対策について挙げる．そして，ネットワーク異常の検出に使用されるツールを挙げ，その具体的な内容を述べる．

2.1.1　異常

システムやデータの中で正常と定義されているパターン以外を総じて異常を呼ぶ．何が正常かの定義はそのシステムやデータの背景に左右されるため，詳細な異常の定義の作成は難しい．

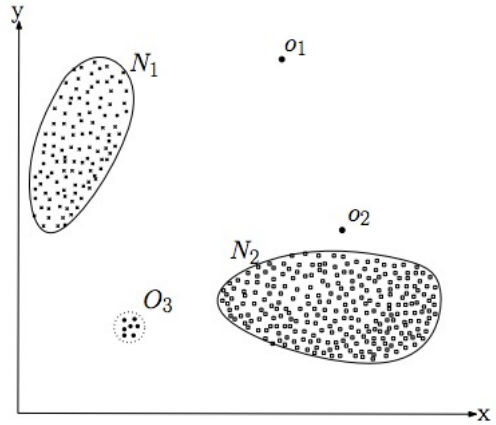
2.1.2　異常の種類

システムやデータ上での異常は主に３種類に分類されることが”Anomaly Detection: A Survey”[11] において言及されている．Point anomalies，Contextual anomalies，Collective anomalies の３種類である．それぞれの異常について説明し，具体例を挙げる．

Point anomalies

Point anomalies とは，ある単一の値が，他のすべてのデータと比べて突出して違う場合を指す．例えば，図 2.1 では，o1 や o2 の値は，N1 や N 群の値とは突出して異なり，これが異常であると分かる．異常検知の研究においてこの単一点の異常に着目することが多い．Point anomalies の検知の具体的な例としては，クレジットカード詐欺の検知が挙げられる．クレジットカードの使用額に着目した時に，今まで一定額範囲内でしか取引がな

かった口座が突如として高額の取引を行った場合などが Point anomalies になる．突如として高額の取引が発生した原因としては，クレジットカード詐欺等が考えられる．

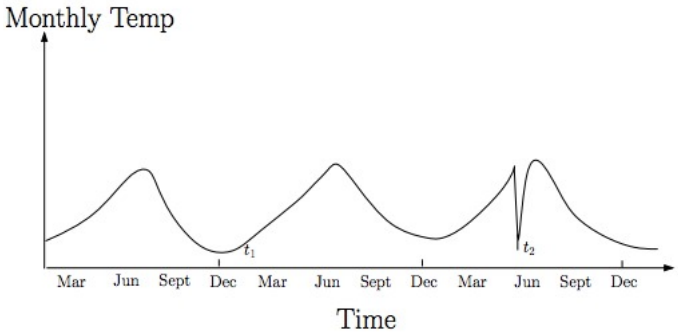


出典)Arindam Banerjee Varun Chandola and Vipin Kumar. Anomaly detection:a survey. ACM Computing Surveys(CSUR), 41(15):15:1-15:58,7 2009.

図 2.1: Point Anomalies

Contextual anomalies

Contextual anomalies とは，データが持つ属性によって異常かどうかが左右される値のことを指す．データが持つ具体的な属性として，緯度・経度や時間などが挙げられている．そして具体的な Contextual anomalies の例として，年間気温の急激な変化が挙げられる．例えば図 2.2 の年間気温のグラフでは，夏に 1.6 度を記録してることが見て取れる．冬に 1.6 度であるのは正常であるが，夏にもかかわらず 1.6 度を記録すれば，なんらかの異常であることが分かる．

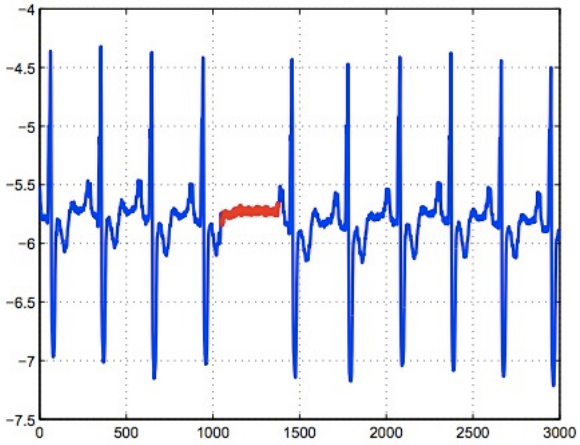


出典)Arindam Banerjee Varun Chandola and Vipin Kumar. Anomaly detection:a survey. ACM Computing Surveys(CSUR), 41(15):15:1-15:58,7 2009.

図 2.2: Contextual Anomalies

Collective anomalies

Collective anomalies とは，単一の値では異常とは見なされないものの，ある値が複数集まることによって，異常となる場合を指す．Collective anomalies の例として，コンピュータ上で発生した操作や動作が挙げられる．例えばコンピュータ上で行われる単一の操作見ているだけでは，異常であるかどうかの見分けはつかない．しかし，操作の流れを見ていくと，異常な動作か否かが分かる．Collective anomalies によるデータの変化例を図 2.3 に示す．



出典)Arindam Banerjee Varun Chandola and Vipin Kumar. Anomaly detection:a survey. ACM Computing Surveys(CSUR), 41(15):15:1-15:58,7 2009.

図 2.3: Collective Anomalies

2.1.3 ネットワーク上の異常

ネットワーク上の異常の種類の分類に関しては，”Characteristics of Network Traffic Flow Anomalies”[12] においての分類方法を参考にした．具体的にはネットワーク上の異常をネットワーク障害，ネットワークへの突発的アクセス集中，ネットワーク侵害の 3 種類に分類した．それぞれの種類の定義と原因について述べた後に，その具体例と影響について述べる．

ネットワーク障害

ネットワーク障害とは，何らかの要因でネットワークが不通になることを指す．ネットワーク障害の原因は LAN ケーブルの接続不良などの物理的な不具合を始め，ネットワーク機器の設定ミスなどのソフトウェア的な不具合など多岐に渡る．ネットワーク障害の具体例としては，ルータの経路設定ミスにより，内部ネットワークからインターネットに接続が出来なくなるなどがある．ネットワーク障害が発生すると，一般企業の場合は電子メールの配信ができないなど業務に支障が出る．また，インターネット接続業者や E コ

マースサイトを運営する企業においてネットワーク障害が発生すると，経営に被害が及ぶだけでなく，社会的信用も低下する．そのため，ネットワーク管理者は，ネットワーク障害の発生をいち早く発見し，原因の究明をして復旧をしなければならない．

ネットワークへの突発的アクセス集中

ネットワークへの突発的アクセス集中とは，個々の通信は正常な通信だが，なんらかの理由で突然大量のアクセスがサーバに集中し，サービス処理能力が低下する異常を指す．ネットワークへの突発的アクセス集中によってネットワークに異常が起こるのは，突発的に集中したアクセスがサーバやネットワーク機器の処理能力を上回るためである．この異常の具体的な例としては，大規模な地震が発生した直後に地震速報などを掲載しているWebサイトに大量のユーザーがアクセスして，サーバが一時的に不安定になるなどがある．突発的アクセス集中によりネットワーク異常が発生すると，企業や組織が提供するサービスに対してアクセス時間の悪化などサービスの品質低下が起こり，最悪の場合サービスが提供出来なくなる．そのため，ネットワーク管理者は，ネットワークへの突発的アクセス集中が起こっても処理出来るようなシステム構成を行う必要がある．また，突発的なアクセス集中によるネットワーク異常が起こった場合もいち早く発見し，原因を究明して適切な対処をしなければならない．

ネットワーク侵害

ネットワーク侵害とは，ネットワークに対するDenial of Service(DoS)/Distributed Denial of Service(DDoS) やスキャンなどの悪意のある攻撃によって引き起こされる，サービス処理能力の低下や通常起こりえない通信を指す．DoSとはサーバやネットワーク機器に対して大量のリクエストや大容量のトラフィックを送信することで，サーバや機器の処理能力を占有し，サービスの提供を不能な状態にすることを指す．一カ所からの攻撃をDoS，複数箇所からの攻撃をDDoSと呼ぶ．また，スキャンとは外部から到達可能な内部ネットワークに関する様々な情報を収集する行為のことを指す．収集される情報としては，内部ネットワーク内で到達可能なホストのIPアドレスや，ホストのOSの種類，ポート番号などで，これら情報をツール等を使用して収集する．ネットワーク侵害の原因は複数ある．第一に悪意を持った攻撃者が標的となる組織や企業になんらかの不利益を目的として，DoSを行う場合である．第二に，悪意を持った攻撃者が標的となる企業や組織に不正アクセスを行う際に，その事前準備として内部ネットワークの詳細な情報収集をするためスキャンを行う場合である．第三にツールやマルウェアが行っている自動的なスキャンなどが原因として挙げられる．ネットワーク侵害の具体例としては，政治的な動機から政府関係のWebサイトに大量の悪意を持ったユーザーがツールを使用して，DDoSを仕掛け，一時的にWebサイトに接続出来なくさせるなどがある．DDoSが発生すると，ネットワークが一時的に不安定になるため，組織や会社の通常業務の妨げになる．またスキャンは，それ自体はなんらかの被害を及ぼすことはないが，その後不正アクセスにつながる

可能性がある．そのため，ネットワーク管理者はネットワーク侵害の発生をいち早く特定し，適切な対処をしなければならない．

表 2.1: ネットワーク異常対策の種類と対策内容・具体例

対策の種類	対策内容	具体例
事前対策	防御	負荷分散装置の設置，ファイヤーウォールの設置
	抑止	ネットワークを切り分ける
	回避	運用マニュアル，運用ポリシーの策定
	予防	運用構成の見直し，定期保守点検
検出	検出	ネットワーク監視ツールによる監視
事後対策	反応	原因の切り分け，対処方法の検討
	軽減	回線を切り替える，サービスの移行
	調査	ログ解析，通信内容の解析
	回復	ネットワークの復旧

2.1.4 ネットワーク異常の対策

ネットワーク異常の対策は，大きく事前対策，検出，事後対策の 3 つに分けることができる．ネットワーク異常の事前対策と事後対策の具体的な対処内容に関しては，”通信の相関関係を利用したネットワークセキュリティ監視手法”[13] にあるネットワークインシデント対策を参考にした．また，表 2.1 に事前対策，検出，事後対策の内容と具体例をまとめる．

事前対策

事前対策とは，ネットワーク異常の発生を防ぐ対策である．ネットワーク異常の事前対策の内容としては，防御，抑止，回避，予防が挙げられる．ネットワーク異常における防御とは，ネットワーク異常による被害を防ぐ対策のことである．具体的には負荷分散装置の導入や，ファイヤーウォールの導入などが挙げられる．抑止とはネットワーク異常が発生した場合に，損害の元となる機器を予め取り除く対応である．具体的には，外部から到達できる内部ネットワークに重要なサービスを設置しないなどの対応である．回避とは，ネットワーク異常の原因を取り除く対策である．具体的には，ネットワーク障害やネットワークへの突発的アクセス集中の原因を取り除くために，運用マニュアルの作成，運用ポリシー作成等を行うことである．また，ネットワーク侵害を引き起こさないために，攻撃者側の費用対効果を悪くするなどの対応がある．予防とは，ネットワーク異常を引き起こす要因を取り除く対応である．具体的にはシステムやネットワークの構成を見直し，定期保守点検の実施，十分な帯域と品質をもつ回線の確保などである．

検出

検出とは，ネットワーク異常の兆候や発生を検知することである．ネットワーク異常の検出は，迅速な事後対策を行うために不可欠である．事後対策の遅延は被害の拡大に繋がるため，検出は特に重要な対策である．ネットワーク異常の検出には，ネットワーク監視ツール等を使用する場合が多い．ネットワーク監視ツールに関しては，第 2.1.5 項で詳しく記述する．本研究は，聴覚によるネットワーク異常検知システムであることから，ネットワーク異常対策の中でもこの検出にあたる．

事後対策

事後対策とは，ネットワーク異常の兆候や発生を確認した際の対策である．ネットワーク異常の事後対策の内容としては，反応，軽減，調査，回復が挙げられる．ネットワーク異常対策における反応とは，検出された異常を元にネットワーク異常の原因の切り分けを行い，対処方法の検討を行うことである．軽減とは，ネットワーク異常による被害が拡大しないための対応である．具体的には，重要なサービスだけ当該ネットワークから切り離す，または違う回線に切り替える等である．調査とは，ネットワーク通信の解析やサーバのログ解析を行うことで異常の原因を調べる対応である．回復とは，ネットワーク異常の原因を取り除き，ネットワーク異常によって停止もしくは不具合を起こしていたサービスを復旧する対応である．

2.1.5 ネットワーク監視ツール

ネットワーク状況を把握し，ネットワーク異常検出のためのツールは主に 3 種類ある．ネットワークモニタリングツール，ネットワークアナライザ，侵入検知システムである．本項では，各種類のネットワーク監視ツールの概要を述べ，それぞれの種類の具体的なツール名を挙げて，その詳細を述べる．

ネットワークモニタリング

ネットワークモニタリングツールは，トラフィック量やネットワーク障害の有無の監視を行うツールである．ネットワークモニタリングツールとしては，Nagios と Icinga が挙げられる．これらのツールは，ネットワーク監視に加えて，サービス監視やリソース監視などを兼ね備えた総合的な監視システムである場合が多い．また，監視だけでは無くサーバへのネットワークの疎通性が無くなった場合や，サービスが停止した場合に管理者に対してメールを送信するなどの機能がある．そのため，ネットワーク障害や，ネットワークへの突発的なアクセス集中などのネットワーク異常の検知が出来る．一方で，監視対象の機器が増えると，設定も複雑になり，ある程度サーバ管理の経験がないと設定が難しい等の欠点もある．

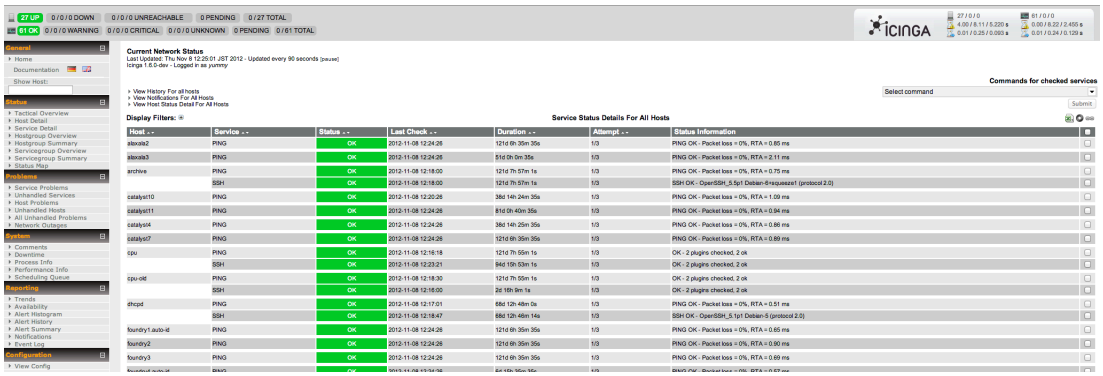


図 2.4: Icinga によるサーバ監視画面

ネットワークアナライザ

ネットワークアナライザは，同一ネットワーク内にあるサーバや PC から発生する通信の内容を閲覧することが出来るツールである．代表的なネットワークアナライザとしては，Wireshark と TCPDUMP が挙げられる．ネットワークアナライザを使用すると，個々のパケットの送信元 IP アドレス，宛先 IP アドレス，使用プロトコル，送受信されたデータ等を閲覧することができる．通信の詳細なデータの閲覧が可能なことから，ネットワーク状況把握や異常検知だけでなく，異常の原因解析を行うことができる．一方で，ネットワークのプロトコルに精通していなければ，ネットワークアナライザを使用しても，何の通信が行われているのか理解出来ないという欠点もある．

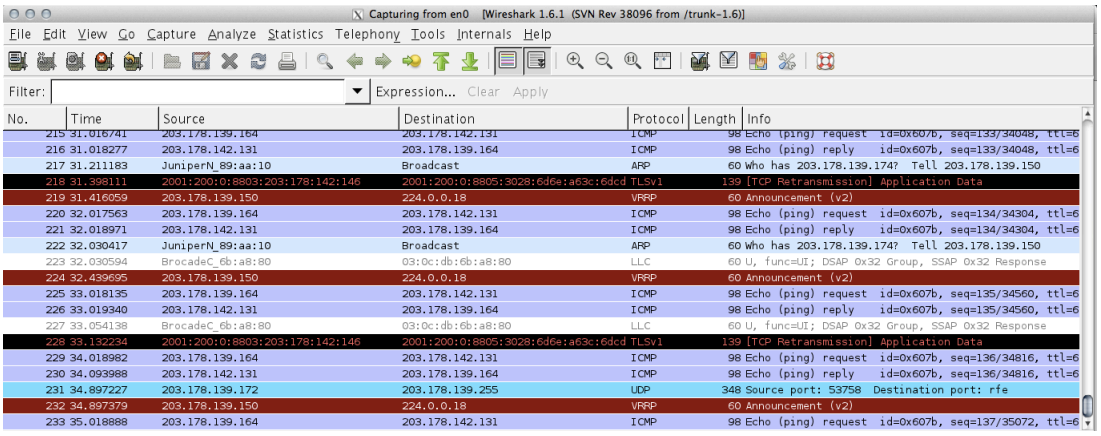


図 2.5: Wireshark 上で表示したネットワーク通信

侵入検知システム

侵入検知システム (Intrusion Detection System,IDS) は，通信内容を監視して，攻撃者によるスキャン，マルウェアによる不正侵入の試み，特定アプリケーションによる通信な

どの検知に広く利用される．侵入検知システムも，ある程度サーバ管理やセキュリティに精通していなければ，使いこなすことが難しい．ネットワークの侵入検知システムには主にミスユース型とアノーマリ型の 2 つある．ネットワーク型の侵入検知システムの他にはホスト型の侵入検知システムがあるが，本論文における IDS は，ネットワーク型の IDS のことを指す．

ミスユース型 IDS

ミスユース型 IDS とは，予め用意した，悪意のある通信の特徴を定義したシグネチャと呼ばれるデータと，監視中のネットワークの通信データを比較して，インシデントの発生を検知するシステムである．シグネチャには送信元および送信先ポート番号，送信元および送信先 IP アドレス，通信中に含まれる文字列，各種ヘッダ等の情報が使用される．ミスユース型 IDS は，シグネチャに登録されている特徴のある攻撃の検知には有効だが，未知の攻撃の検知は難しい．またシグネチャの登録や調整を行う必要があり，使用の際にはある程度 IDS の運用に関して精通していなければならない．シグネチャを使用することからシグネチャ型 IDS と呼ばれることがある．ミスユース型 IDS の代表としては，Snort が挙げられる．

