通信トラヒックを用いたIoTデバイスの機能実行制御システムに関する研究

服部 祐一

目次

内容梗概 1

第 1 章　はじめに 3

1.1　家庭用 IoT デバイスにおける課題 4

1.2　課題に対するアプローチ 5

1.3　研究分野と貢献 6

1.4　本論文の構成 8

第 2 章　関連研究 9

2.1　ユビキタスコンピューティングに関する研究 9

2.1.1　Internet of Things に関する研究 10

2.1.2　スマートホームにおける IoT 11

2.2　IoT のセキュリティに関する研究 11

2.2.1　通信トラヒック分析によるマルウェアの検出 12

2.2.2　IoT 通信のプライバシーに関する脆弱性を示す研究 12

2.2.3　スマートホームの利用者のセキュリティとプライバシーの懸念を示す研究 13

2.3　ネットワークゲートウェイを用いたセキュリティシステム 13

2.3.1　通信の検知システムにおける課題 14

2.3.2　IoT デバイスの機能ごとのアクセス制御の重要性 14

2.3.3 スマートフォンのパーミッション設定とスマートホームのパーミッション設定の比較 . . . 15
2.4 通信トラヒック分析による IoT デバイスの推定 . . . 16
2.4.1 IoT デバイスの通信トラヒックに含まれる個人に関する情報の課題 . . . 17
2.4.2 IoT デバイスの通信方法 . . . 17
2.5 まとめ . . . 18

第 3 章 家庭内の IoT デバイスを安心・安全に利用するための IoT 活動量計の提案 19

3.1 はじめに . . . 19
3.2 システム設計 . . . 20
3.3 アクセス制御の概念 . . . 21
3.4 他のシステムとの違い . . . 22
3.5 システム構成 . . . 23
3.5.1 エッジルーター . . . 24
3.5.2 管理システム . . . 24
3.6 IoT デバイスの実行機能のアクセスポリシー . . . 25
3.7 シナリオを元にしたアクセスポリシー . . . 25
3.8 アクセスポリシーと識別モデルの共有 . . . 27
3.9 IoT デバイスと実行機能の識別 . . . 28
3.10 評価 . . . 28
3.10.1 IoT 活動量計の環境 . . . 28
3.10.2 アクセスポリシーの生成 . . . 28
3.10.3 アクセス制御の評価 . . . 29
3.11 議論 . . . 31
3.11.1 IoT デバイスのファームウェアの更新の影響 . . . 31
3.11.2 同じ接続先を持つ異なる機能 . . . 31

3.11.3 利用者の生活様式の変化 31
3.11.4 異なるプロトコルによる制御 32
3.11.5 宛先 IP の変更 32
3.11.6 IoT 活動量計を運用の問題 32
3.12 まとめ 33

第 4 章 通信トラヒック分析による IoT デバイスの機能推定手法の評価 34

4.1 はじめに 34
4.2 データセット 35
4.2.1 通信トラヒックの収集環境 35
4.2.2 通信トラヒックの収集方法 36
4.2.3 通信トラヒックの加工方法 37
4.2.4 通信トラヒックの評価 38
4.3 通信トラヒック分析による IoT デバイスにおける機能推定手法 39
4.3.1 機能推定手法 39
4.3.2 評価 42
4.3.3 議論 44
IoT デバイスの設定による影響 45
IoT デバイスのファームウェアの更新による影響 46
同じ機能を持つ異なる IoT デバイスの機種の通信トラヒックの類似性 . 47
通信トラヒックが似た機能 48
デバイスや機能の増加による影響 48
4.3.4 まとめ 48
4.4 通信トラヒック分析による数秒間隔での IoT デバイスの機能推定手法 49
4.4.1 機能推定手法 49
4.4.2 評価 50

4.4.3 議論 51
IoT デバイスの設定の影響 51
IoT デバイスのファームウェアの更新による影響 51
利用者の行動に関わらず実行される機能 51
通信トラヒックが似た機能 51
IoT 活動量計の実現に必要な精度 52
4.4.4 まとめ 52

第 5 章 議論と今後の展望 63

5.1 議論 63
5.1.1 実行機能の分類に用いる特徴量 64
5.1.2 IoT デバイスのファームウェアの更新による影響 64
5.1.3 利用者の行動に関わらず実行される機能 65
5.1.4 通信トラヒックが似た機能 65
5.1.5 IoT 活動量計の実現に必要な精度 65
5.1.6 IoT 活動量計を運用の問題 66
5.2 今後の展望 66
5.2.1 IoT デバイスの種別と機能を増やしての評価 66
5.2.2 利用者の行動と関係ない機能の推定 67
5.2.3 他の行動認識技術との連携 67
5.2.4 実際の環境での IoT 活動量計の評価 68

第 6 章 まとめ 69

謝辞 72

参考文献 73

図目次

1.1 既存研究と本研究の通信トラヒックの制御の差異 7
1.2 既存研究と本研究の IoT デバイスの分類の差異 8

3.1 IoT 活動量計の概要 21
3.2 アクセスポリシーと識別モデルの生成の概要 23
3.3 管理システムのデバイス一覧画面 26
3.4 管理システムのシナリオ編集画面 27
3.5 PoC のシステム構成 29

4.1 通信トラヒックの収集環境の構成図 36
4.2 Mi 360° : スマートカメラの散布図マトリクス (1: 静止状態, 2: 話しかける, 3: カメラの向きを変える) 40
4.3 SwitchBot Hub Mini: スマートリモコンの散布図マトリクス (1: 静止状態,2:TV を ON にする,3:TV を OFF にする) 41
4.4 Nature Remo: スマートリモコンの散布図マトリクス (1: 静止状態,2:TV を ON にする,3:TV を OFF にする) 42
4.5 各機種の特徴量の重要度 (スマートカメラ) 57
4.6 各機種の特徴量の重要度 (スマートスピーカー) 58
4.7 各機種の特徴量の重要度 (スマートリモコン) 59
4.8 各機種の特徴量の重要度 (スマートプラグ) 60

表目次

2.1 IDS/IPS と異常検知システムの比較 14
2.2 IoT デバイスの機能の例 15

3.1 IDS/IPS，異常検知システムと提案システムの比較 22
3.2 一つの機能を無効にした場合の，他の機能の動作確認結果 (Amazon Echo Show) 30
3.3 一つの機能を無効にした場合の，他の機能の動作確認結果 (SwitchBot) 30

4.1 通信トラヒックの収集に利用した IoT デバイス一覧 37
4.2 収集した通信トラヒックの機能一覧 38
4.3 評価値の一覧 (1 秒) 39
4.4 利用した特徴量一覧 43
4.5 利用した特徴量一覧 (続き) 44
4.6 機能推定結果の混同行列 (IoT デバイスの機種と実行機能の組み合わせの 16 通り) 45
4.7 機能推定結果の混同行列 (IoT デバイスの機種と実行機能の組み合わせの 16 通り) である表 4.6 のクラスラベル 46
4.8 機能推定結果の混同行列 (実行機能のみの 8 通り) 47
4.9 機能推定結果の混同行列 (実行機能のみの 8 通り) である表 4.8 のクラスラベル 47
4.10 計算した特徴量 54

4.11 計算した特徴量 (続き) 55
4.12 計算した特徴量 (続き) 56
4.13 実行機能推定結果の混同行列
(Ranger 2: スマートカメラ) 61
4.14 実行機能推定結果の混同行列
(Mi 360°: スマートカメラ) 61
4.15 実行機能推定結果の混同行列
(SwitchBot Hub Mini: スマートリモコン) 61
4.16 実行機能推定結果の混同行列
(Nature Remo: スマートリモコン) 61
4.17 実行機能推定結果の混同行列
(Amazon Echo Show: スマートスピーカー) 61
4.18 実行機能推定結果の混同行列
(Google Home Mini: スマートスピーカー) 61
4.19 実行機能推定結果の混同行列
(SwitchBot プラグ: スマートプラグ) 61
4.20 実行機能推定結果の混同行列
(WiFi スマートプラグ: スマートプラグ) 61
4.21 実行機能推定結果の混同行列である表 4.13-表 4.20 のクラスラベル 62
4.22 各デバイスの分類精度一覧 62

内容梗概

本論文では，家庭向けの IoT デバイスに関するセキュリティ上の問題を解決し IoT デバイスを安心・安全に利用するために，通信トラヒックを用いて IoT デバイスの実行機能を分類し，通信トラヒックを制御する IoT 活動量計を提案する．また，IoT 活動量計の実現のための通信トラヒックから抽出した個人を特定できる情報を含まない特徴量での IoT デバイスの実行機能の推定手法について提案と評価を行う．

1 章では，本研究の背景と目的について述べる．課題である IoT デバイスがどのような通信を行っているかを検知し，それをもとに適切な通信のみ許可し通信トラヒックを制御することと通信トラヒックから抽出した個人を特定できる情報を含まない特徴量での IoT デバイスの実行機能を推定することについて概要と貢献を述べる．

2 章では，ユビキタスコンピューティングに関わる研究について述べるとともに，関連研究と本研究の立ち位置について述べる．

3 章では，家庭内の IoT デバイスを安心・安全に利用するための IoT 活動量計と呼ばれるフレームワークを提案し，PoC を実施しその結果を報告する．提案システムでは，事前に収集した通信トラヒックから生成したアクセス制御を用いて，一部の IoT デバイスの特定の機能を許可／拒否することができ，本提案が有益であることを示した．

4 章では，IoT 活動量計の実現のために必要な通信トラヒックの分析のために収集した日本国内で流通しているスマートスピーカー，スマートカメラ，スマートリモコン，スマートプラグの 4 種別の IoT デバイス各 2 機種ずつの計 8 機種の 8 種類の機能の通信トラヒックとその収集方法について述べ，その通信トラヒックを用いた 2 種類の機能推定手法についての評価結

果を述べる．一つは，機能実行時の全通信トラヒックから特徴量を計算し，個人や特定の製造元を特定できる情報を含まない 28 個の特徴量を用いて，ランダムフォレストアルゴリズムによる分類を行い，その精度を IoT デバイスの機種と実行機能の組み合わせ 16 種類と実行機能のみの組み合わせ 8 種類の計 2 種類で評価した．一つは，8 つの IoT デバイスに対して静止を含む 3 種類の機能の推定を 1 秒ごとの特徴量を用いて，ランダムフォレストアルゴリズムで IoT デバイスの機能の実行状態を推定し，その精度を評価した．そして，8 機種のうち 5 機種は 83% 以上の精度で分類できた．また，残りの 3 機種については，通信トラヒックのみからの分類は難しいということを考察として述べ，提案手法において，5 機種において一定の精度で IoT デバイスの実行機能が分類できることを示した．

5 章では，得られた知見から，今後 IoT 活動量計を実現させていくうえで考慮していく必要がある考察を行い，今後の展望と課題について述べる．今後，家庭内の IoT デバイスを安心・安全に利用するための IoT 活動量計の実現に向けて，IoT デバイスの種別と機能を増やしての評価や既存の行動認識技術と連携することによる通信トラヒックから分類することが難しい実行機能に対する分類の検討を行い，スマートホームを模した環境などの実際の環境に近い形での実験を行い IoT 活動量計が実際の環境で動作するかを検証していく必要がある．

6 章はまとめであり，本研究を総括している．

以上のように本研究では，家庭内の IoT デバイスを安心・安全に利用するための IoT 活動量計を提案し，その PoC を行い一部の IoT デバイスについて想定する動作が実行できることを確認した．また，IoT 活動量計の実現のための通信トラヒックから抽出した個人を特定できる情報を含まない特徴量での IoT デバイスの実行機能の推定手法について提案と評価を行い 8 機種のうち 5 機種は 83% 以上の精度で分類できたが，残りの 3 機種については，通信トラヒックのみからの分類は難しいということが分かった．

第 1 章

はじめに

近年，IoT デバイスが一般家庭に普及し，様々な機能を持った IoT デバイスが販売され，様々なシーンで活用されている．総務省の調査によると，2021 年の世界の IoT デバイス数は約 292 億台で，2025 年には約 440 億台まで増加すると予測されている [1]．例えば，家庭で使用される有名な IoT デバイスには，Google Home[2] や Amazon Echo[3] などのスマートスピーカーがある．これらのデバイスには音声ユーザーインターフェース (VUI)[4] が搭載されており，利用者は音声を使ってインターネット検索や家電の操作，音楽再生など様々な機能を実行できる．また，一部のデバイスにはカメラが搭載されており，他の IoT デバイスやスマートフォンとのビデオ通話が可能である．ネットワークカメラもホームセンターや通販サイトで手軽に購入でき，スマートフォンやスマートスピーカーと組み合わせて，子どもの見守りや防犯などに活用されている．これらの IoT デバイスは，基本的にクラウドと連携するように設計されており，その機能によってスマートフォンなどと連携することができる．これらの IoT デバイスは，家庭内の無線ネットワークを介してクラウド上にあるサーバーなどに接続され，デバイスが生成する情報を収集・分析することでサービスを提供する．利用者は主にスマートフォンからこれらのシステムに接続し，デバイスの操作や情報の閲覧ができる．

1.1　家庭用 IoT デバイスにおける課題

IoT デバイスは，インターネットに接続することを前提としているため，セキュリティの面で多くの問題があり，様々な個人情報の漏えいや利用者の同意なしに IoT デバイスの提供元以外のサービスに情報を送信する事案などが発生している．例えば，スマート掃除機に搭載されたカメラに家庭内を盗聴できる脆弱性が発見されたり [5]，家庭用ルーターが第三者の提供するサービスとの連携機能を管理画面上から OFF にした場合でも，第三者宛に情報を送信していることが確認されている [6]．また最近，IoT デバイスを狙った攻撃が増加している．例えば，Zhang ら [7]，Chakraborty ら [8]，Mao ら [9] は，人間には聞こえない音を使って IoT デバイスに接続し，遠隔操作している．2016 年には，Mirai と呼ばれる IoT デバイスに対するマルウェア [10] が流行し，攻撃者が感染したデバイスを用いて大規模な DDoS 攻撃を行った [11]．また，Mirai の亜種も複数確認されており，IoT デバイスは攻撃の脅威にさらされている [12]．独立行政法人情報通信研究機構 (NICT) が無差別サイバー攻撃の全体動向の把握を目的に実施しているサイバー攻撃観測・分析システム「NICTER」[13] の 2023 年度観測報告によると，数年前から Mirai 亜種などの活発な IoT ボット感染活動が観測されており，国内のホスト数はピーク時で約 9000 台に増加している [14]．また，インターネット上の IP に対するスキャンという行為は 2018 年以降増加の一歩をたどっており，2023 年の調査目的スキャンの通信パケット数は，観測された全通信パケット数の約 63.8% を占めている [14]．また，それらのスキャン元は脅威情報提供サービスなどがあり，NICTER の調査で判明している送信元については，Github 上に公開されている [15]. それらのスキャン行為の結果の一つとして認証のかかっていない IoT カメラの動画像情報の第三者からの閲覧などがある [16].IoT デバイスは，安価で容易に設置できる反面，正しくセキュリティの設定やファームウェアの更新を行わないとセキュリティ上の脅威にさらされることになる．

IoT デバイスの普及により我々の生活は便利になるが，これらの IoT デバイスの使用に伴うセキュリティへの配慮も重要である．特に，以下の 3 点に注意する必要がある．

1. IoT デバイスの様々な製品が存在し，すべてのデバイスのセキュリティを継続的に更新することは困難である．大企業が製造するデバイスは，定期的にファームウェアの更新やサポートを受けられる可能性が高いが，中小企業が製造するデバイスは，サービスの早期終了 [17] や企業自体の倒産などの要因により，ファームウェアの更新やサポートが受けられなくなる可能性がある．例として，実際にサポートの切れたルーターの脆弱性では，修正パッチが提供されずに後継機への乗り換えを推奨されている [18][19][20].
2. IoT デバイスの動作はブラックボックスであり，多くの場合，デバイスがどの情報をどこに送信するかという情報を利用者が把握することはできない．最近では，テレビ会議システムである Zoom の事件のように，ネットワーク通信が特定の国を経由している場合があることが判明している [21].
3. IoT デバイスは，PC と異なり，ウイルス対策ソフトなどの不正検知システムを利用者が導入することができない.