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN nmap XMAS"; flow:stateless; flags:FPU,12; reference:arachnids,30; classtype:attempted-recon; sid:1228; rev:7;)
```

図 2.6: snort 用に書かれたスキャンを検知するシグネチャの実例

アノーマリ型 IDS

アノーマリ型 IDS とは，正常状態の通信の特徴を事前に定義しておき，監視中のネットワーク通信が定義された特徴から逸脱した場合，インシデントとして検知するシステムである．具体的には，ネットワーク通信量や宛先 IP アドレス数などの正常状態の値を予め定義しておき，監視するネットワークがその閾値を超えた場合にインシデントとして検知している．これによりシグネチャ型 IDS と違い未知の攻撃にも対応出来る．しかし，正常状態の定義はネットワーク毎に違う．そのため，監視対象に合わせたネットワークの閾値調整が難しく，誤検知も多いのが現状である．

2.2 聴覚ディスプレイ

現在，情報技術を使用した情報伝達をする際には，絵や文字といった視覚情報を使用したグラフィカルユーザーインターフェースが主流となっている．人間には視覚以外にも聴

覚，触覚，嗅覚，味覚といった感覚があり，それぞれの感覚を通じて現実世界の情報を人間に伝達することが出来る．人間の感覚を利用した研究は、Tangible bits[14] などがある．聴覚ディスプレイとは，その中でも人間の聴覚を利用した音による情報伝達を目的としたユーザーインターフェースの形態の一つである．聴覚ディスプレイに関する研究は 20 年以上前から存在する．聴覚ディスプレイの研究は，1992 年に開催された第 1 回 ICAD(International Conference of Auditory Display)[15] を起点に発展してきた．本節では，聴覚ディスプレイの特徴とその種類について述べる．

2.2.1 聴覚ディスプレイの特徴

人間の聴覚は複雑かつ柔軟な感覚で，音の強さ，音色，音源，音高などの微妙な違いを聞き分けることが出来る．視覚にはない聴覚の優位性を用いることで，聴覚ディスプレイは使用方法や使用する機器によっては，グラフィカルユーザーインターフェース (Grafical User Interface,GUI) よりも優れた効果を発揮する場合がある．

聴覚と視覚の特徴

”The SonicFinder, An Interface That Uses Auditory Icons”[16] では，空間と時間の観点からみた人間の聴覚と視覚の特徴を表 2.2 のようにまとめた．聴覚の時間的な特徴としては，変化する情報の表現に適しているが，時間に依存してしまうという点が挙げられている．また，空間的な特徴としては，一度に表示できるメッセージが限られるという特徴が挙げられている．

表 2.2: 聴覚と視覚の特徴の比較表

	時間的特徴	空間的特徴
聴覚	時間に依存する ・変化する情報の表現に適している ・限定された時間のみ有効	空間に依存しない ・見る必要がない ・一度に表示できるメッセージが限定的
視覚	時間に依存しない ・変化しない情報の表現に適している ・いつでも見れる	空間に依存する ・見る必要がある ・特定の範囲で表示できる

2.2.2 聴覚ディスプレイの種類

聴覚ディスプレイには，Audification，Sonification，Earcon，Speech synthesis の４種類がある．それぞれの定義を述べた後に，具体例や使用例を挙げていく．

Audification

Audification とは，時系列データの値を可聴域の音に直接変換することで可聴化し伝達することを指す．具体的な例としては，医療用心拍計や放射線を測定するガイガーカウンターなどがある．Audification の主な使用用途はモニタリングである．また，使用者の熟練度によっては，音を聴くだけで詳細な値の理解が可能である．

Sonification

Sonification とは，情報や知覚化したデータを非音声信号として可聴化し伝達することを指す．Audification との違いは，音に変換するデータ自体を用意する必要があることに加え，音への変換方法も自由にコントロールすることが可能な点である．可聴化を行う側が自由に音を操作できることから，使用用途はモニタリングに加え，データ検索，芸術，ステータス表示，警告など多岐に渡る．本研究はネットワーク上の通信情報を抽出し音に変換することから，聴覚ディスプレイの中でもこの Sonification に位置する．可聴化については第 5 節で，より詳しく取り上げる．

Earcon

Earcon とは，ある特定のイベントを人間に通知したり，他の情報を伝達したりするために使われる短く特徴のある音を指す．イヤー（耳）とアイコンを合成した単語である．通常の視覚的な通知や操作に音を加えることで，人間の作業の効率化や，即時的な情報伝達を行う．Earcon は主にコンピューター上で使用されることが多い．例えばコンピュータ上のファイルを削除した時に通知される音や，コンピューターを起動させた時に通知される音が Earcon である．また，新着メールがメールクライアントに到着した時に通知される音や，マルウェアを発見した時にアンチウィルスソフトウェアから通知される音も Earcon と定義される．

Speech systhesis

Speech synthesis とは，人間の音声をコンピュータ等で人工的に生成した合成音声のことを指す．主に視覚障害者など文字を読むことが困難な人に向けて開発されてきた技術である．その開発目的から音声合成の技術は主にテキストデータの読み上げ等に使われてきた．近年では，合成音声技術の発展から，より人間の発音に近い音が実現され，音声インターフェースはより身近になってきた．具体的な例を挙げると，音声で現在の状態を知らせる掃除機 Cocorobo[17]，ユーザの音声入力に対する結果を音声で通知してくれる Siri[18] などがある．

2.2.3 聴覚ディスプレイの利用形態

聴覚ディスプレイの利用形態には 3 つある．聴覚ディスプレイのみの使用，聴覚ディスプレイと GUI の併用，GUI の補助としての聴覚ディスプレイである．これらの利用形態の詳細と利点を”ヒューマンインターフェースにおける聴覚メディアの利用” [19] を参考にして挙げる．

聴覚ディスプレイのみの使用

聴覚ディスプレイのみを使用する利用形態とは，ユーザが聴覚ディスプレイから出力される音のみで情報を取得する利用形態を指す．多くの場合は視覚情報に頼ることが出来ない状態や機器で使用されることが多い．具体的な例としては，視覚障害をもったユーザが，テキストを音声変換するソフトウェアを利用するなどの利用形態である．

聴覚ディスプレイと GUI の併用

聴覚ディスプレイと GUI を併用する利用形態とは，ユーザが GUI での視覚情報と同時に聴覚ディスプレイからの聴覚情報から情報を取得する利用形態を指す．聴覚ディスプレイと GUI を併用する利点は 5 つある．1 点目としては，視覚情報を邪魔することなく，聴覚により別の情報を表示出来ることである．2 点目としては，情報に対する認識率が向上することである．3 点目としては，タイミングにそった情報が表示可能な点である．4 点目としては，3 次元空間を有効に使用した情報表示が出来ることである．そして 5 点目としては聴覚と視覚情報を同時に受け取ることにより実世界での情報取得に近くなり，情報に対する現実感が生まれる点である．

GUI の補助としての聴覚ディスプレイ

GUI の補助としての聴覚ディスプレイとは，情報の取得としては GUI を使用し，聴覚ディスプレイからの聴覚情報は，あくまで補助として使用する利用形態である．例えば聴覚ディスプレイを使用して状態の変化や通知を音として受け取り，その詳細な中身の閲覧に関しては GUI を使用する方法である．具体例として，メールクライアントががある．ユーザは，メールクライアントが出力する音によってメールが受信したことを認識し，メールの中身に関してはディスプレイを使用して確認する．

2.2.4 可聴化

本項では，可聴化に関してより掘り下げて説明する．可聴化の用途や，具体的な可聴化の手法に関しては”Theory of Sonification”[20] を参考にした．また，一般的に可聴化の際に使用される音について挙げる．

2.2.5 可聴化の用途

可聴化の用途に関しては，警告，モニタリング，データ探索，芸術の４つに分類される．

警告: ある特定の事象の発生や兆候を知らせるもの，または即時的に反応しなければいけない事象を知らせるものを指す．警告の可聴化は単純かつ分かりやすい音で表現される．警告の具体例としては，火災報知機や，ドアベルなどが挙げられる．

モニタリング: 現在進行形で起こっているプロセスを監視することを指す．モニタリングの具体的な例としては，ネットワーク通信の可聴化が挙げられる [21]．音によるモニタリングによって，人はディスプレイを見ることなく，微小なデータの変化も聴覚で感知することが可能になる．

データ探索: 予め用意されたデータを特定の規則に基づき音に変換することを指す．データ探索の具体的な例としては，地震波データの可聴化が挙げられる [22]．データを可聴化することによって，データの全体像を音の変化で把握することが可能となる．

芸術: 可聴化によって単に情報を伝達するだけでは無く，作曲技法を用いたものを指す．具体例としては，地球上の空気圧や風の方向など様々なデータを可聴化して，音楽として纏めた例が挙げられる [23].

本研究は，モニタリングをその用途として可聴化を行う．

2.2.6 可聴化の手法

可聴化の手法に関しては，効果的な手法は確立されていない．手法は確立されていないものの，既存の可聴化の研究やシステムは，主に３つの可聴化手法に分類することができる．モデルベースによる可聴化，パラメータマッピングによる可聴化，ストリームベースによる可聴化の 3 つである．本項ではそれぞれの可聴化手法の具体的な内容と，その例を挙げる．

モデルベース

モデルベースによる可聴化とは，可聴化の元となるデータに対して，音を事前に割り当てておき，仮想的な楽器またはオブジェクトとして扱う方法である．ユーザは自らデータに対して働きかけることよって，定義した仮想的な楽器またはオブジェクトから返って来た音でデータを把握する．

パラメータマッピング

パラメータマッピングによる可聴化とは，可聴化の元となる多次元のデータを，音の要素に割り当てる方法である．ここでいう音の要素とは，音の周波数，振幅，高低，速度のことを指す．既存の可聴化分野における研究では，パラメータマッピングによる可聴化が使われることが多い．

ストリームベース

ストリームベースによる可聴化とは，聴覚の情景分析 (音脈分儀) を用いた可聴化手法のことを指す．聴覚の情景分析とは，複数の音を聴いた際の人間の認識について説明したものである．人間は意識せずとも，複数の音を単一の音の集まりとしてでは無く，個々の音の属性を認識して，その音をグループとして認識している．

2.2.7 可聴化に使用される音

可聴化の際に使用される音は自然音，動作音，楽器音，合成音がある．自然音とは自然界の音のことを指す．具体例としては虫の鳴き声，動物の声，雨の音，波の音などが挙げられる．自然界の音の特徴としては，全ての人間が日常的に聴く音であることから，音が受け入れられ易いという利点がある．動作音とは，物が動く時に発生する音のことある．具体的にはドアが閉まる音，ゴミが捨てられる音などが挙げられる．動作音の特徴としては，伝達される情報の内容が直感的に理解出来ることである．楽器音とは，音楽を奏でるために用いる器具から出される音のことである．具体的には，バイオリンの音色，ドラムの音色，ピアノの音色などが挙げられる．楽器音の特徴としては，より音楽的になるということである．電子音とは，電気的に発生された音のことを指す．具体的には，サイン波の周波数を元とした音や，矩形波を元とした音などが挙げられる．電子音の特徴としては，周波数や音のリズム等のパラメーター操作がしやすく，かつ音の変化が分かりやすいことである．

表 2.3: 可聴化に使用される音の種類と例

音の種類	具体例
自然音	虫の鳴き声，動物の声，雨の音，波の音
動作音	ドアが閉まる音，ゴミが捨てられる音
楽器音	バイオリンの音色，ドラムの音，ピアノの音
電子音	サイン音，矩形波音

2.3 まとめ

本研究は，音を利用した聴覚によるネットワーク異常検知システムである．そのため本章では，まず異常とは何かを取り上げ，具体的な異常の種類を 3 つ挙げた．またネットワーク上で実際に起こる異常について述べ，その異常の種類を 3 つ挙げ，その異常が起こす被害と具体例を挙げた．その後ネットワーク異常対策を，事前対策，検出，事後対策の 3 つに分類し，具体的な対策内容と例を挙げた．また，対策の中でも検出の重要性について取り上げた．最後にネットワーク異常検知の際に用いるネットワーク監視ツールを挙げ，その具体的な機能やツール名を挙げた．その後，音を利用したユーザーインターフェースである聴覚ディスプレイについての具体的な特徴や種類，そして利用形態について述べた．また，音をインターフェースとして使用する場合の優位性を論じた．そして最後に，可聴化についての詳細な説明と共に，可聴化の対象や手法について挙げた．

第3章　関連研究

本論文では，音を利用したネットワークの異常検知について扱う．そのため本章では，音によるネットワークモニタリングやログモニタリングに関しての既存研究について述べる．そしてそれぞれの研究の具体的な内容について述べた後，その問題点を指摘する．

3.1　ログの可聴化

本節では，ネットワークやサーバの監視を目的とした，ログの可聴化システムについて述べる．代表的な既存のログ可聴化システムは 2 つある．WebMelody[24] と Peep[25] である．本節では，その 2 つの可聴化システムの詳細について述べる．その後，既存のログ可聴化システムが抱える問題について述べる．

3.1.1　WebMelody

WebMelody は Web サーバ (Apache[26]) に来たアクセスをログとして保存し，ほぼリアルタイムに音に変換するシステムである．アクセスログを音に変換することで，Web サーバの管理者が Web サーバに対する DDoS や Web サーバの不調をほぼリアルタイムで検知することを目指したものである．可聴化する情報としては Apache に来たアクセスの中でも HTTP リクエストとレスポンス，そしてそのパラメーターをである．そして，それらの情報を使用者の判断で，特定の楽器音に割り当てる．また扱う楽器音は予め録音した音を使用している．

3.1.2　Peep

Peep は，サーバ上のログを解析しその内容に対して鳥の鳴き声や滝の音などの自然の音を割り当てたシステムである．具体的には，通信量やサーバ負荷などの継続的に監視しなければならない数値は滝の音や風の音に割り当てられている．また，メールの送受信等の不定期な通信は，鳥の鳴き声に割り当てられている．PeeP は通信量やサーバ負荷，メールの送受信等を可聴化することによってスパムメールや，過剰な通信量，サーバへの過負荷の検知を目指したものである．

3.1.3 既存のログ可聴化の問題点

既存のログ可聴化システムの問題について述べる．既存のログ可聴化システムは 2 つの問題がある．第一に，異常の検知精度も元となるログに左右されるという問題がある．ログで出力されていない情報や異常に関しては，使用者は知ることが出来ない．それ故にログで記述されない問題が起こった場合対処も出来ない．そして第二に，一度に可聴化できるログに限りがあるという問題がある．PC 上のログをすべて可聴化することは難しいため，予めシステム側が可聴化するログの種類を選定している．そのため，使用者が柔軟に聞きたいログの音を選定することが出来ない．これらの欠点を補うため，ネットワーク通信そのものを解析して，その情報を音にするという手法がある．

3.2 ネットワーク通信の可聴化

本節では，ネットワーク監視を目的とした，ネットワーク可聴化システムについて述べる．代表的な異常検知のためのネットワーク可聴化システムは 2 つある．Stetho[21] と Sound-Assisted IDS[27] である．本節では，その 2 つのネットワーク可聴化システムの詳細について述べる．そしてその後，既存のネットワーク可聴化システムが抱える問題について述べる．

3.2.1 Stetho

Stetho はリアルタイムに TCPDUMP で出力されたパケットの情報を MIDI に変換して音として出力するシステムである．具体的には，特定のプロトコルに対して特定の楽器音を出力している．可聴化しているプロトコルの種類としては，SSH，SMTP，HTTP，ICMP を含めたネットワーク上で頻繁に使用されている 8 種類のプロトコルである．Stetho は出力される音の変化によって，システム管理者がネットワーク状態の変化を認識することを目指している．

3.2.2 Sound-Assisted IDS

Sound-Assisted IDS は，リアルタイムに通信のフロー情報をピアノ音に変換して出力するシステムである．可聴化する通信のフロー情報は，パケットの流量とパケット数である．パケットの流量とパケット数を元に，出力するピアノ音の音階や，音の振れ幅等を調整する．Sound-Assisted IDS では，セキュリティインシデントが発生した際に，音が出力されるようマッピングを工夫している．そのため，Sound-Assisted IDS を利用することによって，システム管理者は DoS 攻撃やポートスキャン等攻撃が検知できるとしている．

3.2.3 既存のネットワーク可聴化の問題点

既存のネットワーク可聴化システムの問題について述べる．既存のネットワーク可聴化システムには 2 つの問題がある．第一に，ログの可聴化にも言える問題だが，特定のパケットの情報に対して特定の楽器音や自然音を割り当てるシステムでは，ユーザが事前に情報と音のひも付けを学習する必要がある．そのため，直感的にネットワーク監視が行えているとは言えない．第二に，ネットワーク異常やセキュリティインシデントの定義をシステム側で行っている場合，異常検知の精度がシステム側の設定で左右される問題がある．

3.3 まとめ

本章では，音を使用した異常検知手法として，ログの可聴化とネットワーク通信の可聴化の 2 つを挙げた．ログの可聴化では，使用するログや，ログの精度に音が左右されてしまうという問題点があることを挙げた．また，ネットワーク通信の可聴化では，特定の通信情報に特定の音を割り当てたり，通信情報に対して楽器音を割り当てるだけでは，人間にとって直感的ではないという問題を挙げた．よって，ネットワークの異常をより人間にとって直感的かつ，容易に音の変更が可能な新しい手法を考案する必要がある．

第4章　音によるネットワーク異常検知手法の提案

本論文では，通信情報を音に変換することで，人間の聴覚を利用したネットワーク異常の検知手法を提案する．本章ではまず，提案手法の具体的な内容について記述し，既存研究との違いについて述べる．そして，インターフェースとして音を使用することの利点について述べる．その後，提案手法によってどのように異常が検知出来るのかを記述し，想定される利用例を挙げる．また，本提案手法の実現に不可欠な機能要件を挙げ，その具体的な達成内容について言及する．

4.1　提案手法

通信情報を音の要素に変換することで，人間の聴覚を利用した直感的なネットワーク異常の検知手法を提案する．変換する通信情報とは，通信の流量や，パケット数などの通信を指す．また音の要素とは，音高，音量，音色のことを指す．本節では，提案手法と既存研究についてまず述べ，その後，音を利用する利点について述べる．

4.1.1　既存研究との違い

本提案手法と既存研究との最大の違いは，ポート番号や，プロトコル情報などの特定の情報に，特定の音を割り当てるのではなく，通信情報を直接，音の周波数や，音のリズムに変換している点である．既存研究のシステムでは，ユーザは予め，音と情報とのひも付けを理解している必要性があった．また，音を聞きながら異常を検知するためには，ただ音を聴くだけでは無く，出力されている音の種類について注意深く聴く必要があった．そのため直感的に異常を検知できるとは言えなかった．本研究では，通信情報を音に割り当てることにより，本システムに関する予備知識なしで，直感的なネットワークの異常検知を可能とした．

4.1.2　音を使用する利点

音を利用したネットワークの異常検知は，通常の GUI ベースの異常検知と比較して，4つの利点がある．まず，ネットワークや TCP/IP に関する知識が乏しくとも，音の変化の

みで異常を検知できる点がある．前章で挙げた従来の異常検知システムでは，ユーザが事前にネットワークに精通した上で，ネットワーク異常の設定や発見を行う必要があった．2点目としては，画面を見続ける必要がなくなることである．音を使用することで，ネットワーク状態監視のために，ユーザが画面を常時監視する必要がなくなることである．3点目としては，複数パケットを音にすることで情報が要約できることである．4点目としては，視覚障害をもつユーザでも音を聴くことによって，ネットワーク状態が分かるという点が挙げられる．

4.2 提案手法によるネットワーク異常検知の戦略

本節では，本提案手法でどのようにネットワーク異常が検知できるのかについて論じる．

本提案手法は，通信の情報を主に音の要素 (音高・音量・音色) に変換することで、音の変化により通信状態の変化を直感的に理解できるネットワーク異常検知手法である．. 提案手法による直感的なネットワーク異常検知とは，事前に正常状態のネットワークが起こす音の変化を，人が感覚的に把握することによって，ネットワーク異常発生に伴う音の変化を聞いた時に，その音の違いから直感的にネットワーク異常を検知する手法である．本提案手法では，シグネチャや閾値による異常の定義を行う必要がない．そのため環境が違うネットワーク毎に，異常の閾値を設定する手間等も省ける．

4.3 想定される利用例

本システムの主なユーザーとしては，ネットワーク管理者や，システム管理者を対象とする．また利用場所としては，組織の中での重要なサーバや，ネットワークの上流にある機器に設置することを想定する．具体的な利用方法としては3点ある．1点目としてはリアルタイムに生成される音を聞き続けることによって，異常を含むネットワークの状態を把握する方法である．使用者は本システムが出力する音を流した部屋に滞在することで，ネットワーク監視を行いつつ他の作業を行うことが可能になる．2点目としては，既存の異常検知ツールと併用して使用する方法である．既存のツールと併用して使用することで，音を補助的な役割とする．3点目としては，事前に保存した通信のデータを本システムで読み込み，音に変換する方法である．通信データを読み込ませることで，過去の通信に何かしらの異常がなかったかを探ることが可能となる．

4.4 要求事項