1.2　課題に対するアプローチ

我々は，上記の問題を解決するために，IoT デバイスがどのような通信を行っているかを検知し，それをもとに適切な通信のみ許可することができる通信トラヒックを制御する機能と IoT デバイスがどのような通信を行っているか可視化することで利用者が IoT デバイスの動作状況を理解することを可能にする機能を持つプラットフォームである IoT 活動量計を提案する．IoT 活動量計の実現手段として我々は，IoT デバイスの通信トラヒックに着目し，そのパターンから IoT デバイスの機種及び IoT デバイスでどのような機能が実行されているかを推定し，その結果をもとに通信トラヒックを制御する．既存の研究では，IoT デバイスの機器ごとの通信トラヒックの制御はあるが IoT デバイスが実行する機能単位での通信トラヒックの制御は新しい．機能単位での実行を制御することができれば，悪意のあるマルウェアによる通信などの利用者の想定していない通信も防ぐことができる．また，家庭での利用を想定した場

合，例えば，深夜に子供がスマートスピーカーを使って友人とビデオ通話をするという状況を親が制限させたい場合に，既存の手法であれば，スマートスピーカーの通信を全て遮断することになるが，IoT 活動量計を使い，夜中にスマートスピーカーでビデオ通話の機能の通信を遮断する設定を入れればスマートスピーカーの音楽再生などのビデオ通話以外の機能は利用可能な状態のまま，ビデオ通話の通信のみを遮断できる．また，IoT デバイスの機能の実行の可否の設定を，スマートフォンのパーミッション設定のように機能ごとに通信の可否を可視化し，簡単に設定できる機能を提案している．また，通信トラヒックだけでは推定できないものを考慮して既存のスマートホームに設置されるセンサから得られる情報と連携して通信を制御する機能も提供する．IoT 活動量計が家庭に導入されれば，利用者が家庭に設置された IoT デバイスの状況を容易に理解することができるとともに，それらの機能単位での制御を行うことにより，家庭内の IoT デバイスを安心・安全に利用することができるようになる．

1.3　研究分野と貢献

本論文で紹介する研究は，ユビキタスコンピューティングの分野で重要な研究であり，様々な外部からの攻撃にさらされている家庭における IoT デバイスの安心・安全な利用を実現するうえで重要な研究といえる．現在，IoT デバイスは様々なデバイスが実用化されており，家庭においてもスマートスピーカーやスマートキー，スマートリモコンなど様々な IoT デバイスが利用されている．一方ほとんどの IoT デバイスはインターネットとの通信が必要であり，その為，ネットワークに関連した脅威にさらされている．下記に本研究の貢献についてまとめる．

1. IoT デバイスがどのような通信を行っているかを検知し，それをもとに適切な通信のみ許可し通信トラヒックを制御するプラットフォームである IoT 活動量計を提案する．

   貢献: 本提案によって IoT デバイスが適切な通信のみを行うことができ，IoT デバイスが利用者の意図しない通信を行うというセキュリティ上の問題を解決することができ，家庭内における IoT デバイスの安心・安全な使用を実現することができる．既存研究と

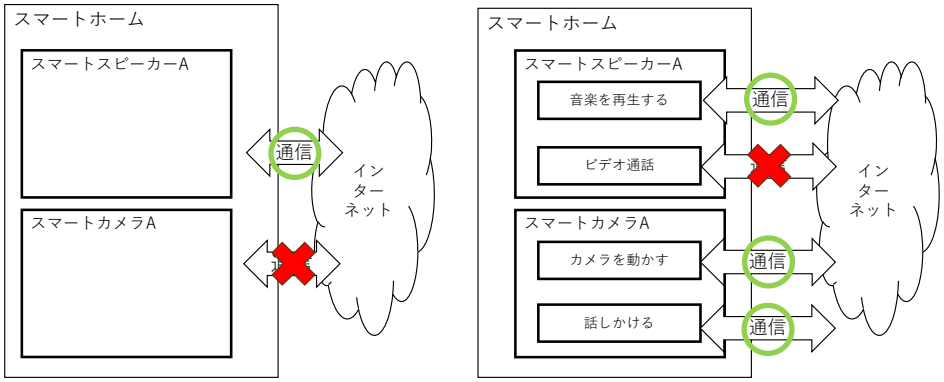

図 1.1: 既存研究と本研究の通信トラヒックの制御の差異

本研究の通信トラヒックの制御の差異を図 1.1 に示す.

2. 通信トラヒックから抽出した個人を特定できる情報を含まない特徴量で IoT デバイスの実行機能を推定する.

   貢献: 通信トラヒックからの IoT デバイスの機種の推定は多く行われているが，複数の IoT デバイスの通信トラヒックのデータセットを用いた IoT デバイスの実行機能の推定は新しい．既存研究と本研究の IoT デバイスの分類の差異を図 1.2 に示す．また，機能実行中のすべての通信トラヒックを使うのではなく，数秒間隔での IoT デバイスの実行機能の推定を行うことは，通信状況の可視化や通信許可などに活用することができる．また，利用者の意図しない通信を遮断するためには，利用者の意図する実行機能の推定を行うことが重要である.

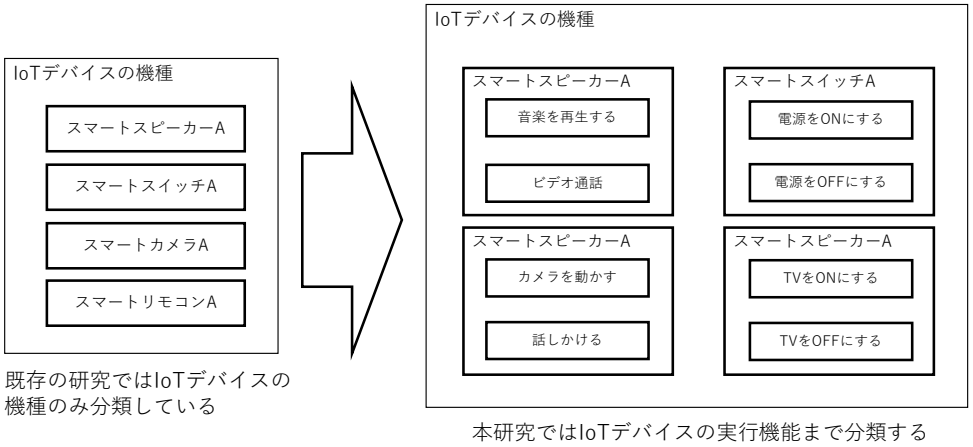

図 1.2: 既存研究と本研究の IoT デバイスの分類の差異

1.4　本論文の構成

本論文の構成は以下の通りである．2 章では，本研究で扱う問題に関連する分野であるユビキタスコンピューティング，Internet of Things などについて説明し，IoT デバイスの通信制御と実行機能の分類に関係する関連研究について述べる．3 章では，我々が提案する家庭内の IoT デバイスを安心・安全に利用するための IoT 活動量計の研究について述べる．4 章では，IoT 活動量計を実現するための通信トラヒック分析による IoT デバイスの実行機能の推定手法の評価について述べる．5 章で議論と今後の展望について述べ，6 章でまとめる．

第 2 章

関連研究

スマートホームや IoT デバイスに関する研究は様々なものがある．本章では，関連のあるユビキタスコンピューティングや IoT，スマートホームについて説明し，IoT デバイスの識別とプライバシーに関する関連研究について述べる．そして，我々が提案する IoT デバイスの実行機能での制御機能をもつプラットフォームの必要性と，それを実現するための IoT デバイスの実行機能の分類の必要性について述べる．

2.1 ユビキタスコンピューティングに関する研究

ユビキタスコンピューティングという概念は，1989 年に米 Xerox 社パロアルト研究所の Mark Weiser が提唱した概念である [22]．ユビキタスコンピューティングでは，あらゆるものにコンピューターが組み込まれこれらが分散協調処理を行うことによって人間のあらゆる活動をサポートし，また，コンピューターが日々の生活環境と区別がつかないほど，その中に溶け込み見えなくなるものとなる．ユビキタスコンピューティングの実現には，様々な技術の発展が必要であり，様々な研究がおこなわれている．主な研究分野である 3 つを下記に述べる．

1. 情報の収集

   情報の収集に関する研究分野では，ウェアラブルセンシング [23] や，センサネットワーク [24] などの研究分野がある．スマートフォンや IoT デバイスが普及しているおかげ

で様々なセンサデータを収集することが可能になったが，実環境でのセンサデータの収集は，収集したセンサデータに対するラベル付けや継続的にセンサデータを収集するための利用者の動機づけの維持などの課題がある [25][26].

2. 収集したデータの分析

   収集したデータの分析に関する研究分野では，収集した様々なデータに対する分析を行う．大量のセンサデータや通信トラヒックを人間がデータを眺めて分析することは，データが少量であれば可能な場合もあるがデータが大量となる場合は不可能である．そのため，機械学習を用いてデータ分析を行う．分析するデータは収集された情報によって様々であり，農業においては，農家作業技術を数値化し分析するもの [27] やリモートセンシングによって農地診断情報を分析するもの [28]，介護では介護施設のコールセンターの記録を分析するもの [29] や介護記録を分析するもの [30]，医療では，看護師の介護行動を分析するもの [31][32]，スマートホームでは，スマートホーム内のセンサデータから宅内での行動生起の時点を分析するもの [33] や生活行動のデータを分析するもの [34] など様々である．

3. 分析結果の応用

   分析結果の応用では，実世界に分析結果を応用する研究分野であり，応用先によって様々な研究がある．例えば，介護分野であれば転倒検知システム [35] や介護記録の自動化 [36] などがあり，スマートホーム分野であれば，個人識別システム [37] や日常生活の認識 [38] などがある．我々の提案している IoT 活動量計は，スマートホームの分野で用いられることを想定している．

2.1.1　Internet of Things に関する研究

IoT(Internet of Things) とは，モノのインターネットと呼ばれ従来ネットワークに接続されていなかったあらゆるモノがインターネットに接続され相互に繋がる仕組みである．様々なモノがインターネットと繋がることにより，様々な工場機材のセンサや人工知能技術を活用し

たスマートファクトリー [39] やビル内に設置されたセンサから人流などを分析し，空調や照明を制御するスマートビル [40]，ビニールハウスでの環境センサなどを用いて環境制御などを行うスマート農業 [41] といった業務用途から，エアコンや照明の自動操作，遠隔での鍵の開閉といった家庭での利用まで幅広い用途で利用されている．総務省の調査によると，2021 年の世界の IoT デバイス数は約 292 億台で，2025 年には約 440 億台まで増加すると予測されている [1]．家庭用の IoT デバイスは，ホームセンターや通販サイトで手軽に購入できるほど普及しており，設置についてもスマートフォンを使った簡単な操作で行うことができる．また，IoT デバイスのセキュリティ上の問題は年々増加しており，IoT デバイスの開発の面に対しても独立行政法人情報処理推進機構から「IoT 開発におけるセキュリティ設計の手引き」が公開されている [42].

2.1.2　スマートホームにおける IoT

スマートホームとは，子育て世代，高齢者などの様々な生活様式や需要に合ったサービスを IoT により実現する新しい暮らしである [43]．様々な家電や IT 機器などのあらゆるデバイスがネットワークに接続されることにより，家電の遠隔操作，家族の見守り，防犯などの様々なサービスを実現することができる．その実現のために IoT デバイスは必要不可欠であり，あらゆるデバイスがネットワークに接続されるため，それらがネットワーク経由の脅威にさらされる恐れがある．そのため，それらを安心・安全に利用する仕組みも必要となるため，本研究では，IoT デバイスを安心・安全に利用するための IoT 活動量計を提案している．

2.2　IoT のセキュリティに関する研究

IoT のセキュリティについては，マルウェアに感染した IoT デバイスを検知する研究やそれらを利用する利用者のプライバシーの問題に関する研究がある．

2.2.1　通信トラヒック分析によるマルウェアの検出

通信トラヒックの分析は，マルウェアの検出にもよく使われる．

Bendiab ら [44] は，新しいマルウェアの検出と分類を高速化するために，深層学習と視覚表現を用いた新しい IoT マルウェアの通信トラヒック分析のアプローチを提案している．彼らは，異なる通信トラヒックから収集された，正常な通信トラヒックとマルウェアの通信トラヒックの 1000 個の pcap ファイルからなるデータセットを作成し，それらを分析した結果，マルウェアの通信トラヒックを 94.50% の精度で検出した．

Nobakht ら [45] は，DEMD-IoT(Deep Ensemble Malware Detection for IoT) と呼ばれる，深層学習とアンサンブル学習アルゴリズムに基づく高度で知的な IoT マルウェア検出モデルを提案した．彼らは，IoT 通信トラヒックを含む IoT-23 データセットを使用して DEMD-IoT を評価し，その結果，99.9% の精度を達成した．

本研究では，悪意のある通信を検知するのではなく，IoT デバイスの正常な実行機能の通信トラヒックを分類する．通信トラヒックから正常な実行機能を分類することで，利用者が必要な通信をより適切に制御できる環境を構築することを目指す．

2.2.2　IoT 通信のプライバシーに関する脆弱性を示す研究

Apthorpe ら [46] は，暗号化された IoT デバイスの通信のプライバシーに関する脆弱性を報告した．市販の IoT デバイス 4 機種 (睡眠モニター:Sense，室内用防犯カメラ:Nest Cam，リモートスイッチ:Wemo，スマートスピーカー:Amazon Echo) の通信トラヒックを分析し，暗号化された通信トラヒックの送受信レートから利用者の行動を把握できることを実証し，新しいプライバシーの脅威を利用者に与えることを警鐘している．攻撃者から利用者の行動を推定できないように通信トラヒックを保護することは重要だが，セキュリティ監視のために活動情報を可視化し，利用者に報告することも重要なことである．

Dong ら [47] は，スマートホームのネットワーク上で発生する通信トラヒックから個人情報

がどのように漏えいするかを調査し，通信パケット間の時間的関係を利用したデバイス識別のフレームワークを提案し，高い精度でデバイス種別の識別を行った．それにより，IoT ネットワークの通信は，暗号化で保護されている場合やネットワークゲートウェイで加工されている場合でも利用者のプライバシーに対して大きな課題があることを示唆している．

これら研究の結果から利用者に利用している IoT デバイスの状態を可視化し提供することは利用者のデバイスのセキュリティに対する意識を高めることに貢献できるため，我々の提案する IoTIoT 活動量計では，IoT デバイスの状態を可視化することを提案している．

2.2.3　スマートホームの利用者のセキュリティとプライバシーの懸念を示す研究

Zeng ら [48] は，スマートホームを利用する利用者のセキュリティとプライバシーに関する懸念について研究している．彼らは，スマートホームに住む 15 人にインタビューを行い，スマートホームの利用方法とセキュリティやプライバシーに関する意識，期待，行動などを調査した．その結果，利用者はスマートホームデバイスのセキュリティに特に関心を持っていないと結論づけた．しかし，デバイス情報の可視化システムを構築することで，利用者のデバイス関連のセキュリティへの関心を高めることができる可能性があるとしている．

2.3　ネットワークゲートウェイを用いたセキュリティシステム

Miettinen ら [49] は，ネットワークに接続された IoT デバイスの種類を自動的に特定し，脆弱なデバイスの通信を制限することにより，被害を最小限に抑えることができるシステムを提案した．しかし，彼らの提案は，個々のデバイスの種類に固有の通信動作をプロファイリングすることで IoT デバイスを特定し，IoT デバイスの推定結果に基づいて脆弱なデバイスの通信を制御するものである．しかし，この研究では，IoT デバイスの機能に応じた通信の制御は行っていない．我々は，IoT デバイスの機能単位での通信の制御を行うことを提案している．その実現のためには，IoT デバイスの実行機能の特定を行う必要がある．

表 2.1: IDS/IPS と異常検知システムの比較

	IDS/IPS	**異常検知システム**
デバイスでのアクセス制御	あり	あり
DDoS[51] の防御	あり	あり
既知の攻撃 [52] の防御	あり	部分的
ゼロデイ攻撃 [53] の防御	なし	部分的

2.3.1　通信の検知システムにおける課題

通信の検知システムは，様々なものがある．情報セキュリティ分野での代表的なものとして通信を監視し，不正な通信を検知する不正侵入検知システム (IDS) やそれに加えて通信の遮断まで行う不正侵入防止システム (IPS) がある．オープンソースの IDS/IPS としては，Snort[50] が有名である．また，人工知能を活用して平常時の状態を学習し平常時から外れた場合を異常として検知する異常検知システムがある．IDS/IPS と異常検知システムの比較を図 2.1 に示す．これらの通信の検知システムでは，IoT デバイスの実行機能ごとのアクセス制御は行われていない．本研究では，IoT デバイスの実行機能を推定し，IoT デバイスの実行機能ごとのアクセス制御を行う．

2.3.2　IoT デバイスの機能ごとのアクセス制御の重要性

IoT デバイスには，デバイスの種類によって様々な機能が実装されている．例えば，スマートスピーカーであれば，利用者が音声で指示することによって音楽を再生する機能やビデオ通話の機能などがある．また，IoT デバイスには，利用者の指示がなくとも実行される機能も存在する．例えば，時刻同期やファームウェアの更新といった IoT デバイス自身が定期的に実行する機能である．IoT デバイスの機能の例を表 2.2 に示す．これらの IoT デバイスの機能を分類することは，重要な課題であるが，既存の研究では IoT デバイスの識別が主であり，IoT デ

表 2.2: IoT デバイスの機能の例

利用者の行動に紐づく機能の例	利用者の行動と関係ない機能の例
ビデオ通話	ファームウェアの更新
家電の操作	時刻同期
音楽の再生	ログの送信
電源の操作	死活監視
ニュースの再生	センサデータの送信

バイスの実行機能の推定は行われていない．特定の IoT デバイスの機種の実行機能をすべて推定できれば，その IoT デバイスで必要な通信トラヒックを全て把握できることになるため，利用者の意図しない通信トラヒックであるマルウェアの通信などを遮断することに繋がる．

2.3.3　スマートフォンのパーミッション設定とスマートホームのパーミッション設定の比較

スマートフォンの利用するリソース (通信，センサ，外部ストレージなど) の管理は，プライバシーやセキュリティの観点からも重要な課題である．現在，スマートフォンのパーミッションは可視化されており，アプリケーションごとにパーミッションを設定する方法と，パーミッションごとにアプリケーションを設定する方法の 2 種類で管理することが可能である．また，Android 端末のパーミッションには，「常に許可 (位置情報のみ)」，「毎回確認」，「アプリの使用中のみ許可」，「許可しない」の 4 種類がある [54]． 過去に，利用者の同意なしにアプリケーションが位置情報を取得し，プライバシー上の問題があったため，このような機能が実装された．スマートホームにとって，IoT デバイスは，スマートフォンのアプリケーションに相当するものである．スマートホームの場合，かつてのスマートフォンと同様，様々な製造元が開発した IoT デバイスが混在しており，どの IoT デバイスが何をしているのかを把握することが困難である．また，IoT デバイスが不必要かつ利用者の許可なく第三者の通信先と通信してい