本節では，本提案手法が有効に機能するための必要な機能要件を挙げる．機能要件として，不快を感じさせない音，通信状態変化の明確性，インターフェースの柔軟性の３つを挙げ，達成すべき内容を述べる．

4.4.1 不快を感じさせない音

音の変化を使用した異常検知という本研究の特性上，ユーザは音を聞き続ける必要がある．そのため，出力される音はユーザにとって不快を感じない音である必要性がある．もしユーザが出力される音が不快であると感じると，本研究の使用が困難になる．そのため，不快に感じさせない音は重要な機能要件である．達成すべき具体的な内容としては，まず個々の音自体の質を高めることある．個々の音の質が可聴化のクオリティの根本となるからである．また，個々の音の質を高めながら音の組み合わせやリズムにも配慮する．個々の音の質がいくら良くとも，音の組み合わせやリズムが単調だと，不快に感じる可能性があるからである．音が不快でないかどうかの具体的な指標としては，長時間聞き続けることが出来るか否かで判断する．

4.4.2 通信状態変化の明確性

ネットワーク状況の変化を音で知覚するには，ネットワーク状況の変化と共に出力される音にも何らかの変化が必要である．本研究では，音の変化の差でネットワーク上の状態や，異常の有無の知覚を目指すことから，音の変化が人間の知覚可能な範囲である必要性がある．音の変化が明確かつ直感的に異常状態の把握が可能であればあるほど，ネットワーク上の異常の発生の際の対応の速さにもつながるため，通信状態の変化の明確性は，本研究の中でも特に重要な機能要件である．しかし，ただ音を変化させるだけでは，ネットワークの状態の変化は知覚出来るが，異常かどうかの判断はつかないということになりかねない．そこで具体的な達成事項としては，音の変化のみで攻撃が実際に検知できることを目指す．

4.4.3 インターフェースの柔軟性

本研究は，ユーザーインターフェースとして音を使用するため，ユーザは音を聴く必要がある．人間の音に対する感性や感覚は個々によって違う．ある人には心地の良い音でも，他の人に不快な音である場合がある．そのため，本研究では必要に応じてユーザ自身が音をチューニング出来る必要性がある．出力される音の種類の変更が容易に出来る機能を要件として挙げる．具体的には，細かい音の数値等の指定をする必要なく，直感的かつ柔軟に設定を変更できなければならない．

4.5 まとめ

本章では，本研究の提案手法の具体的な内容について述べた．そして，既存研究と本提案手法の違いについて述べた．その後，本提案手法を用いた具体的な異常検知の戦略について述べた．また，本提案手法の実現に不可欠な機能要件を挙げ，その具体的な達成内容について言及した．

第5章　音の設計

本研究では，インターフェースとして音を使用することから，出力する音は重要である．第4.4節で要求事項として挙げたように，出力する音は不快を感じさせない音に加え，通信状態変化が明確に分かる音である必要があると述べた．そこで本章では，まずユーザに不快を感じさせない音とはどういった音なのかについて述べる．そして，具体的な音の設計について記述する．その後，通信状態が音のみで明確に理解出来るようになるには，通信の要素と音の要素をどのようにひも付けると良いかについて述べる．

5.1　音とは

音とは，空気の振動 (音波) で，物理的には疎密波と呼ばれる現象である．[28] 人間の聴覚は，空気の振動を鼓膜にうけ，それを電気信号に変換し脳で処理することによって音を認識する．そのため音は，物理的な側面と，人間の聴覚を元とした心理的な側面 (音響心理学) の2つを持っている．本章では，音響心理学の側面からみた場合の音について述べる．

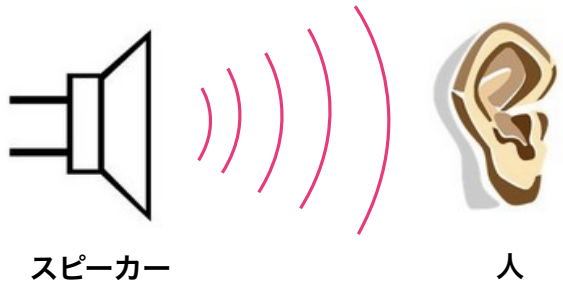


図 5.1: 音が伝わる仕組み

5.1.1　音の三要素

音は，音高，音量，音色の3つの要素で構成される．音の要素を図5.2で示す．本項では，それぞれの要素の定義と，具体的な内容について説明する．

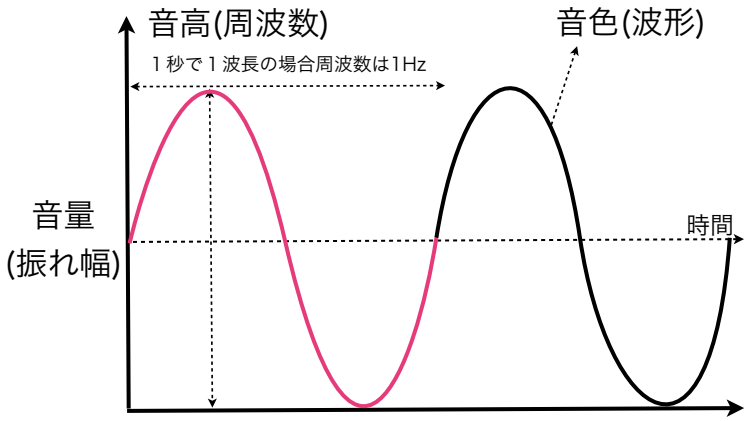


図 5.2: 音の三要素

音高

音高とは，音の周波数を元に感じる，音の高低のことである．周波数とは，一秒毎に音波の波が繰り返される回数のことを指す．人間の聴覚は，周波数が高いと音が高いと感じ，音の周波数が低いと，音が低いと感じる．それ故に，音高の尺度は，高低という一次元的なものであると位置づけることが出来る．また音高には，直線上昇的な側面と，循環的な側面の 2 つの側面がある．音高の直線上昇的な側面とは，周波数の上昇につれて音も高く感じることである．また音高の循環的な側面とは，周波数の上昇と共に上昇する音階 (ドレミファソラシド) が，一定間隔の周波数の上昇で一巡することである．一巡するための周波数の間隔を，オクターヴと言い，音高が一オクターヴ上の音は，必ず周波数が 2 倍であるという法則をもつ．

音量

音量とは，人間が感じる音の強さのことである．人間の聴覚は，音の強さが強いと音が大きいと感じ，音の強さが弱いと，音が小さいと感じる．それ故に，音量の尺度は，音の大小という一次元的なものであると位置づけることが出来る．

音色

音色とは，音の質や音の聞こえ方のことである．音色には識別的側面と，印象的側面の 2 つの側面がある．音色の識別的側面とは，音色によって人間が演奏中で使用されている楽器の種類を識別できることを指す．また音色の印象的側面とは，人間が音色を聴いた時に，その音に対して,「音が豊かである」や「音が貧弱である」等の印象を受けることを

指す．音高や音量と比べ，音色は複数の音の物理的性質と密接に関係しており，非常に複雑な音の要素である．

5.2 音楽とは

音楽とは，ある規則にそって構成された音の集まりである．人間は，構成された音の音高や音色の変化の流れを，音楽として認識している．

5.2.1 音楽の三要素

音楽は，西洋音楽的な観点から見た時，リズム，メロディ，ハーモニーの 3 つの要素で構成される．本項では，それぞれの要素の定義と，具体的な内容について説明する．

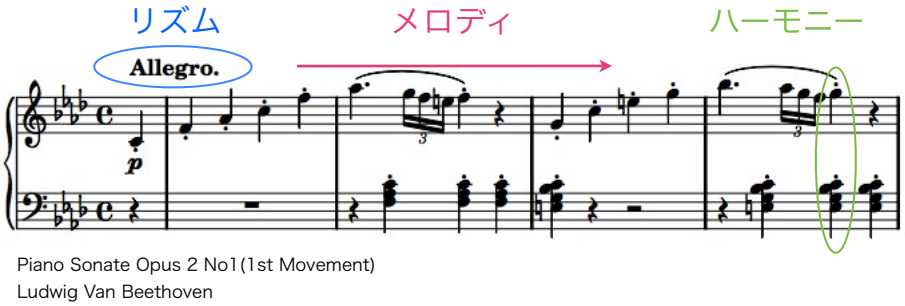


図 5.3: 音楽の三要素

リズム

リズムとは，一定のパターンを持つ音列の繰り返しのことを指す．リズムとして構成される音のパターンは，音の強弱や，休止の長短で表現される．音列のパターンを拍子といい，拍子を構成する音を拍と呼ぶ．音楽に使用される拍子は，2 拍子，3 拍子，4 拍子が一般的であり，拍子を構成する各拍には強弱がつけられている．また，リズムが刻まれる速度のことをテンポと呼ぶ．リズムは音楽の三要素の中でも一番，音楽の根本を成しているものであり，非常に重要な要素である．

メロディ

メロディとは，音の音高の変化によって生まれる音の流れのことを指す．メロディは，音楽の中でも情感の元となる部分である．また，西洋音楽的な観点から見たとき，メロディを作る音高は,「ドレミファソラシ」などの音階に従って作成されることが一般的である．

ハーモニー

ハーモニーとは，音高が違う複数の音を同時に奏でる時に生まれる響きの流れのことを指す．音高が違う 2 音以上重ねた音のことを和音を呼ぶ．和音の響きは音同士の干渉によって生まれ，和音の中でも協和する音を協和音，協和しない音を不協和音と呼ぶ．また，和音をある規則にそって奏でることを，進行と呼び，ハーモニーの重要な部分を構成している．

5.3 不快を感じさせない音の設計

音の三要素と，音楽の三要素を利用して，不快を感じさせない音を設計する．

5.3.1 音高の設計

人間が不快に感じない音高の出力範囲と，出力方法について述べる．まず，不快に感じない音高について論じる．人間の可聴域は周波数にして，20Hz から 20000Hz の間といわれている．さらに，可聴域の中でも人間が聴きやすいと感じる音は，500Hz から 5000Hz である．そこで，使用する音高の音階は 500Hz から 5000Hz 以内の音階に限定する．また，使用する音を人間が聴きやすい音に限定するのは，既存の可聴化の研究でも望ましいこととされている．次に音高の出力方法について述べる．音楽において音高はただ適当な周波数で出力するのでは無く，音律に従った音階によって音を出力する．音律には様々な種類があり，平均律，純正律，中全音律，ピタゴラス音律などがある．本システムは，平均律を元とした音階を採用する．平均律は，1 オクターヴを 12 等分した音律のことであり，現在の音楽の中で一般的に使用されている音律であることから，本システムは平均律を採用する．

音階	ド	ド＃	レ	レ＃	ミ	ファ	ファ＃	ソ	ソ＃	ラ	ラ＃	シ
周波数	261.62	277.18	293.66	311.12	329.62	349.22	369.99	391.99	415.30	440.0	466.16	493.88

図 5.4: 平均律の音律に対応している音階

5.3.2 音量の設計

音量とは，人間が感じる音の強さのことであり，最も単純な音の要素である．それ故に，多くの可聴化システムで使用されている．しかし音量を可聴化に使用する際には様々

な問題がある．1 点目は音の大きさの判断が難しい点である．2 点目は，音の大きさに対する記憶が残りにくい点である．3 点目は音高に比べると印象が薄い点である．4 点目は，周囲の音で出力される音量に対する認識が惑わされる点である．それ故に，様々な環境において音の大きさによってデータの違いを正確にはかることが難しい．また，音の大きさは，音高などによって干渉されることが多い．それ故に音の大きさの最も有効な使い方は，音の大きさを三段階ほどに分けて，2 か 3 段階のデータの違いを音の大きさで表現することである．

5.3.3 音色の設計

本システムは，音色に楽器音を採用する．4 章でも書いたように，本提案手法は通信の要素を音の要素に変換し，音の変化でネットワーク異常を検知するというものである．そのため，使用する音は，ユーザにとって音の要素の変化が分かりやすい音でなければならない．自然音，動作音，楽器音，電子音の中で，音の要素の変化が分かりやすいのは，楽器音と電子音である．電子音は確かに音の変化が分かりやすいが，長期的に聞き続けるのには不向きである．反対に楽器音は，音の変化が分かりやすく，電子音よりも身近で音楽的な音で，長時間聞いていてもユーザに不快感を与えにくい．そこで，本システムでは楽器音を採用した．

5.3.4 リズムの設計

本システムで使用するリズムは 1 拍子に固定し，主にテンポを変更する音の要素の対象とする．最初にテンポの出力範囲について述べる．まず使用するテンポとしては，極端にゆっくりとしたテンポは使用しない．極端にゆっくりなテンポの場合，音列のまとまりが無くなり，リズムとして認識することが出来ないからである．逆に極端に速いテンポの場合，音列としてでは無く，継続的に流れる単音として認識する．そのため，極端に速いテンポや，極端に遅いテンポは使用しない．

5.3.5 ハーモニーの設計

ハーモニーは，和音と，和音を使用した音楽の流れのことを指す．本システムにて使用する音は，主に和音として出力する．和音を使用する利点としては，単音よりもより美しい響きを出力することが可能な点である．和音には様々な種類があり，三和音，四和音，五和音と，出力する音の数で名前の数が変化する．西洋音楽の音楽理論では，三和音が基本であることから，本システムでも三和音を採用する．また和音は，音階の組み合わせの違いにより長三和音，短三和音，減三和音，増三和音に分かれている．それぞれの和音によって人が受ける印象は違い，長三和音は，楽しい音や安定した音という印象を受ける．短三和音は，暗くて悲しい音という印象を受ける．増三和音は，不安定で落ち着かない音という印象を受ける．減三和音は，不安定で緊張感のある音という印象を受ける．これら

の印象の違いから，本システムでは出力する和音として，ユーザに出来るだけ不快感を与えない，楽しく安定した印象のある長三和音を採用する．長三和音は，根音に長三度と完全五度を加えた音で構成される和音である (図 5.5)．和音の進行方法 (配置順序) にも様々な種類があるが，本システムではすべて長三和音を使用するため，和音進行に関しては調整しないものとする．

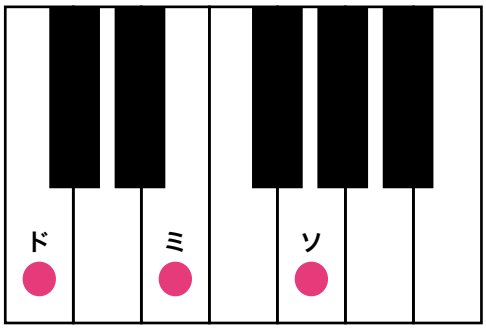


図 5.5: ドを根音とした時の長三和音 (ピアノ)

5.4 通信の要素と音の要素のひも付け

第 4.4 節で挙げたように，本提案手法によるネットワーク異常検知の実現には，音のみで通信状態変化が明確に認識出来ることが必要事項である．そのため，通信情報と音の要素のひも付けは，非常に重要である．本節では，まず可聴化する通信情報の要件を挙げる．その後，挙げた要件を元に通信情報と音の要素のひも付け方法について述べる．

5.4.1 可聴化する通信情報の要件

本項では可聴化する通信情報に必要な要件を 2 つ挙げ，その理由について記述する．

- **値に変化があること**: 通信の変化を音の変化として表現するため，可聴化の元となる通信情報の値に変化が無いと音も変化しない．音が変化しないと，ネットワーク状態の変化も分からない．さらに，音の変化が無いと音が単調になり，ユーザにとって不快であると思われる．そのため，音に変換する通信情報は，短時間で変化する値で無ければならない．

- **異常時に値が大きく変化すること**: 音の変化によって，ネットワーク異常を検知するという提案手法から，可聴化する通信情報はネットワーク異常発生時に，正常時と比較して値が大きく変化するものでなければならない．値が大きく変化し，音も大きく変化しなければ，ユーザが異常に気がつかない可能性があるからである．具体的には，第 2 章で挙げた 3 種類のネットワーク異常 (ネットワーク障害，ネットワーク

への突発的アクセス集中，ネットワーク侵害) において大きく値が変化する通信情報が望ましい．

5.4.2 可聴化方法

可聴化の際に必要な事項は，可聴化する通信情報と音の要素の割当，その極性である．

可聴化する通信情報

第 5.4.1 項で挙げた可聴化する通信情報に必要な要件から，可聴化するネットワーク通信の情報は，時間当たりのパケット数と，時間当たりのパケットの流量を採用した．パケットの流量とパケット数を採用した理由は 2 つある．第一に何らかの通信が発生すれば，パケットは送受信され，パケットの流量とパケット数は変化する．そしてユーザが通信を発生させる様な操作 (Web 閲覧やメール送信) を行わなくとも，常に何らかの通信が流れていることが多い．そのためパケットの流量とパケット数は絶えず変化しており，第一の要件を満たすからである．第二にネットワーク異常が発生した場合，パケットの流量とパケット数は大きく変化することが多く，第二の要件を満たすからである．例えば，ネットワーク侵害が発生した場合，通常の通信の上になんらかの異常な通信が上乗せされる．また，突発的なアクセス集中が発生した場合，大量の通信が発生する．そして，ネットワーク障害が発生し，ネットワークが不通になった場合には，通信の発生が起こらない．このことからすべてのネットワーク異常において，パケット数とパケットの流量は大幅に変化することが分かる．

可聴化する通信情報を単位時間当たりの量で扱う理由は，時間単位で区切ることによってリアルタイム性が確保できるからである．また，時間軸はすべてのネットワークにおいて，共通の軸になりえるからである．パケットの流量は，2 秒間隔で区切ることする．またパケット数は，5 秒間隔で区切ることとする．

割当

本項では，第 5.4.2 項で挙げた，可聴化する通信の情報として挙げたパケットの流量と，パケット数を，何の音の要素に割り当てるのかについて述べる．まず，時間当たりのパケットの流量を，音高と，音量に割り当てた．パケットの流量は，ネットワーク異常を検知するに当たり，最重要の情報である．そのため，音高と音量という 2 つの音の要素に割り当てた．2 つの音の要素に割り当てることによって，より音の変化の明確性が向上することも既存の可聴化についての研究でも判明している [20].

時間あたりのパケット数はリズム (テンポ) に割り当てた．ネットワークアナライザーを使用した時，時間当たりに流れるパケット数が増加すれば，画面の更新速度が上昇する．このことから，時間あたりのパケット数をリズム (テンポ) に割り当てるのが適していると判断した．

極性

可聴化における極性とは，可聴化情報の値の変化方向と，音の要素の変化方向の割当のことである．例えば，可聴化する値が増加すると，音量や音高が高くなる方向に割り当てる等である．極性は人間の直感と大きく関係しており，適切に極性を割り当てないと，音で直感的に情報が理解出来るようにはならない [29]．例えば，流量が増加したら，音高を高くするのが直感的なのか，音高を低くするのが直感的なのかについて配慮する必要がある．また，人によって，直感的と感じる極性の割当は違うという問題もある．本システムでは，データの増加方向と，音の要素の増加方向は正の方向で一致させる．具体的な極性の割当についてを挙げる．時間当たりのパケットの流量が増加したら，音高の増加させる．さらに，音量も増加させる．時間あたりのパケット数が増加したら，リズム (テンポ) を速くする．

5.5 まとめ

本章では，まず，音や音楽の定義について述べ，音や音楽を構成する要素を挙げた．また，前述した音や音楽の要素を踏まえて，不快でない音にするための具体的な音の設計について記述した．その後，提案手法から可聴化する通信情報として必要な要件について述べた．そして，具体的な可聴化する通信情報を挙げ，その可聴化方法について述べた．

第6章　実装

本章では，第 4 章で提案した手法を用いたシステムの設計と実装について記述する．まず第 4.4 節で記述した要求事項と，第 5 章で述べた音の設計を元に，本研究の設計概要について述べる．そして，本研究の実装に対する設計要件について述べる．また，実際に実装した実装物の概要について述べ，その中身の詳細ついて述べる．

6.1　設計

本節では第 4 章で提案した，通信情報を音に変換し，音の変化によって人がネットワーク異常を検知する手法を元にした実装の設計を行う．ネットワーク部分の処理を行うためのパケットキャプチャ部，必要な情報を可聴化用に加工する情報加工部，加工された情報を可聴化する音声変換部の 3 つの部分に分けた．図 6.1 では，本実装の設計概要を示している．

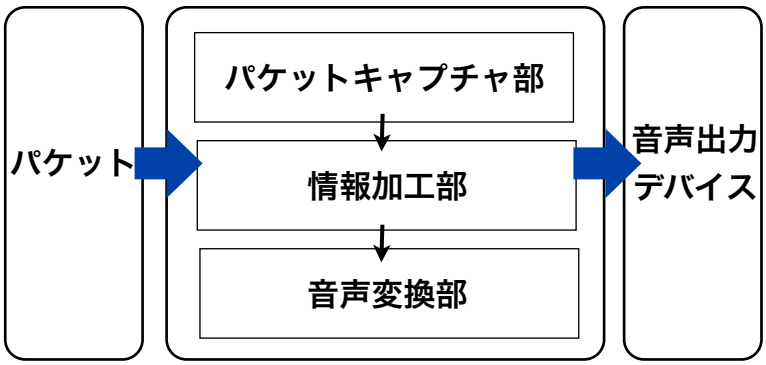


図 6.1: 設計概要図

また，本システムは，主に会社内や組織内にあるシステムのネットワーク監視への利用を想定して設計する．そのため，本システムの実行想定環境は，ネットワークの境界，もしくはネットワークセグメントの接続点での動作を想定している．本システムの実行想定環境の例を図 6.2 に示す．

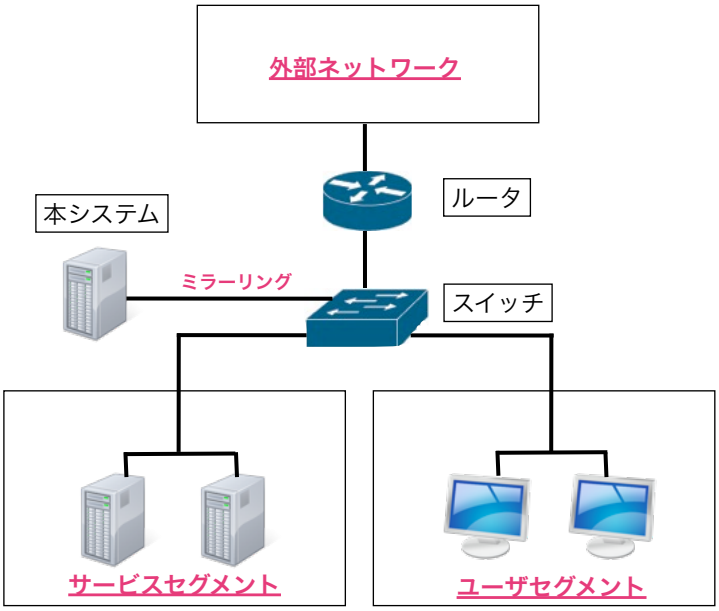


図 6.2: 本システムの実行想定環境例

6.1.1 設計要件

音によるネットワーク異常検知システムの実装に対する設計要件をまとめる．

- **音の変更が容易に可能なこと**: 第 4.4 節で要求事項として述べたように，音に対する感性や感覚は人によって違うため，音の変更が容易に出来るような柔軟なインターフェースが必要である．出力する音を変更するための細かい数値の入力や，マニュアルの熟読の必要なく，音が変更出来る機能が必要である．また，ここでいう音の変更とは，音の聞こえ方の根幹を担っている音色の変更のことを指す．

- **音と通信内容に大幅な遅延がないこと**: ネットワークの異常が発生した場合，迅速に対処しなければ，多大な被害が発生してしまう．そのためネットワーク異常の検出は非常に重要であると，第 2.1.4 項で述べた．本提案手法では，音の変化によってネットワーク異常を検出することから，通信内容に対して，変換した音が遅延すると，異常の検出も遅れてしまう．そのため，通信内容と可聴化された通信間のタイムラグ発生を防がなけらばならない．

- **リアルタイム処理とバッチ処理が可能なこと**: 本システムは，迅速なネットワーク異常検知のため，リアルタイムでの使用が推奨される．そのため，リアルタイムに通信データを読み込む機能が必要である．また，リアルタイム処理に加え，通信ファイルを読みこみバッチ処理的に可聴化が出来る機能も必要である．これはユーザが本システムによる音を聴いていない時に異常が起きた場合，異常に対処することができないからである．

6.2 実装したシステムの構成

本研究で実装したシステムは，パケットキャプチャ部，情報加工部，音声変換部の 3 つの部分で構成される．図 6.3 にて実装の全体図を示している．パケットキャプチャ部は，トラフィックからパケット単位でデータを読み込む．読み込んだパケットから必要な情報だけ取り出して，情報加工部に渡す．詳細は，第 6.2.1 項で述べる．情報加工部では，パケットキャプチャ部から受け取った情報を加工し，音声出力部にデータを渡す．詳細は，第 6.2.2 項で述べる．音声出力部は，情報加工部から受け取ったデータを音に変換する．詳細は，第 6.2.3 項で述べる．また，実装環境に関しては表 6.1 に記載する．

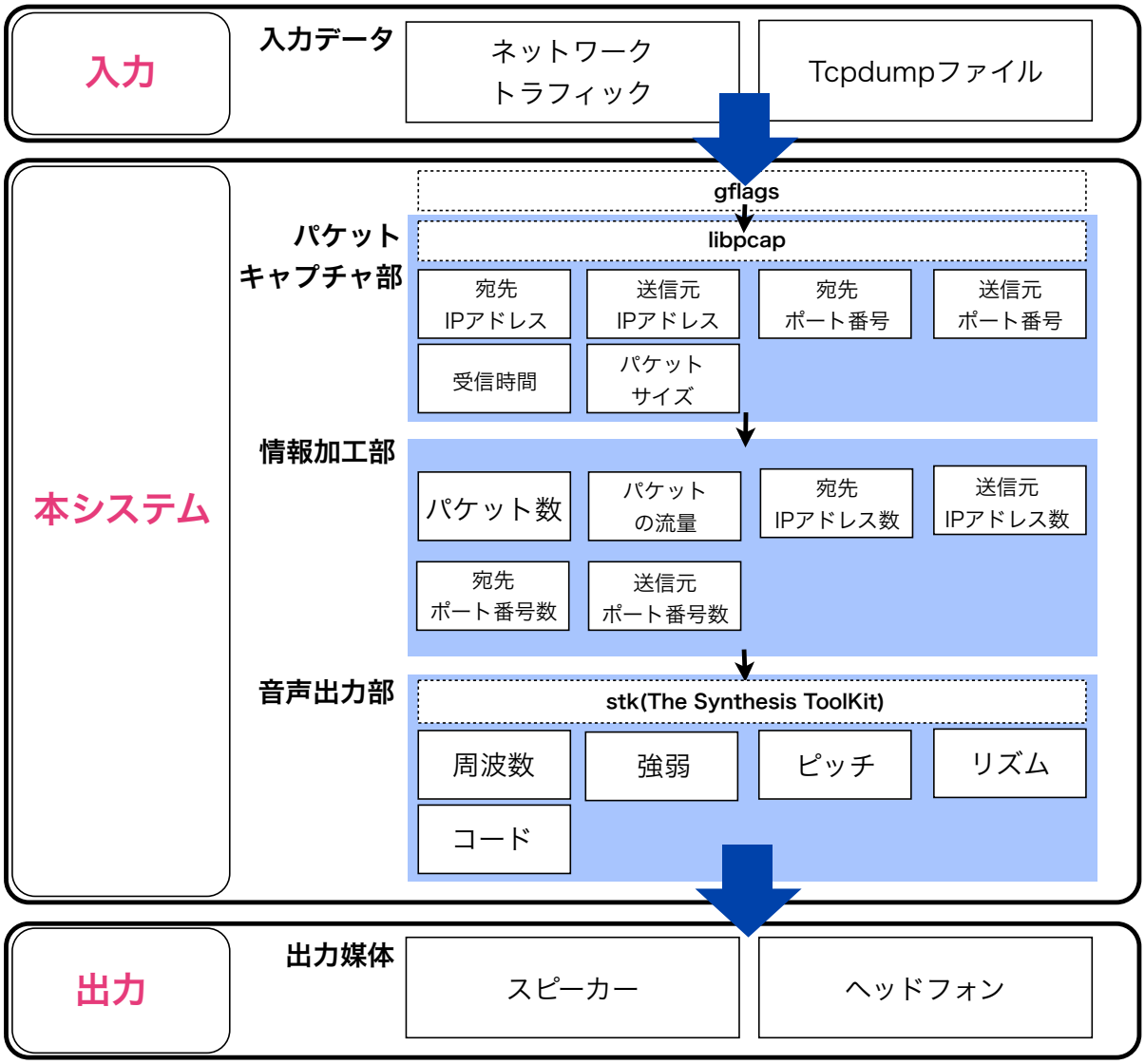


図 6.3: 実装概要図

表 6.1: 実装環境

要素名	属性	利用環境
OS	実機	MacOSX Lion 10.7[30]
言語		C++ [31]
コンパイラ	C++	gcc version 4.2.1[32]
ライブラリ	コマンドライン処理	gflags version 2.0[33]
	パケットキャプチャ	libpcap version 1.15[34]
	シンセサイザー演算	stk(The Systhesis ToolKit) 4.4.3 [35]

6.2.1 パケットキャプチャ部

パケットキャプチャ部は，通信データを読み込み，その中からパケットヘッダの情報を抽出する部分である．本項では，パケットキャプチャ部が対応している，通信データの入力形式と，パケットヘッダから取得する情報について記述する．

入力形式

パケットキャプチャ部では，ネットワークインターフェースからの入力と，ファイルからの読み込みの両方に対応している．具体的には，libpcap を利用して，ネットワークインターフェースからのパケットキャプチャ，または TCPDUMP が出力するファイル形式からの入力に対応している．この様に両方の形式に対応することで，音によるリアルタイムなネットワーク監視と，過去の通信の可聴化が実現可能になった．

取得情報

パケットキャプチャ部では，パケットデータを読み込んだ後，パケットヘッダの情報を抽出する．パケットから取得する情報は，送信元 IP アドレス番号，宛先 IP アドレス番号，送信元ポート番号，宛先ポート番号，パケットサイズ，パケットの受信時間，TCP パケットのフラグ情報の 7 つである．これらの情報は，1 パケット毎に取得する．また取得した情報は，パケットヘッダを保存する構造体を使用して (図 6.4)，連結リスト方式ですべて保存する．連結リストで保存された情報は，情報加工部に渡されてる．

```
struct PacketHeaderData{
  char source_ip_address[16];
  char destination_ip_address[16];
  int source_port;
  int destination_port;
  long packet_length;
  long time;
  int tcp_flag;
};
```

図 6.4: パケットヘッダを保存する構造体

6.2.2 情報加工部

情報加工部は，パケットキャプチャ部で抽出したパケットヘッダの情報を加工する部分である．情報加工部では，すべての情報を時間を軸に加工する．具体的には，時間当たりのパケット数や時間当たりのパケットサイズの合計等である．図 6.2.2 に時間あたりのパケットサイズの合計を計算する部分を掲載する．

```
int PacketAnalysis::packet_size_sum(vector<PacketHeaderData>& Packet){
  int i;
  int last_element_number=Packet.size()-1;

  if((Packet[last_element_number].time - get_time_for_packet_size_sum)
    >=INTERVAL_TIME_ONE){

    return_packet_size_sum  =  0;
    for(i = 0;i<Packet.size();i++){
      if(Packet[i].time>get_time_for_packet_size_sum)
        return_packet_size_sum += Packet[i].packet_length;
    }
    get_time_for_packet_size_sum=Packet[last_element_number].time;
  }
  return return_packet_size_sum;
}
```

図 6.5: 情報加工例

情報加工部で加工された情報は，音声変換部に渡される．また，情報加工部ではパケットキャプチャ部にて取得されたパケットヘッダの情報を取得しているが，現時点では，送

信元 IP アドレス番号，宛先 IP アドレス番号，送信元ポート番号，宛先ポート番号，TCP パケットのフラグ情報は使用していない．

6.2.3 音声変換部

音声変換部は，情報加工部から受け取ったデータを音声情報へと変換し，音声出力デバイスに音を送る部分である．本部分では，シンセサイザー演算ライブラリである The Systhesis Toolkit(stk) を利用して，実装を行った．音声変換部では，まず出力する音に関しての初期設定を行った後，マルチプロセスを使用し，音高や音量を細かくコントロールする仕組みになっている．音声変換部の概要を図 6.6 にまとめた．

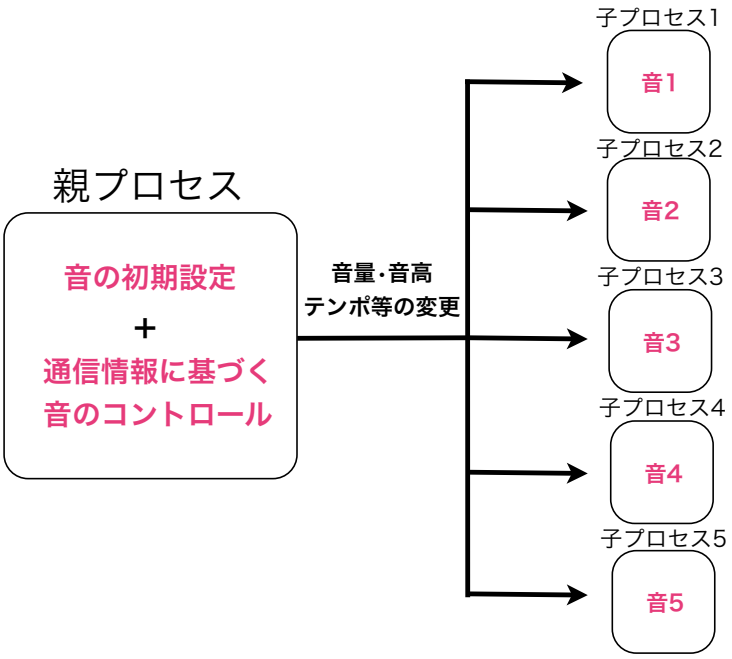


図 6.6: 音声変換部の概要

音変換のコントロール

親プロセスは，定期的に子プロセスに対して音の変更に関する情報を送り，子プロセスが出力する音をコントロールしている．送る情報は，音量，音高，テンポの情報である．親プロセスは，子プロセスに情報を送る際に，共有メモリを利用して，情報を送る．共有メモリを利用することで，リアルタイムに通信情報を音へと変換できるようにした．

和音の生成

和音の出力には，複数の音高の違う音を重ね合わせ，同時に音を出力する必要がある．そのため，和音の生成には，複数の音の音高を調整し，かつ同時に出力するよう実装しなければならない．本システムでは和音の生成を，マルチプロセスを使用し実現した．具体的には，複数子プロセスを生成し，1 プロセスが 1 つの音を出力するように設定した．そして，和音として扱いたいプロセスに関しては，和音の根音 (和音を構成する複数音の中で一番低い音高の音) から和音の規則に基づき，周波数をずらして出力した．例えば，長三和音を生成する場合根音を担うプロセスは，基となる周波数の音階で出力する．そして，2 音目 (第三音) を担うプロセスは，4 つ音階をずらした周波数で出力する．そして，3 音目 (第五音) を担うプロセスは，3 つ音階をずらした周波数で出力する．これらの 3 音を同時に出力すると和音が完成する．以上の和音生成プロセスを図 6.7 にまとめた．

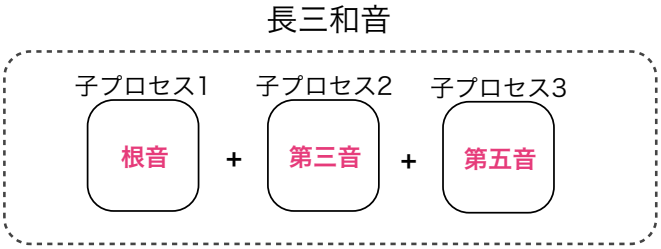


図 6.7: マルチプロセスによって生成される和音

テンポの生成

本システムにおいて，どのようにリズムを生成し，そのテンポを調整したかについて述べる．まず本システムは，使用するリズムが 1 拍子であることから，音を一定間隔で出力した．また，音を出力する間隔を調整することでテンポの調整を行った．出力される単音とその次に出力される音の時間間隔の幅を 11 段階用意した．そして，テンポとして変換されるデータの数値の増減によって，テンポの速さを調整した．

音の出力

本システムでどのように音を出力するかについて述べる．本システムは，シンセサイザー演算ライブラリで計算した音の情報をアナログ情報に変換してから，デバイスに出力する．デジタル情報からアナログ情報への変換も，The Systhesis Toolkit(stk) で行った．

本システムでは使用する音声出力媒体としては，ヘッドフォンや，PC の内蔵スピーカーを想定する．

6.2.4 実行

本項では，本システムを実行するための方法と，実行後の挙動について記述する．本システムは，インターフェースの指定や，楽器音の指定，パケットヘッダの情報と，音の要素の割りあてにコマンドラインフラグを使用した．パケットヘッダの割り当てと，音の要素の割り当てに関しては，初期設定では第 5 章で行った音の設計を基に設定されている．ユーザがその割当を変更したい場合，コマンドラインフラグを使用して変更が可能である．コマンドラインフラグの部分は，gflags を利用して実装した．コマンドラインフラグの一覧を表 6.2 に示す．

表 6.2: コマンドラインフラグ一覧

コマンドラインフラグ	説明
-interface	インターフェースの指定
-file	読み込むファイルの指定
-instrument	使用する楽器の指定
-frequency	音高
-loudness	音量
-rythm	テンポ

本システム実行時に使用するコマンドラインフラグの例を図 6.8 に示す．図 6.8 のコマンドラインフラグでは，sample.pcap という tcpdump のファイルを読み込んでいる．また，音の初期設定をコマンドラインフラグ上で明示的に表示している．