る可能性があることも問題である [6]．つまり，現在のスマートフォンと同様に，スマートホームでも IoT デバイスごとに実行する機能を制御することが必要である．我々の提案する IoT 活動量計では，IoT デバイスごとに実行する機能を制御することを提案している．

このように，IoT デバイスごとの通信の制御を行う研究はあるが，IoT デバイスの機能に応じた通信の制御は行われていない．我々は，IoT デバイスの機能単位での通信の制御を行うことを提案している．その実現のためには，IoT デバイスの実行機能の特定を行う必要がある．

2.4　通信トラヒック分析による IoT デバイスの推定

本研究では，IoT デバイスの通信トラヒックを解析することで実行機能を推定しているが，先行研究として IoT デバイスの識別手法が研究されている．

Meidan ら [55] は，機械学習を用いた通信トラヒックの解析による IoT デバイスと非 IoT デバイスの識別方法を提案した．彼らは，Wi-Fi に接続されたデバイスの通信トラヒック情報を含む保存ファイルを解析し，送信元アドレス，送信先アドレス，ポート番号などの特徴を抽象化し，教師あり機械学習を用いて 2 段階でデバイスを識別している．第 1 段階では，IoT デバイスであるか否かを識別しており，第 2 段階では，予め登録された IoT デバイスの一覧から IoT デバイスの種類を特定した．その結果，99% の精度で IoT デバイスの種類を特定した．

Sivanathan ら [56] は，スマートシティとキャンパス内における IoT デバイスの識別方法を提案した．キャンパス内に 21 台の IoT デバイスを設置し，3 週間の通信トラヒックを収集した．そして，通信トラヒック (トラヒック負荷，信号パターン，活性時間と非活性時間の分布など) を分析し，教師あり学習アルゴリズムを用いてデバイスを識別した．その結果，95 %の精度で IoT デバイスの種類を特定した．Sivanathan ら [57] は，モジュラーデバイス分類アーキテクチャを開発し，教師なしクラスタリング手法を使用し，実際の IoT デバイスの通信トラヒックを使用して 94% 以上の精度で 10 種類のデバイスを識別した． また彼らは，実際の IoT デバイスの通信トラヒックを使用して 12 種類のデバイスに対して 94% 以上の精度で行動

の変化を検出するクラスタリングモデルによるモジュラーデバイス分類アーキテクチャを開発した [58].

これらの研究では，高い精度で IoT デバイスの機種を特定し，また，IoT デバイスの行動の変化の検出を行っている．しかし，これらの研究では，IoT デバイスの機能の分類は行っていない．本研究では，IoT デバイスの実行機能の特定を行う．

2.4.1　IoT デバイスの通信トラヒックに含まれる個人に関する情報の課題

IoT デバイスの通信トラヒックには，宛先 IP アドレスや MAC アドレスなど，個人や製造元に関連する情報が含まれている．また，多くの場合，IoT デバイスはクラウド上のサーバーと WebAPI を通して通信を行っている．通常は，クラウド上のサーバーと WebAPI の通信の内容には，利用者のアカウント情報やアクセストークンといった重要情報が含まれることがある．そのため，これらの情報は学習に使わない形で特徴量を選定する必要がある．本研究では，通信トラヒックのパケット数やパケットサイズといった量に関する特徴量のみを利用することでこれらの情報を学習に使わない手法で分類を行う．

2.4.2　IoT デバイスの通信方法

多くの IoT デバイスは，インターネットと接続することによって，遠隔での家電の操作や音楽の再生といった機能を提供している．それらの通信は HTTPS などの技術によって暗号化されて通信されている．これは，通信トラヒックが暗号化されずに行われた場合，途中の経路で通信トラヒックの中身を把握することができ，その中に重要な情報が含まれている場合，その情報が漏えいする恐れがあるためである．ネットワークのセキュリティ製品の中には暗号化している通信トラヒックを復号化して中身を確認し，セキュリティ上の問題がないか確認する Web プロキシなどのセキュリティ製品がある．オープンソースの Web プロキシとしては，Squid[59] が有名である．これらの製品は，Web プロキシが生成するサーバ証明書のルート証明書をあらかじめ対象の PC などに導入することによって復号化を実現している．通常の IoT

デバイスではそれらを導入することは容易ではないため，通信の中身まで確認して機能を分類することは現実的ではない．そのため，我々が提案している手法である通信トラヒックから抽出した個人を特定できる情報を含まない特徴量での IoT デバイスの実行機能の推定は，IoT デバイスに対して証明書の導入などの特殊な操作を行う必要がないため，IoT 活動量計を実際に一般家庭に設置すると考えた場合に理にかなっている．

このように，通信トラヒックから高い精度で IoT デバイスの機種を特定する研究は多くあるが，IoT デバイスの機能の分類は行われていない．本研究では，通信トラヒックから IoT デバイスの実行機能の特定を行う．

2.5　まとめ

IoT デバイスに限らず通信トラヒックを制御してセキュリティ上の脅威に対応する製品や提案は多くあるが，IoT デバイスの実行機能に対する制御を行う仕組みはない．そのため，我々は，家庭内の IoT デバイスを安心・安全に利用するために IoT 活動量計というプラットフォームを提案する．また，通信トラヒックから IoT デバイスの機種を判別する試みは多くあるが，複数の IoT デバイスの通信トラヒックのデータセットを用いた IoT デバイスの実行機能の推定は新しい．また，機能実行中のすべての通信トラヒックを使うのではなく，数秒間隔での IoT デバイスの実行機能の推定を行うことで，通信状況の可視化や通信許可などに活用することができる．

第 3 章

家庭内の IoT デバイスを安心・安全に利用するための IoT 活動量計の提案

本章では参考文献 [60] を引用し，提案している家庭内の IoT デバイスを安心・安全に利用するための IoT 活動量計のシステム設計や実現方法について述べる．

3.1 はじめに

1 章で述べた IoT デバイスに関する問題は，IoT デバイスの必要な機能のみに通信を許可する制御を行うことで解決できる．本研究では，家庭内の IoT デバイスを安全に利用するための IoT 活動量計と呼ばれるフレームワークを提案する．IoT 活動量計は，通信トラヒックのパターン分析に基づいて IoT デバイスの種類とその実行機能を特定し，家庭内のどの IoT デバイスがどのような通信を行っているかを利用者が把握できるようにする．同時に，その機能に関連する通信を一時的または恒久的に遮断するなどの操作をスマートフォンから簡単に制御できる．スマートフォンの権限は可視化され，管理することができる．家庭内の IoT デバイスに対して，スマートフォンアプリごとに権限を設定することを提案する．また，スマートフォンの権限設定と同様に，機能ごとに権限を可視化し，簡単に設定できる機能を提案する．

1. 家庭内における IoT デバイスの安心・安全な使用を保証すること

我々は，家庭内における IoT デバイスの安心・安全な使用を保証するために，IoT 活動量計と呼ばれるフレームワークを提案する．IoT 活動量計は，スマートフォンのアプリケーションの権限設定のように，IoT デバイスの実行機能の権限を設定できる機能を開発した．また，センサによる在宅検知のような既存の行動認識技術と連携させることで，例えば，スマートロックと呼ばれるクラウド経由で操作可能なネットワークに接続された鍵では，スマートロックの状態に応じて，外出時と在宅時の通信許可を自動的に切り替えることができる．

2. 提案システムのアクセス制御の評価

   3 つの IoT デバイスで 6 つの機能の評価を行い，提案システムを用いて，接続先の異なる機能を制御できることを示す．

3.2　システム設計

図 3.1 に提案する IoT 活動量計の概要を示す．本研究では，IoT 活動量計が一般家庭で使用され，複数の IoT デバイスが有線または無線で家庭におけるインターネットとの出入り口であるルーターに接続されていると仮定する．このため，接続されたすべての IoT デバイスから送受信される通信トラヒックがルーターによって収集することができる．IoT 活動量計では，この通信トラヒックを各デバイスの機能を特定するために使用する．また，スマートホーム内に設置されている各種センサの情報も用いることで各デバイスが実行した機能を推定する精度を向上させる．

我々は，IoT デバイスが家庭用ルーターを介してクラウドシステムに接続されていることに注目した．スマートホーム内のすべてのデバイスが接続されているルーター上で，その通信トラヒックからデバイスが実行する機能を特定し，予めスマートフォンなどから設定した内容に基づき通信の可否を制御する．また，特定した機能や通信パケットの状態をクラウド経由で利用者に表示することで利用者はいつでもスマートホームの状況や各デバイスの状態を確認で