```
./sonification -interface=file -file=sample.pcap -instrument=plucked
 -frequency=packet_size -rythm=packet_number -loudness=packet_size
```

図 6.8: 実行例

本システムを実行した時にどのようなことが起こるのかを述べる．本システムが出力する音を波形図に変換したものを図 6.9 に示す．

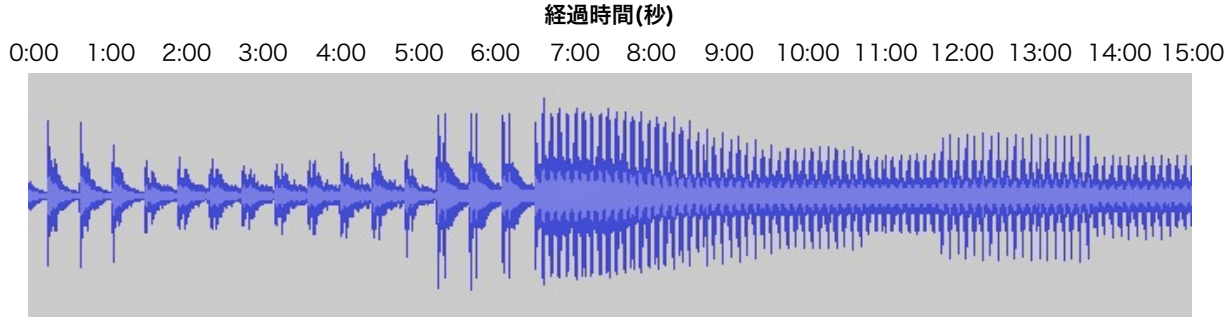


図 6.9: 本システムから出力される音

波形図は，音の音量や，音色，音高を時間軸上で分析したものである．横軸が時間軸，縦軸が，振れ幅 (音量)，波形が音色，波の周期が周波数 (音高) である．波形図から，一定間隔で音が出力されていることが分かる．また，音量や音高も時間の経過とともに変化していることが分かる．

6.3 まとめ

本章では，本研究で開発したシステムの具体的な設計と実装を記述した．設計の部分では，まず設計の概要について説明し，本システムの想定利用環境について述べた．また，本システムの実装に必要な設計要件を挙げた．その後，本システムの実際の実装概要について記述した．また，本システムのパケットキャプチャ部，情報加工部，音声変換部などの部分についての具体的な実装の内容について記述した．また，本システムの実行方法や，実行時の挙動についても記述した．

第7章　検証・評価

本章では，第 6 章で実装したシステムの検証と評価について述べる．まず最初に，第 4 章で提案した手法が実現できているかを検証した．検証実験について述べる．その後，本システムによる異常検知に対する評価実験について述べる．また，システムの評価以外にも本システムが出力する音に対する評価を，SD 法や唾液アミラーゼ値を使用して検証したことについて記述する．最後に，評価実験で得られたデータから音とシステムに対する評価の考察を行う．

7.1　検証

本節では，第 4 章で提案した「通信情報を音の要素に変換することで，音の変化によりネットワーク異常を検知する」という手法が実現できたかについてを述べる．

7.1.1　検証実験概要

提案手法が実現できたかを実証するために検証実験を行った．本検証実験の概要を図 7.1 に示す．本検証実験では，予め用意しておいた通信を本システムを使用して可聴化し，その音を複数の被験者に聴いて貰った．また被験者には，音を聴きながら，その音の変化を通じてネットワーク異常を感じた瞬間の時間を記録して貰った．

図 7.1: 検証実験概要

本検証実験の参加人数と，実験期間は以下に述べる．

- 期間:2012 年 12 月 27 日-2013 年 1 月 10 日
- 検証実験用 Web サイト:http://isc.sfc.wide.ad.jp/〜asp/evaluation.html
- 参加人数:23 人
- 可聴化対象サーバ:isc.sfc.wide.ad.jp

7.1.2 検証実験の構成

本実験では，被験者にサーバに来た 7 分間の通信を可聴化した音を，録音したものを 2 つ聞いて貰った．本研究の提案手法による異常検知の戦略としては，最初に正常な可聴化通信をユーザ自身が感覚で把握して貰い，その後，音の変化でネットワーク異常を検知するというものである．そのため，どちらの録音も最初の 4 分間は正常な通信を可聴化したものを収録した．その後の後半 3 分間の可聴化通信は，異常がある通信の音と，正常な通信のみの音に分かれる．被験者にはこの 2 つ通信を聞いて貰い，前半の 4 分間は正常な音を学習して貰い，その後の 3 分間で異常があったを感じた瞬間に，その検知時間を記録して貰った．ここで述べている異常があったと感じた瞬間とは，異常の発生が開始された瞬間のことを指す．また，被験者には事前に通信の中に異常があるかどうかに加え，異常が複数発生することは知らせずこの実験を行って貰った．

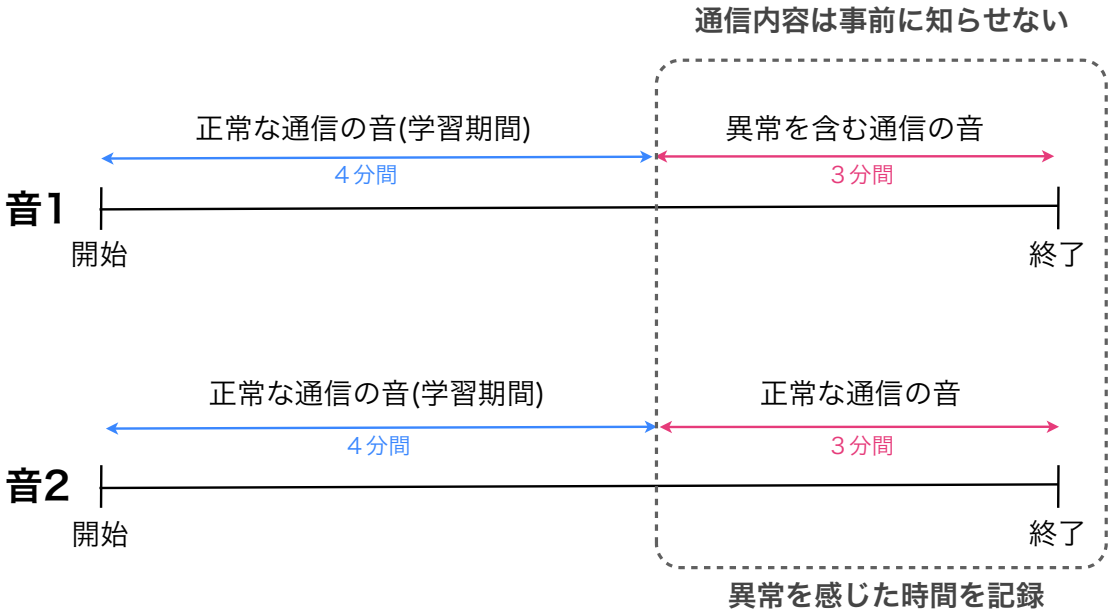


図 7.2: 検証実験内容

音 1 が異常を含む通信を可聴化したもので，音 2 がすべて正常な通信を可聴化したものである．具体的には，音 1 は 4 分以降 nmap[36] によるポートスキャン (Tcp connect スキャン) と DoS(Slowloris)[37] が行われている通信である．ポートスキャンの通信は，通信開始後 4 分 30 秒から 4 分 31 秒 (270 秒〜271 秒) にかけて行われている．また，DoS の通信は通信開始後 5 分 43 秒から 6 分 25 秒 (343 秒〜385 秒) にかけて行われている．2 つの可聴化した通信の波形図を図 7.3 に示す．波形図の生成には，Audacity[38] を使用した．波形図は，音の音量や，音色，音高を時間軸上で分析したものである．横軸が時間軸，縦軸が，振れ幅 (音量)，波形が音色，波の周期が周波数 (音高) である．

波形図を使用して，可聴化した通信の音から，音 1 と音 2 の違いを述べる．音 1 ではポートスキャンを行った 270 秒から 271 秒付近では，振れ幅が急に大きくなり，かつ波の周期が非常に短くなっていることが分かる．また，DoS 攻撃を行った 343 秒から 385 秒付近でも振れ幅が大きく，かつ波の周期が非常に短くなっていることが分かる．音 2 では，振れ幅や波形に多少の変化は見られるものの，急激な振れ幅の増大や，周期の変化は見られなかった．

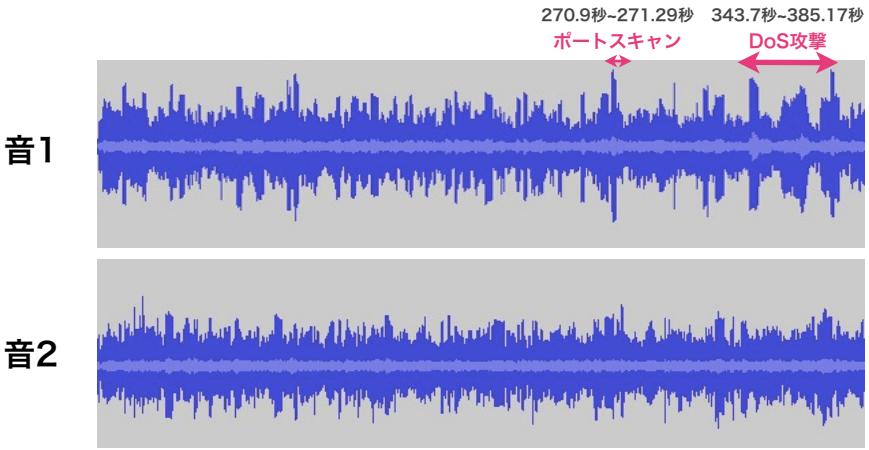


図 7.3: 可聴化した通信の波形図

本検証実験を行うために，可聴化した通信の録音を聴きながら，異常を感じた際にその時間を記録するための Web サイトを構築した．本 Web サイトを図 7.4 に掲載する．異常を感じた際には,「異常を感じた」ボタンを押すと，音の開始時点の経過時間が自動的に記録されるようになっている．また，被験者には Web サイトを通じて結果を送信して貰った．本実験を行う際には，出力する音声デバイス (スピーカー，ヘッドフォン等) を限定せず，被験者の任意で行った．

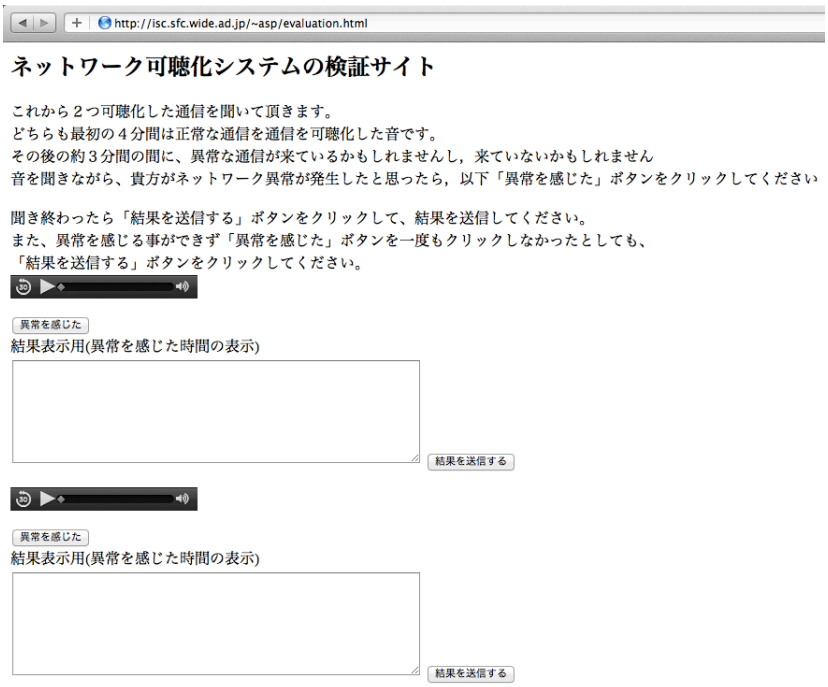


図 7.4: 検証実験用サイト

7.1.3 実験結果

検証実験で得られた結果について述べ，その結果の有意性についてを論じる．

音 1 の結果

音 1 で各被験者が異常を感じた瞬間の時間を図 7.5 に示す．図の縦軸が被験者であり，横軸が経過時間を示している．図から，音 1 の結果について述べる．音 1 に対して被験者が異常と感じた瞬間は大きく分けて 3 つに分かれる．(1) ポートスキャン直後，(2)288 秒付近，(3)DoS 攻撃の間である．個々の内訳について詳しく述べる．

まず，(1) ポートスキャン付近では，全ての被験者はポートスキャンが発生した直後に「異常を感じた」ボタンを押している．本システムでは通信が音程や音量の変化として出力されるまで 2 秒かかる．さらに，ポートスキャンの通信がテンポの変化として出力されるまでは 5 秒かかる．それ故に．270 秒〜271 秒の間に発生したポートスキャンの通信が音程，音量，テンポの変化に現れるのは 276 秒付近と言える．ほぼ全ての被験者が 277 秒付近で異常を検出していることから，被験者はポートスキャンによる音の変化から 1 秒後には異常を感じたこととなる．

次に，(2)288 秒付近で，被験者の多くが異常を検知したことについて述べる．288 秒付近において，事前にネットワークに異常を発生させる様な通信を行っていないにも関わらず，被験者の多くが異常と判断した．288 秒以前の通信の内容を見てみると，292 秒付近

でルータが短期間に大量に ARP 通信を発生させていることが分かった．ルータが 1 秒以内に 154 個の機器 (IP アドレス) に対して ARP 通信を送信したことによって，音が変化したと思われる．その音の変化を受け，被験者の多くはネットワークに異常が発生したと判断したと考えれられる．それ故に，(2)288 秒付近では多くの人が誤検知をしてしまったと言える．

最後に，(3)DoS 攻撃の間について述べる．343 秒〜385 秒の間に発生した，DoS 攻撃の間に被験者が異常を感じた瞬間は，350 秒付近と，375 秒付近の 2 つに分かれた．2 点の詳細について述べる．まず，最初に 350 秒付近についてだが，DoS 攻撃が 343 秒付近で開始されており，攻撃 PC から対象サーバに対して大量の通信が送信されている．DoS 攻撃によって引き起こされた音の変化によって，被験者は 350 秒付近で異常と判断したと考えられる．次に 375 秒付近の詳細について述べる．375 秒以前の通信の内容を見てみると，370 秒前後から DoS 攻撃を行っている攻撃 PC に対して，サーバが順次返信を送信してることが分かった．攻撃 PC から来た DoS 攻撃の通信に加え，サーバが，DoS 攻撃に対する返信を行っている通信が上乗せされたことで，音に変化が起こったと考えられる．それにより被験者は異常が発生したと判断したと考えられる．370 秒付近に発生した通信は DoS 攻撃によって引き起こされた通信と言えることから，被験者が 375 秒付近に異常が発生したと判断したことは誤検知ではないと考えられる．

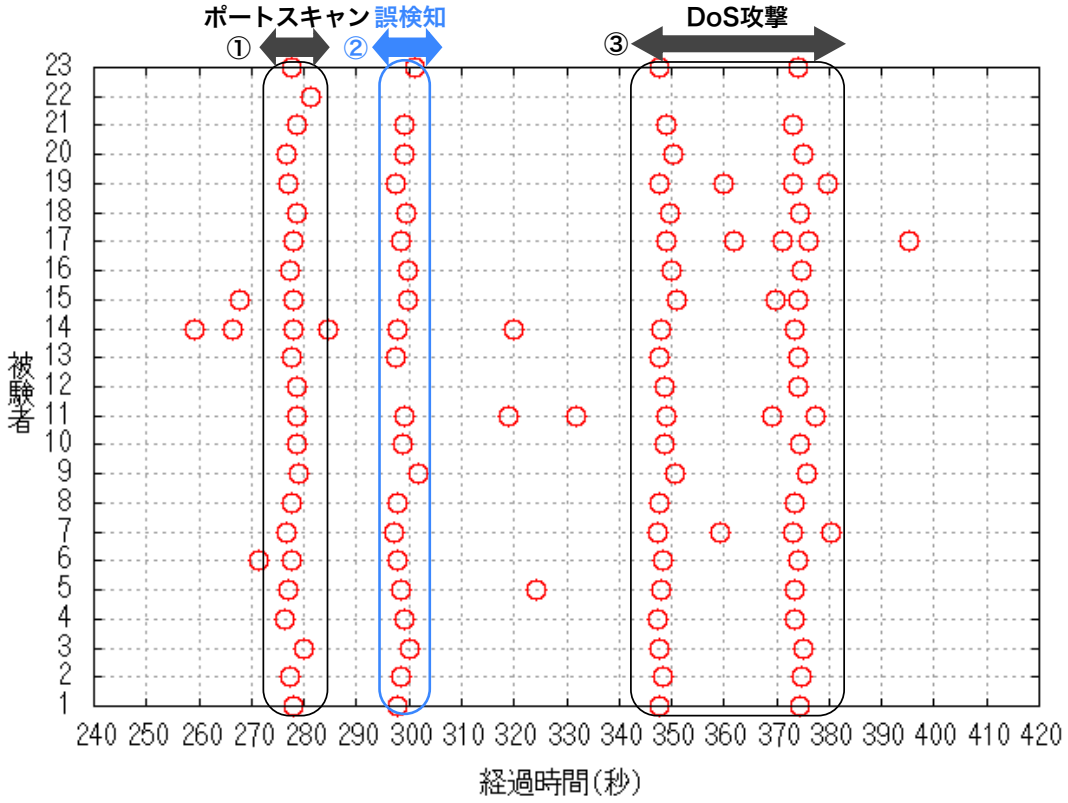


図 7.5: 音 1 に対して異常を感じた瞬間

また図 7.5 の他にも，音 1 に対して被験者が「異常を感じた」ボタンを押した回数のヒストグラムを作成した．図 7.6 に作成したヒストグラムを示す．図の縦軸が被験者の数で，横軸がボタンが押された回数である．図から音 1 の結果について述べる．

まず「異常を感じた」ボタンが押された回数は 4 回が最多であった．図 7.5 でも示したように，ネットワーク異常により大きく音が変化した瞬間は 3 回である．それにも関わらず，21 人の被験者が 4 回以上ボタンを押した．反対に 2 回以下ボタンを押した被験者は 1 人であった．このことから，ネットワーク異常の発生を見逃す (false negative) 被験者は少なかったと言える．反対に，ネットワーク異常が発生していないにも関わらず異常と判断する (false positive) 被験者が多かったと言える．

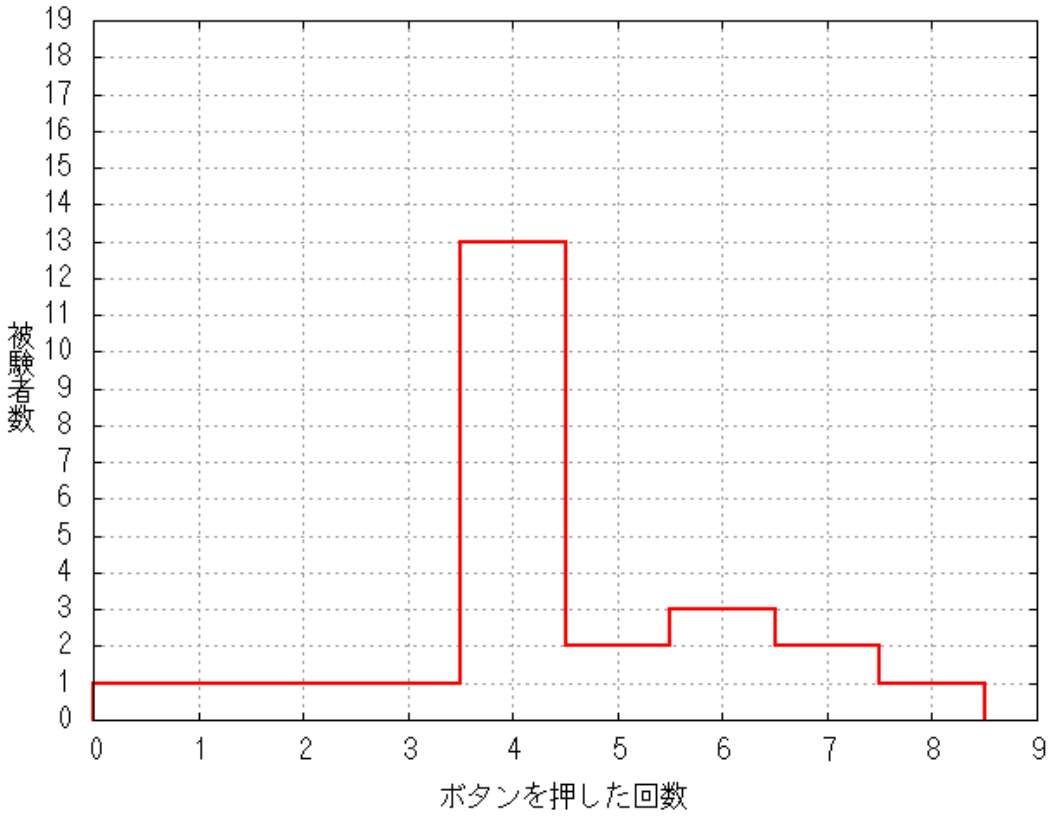


図 7.6: 音 1 のヒストグラム

音 2 の結果

音 2 で各被験者が異常を感じた瞬間の時間を図 7.7 に示す．図の縦軸が被験者であり，横軸が経過時間を示している．図から，音 2 の結果について述べる．音 2 では，事前にネットワークに異常を発生させる様な通信を行っていない．そのため，被験者が異常を感じた瞬間はすべて誤検知にあたる．音 2 の内容に対してなんらかの異常を感じた被験者が

6 人，異常を感じなかった被験者が 17 人になる．また，音 2 でなんらかの異常を感じた被験者 6 人の内，複数回異常を検知した人は 5 人いた．

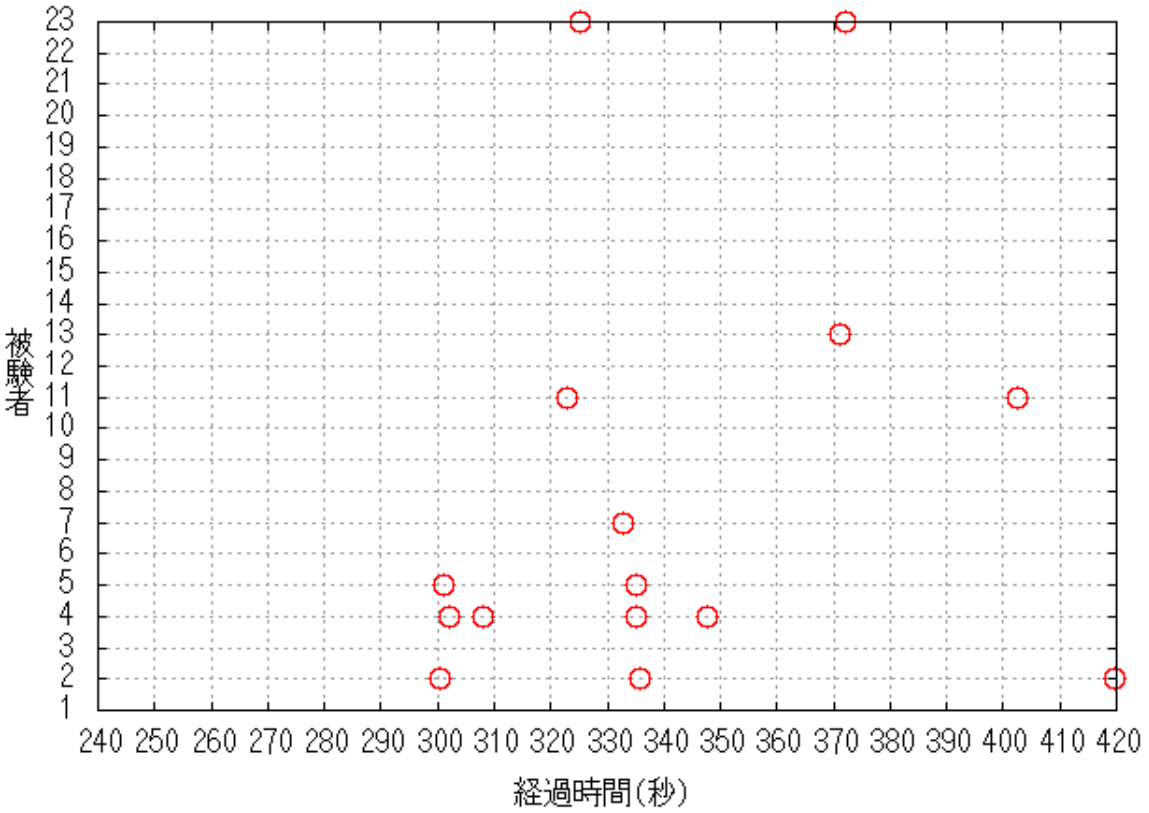


図 7.7: 音 2 に対して異常を感じた瞬間

また図 7.7 の他にも，音 2 に対して被験者が「異常を感じた」ボタンを押した回数のヒストグラムを作成した．図 7.8 に作成したヒストグラムを示す．図の縦軸が被験者の数で，横軸がボタンが押された回数である．図から音 2 の結果について述べる．

まず，音 2 では事前にネットワークに異常を発生させる様な通信を行っていないため，「異常を感じた」ボタンが押される回数は 0 回であることが期待される．そして実際に音 2 に対して被験者がボタンを押した回数の再頻出値は 0 回であった．そのため，被験者の多くは正常な通信の音を学習できたと言える．

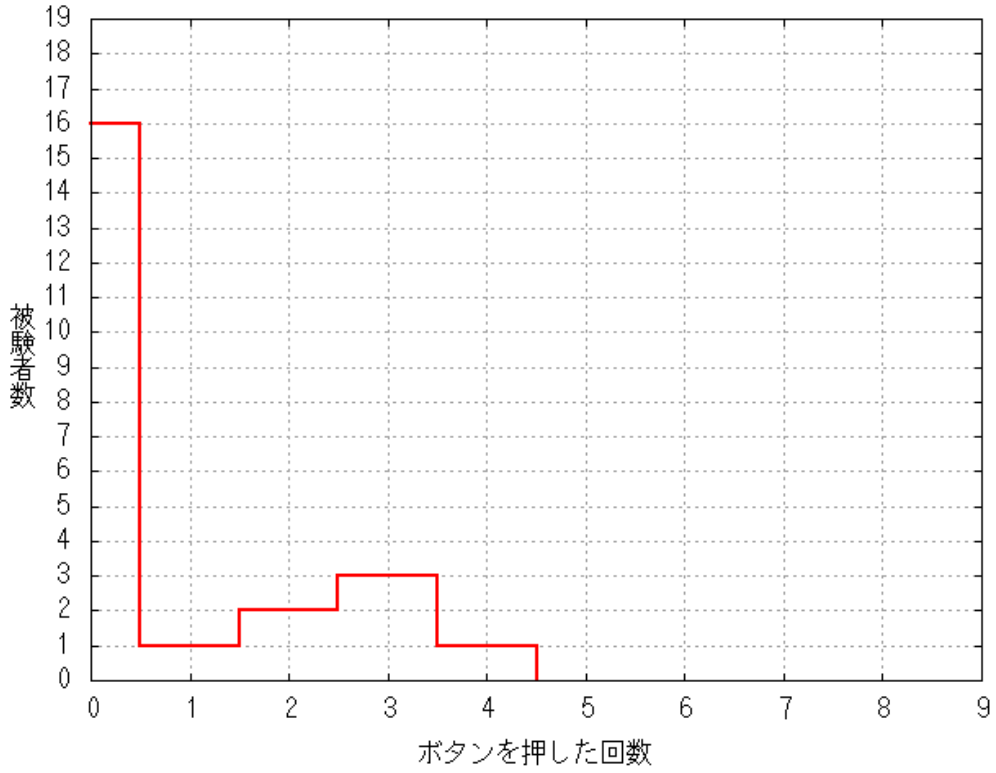


図 7.8: 音 2 のヒストグラム

実験結果の有意性

本検証実験は，本論文の提案手法である「通信情報を音の要素に変換することで，音の変化によりネットワーク異常を検知する」ことが実現できたかを検証するものであった．実験の結果から音 1 ではネットワーク異常が発生した直後に，多くの被験者が音の変化により異常を感じたという結果が出た．しかしこの結果からは，被験者が音の変化によりネットワーク異常を検知し,「異常を感じた」ボタンを押したかが厳密には証明出来ない．なぜならば偶然被験者が，ネットワーク異常が発生した付近の時間帯で「異常を感じた」ボタンを押した可能性があるからである．

そこで本項では，実際に収集したデータが本当に有意か否かを t 検定 [39] を使用して検証する．t 検定とは，2 つのデータに差があるのか，差があったとして，その差は偶然生じた物か否かを検証する検定である．そのため，本検証実験のデータの有意性を検証する検定として採用した．本検定では音 1 と音 2 に対して，被験者がボタンを押した回数のデータを用いて検定をする．各音に対する「異常を感じた」ボタンの押下回数は，表 7.1 に示す．また本検定を行う前提として，異常通信の回数に対するボタンの押下回数は正規分布に従うものとする．

表 7.1: 各音に対するボタンが押された回数

被験者	ボタンの押下回数 (音 1)	ボタンの押下回数 (音 2)
1	4	0
2	4	3
3	4	0
4	4	4
5	5	3
6	5	0
7	6	2
8	4	0
9	4	0
10	4	0
11	7	3
12	3	0
13	4	1
14	8	0
15	6	0
16	4	0
17	7	0
18	4	0
19	6	0
20	4	0
21	4	0
22	1	0
23	4	0

t 検定を行うにあたり，まず最初に帰無仮説 (証明したい仮説の反対の仮説) 「ボタンを押された回数からは異常通信回数に差は読み取れない」を立てた．t 検定によりこの帰無仮説が否定できることが出来た場合，被験者がネットワーク異常による音の変化を基に「異常を感じた」ボタンを押したということが証明される．有意水準は 5 %として t 検定を行った．t 検定により得られた結果を表 7.2 に示す.

表 7.2: t 検定の結果

	音 1	音 2
平均	4.6086956521	0.7826086956
分散	2.2490118577	1.72332015810
観測数	23	23
ピアソン相関	0.1164470834	
自由度	22	
P(T<=t) 片側	0.0000000008	
t 境界値 片側	1.7171443743	
P(T<=t) 両側	0.0000000017	
t 境界値 両側	2.0738730679	

図を元に，t 検定の結果について述べる．t 検定では，P 値が 0.05 以下の場合，有意性ありと見なされる．この検定の結果，t 検定の片側検定では P 値は 0.0000000008，両側検定では，P 値は 0.0000000017 であった．このようにどちら検定でも P 値が 0.05 以下であることが分かった．そこで本検証結果は有意性があると言える．そのため，帰無仮説は棄却することができ，被験者は発生したネットワーク異常の通信を元とした音の変化によって「異常を感じた」ボタンを押したものと考えられる．

7.1.4 考察

検証実験の結果とデータの検証結果を踏まえ考察を行う．本検証実験から，音の変化を利用した本異常検知システムでは，誤検知もあるが直感的に異常な通信を発見することが出来ると言える．さらに今回の検証実験では，正常な通信の音の学習は 4 分間という短い時間であったが，学習時間をより長期間とれば，誤検知を減らせる可能性はある．さらに，今回の検証実験ではサーバで送受信される通信を可聴化した音を聴いてもらったが，様々な通信の音を用意して被験者に予め聴かせることによって，より正確な判断を促すことが出来ると考えられる．

また，被験者が音の変化でネットワーク異常を検知する際には，音高，音量，テンポが全て変化した後に異常が発生したと判断した．この結果から，単一の音の要素の変化だけでなく，複数の音の要素が変化することで，人間にとって音が変化したと認識して貰いやすくなることが考えられる．

7.2 評価

本節では，第 6 章で行った実装の評価について述べる．ここでは，評価として本システムを実際に使用して，異常を検知できたかや，その音に対する評価実験を行った．本節の最後に実験により得られた結果から，本システムについて考察を行う．

7.2.1 評価実験概要

実装したシステムと可聴化した音に対しての評価実験を行った．評価実験概要を図 7.9 に示す．本評価実験では，本システムの実際の運用を想定した評価を行った．被験者全員に一部屋に集め，スピーカーを通して 1 時間監視対象サーバの通信を可聴化した音を聴かせた．被験者には事前に知らせずに監視対象サーバに DoS 等の攻撃を仕掛け，その音の変化に被験者が気がつくかを検証した．また，ネットワーク異常の発生に気がついた被験者がどの様な行動を取るのかについても記録した．

実験中，音を流し続けた部屋内では，被験者には自由行動を許可した．ただし実験中の飲食，ヘッドフォンを使用した音楽や動画の鑑賞，PC の電源を切る，PC のネットワーク接続切断，極度の負荷がかかる行動，の 5 点の行動は禁止とした．また実験終了後，被験者が音を聴き続けてどう感じたかを生理学的視点や感性工学的視点から評価を取った．

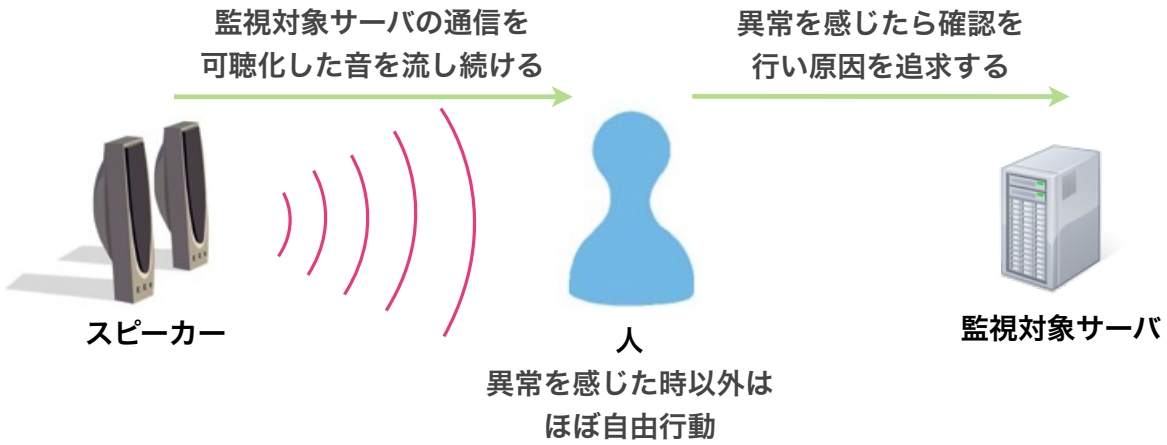


図 7.9: 評価実験概要図

本評価実験の参加人数と，実験期間について以下に述べる．

- 期間:2013 年 1 月 9 日 14 時 40 分-15 時 40 分
- 場所:慶應義塾大学湘南藤沢キャンパス デルタ館 North201[40]
- 参加人数:7 人
- 可聴化対象サーバ:isc.sfc.wide.ad.jp

また，参加した 7 人に対してネットワークに関しての知識と技術的背景について事前にアンケートを行った．その結果を以下に示す．アンケートでは，ネットワークに関しての知識と技術的背景を 5 段階で表した．アンケートの結果全ての被験者は，最低でも TCP/IP に関して一通りの知識があるとの回答が得られた．

質問	人数
1) ネットワークについての基本的な知識(IPアドレス等)を知らずインターネットを使用してWebサイトを閲覧する程度である	0
2) ネットワークについての基本的な知識(IPアドレス等)はあるがインターネットを使用してWebサイトを閲覧する程度である	0
3) TCP/IPに関しての一通りの知識はあるが, 自分でサーバの作成やサーバのネットワーク設定を行ったことはない	2
4) TCP/IPに関しての一通りの知識はあり, 自分でサーバ作成やサーバのネットワーク設定を行ったことがある	4
5) TCP/IPのプロトコルの詳細について知っており, 普段からネットワークの運用をしている	1

(回答者: 7 人)

図 7.10: 事前調査アンケート

評価実験の様子を図 7.11 に示す．

図 7.11: 評価実験の様子

7.2.2 評価実験の構成

行った評価実験の構成について述べる．本実験の構成を図 7.12 に示す．

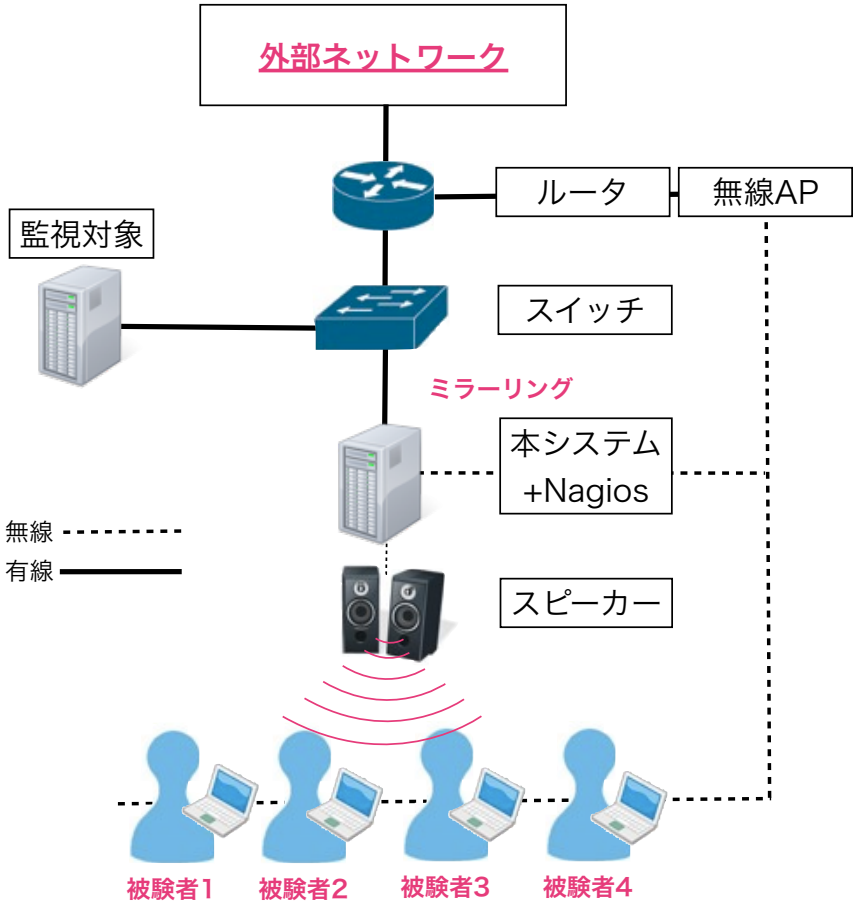


図 7.12: 評価実験構成図

監視対象サーバは，筆者が所属する大学の研究室ネットワーク内に設置されているサーバである．また，監視対象サーバの環境は， Ubuntu 12.04.1 LTS[41]/Linux 3.2.0-34-generic である．本実験では，監視対象のサーバが送受信している通信を本システムで可聴化するため，監視対象サーバの上流に属しているスイッチ (Catalyst 3750[42]) にてポートミラーリングを行った．また本システム以外でも，Nagios で監視対象サーバを監視した．本実験で，被験者が本システムでネットワーク異常を検知した場合，Nagios を使用して原因究明を行ってもらった．また，実際に監視対象サーバにログインして，原因究明を行ってもらうため，監視対象サーバには予め，被験者全員のアカウントを作成した．また，異常の原因究明を行って貰う PC は各自の物を使用した．

また本実験ではシステムに対する評価として，被験者がネットワーク異常によって起きた音に変化に対して，どのように行動するかを観察する．そのため，実験中に異常を発生させる通信を監視対象サーバに送信した．実験中の通信内容について，図 7.13 に示す．

具体的な通信内容に関して，被験者には事前に通知せずに実験を行った．実験前半の 30 分間は，被験者に正常な通信の音を学習して貰うため，ネットワーク異常を発生させる通信は行わなかった．そして実験後半の 30 分間，ネットワーク異常を発生させる通信を監視対象サーバに送信した．具体的には 15:20 時点にて，nmap[36] によるポートスキャン (Tcp connect スキャン) を行った．さらに，15:30 から 15:37 にかけて DoS (Slowloris)[37] を行った．

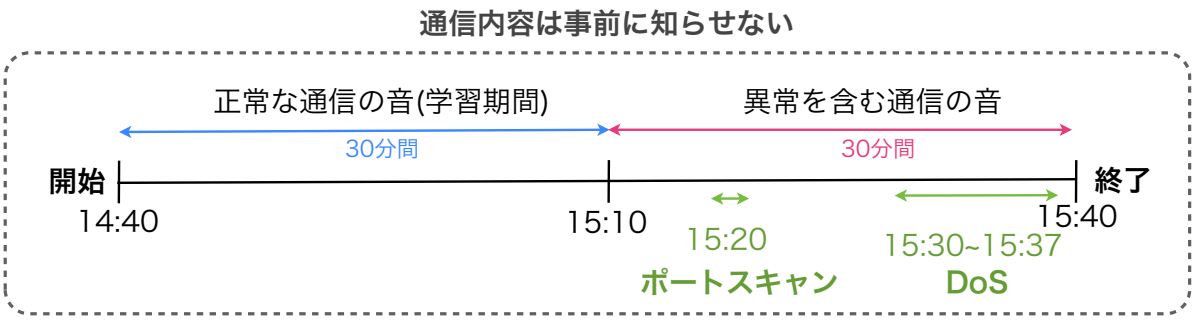


図 7.13: 監視対象サーバの通信内容

7.2.3 システムの評価

本実験では被験者が，本システムが出力する可聴化された通信の音に対して，どの様に行動するかの記録を取った．また被験者がネットワーク異常によって起こった音に変化に対して，どの様に行動するかの記録も取得した．本項では，それぞれの具体的な評価方法とその結果について述べる．そして得られた結果から，考察を行う．

被験者の行動

本システムに対する被験者の行動を定量的に判断するため，被験者はネットワーク異常を感じた際に Nagios や監視対象サーバにアクセスすることを事前に指示した．被験者が Nagios の Web インタフェースにアクセスした時間について図 7.14 に示す．図の縦軸が被験者であり，横軸がアクセス時間を示している．図からネットワーク異常が発生した際に，被験者がどのように行動したかを述べる．

まず (1) ポートスキャンが発生した 15:20 付近で，集中的にアクセスをした被験者は 1 と 2 だけであった．また被験者 1，2 は，ポートスキャンが発生する直前でも，集中的に Nagios にアクセスしている．そのため，被験者がポートスキャンによって引き起こされた音の変化から異常が検知出来たとは言い切れない．次に (2)Dos が発生した 15:00 から 15:37 付近では，被験者 1,2,3,5 が 15:00 を境に集中的にアクセスしてることが分かる．被験者 6 と 7 は Nagios にはアクセスしているものの，15:30 以前の行動と差異が見られなかった．

最後に実験全体を通して被験者がどのような行動を取ったか述べる．まず実験開始後の後半 30 分間は正常な通信のみであったにも関わらず，6 人の被験者が Nagios に複数回アクセスした．また 14:45 から 14:55 にかけて被験者が頻繁にアクセスしたことが分かる．さらに，実験全体を通して頻繁に Nagios にアクセスする被験者もいた．そして被験者 4 は，ネットワーク異常が発生した際に一度も Nagios にアクセスしていないことが分かる．

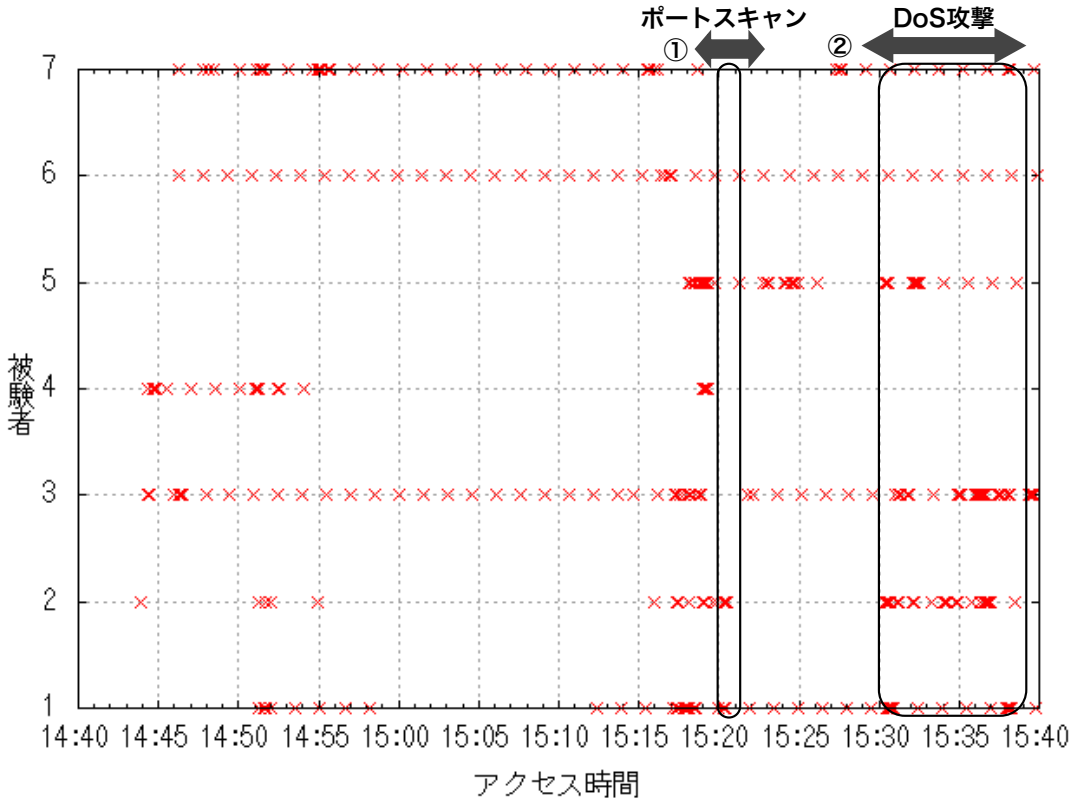


図 7.14: Nagios へのアクセス時間

被験者が監視対象サーバへログインした時間について図 7.15 に示す．図の縦軸が被験者であり，横軸が経過時間を示している．図 7.15 からネットワーク異常が発生した際に，被験者がどの様に行動したかを述べる．まず，各被験者がログインした時間は分散していることが分かった．また，ポートスキャンや DoS などのネットワーク異常が発生した直後に，被験者のログイン時間において特徴となるような箇所は見られなかった．さらに，被験者 6 に関しては実験中一度もログインした形跡が見られなかった．

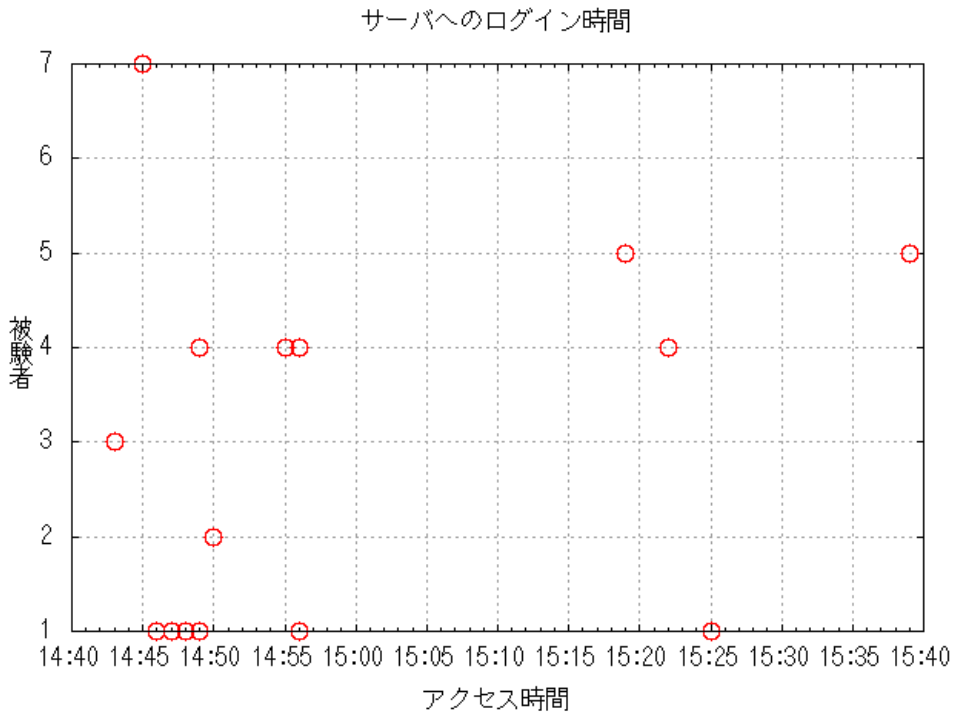


図 7.15: 監視サーバへのログイン時間

異常の検知

本項では，被験者が本システムで出力される音の変化によって発見できた異常について述べる．被験者には，各自が検知した異常について，その時間帯と推測した異常の原因を報告して貰った．本実験中では被験者 7 人中 4 人が異常があったと報告した．具体的な報告の内容について述べる．

まず，異常を感じたと報告した被験者について記述する．異常を感じたと報告した被験者全員が 15:30 分付近に何かしらのネットワーク異常が発生したと報告した．その報告された異常の原因の推察内容としては，原因不明が 1 件，ブルートフォースが 2 件，プロセス数の急上昇が 1 件であった．ネットワーク運用やサーバ作成の経験が無い被験者についても，15:30 分で発生した DoS 攻撃の発生を報告している．また，異常を報告した被験者の内 1 人は，15:16 分にブルートフォースがあったと報告しており，誤検知が発生していた．そして，15:20 分に発生したポートスキャンについて報告する被験者はいなかった．

次に，異常を報告しなかった被験者について述べる．異常を報告しなかった被験者は，7 人中 3 人である．被験者が異常を報告しなかった理由としては 2 点あった．1 点目としては，被験者が他のことに集中しており音の変化に気がつくことが出来なかった点である．そして 2 点目としては，正常な通信と異常な通信の見分けがつかなかった点である．2 点目の原因を被験者に調査した所，正常時の音の変化を聞き，異常が発生した判断し Nagios

等で確認を行った所，異常が発見出来なかったためであった．そのため，被験者の中での正常と異常の判断が曖昧になってしまったと考えられる．

考察

本評価実験の結果を踏まえ考察を行う．本実験結果から本提案手法による異常検知では以下の問題があると考えられる．第一に発生期間の短いネットワーク異常は音の変化も短いため，使用者に異常と判断されない，または異常を見逃される恐れが高いと考えられる．第二に使用者が，仕事や作業に集中している場合音の変化に対する認識が低下し，ネットワーク異常による音の変化に気がつかない恐れが高いと考えられる．

反対に DoS 攻撃などの長期間に渡る異常の場合は，音も長期的に変化し，異常として発見されやすいと考えられる．また，正常な通信による音の変化と，異常な通信による音の変化の判別は，個々の曖昧な判断に基づくと異常検知の精度にばらつきが出ることが分かった．そのため，本システムの実際の導入の際には，正常な通信を被験者に事前に学習させるのが好ましいと考えられる．

7.2.4 音の評価

本システムが出力する，可聴化された通信の音に対しての評価を，複数の手法を通じて行った．具体的には，生理学的評価方法，感性工学的評価，アンケート調査を行った．本項では，それぞれの具体的な評価方法と，その結果について述べる．最後に得られた結果から，考察を行う．

生理学的評価

可聴化された通信の音に対する人間の反応を，生理学的視点からの検証を行った．本実験では，生理学的な指標として，人間のストレス値を使用した．具体的には実験開始直後と，実験終了後の人間のストレス値の差から，音に対してストレス感じた度合いを計る．ストレス値を計測する方法として，唾液アミラーゼモニター (図 7.16) を使用した．唾液アミラーゼモニターとは株式会社ニプロが発売している，酵素分析装置のことである [43]．唾液中に含まれる消化酵素の一つである唾液アミラーゼを測定し，人間のストレス度合いを計る装置である．唾液中のアミラーゼ値は人間がストレスを感じると上昇し，リラックスすると下降する性質がある．測定されるアミラーゼの値には個人差がある．

図 7.16: 唾液アミラーゼモニター

本実験では，実験開始直後と実験終了後の被験者のストレスの値を測定した．その結果を図 7.17 に示す．

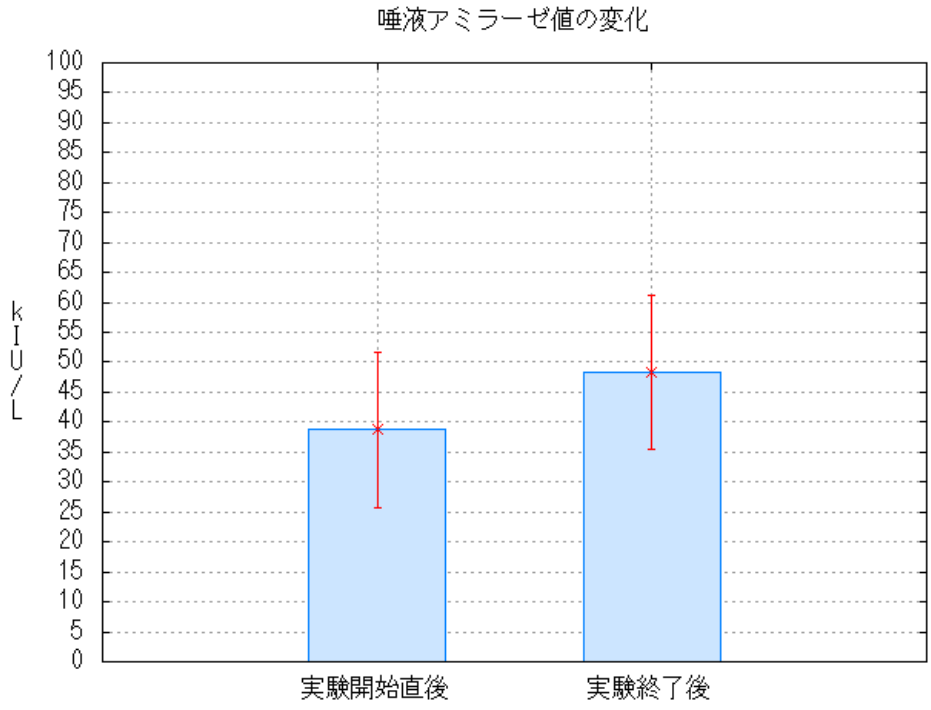


図 7.17: 唾液アミラーゼ値の変化

被験者 7 人のアミラーゼ値の平均値を棒グラフで，標準誤差をエラーバーで表現した．また，kIU/L とは，唾液 1 リットル中に含まれるアミラーゼの値を示している．k は Kg,

I は国際単位，U はユニットという意味である．実験開始直後の唾液中アミラーゼ値は 38.71kIU/L で，標準誤差は 13.02 であった．そして，実験終了後の唾液中アミラーゼ値の平均値は 48.28kIU/L で，標準誤差は 12.92 であった．

また，唾液中のアミラーゼ値に対応したストレス度合いの目安についてを表 7.3 にまとめた．実験開始直後では「ややストレスあり」だったストレスの度合いが，実験終了後には「ストレスあり」の段階に変化した．

表 7.3: ストレス値の目安

数値 (単位は kIU/L)	ストレス度合いの目安
0-30	ストレス無し
31-45	ややストレスあり
46-60	ストレスあり
61 以上	強いストレスあり

感性工学的評価

可聴化された通信の音に対する被験者の反応を，感性工学的な視点からの検証を行った．具体的には実験終了後に，SD 法と呼ばれる感性アンケートを行った．SD 法 [44] とは，semantic differential 法の略であり，心理学者オズグッド (C.E.Osgood) により考案された，感性を測定する方法である．様々なモノやコトなどに対するイメージや，それらから受ける感覚的刺激を計る方法である．SD 法では具体的に，反意語のある修飾語 (「明るい-暗い」等) を複数用意し，それらを両端に置いた多段階の評価尺度に対して評点を付けるということを行う．

本実験で使用した SD 法調査では，本システムの音に対して感じた評価を測定するため，使用する修飾語は「SD 法に用いる修飾語対の例」[44] から主に音に関係するものを選択した．評価尺度は 7 段階に設定し，評価項目として 20 個の修飾語を使用した．使用する修飾語に関しては SD 法テスト作成手順 [44] に従って評価性，力量性，活動性の修飾語対を決められた配置順序に配置した．また，本 SD 法のテストでは被験者の好みをより細かく把握出来るよう評価段階を 7 段階とした．SD 法で得られた結果から，プロフィール分析を行ったものを図 7.18 に示す．プロフィール分析とは，評価尺度ごとに評価者間の平均値を算出し，折れ線グラフで表現したものである．プロフィール分析を使用することで，評価対象に対するイメージが可視化出来る．

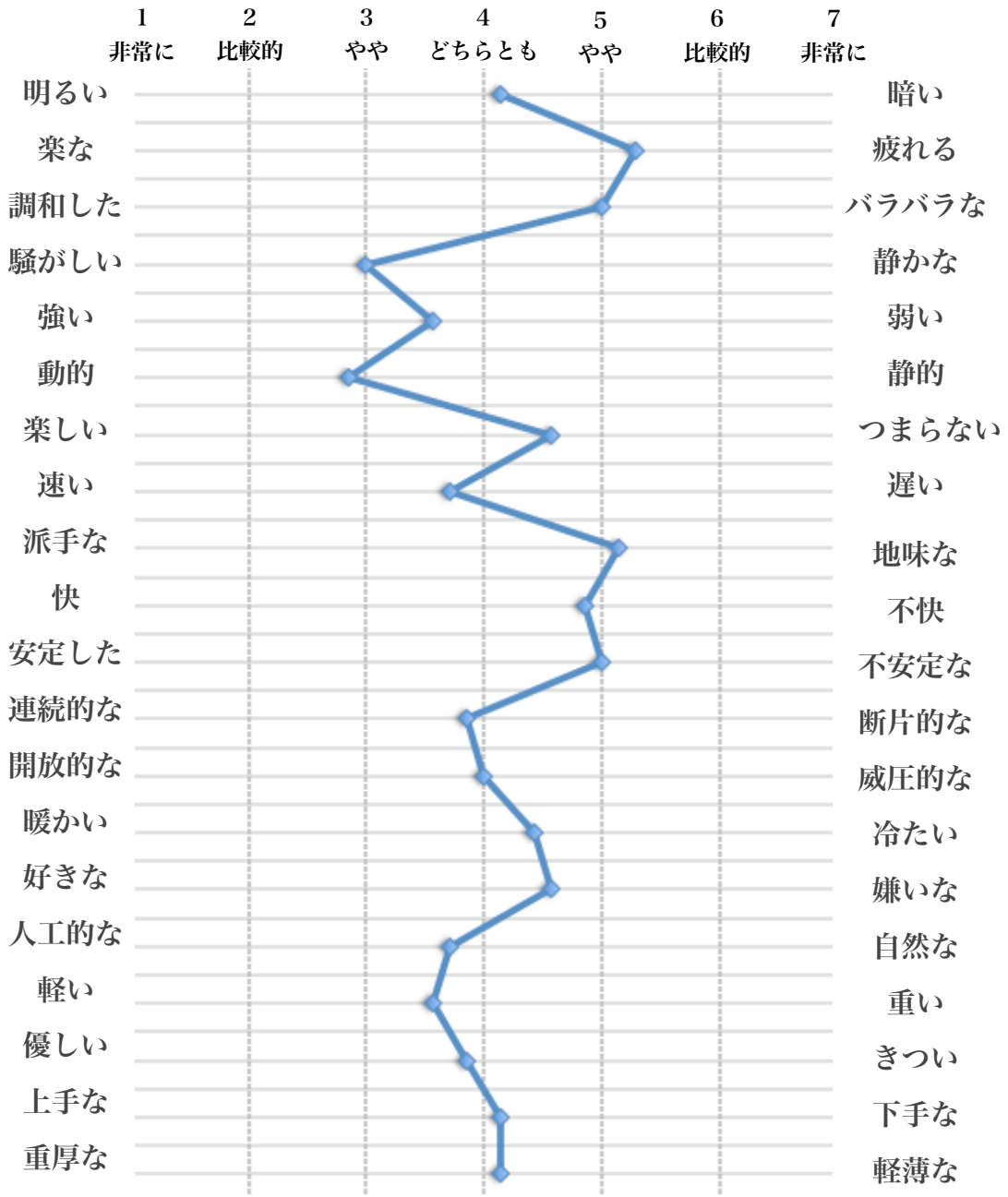