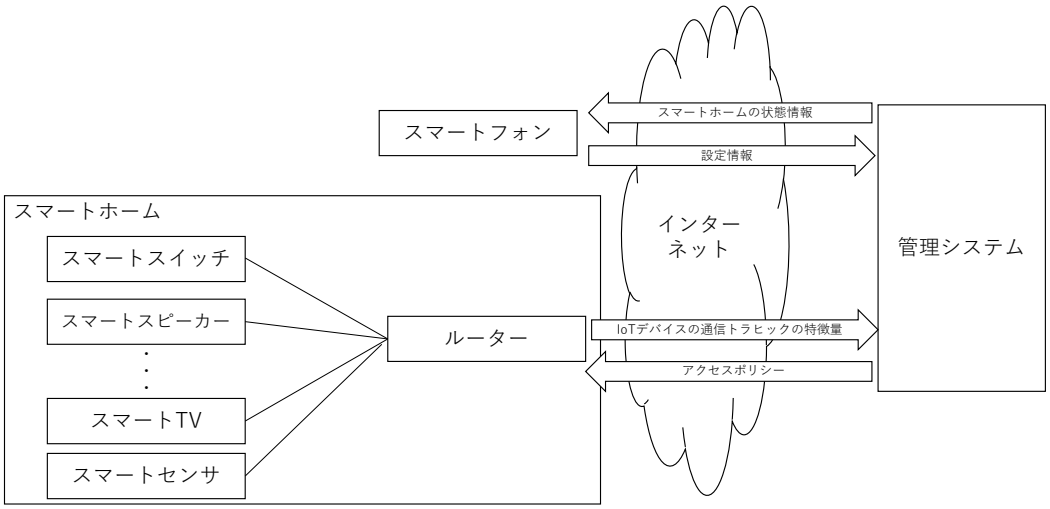

図 3.1: IoT 活動量計の概要

きる．

3.3　アクセス制御の概念

IoT 活動量計とは，利用者が簡単に IoT デバイスを登録し，動作状況を確認できるフレームワークと定義する．スマートフォンでは，アプリケーションを導入する際に，”このアプリケーションはマイクへのアクセスを要求しています”といったポップアップが表示される．また，スマートフォンの設定画面から，各機能にアクセス許可が出ているアプリケーションの一覧を確認することもできる．このように，スマートフォンではスマートフォン上でアプリケーションの設定が可視化されることで，安心してアプリケーションを利用できる仕組みがある．これらと同様に，IoT 活動量計でも IoT デバイスの動作をスマートフォン上のアプリケーションと同様に可視化することで，IoT デバイスが利用する機能や通信パケットの状態をスマートフォンなどの画面上に表示することにより，利用者はセキュリティを気にすることなくデバイ

表 3.1: IDS/IPS，異常検知システムと提案システムの比較

	IDS/IPS	異常検知システム	提案システム
IoT デバイスの実行機能でのアクセス制御	なし	なし	あり
シナリオを元にしたのアクセス制御	なし	なし	あり
デバイスでのアクセス制御	あり	あり	あり
DDoS の防御	あり	あり	なし
既知の攻撃の防御	あり	部分的	なし
ゼロデイ攻撃の防御	なし	部分的	なし

スを利用することができる．

3.4　他のシステムとの違い

特定の通信ポートや通信先，通信動作を検知・遮断するための IDS や IPS，家庭用ルーターに搭載されている簡易ファイアウォールなど様々な製品があるが，IoT デバイスの実行機能による通信を遮断できる製品はない．また，提案システムでは，シナリオに基づいた通信の許可・不許可を設定できるようにし，時間や利用者の操作，各種センサの状態に応じて設定できるように実装している．例えば，「平日の 19 時から 24 時までは Amazon Echo の音楽再生を許可し，それ以外は遮断する」という設定が可能である．また，各種センサと連携することにより，部屋の明るさや音といった状況と組み合わせて設定することが可能である．

IDS/IPS，異常検知システムと提案システムの比較を表 3.1 に示す．提案システムは，IDS/IPS や異常検知システムとは異なり，既知の攻撃や DDoS 攻撃に対してではなく，IoT デバイスの機能の実行の時点で機能を制御することを目的とし意図しない操作やプライバシーの側面から IoT デバイスの機能を制御する．

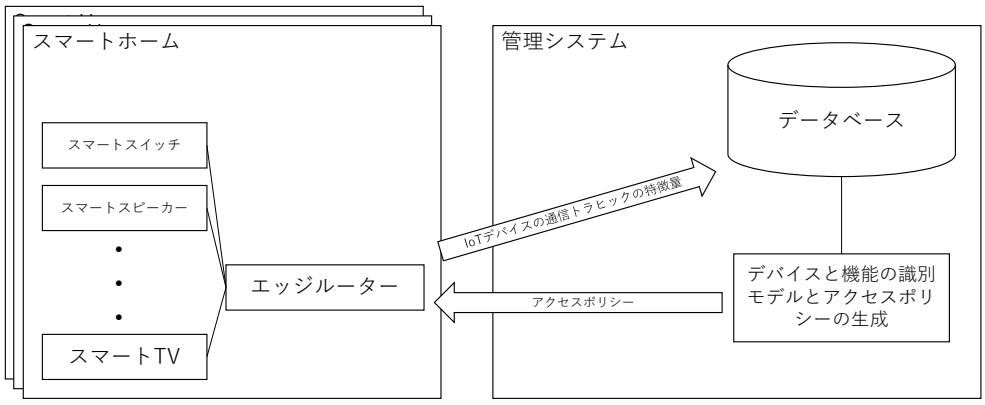

図 3.2: アクセスポリシーと識別モデルの生成の概要

3.5　システム構成

IoT 活動量計は，エッジルーターと管理システムで構成される．エッジルーターは一般家庭に設置されることを想定して設計されており，有線または無線で IoT デバイスや PC に接続される．エッジルーターは，通信トラヒックの特徴に基づいてアクセスポリシーを生成し，アクセス制御を行う．管理システムは利用者が操作することにより，デバイスの機能ごとに通信を許可するかどうかを設定できる．この設定は自動的にエッジルーターに反映され，その設定を元にアクセス制御を実現する．各デバイス機能に対する通信の可否は，単純な許可と遮断設定と，複数の条件を持つシナリオの 2 種類が実装されている．詳細は 3.6 節と 3.7 節で述べる．図 3.2 にアクセスポリシーと識別モデルの生成の概要を示す．エッジルーターに蓄積されたデバイスの通信トラヒックの特徴は管理システムに送られる．そして，既存のアクセスポリシーやモデルの更新，新しい IoT デバイスや機能のアクセスポリシーやモデルの構築に利用する．

3.5.1　エッジルーター

エッジルーターはソフトウェアルーターである VyOS[61] を元に構築されており，IoT デバイスや PC と有線または無線で接続される．家庭内に設置することを想定した構成であるため，エッジルーターのグローバル IP アドレスは動的 IP アドレスが割り当てられることを想定している．そのため，管理システムへの接続は，基本的にエッジルーター側から行う．

エッジルーターから管理システムに通信する主な機能は以下の通りである：

1. DHCP リース情報を管理システムに送信する．
2. 管理システムから設定情報を定期的に受け取る．
3. メモリの使用状況などエッジルーターの状況を管理システムに送信する．
4. 通信状況を管理システムに送信する．
5. 通信トラフィックの特徴を管理システムに送信する．

機能 1 は，接続された IoT デバイスを含むネットワークデバイスに関する情報を管理システムに送信する．この情報は，機能 5 の通信トラヒックの特徴とともに，IoT デバイスとその実行機能を識別するために使用される．機能 2 は，利用者が設定した実行機能の許可と遮断の設定やシナリオを管理システムから受信し，エッジルーター側で通信トラヒックを制御するための機能である．機能 3 はメモリの使用状況などを管理システムに送信し，主にエッジルーターの状態監視を行う．機能 4 は，通信トラヒックの状態を管理システムに送信し，管理システム上でグラフを描画し，IoT デバイスが通信しているかどうかを確認するために使用される．機能 5 は，管理システム上でアクセスポリシーと識別モデルの生成を行うために利用される．

3.5.2　管理システム

管理システムは Web アプリケーションとして構築され，利用者がスマートフォンや PC の Web ブラウザから接続できるように設計されている．主な機能は以下の通りである：

I. エッジルーターの管理

II. 接続デバイス管理

III. シナリオ管理

IV. 利用者管理

機能 I は，利用者が複数エッジルーターを所有することを考慮して複数のエッジルーターを管理するために利用する．機能 II は，各エッジルーターに接続されているデバイスを管理する機能である．IoT デバイスの実行機能ごとに許可と遮断の設定や，デバイスの名称を設定することができる．この機能は将来的に IoT デバイスにラベルを設定することも想定しており，手動でデバイス名を変更することもできる．図 3.3 に管理システムのデバイス一覧画面を示す．機能 III は，単純な通信の許可と遮断だけでなく，通信を許可する時間帯や，利用者の管理システム上のボタン操作などの連続する内容をシナリオとして登録することで，特定条件下でのアクセス制御を可能にしている．機能 IV は，複数の人が生活する一般家庭への設置を想定し，複数の利用者がエッジルーターを管理できるように実装している．