図 7.18: SD 法によるアンケート

SD 法のプロフィール分析によって得られた結果について述べる．全 20 項目の内 17 項目の平均値が 3 以上 5 以下の値で，区分としては「やや」「どちらでもない」の内になった．回答項目の中で，回答の平均値が 3 以上 5 以下の値にならなかった項目は「楽な-疲れる」「動的-静的」「派手な-地味な」の 3 項目であった．まず「楽な-疲れる」の項目の平均値は 5.28 であった．また「動的-静的」の項目の平均値は 2.85 であった．そして「派手な-地味な」の項目の平均値は 5.14 であった．本結果から，本システムが出力する音が動

的かつ地味な音であるため，被験者に疲労感を感じさせてしまったと考えられる．

5 段階評価アンケート

可聴化された通信の音に対してどう感じたかを，実験終了後に 5 段階評価アンケートで調査した．アンケートでは，音の聞き取り易さ，音の変化の明瞭性，システムの使用感や音の変化の主観的な感想を中心とした 5 つの質問事項を記述した．各質問事項に対して，「そう思わない」「ややそう思わない」「どちらでもない」「ややそう思う」「そう思う」の 5 段階を回答して貰った．5 段階評価アンケートの質問事項とその結果を図 7.19 に示す．それぞれの質問事項の回答に 1 から 5 までの値を付与して，各質問事項への回答の平均値と標準偏差を求めた．

(1.そう思わない 2.ややそう思わない 3.どちらでもない 4.ややそう思う 5.そう思う)

質問	平均値	標準偏差
1) 音は聞き取りやすかった	**4.0**	**0.53**
2) 音の変化は明瞭だった	**3.28**	**1.16**
3) 音を聞き続けることができた	**3.0**	**0.53**
4) 音の変化とネットワークの変化を自分の中で結びけることができた	**2.28**	**1.38**
5) 本システムの使用に疲労を感じた	**3.4**	**0.72**

(回答者: 7 人)

図 7.19: 5 段階アンケート評価

また 5 段階アンケート以外にも，自由記述で本システムについての感想を記述してもらった．書いてもらった感想に関しては，付録に掲載する．さらに本アンケート調査を行う際に使用した質問用紙も付録に掲載する．

考察

本システムが出力する音に対する評価データを踏まえ考察を行う．本システムが出力する音は疲労感は若干高いものの，音や音の変化自体は聞き取りやすかったと考えられる．音に対する疲労感の原因としては，動的かつ地味な音であるため，長時間聞くには不向き

と考えられる．そのため，より静的で柔らかい音を採用すれば，使用者の音に対する疲労感は軽減すると考えられる．

7.3 全体の考察

提案手法の検証と，システムに対する評価を踏まえた上で，考察を行う．まず，ネットワーク通信を音の要素に変換し，その音の変化を聞くことによってネットワーク異常の検知をするという提案手法の有効性を示す事が出来た．また，出力する音も，使用者にとって聞き取り易くかつ音の変化も分かり易いものが実現できた．さらに，ネットワークに詳しくない使用者でもネットワーク異常を発見することが出来た．

だたし，本システムの実際の運用については課題が残る．まず，実運用中ではポートスキャンなど発生期間が短い異常は見逃されやすいことが分かった．また他の作業に集中していると音を聞いてるにも関わらず，音の変化に対する認識力が低下し，ネットワーク異常の発見が出来ない場合があることが分かった．さらに，長時間音を聞き続けることによって使用者は疲労を感じることが分かった．

7.4 まとめ

本章では，まず第 4 章で提案した手法に関しての検証を行った．検証のために検証実験を行い，その実験結果について述べた．また，得られたデータの有意性についても述べた．その後，実験結果から考察を行った．次に，第 6 章で実装したシステムの評価と，可聴化通信に対する音の評価を行った．そして最後に，得られた評価に対しての考察を行った．

第8章　結論

本章では，本研究を行った背景や提案した手法についてまとめる．その後，第 1.2 節で示した目的の中で達成された部分を述べる．最後に，本論文の結果を踏まえ，本研究の今後の展望について記述する．

8.1　まとめ

本研究では，通信の情報を主に音の要素 (音高・音量・音色) に変換することで、音の変化により通信状態の変化を直感的に理解できるネットワーク異常検知手法を実現した．

既存のネットワーク異常検知システムは，そのシステムを利用する上で様々なコストがかかる問題がある．例えば，システムを使用してネットワークの状況を把握するには，事前に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，ネットワーク異常の把握には時間や手間などを要する．さらに，ネットワーク監視のため監視画面を凝視する必要がある．

そこで本論文ではネットワーク監視コスト軽減を目的として，通信の情報を主に音の要素 (音高・音量・音色) に変換することで、音の変化により通信状態の変化を直感的に理解できるネットワーク異常検知手法を提案した．提案手法による直感的なネットワーク異常検知とは，事前に正常状態のネットワークが起こす音の変化を，人が感覚的に把握することによって，ネットワーク異常の発生に伴う音の変化を聞いた時に，その音の違いから直感的にネットワーク異常を検知する手法である．既存の音による異常検知システムは，パケット情報やフロー情報に対して特定の楽器音や自然音に割り当てていたため，使用者は事前に音の割当を学ばなければならず直感的に使用できなかった．

本手法の提案に伴い、本手法を実現するシステムを設計・実装した．そして本実装が有効であることを示すため，検知精度や出力する音に対しての多角的な検証・評価を実施した．その結果，事前知識が無くとも，音の変化のみでネットワーク異常検知が行えることを実証した．本研究により，ネットワークの知識やネットワーク異常検知のソフトウェアの利用経験がない者でも直感的な異常検知が可能となった．また，ネットワーク監視画面を凝視し続ける必要がなくなった．これにより，ネットワークの総合的な監視コストが軽減された．

8.2 今後の展望

本研究の展望について述べる．本研究の今後の展望としては，ネットワーク異常発生時の認識の向上と，使用者に負担がかからない音の使用が挙げられる．

8.2.1 ネットワーク異常発生時の認識の向上

本システムを使用することで，音の変化を聴くのみでネットワーク異常検知が行えることができた．しかし，実運用上でのネットワーク異常の検知精度に関してはまだ課題が残る．その理由の 1 つとして，使用者が音を聞きながら別の作業等に集中している場合，音の変化に対する認識が低下することが挙げられる．そのため，今後の展望としては，異常発生時の音をより「異常であると」認識しやすくする必要があると考えられる．

8.2.2 使用者に負担がかからない音

本システムが出力する可聴化された通信の音は，その音や音の変化自体は聞き取り易く，ネットワーク異常も検知することが出来た．また，1 時間程度なら本システムが出力した音を聞き続けることに大きな問題はなかった．しかし，動的かつ地味な音であるため，長時間聴くと，使用者に疲労感を感じさせた．また疲労感に伴い使用者のストレス値も向上させてしまった．そのため，長時間の使用に不向きであった．そこで，今後の展望としては，より使用者に負担のかかりにくい音の使用が考えられる．

謝辞

本論文の執筆にあたり，ご指導頂いた慶應義塾大学環境情報学部学部長 村井 純博士，同学部教授 徳田 英幸博士，同学部教授 中村 修博士，同学部准教授 楠本 博之博士，同学部准教授 高汐 一紀博士，同学部准教授 三次 仁博士，同学部准教授 植原 啓介博士，同学部専任講師 中澤 仁博士，同学部准教授 Rodney D.Van Meter III 博士，同学部教授 武田 圭史博士，同大学政策・メディア研究科 特任講師斉藤 賢爾博士，同研究科特任講師 佐藤 雅明博士，同研究科特任講師吉藤 英明氏に感謝致します．

特に武田圭史博士は，入学当初から熱心に研究指導をしてくださり，研究に行き詰まった際も的確な助言と叱咤激励を頂きました．また研究指導だけではなく，今後の人生を生きる上での多くの大切なことを教わりました．重ねて感謝申し上げます．

そして慶應義塾大学政策・メディア研究科卒業生の水谷 正慶博士，上原 雄貴氏，重松 邦彦氏，六田 圭祐氏，金井 瑛氏，同学科博士課程永山 翔太氏， 岡田 耕司氏，堀場 勝広氏，慶應義塾大学卒業生の朝永 愛子氏に感謝致します．研究の仕方や論文の書き方，その他研究を進める上での様々なことを教わりました．また常に先輩として模範となるべき姿を示してくださいました．本当に感謝致します．大学卒業後も先輩達の様な人間に少しでも近づけるよう精進したいと思います．また，大学院受験や自身の論文執筆，そしてインターンシップで多忙であるにも関わらず，常に親身になって研究相談に乗って頂いた同学科修士課程の碓井 利宣氏に感謝致します．

また慶應義塾大学卒業生の福岡 英哲氏，相見 眞男氏，Doan Viet Tung 氏，梅田 昴翔氏，吉原 洋樹氏，Vu Xuan Duong 氏，Pham Van Hung 氏，同大学政策・メディア研究科修士課程の小澤みゆき氏，加藤 碧氏，石崎 香織氏，関根 冬輝氏，山本 知典氏に感謝致します．同じ時期に研究室に所属し，時には同僚として，そして時には人生の先輩として，私の研究室生活を支えていただきました．

国際医療福祉大学三田病院眼科 綾木雅彦氏に感謝致します．本研究の評価実験を行うに当たって，実験に使用する機器を貸して頂き，感謝致します．また，生理学的な知見からの意見を頂き，大変お世話になりました．

村井研究室秘書の 渡辺 康恵 氏，比嘉 宏美 氏，宇佐美 由美子 氏，青木 りか氏，渋谷 雪絵 氏に感謝します．研究生活において，書類の提出や発表会のスケジュール調整など，様々な場面で本当にお世話になりました．ありがとうございました．

研究室で苦楽を共し，共に卒業論文を執筆した鴻野 弘明氏，小松 真氏，有馬 怜文氏，吉原 大道氏，由井 卓哉氏，Nguyen Anh Tien 氏に感謝致します．同じ学問の分野の仲間として切磋琢磨することが出来ました．また彼らのお陰で研究室での生活が非常に楽しいものとなりました．卒業後もぜひまた遊んでいただければと思います．そして研究室で共に生活を送った，藤原 龍氏，大矢 崇夫氏，澁田 拓也氏，山岸 祐大氏，倉田 彩子氏，後上 峻一氏，小澤 麗氏，露木 航平氏，中安 恒樹氏．水谷 伊織氏，廣田 一貴氏，川本 卓也氏，八木橋 優氏，村田 紘司氏，福山 翔一郎氏，三條場 直希氏に感謝致します．彼らと一緒に過ごすことで多くの事が得られました．

また，研究に協力をしていただいた，佐藤 文啓氏，大野 三津夫氏，恩田 優氏，高岡 賢二氏，星出 直柔氏，三ツ木 あかね氏，上原 英則氏，深谷 哲史氏，吉田 裕氏，原 雄太氏，生方 悠介氏，武田 知也氏，深澤 匠氏，山田 夏才氏，芹澤 親氏 Tran Ngoc Anh 氏，高橋 直道氏，小澤巧治氏，桜井 祐揮氏，越光 祐也氏，塚越 広彬氏，丸山 祐輝氏に感謝申し上げます．研究に対する様々な視点からの意見や指摘は非常に参考になりました．皆様の指摘のお陰で，研究がより良くなりました．

徳田・村井・楠本・中村・高汐・バンミーター・植原・三次・中澤・武田合同研究プロジェクトの皆様に感謝いたします．皆様のお陰で，非常に楽しい 4 年間を過ごすことが出来ました．特に 1 年生の時から研究会に所属していた私にとって，研究室で過ごした時間は，私の大学生活そのものと言っても過言ではありません．本当に感謝申し上げます．

また，デルタ館に生息している猫 (社長，専務，常務，平) に感謝申し上げます．研究に疲れた時に私の心を優しく癒してくれました．研究室の生活で，楽しい時も辛い時もいつもそばに居てくれ，本当に感謝申し上げます．特に猫 (社長) には入学当初からデルタ館の先輩として大変お世話になりました．もう会えないのが残念ですが，卒業後もお参りに行きます．

CNS コンサルタントの皆様に感謝致します．特に，岩崎久美子氏，池垣 雅子氏，郷津 加奈子氏，橋場 友秀氏，後藤 洋紀氏，満友 佳乃氏，薄井 唯氏，千葉 智史氏，菊池 幹生氏，山田 加奈氏に感謝致します．彼らのお陰で研究室以外の学生生活が大変豊かなものとなりました．個性的なメンバーのため，研究室では絶対聴けないような興味深い話をすることが出来ました．また，勤務の際にも何かと助けて頂きましたこと，重ねて感謝申し上げます．

最後に，大学入学からの 4 年間だけでなく 22 年間をあらゆる面で支えていただいた父，中島 賢二，母，中島 まき，兄，中島宏文に心から感謝致します．

以上を持って謝辞といたします．本当にありがとうございました．

参考文献

[1] 総務省総合通信基盤局電気通信事業部データ通信課. 我が国のインターネットにおけるトラヒック総量の把握. http://www.soumu.go.jp/main_content/000149220.pdf, 3 2012.

[2] Cisco. Cisco visual networking index: Global mobile data traffic forecast update, 2011 2016. http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.pdf, 2 2012.

[3] 一般財団法人 日本情報経済社会推進協会. 情報化白書 2012. http://books.shoeisha.co.jp/book/b94669.html, 11 2011.

[4] 経済産業省. 平成２３年情報処理実態調査報告書の概要. http://www.meti.go.jp/press/2012/07/20120718001/20120718001-2.pdf, 7 2012.

[5] 総務省. 平成２３年通信利用動向調査の結果. http://www.soumu.go.jp/johotsusintokei/statistics/data/120530_1.pdf, 5 2012.

[6] Ethan Galstad. Nagios. http://www.nagios.org/, 5 2002.

[7] Icinga. https://www.icinga.org/, 5 2009.

[8] Martin Roesch. Snort. http://www.snort.org/, 1998.

[9] Steven McCanne Van Jacobson, Craig Leres. Tcpdump. http://www.tcpdump.org/, 1987.

[10] Gerald Combs. Wireshark. http://www.wireshark.org/, 6 2006.

[11] Arindam Banerjee Varun Chandola and Vipin Kumar. Anomaly detection:a survey. *ACM Computing Surveys(CSUR)*, 41(15):15:1–15:58, 7 2009.

[12] Paul Barford and David Plonka. Characteristics of network traffic flow anomalies, 2001.