3.6　IoT デバイスの実行機能のアクセスポリシー

アクセスポリシーは，IoT デバイスの機能ごとに作成し，機能の許可と拒否を行う．アクセスポリシーにより，通信の宛先及び送信元やポート番号の許可と遮断が可能となる．エッジルーターは管理システムから定期的にアクセスポリシーを受信し，ソフトウェアルーターのファイアウォールルールとして適用する．将来的には，エッジルーターから送信される通信トラヒックの特徴に基づいてアクセスポリシーを自動生成を行うことを想定している．

3.7　シナリオを元にしたアクセスポリシー

IoT 活動量計では，IoT デバイスの実行する機能ごとの単純な通信の可否だけでなく，通信を許可する時間帯や利用者のボタン操作，連携しているセンサの状態などをシナリオとして管

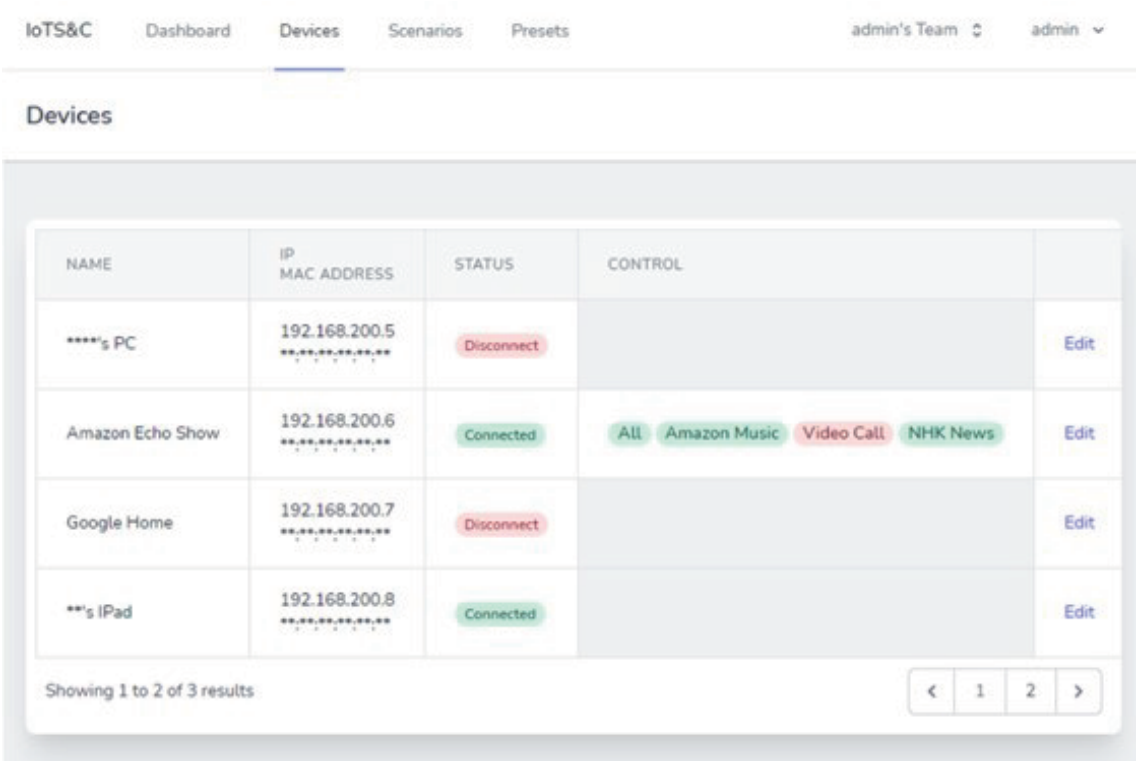

図 3.3: 管理システムのデバイス一覧画面

理システムに登録することで，アクセス制御を実現することができる．シナリオを構成する要素をコントロールと呼ぶ．シナリオは複数のコントロールから構成される．コントロールの例を以下に示す：

- 利用者が管理システムのボタン 1 をクリックする
- 平日 10:00〜19:00
- IoT デバイス 1 の機能 A の通信を遮断

図 3.4 は管理システムのシナリオ編集画面である．ここでは，平日の 10:00〜11:00 の間だけ Amazon Echo の音楽再生通信を許可するシナリオを定義している．

現在の実装では，以下のものがコントロールとして使用されている．

- IoT デバイスの実行機能の許可と遮断
- 管理システム上のボタン

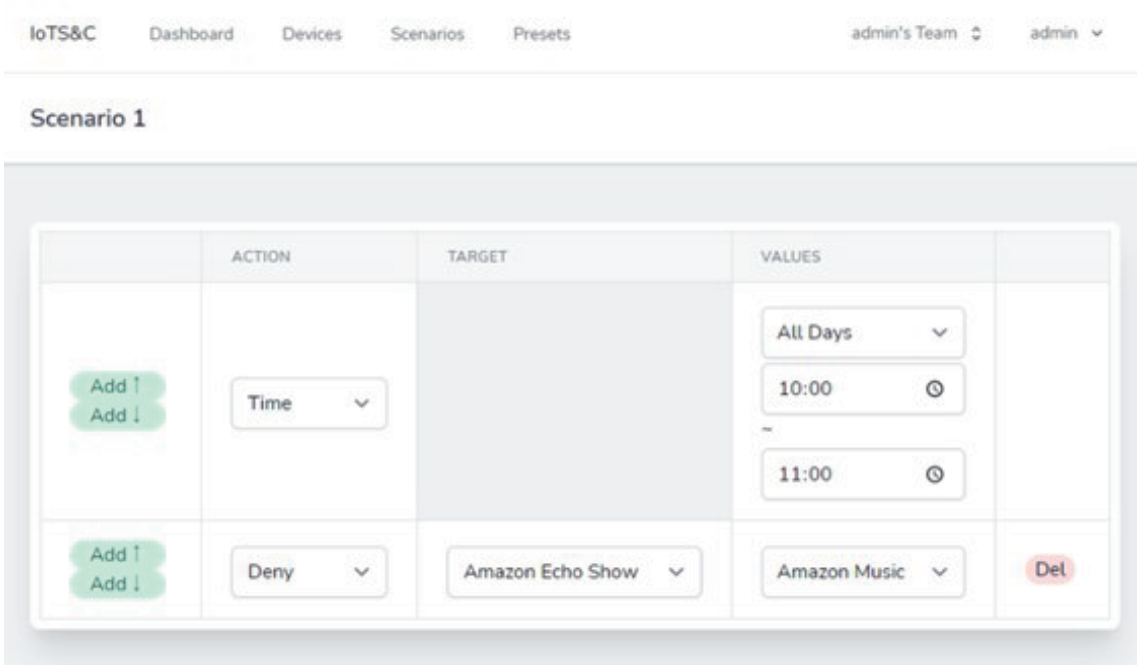

図 3.4: 管理システムのシナリオ編集画面

- 時間指定
- 連携しているセンサの状態

3.8　アクセスポリシーと識別モデルの共有

IoT 活動量計では，エッジルーターから収集された特徴量が管理システムに集約される．その特徴量は，既存のアクセスポリシーやモデルを更新したり，新しい IoT デバイスや機能のアクセスポリシーやモデルを構築したりするために利用することを想定されている．多くの IoT デバイスの通信は暗号化されているとはいえ，デバイスの使用頻度や通信先などの情報を隠すことはできない．しかし，そのような情報を収集し，利用者と紐づいた形で保存することは，利用者のプライバシーに関わる懸念が生じる．この懸念を払拭するため，IoT 活動量計では，収集の段階ではエッジルーターと機能との紐付けを行わない．デバイス，実行機能，通信先，特徴量のみを紐付けることで，特定の利用者に紐付けられる情報が保存されないようにしている．

3.9　IoT デバイスと実行機能の識別

機械学習技術は，通信トラヒックからのデバイスと実行機能の識別に使用される．デバイス識別と実行機能識別の詳細は 4 章で述べる．

3.10　評価

提案システムでは，アクセスポリシーの自動生成とデバイス・実行機能の識別を除くアクセス制御に関する機能を開発した．この場合，アクセスポリシーは 3.10.2 節に従って手動で作成した．そして，提案システムにおけるアクセス制御が各デバイス機能に対して正しく動作することを検証した．提案システムにおけるデバイス識別と機能識別の精度を評価し，最後に提案システムにおける機能ごとのアクセス制御を実装し，その動作を確認した．