[13] 水谷 正慶. 通信の相関関係を利用したネットワークセキュリティ監視手法, 2007.

[14] Hiroshi Ishii and Brygg Ullmer. Tangible bits: towards seamless interfaces between people, bits and atoms, 1997.

[15] International conference on auditory display. http://www.icad.org/, 10 1992.

[16] William W. Gaver. The sonicfinder: an interface that uses auditory icons. *Hum.-Comput. Interact.*, 4(1):67–94, 3 1989.

[17] シャープ株式会社. Cocorobo. http://www.sharp.co.jp/cocorobo/product/v100/, 6 2012.

[18] Inc. Siri. Siri. http://www.apple.com/ios/siri/, 4 2011.

[19] 和氣 早苗. **ヒューマンインターフェースにおける聴覚メディアの利用-聴覚ディスプレイのデザイン**-. PhD thesis, 大阪大学大学院基礎工学研究科, 2003.

[20] Bruce N. Walker and Michael A. Nees. Theory of sonification. http://sonification.de/handbook/download/TheSonificationHandbook-chapter2.pdf, 11 2011.

[21] Hiroyuki Ohno Masahiko Kimoto. Design and implementation of stetho:network sonification system, 9 2002.

[22] Zhigang Peng. Earthquake sound of the mw9.0 tohoku-oki, japan earthquake. http://geophysics.eas.gatech.edu/people/zpeng/Japan_20110311/, 2012.

[23] Marty Quinn. Music of the earth, sun, planet and space volume one. http://www.drsrl.com/datamusic/volume-1/datamusic.html, 2005.

[24] A. Santis M. Barra, T. Cillo. Webmelody: Soni cation of web servers, 2000.

[25] Alva L. Couch Michael Gilfix. Peep (the network auralizer): Monitoring your network with sound, 12 2000.

[26] Rob McCool. Apache. http://httpd.apache.org/, 1995.

[27] Lei Qi, Miguel Vargas Martin, Bill Kapralos, Mark Green, and Miguel Garcia Ruiz. Toward sound-assisted intrusion detection systems. 2007.

[28] 岩宮眞一郎. **図解入門最新音楽の科学がよくわかる本ー音楽と人とのかかわりを科学的に考察する**. 秀和システム, 2012.

[29] John G.Neuhoff. Perception, cognition and action in auditory displays. http://sonification.de/handbook/download/TheSonificationHandbook-chapter4.pdf, 11 2011.

[30] Apple Inc. Macosx 10.7. http://www.apple.com/jp/osx/, 2011.

[31] Bjarne Stroustrup. C++, 1983.

[32] Jr Leonard H. Tower. Gnu compiler collection. http://gcc.gnu.org/, 1987.

[33] Google. gflags. http://code.google.com/p/gflags/, 2008.

[34] Lawrence Berkely Laboratory. Libpcap version 1.15. http://sourceforge.net/projects/libpcap/, 2008.

[35] Perry R. Cook and Gary P. Scavone. The synthesis toolkit. https://ccrma.stanford.edu/software/stk/, 1995.

[36] Gordon Lyon. nmap. http://nmap.org/, 9 1997.

[37] RSnake. Slowloris. http://ha.ckers.org/slowloris/, 6 2009.

[38] The Audacity Team. Audacity. http://audacity.sourceforge.net, 5 2000.

[39] William Sealy Gosset. T 検定. http://www.encyclopediaofmath.org/index.php/Student_test, 1908.

[40] 慶應義塾大学. 湘南藤沢キャンパス デルタ館. http://www.keio.ac.jp/ja/access/sfc.html, 1990.

[41] Ltd. Canonical. Ubuntu 12.04. http://www.ubuntu.com/, 10 2004.

[42] Inc Cisco Systems. Catalyst3750. http://www.cisco.com/web/JP/product/hs/switches/cat3750/index.html, 8 2003.

[43] ニプロ株式会社. 唾液アミラーゼモニター. http://www.nipro.co.jp/ja/news/2007/document/071217_2.php, 12 2007.

[44] 長沢信也 and 神田太樹 共編. **数理的感性工学の基礎 -感性商品開発へのアプローチ-**. 海文堂, 2010.

付録 A アンケート調査用紙

本研究の評価実験後に行ったアンケート調査に使用した用紙を掲載する.

アンケート調査

氏名＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

【本調査について】

ご記入頂いた内容は卒業論文以外で使用することはありません。氏名は、アンケートご協力の御礼に卒論の謝辞に本アンケート協力者氏名を掲載したいと考えているため、ご記入お願いします。また、本アンケートで分からない事があったら、質問してください。

■事前調査

・貴方のネットワークに関しての知識と経験についてお聞きします。
(選択肢の中で 1 つに○を付けてください)

1） ネットワークについての基本的な知識(IP アドレス等)を知らず、
インターネットを使用して Web サイト閲覧する程度である。

2） ネットワークについての基本的な知識(IP アドレス等)はあるが、
インターネットを使用して Web サイト閲覧する程度である。

3） TCP/IP に関しての一通りの知識はあるが、
自分でサーバの作成や、サーバのネットワーク設定を行ったことはない。

4） TCP/IP に関しての一通りの知識はあり、
自分でサーバ作成や、サーバのネットワーク設定を行った事がある。

5） TCP/IP のプロトコルの詳細について知っており、
普段からネットワークの運用をしている。

■ SD 法調査(感性アンケート)

これから、本システムに対する印象や感情的なイメージを SD(セマンティックでファレンシャル)法を用いて調査します。各項目の中で当てはまるもの 1 つに○をつけてください。率直に貴方が感じたままに記入してください。

	1 非常に	2 比較的	3 やや	4 どちらとも	5 やや	6 比較的	7 非常に	
明るい	---	----------	----------	----------	----------	----------	----------	--- 暗い
楽な	---	----------	----------	----------	----------	----------	----------	--- 疲れる
調和した	---	----------	----------	----------	----------	----------	----------	--- バラバラな

	1 非常に	2 比較的	3 やや	4 どちらとも	5 やや	6 比較的	7 非常に	
騒がしい								静かな
強い								弱い
動的								静的
楽しい								つまらない
速い								遅い
派手な								地味な
快								不快
安定した								不安定な
連続的な								断片的な
開放的な								威圧的な
暖かい								冷たい
好きな								嫌いな
人工的な								自然な
軽い								重い
優しい								きつい
上手な								下手な
重厚な								軽薄な

■５段階評価アンケート(感想)

これから、本システムについての５段階評価アンケートに回答していただきます。率直に貴方が感じたままに記入してください。

1）音は聞き取りやすかった

1.そう思う　2.ややそう思う　3.どちらでもない　4.ややそう思わない　5.そう思わない

2) 音の変化は明瞭だった

1.そう思う　2.ややそう思う　3.どちらでもない　4.ややそう思わない　5.そう思わない

3　音を聞き続ける事ができた

1.そう思う　2.ややそう思う　3.どちらでもない　4.ややそう思わない　5.そう思わない

4) 音の変化とネットワークの変化を自分の中で結びつける事ができた

1.そう思う　2.ややそう思う　3.どちらでもない　4.ややそう思わない　5.そう思わない

5) 本システムの使用に疲労を感じた

1.そう思う　2.ややそう思う　3.どちらでもない　4.ややそう思わない　5.そう思わない

■コメント

本システムに対する感想・意見・批判等、忌憚のない意見をご記入ください。

アンケート調査はここで終了です。
貴重なお時間を頂き、アンケート調査にご協力していただきありがとうございました。

付録B アンケート調査結果

- 聞きやすく，分かりやすいが，音がつまらなく機械的に感じた.
- 作業に集中していると異常を見逃してしまった.
- 「単一の音」の連続であり，メロディィがない.
- もっと良い高音質のライブラリを使うだけでストレスはだいぶ変わりそう.
- 何をすればよいのか分かりにくかった部分がありました.
- 音は特に不快さを感じませんでした.
- 音はもう少し明るい調子のほうがやりやすく感じた.
- 音よりもシステムのチェックのほうが大変だと感じた.
- 「あれ？なにか障害発生しているのかな？」と何回か思ったが，実際に nagios,log 等見ても何も出ていなかったので，なにが問題だったのか分からなかった.
- もう少し，テンポが軽快だと良いと思いました.
- ORF のピアノのは良かったと思います.
- もうちょっと長いスパンで実験 (1 week とか) 出来るといいと思います.
- 前説明なしの状態からだと，異常がどの音のときなのか明確に判別できないのではないでしょうか.

付録C ポスター発表資料

Grace Hopper Celebration 2011

Design and Implementation of a Network Traffic Sonification System for Anomaly Detection

Asuka Nakajima†, Kunihiko Shigematu‡, Masayoshi Mizutani §, Keiji Takeda†, Jun Murai†

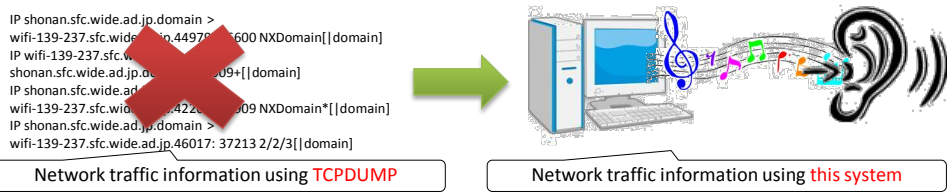
† Keio University Faculty of Environment and Information Studies, Japan

‡Keio University Graduate School of Media & Governance, Japan

§ Tokyo Research Laboratory, IBM Research, Japan

Purpose & Method

Facilitate the understanding of network state, including detection of abnormal traffic, by representing network state as sound



Functional Requirements

Versatile user interface

This system basically runs on a web browser, which is installed in most computers by default.

Sounds that are not uncomfortable

Applying comfortable sound is a necessary factor for this system.

Ability to represent abnormal state

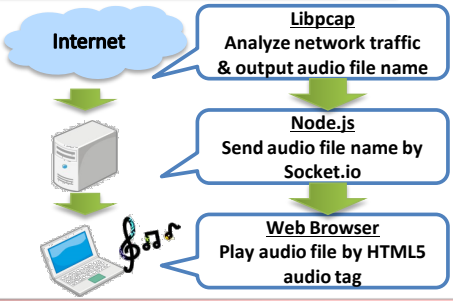
This system records network traffic data, when it is steady state.

Sonification Method

Allocate instrument sound to Packet size & Port number information

Data	Packet size	Port number
Melody	Main Melody	Sub Melody
Instrument	Piano 	Xylophone・Bell 

Implementation

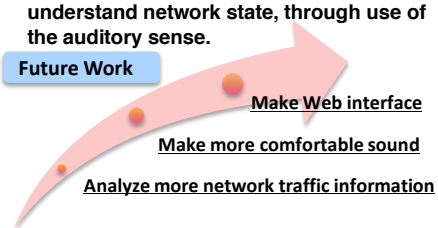


Summary & Future Work

Summary

Implemented a system which allow user to understand network state, through use of the auditory sense.

Future Work



Grace Hopper Celebration 2011

付録D ポスター発表資料