3.10.1　IoT 活動量計の環境

概念実証 (PoC) として，仮想マシンとアクセスポイント上に IoT 活動量計を構築した．提案するシステムに Amazon Echo Show，SwitchBot Hub Mini[62]，SwitchBot プラグ [63] を接続し，iPad の Web ブラウザから特定の機能を許可・拒否できることを検証する環境を構築した．システム構成を図 3.5 に示す．この構成で通信トラヒックを収集し，収集した通信トラヒックからアクセスポリシーを生成した．

3.10.2　アクセスポリシーの生成

Amazon Echo Show の Amazon Music 機能，NHK ニュース機能，ビデオ通話機能，SwitchBot プラグの電源 ON/OFF 機能，SwitchBot Hub Mini の音響機器の ON/OFF 機能，TV の ON/OFF 機能の通信トラヒックを収集した．各機能の通信トラヒックを 10 回収集し，機能を実行する前の 5 秒前からデバイスに動作を指示した後の 5 秒後までの通信トラヒックを切り出した．そして，次に，送信元/宛先ポート，送信元/宛先 IP アドレス，プロト

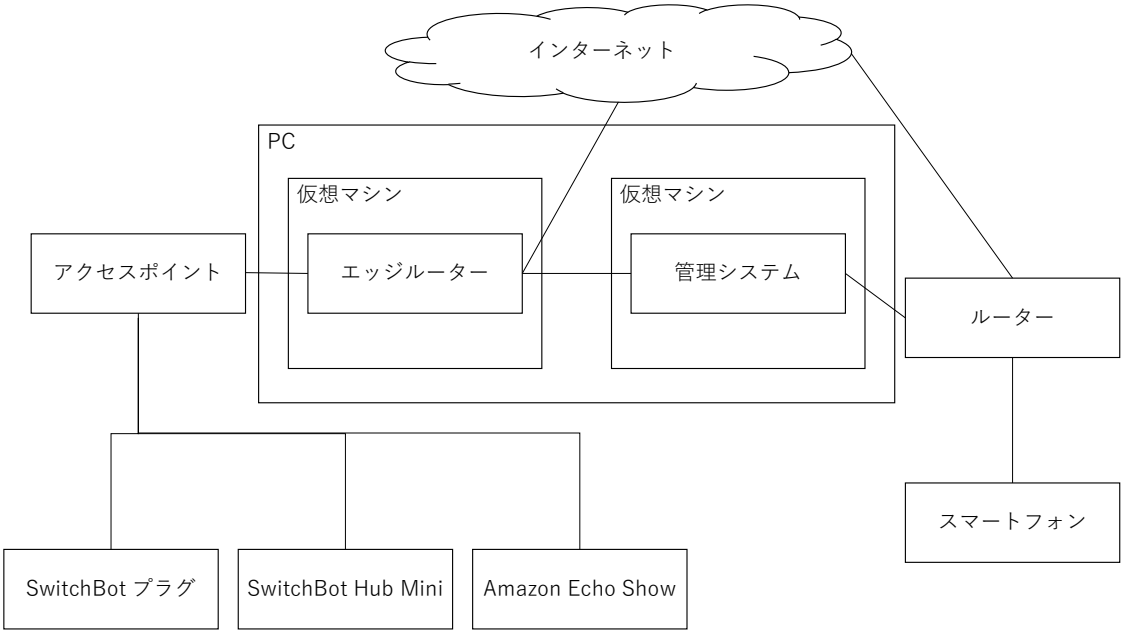

図 3.5: PoC のシステム構成

コル (TCP と UDP) ごとの通信パケット数を計測した．DNS と NTP はすべての機能で使用されている可能性があるため除外した．そして，TCP/UDP と宛先 IP アドレスの組み合わせの先頭を除外ルールとして採用した．ただし，一部の機能では CDN を利用しており，その IP アドレスは利用するたびに変更される可能性がある．そこで，IP アドレスから FQDN を取得し，DNS レコードから IP アドレス範囲を取得して利用した．

3.10.3　アクセス制御の評価

Amazon Echo Show の Amazon Music，NHK ニュース，ビデオ通話機能，SwitchBot の電源 ON/OFF，音響機器の ON/OFF，TV の ON/OFF 機能の 2 つのアクセスポリシーの評価を行った．アクセスポリシーの評価は下記の 2 つの観点で行った．

1. ある機能が無効化されたときに他の機能が機能するかどうか．

表 3.2: 一つの機能を無効にした場合の，他の機能の動作確認結果 (Amazon Echo Show)

機種	無効にした機能	Amazon Music	NHK ニュース	ビデオ通話
Amazon Echo Show	Amazon Music	実行できない	実行できた	実行できた
Amazon Echo Show	NHK ニュース	実行できた	実行できない	実行できた
Amazon Echo Show	ビデオ通話	実行できた	実行できた	実行できない

表 3.3: 一つの機能を無効にした場合の，他の機能の動作確認結果 (SwitchBot)

機種	無効にした機能	電源の ON/OFF	音響機器の ON/OFF	TV の ON/OFF
SwitchBot プラグ	電源 ON/OFF	実行できない	実行できた	実行できた
SwitchBot Hub Mini	音響機器の ON/OFF	実行できた	実行できない	実行できない
SwitchBot Hub Mini	TV の ON/OFF	実行できた	実行できない	実行できない

2. 時間を使ったシナリオを元にしたポリシーが正しく機能するかどうか.

その結果，Amazon Echo Show は，1 つの機能を拒否しても，他の 2 つの機能は動作することを確認した．しかし，SwitchBot Hub Mini は，同じデバイスの他の機能までブロックしてしまった．これらの結果を表 3.2 と表 3.3 に示す．また，シナリオを元にしたポリシーの有効性を確認するため，Amazon Music の機能を 10:00〜11:00 の間に動作しないように設定し，その時間帯のみ動作しないことを確認した.

3.11　議論

3.11.1　IoT デバイスのファームウェアの更新の影響

IoT デバイスは，定期的にファームウェアの更新が発生する．その際に通信先や通信量などに変化が生じる可能性がある．また，スマートスピーカーなどの第三者が提供するアプリケーションを追加で導入することが可能な IoT デバイスではアプリケーションの更新も考慮する必要がある．

3.11.2　同じ接続先を持つ異なる機能

提案システムでは，同じ接続先の異なる機能をすべて制御することはできない．同じ接続でも機能が異なる場合に対応するためには，IP アドレスやポートだけでなく，通信量や通信内容でも識別する必要がある．暗号化されていない通信であれば，通信内容で判別することも可能だが，最近の IoT デバイスの通信は暗号化されているため，現実的ではない．もちろん，Web プロキシを利用して HTTPS 通信の内容を確認する方法もあるが，Web プロキシ用の証明書を導入する必要があるなど，利用者に大きな負担を強いるため，実現は難しい．

3.11.3　利用者の生活様式の変化

利用者の生活様式，つまりデバイスの使用パターンは，転職や進学などのイベントによって変化する．接続先が異なる機能はその影響を受けにくい．しかし，時刻や曜日などの情報に基づいて制御を行う場合には，そのような機能にも影響が及ぶと考えられる．時間帯や曜日などの情報に基づく制御を補助するためには，センサなどと連携して部屋の状況を確認する必要がある．

3.11.4　異なるプロトコルによる制御

SwitchBot Hub Mini は，遠隔でのコマンドの実行に TCP を，家電への送信に赤外線方式を採用したスマートリモコンである．このような IoT デバイスの場合，最初に TCP で指示を出しても，その部分の通信はほとんど同じであり，特定の機能だけを制御することはできない．そのため，機能を制御するにはスマートリモコンを複数用意するしかない．通信が暗号化されていなければ，通信内容から機能を特定することも可能だが，最近の IoT デバイスの通信は暗号化されているので現実的ではない．

3.11.5　宛先 IP の変更

ソフトウェアルーターの設定では FQDN を指定できないため，IP アドレスを指定して制御する必要がある．配信先が CDN を利用している場合，配信先には複数の IP アドレスが存在するため，1 つの IP アドレスで制御することはできない．IP アドレスから FQDN を取得し，DNS レコードから IP アドレスの範囲を取得するなどの対策が必要である．ただし，IoT デバイスの製造元が FQDN 情報を変更した場合，設定されている IP アドレスも変更する必要がある．そのため，定期的にソフトウェアルーターの設定を更新する必要がある．

3.11.6　IoT 活動量計を運用の問題

IoT 活動量計は，管理システムをクラウド上のサーバーに構築する想定で設計されている．そのため，実際に多くの利用者に利用してもらうためには，そのクラウド上のサーバーを誰かが運用していく必要がある．その運用を誰が行うかについては，IoT デバイスの製造元が運用すると競合他社との関係性などのために対応が偏る可能性があるので，IoT デバイスを製造していない中立的な機関が運用することが望ましい．

3.12　まとめ

本研究では，家庭内の IoT デバイスを安心・安全に利用するための IoT 活動量計と呼ばれるフレームワークを提案した．また，本提案機能を搭載したルーターと利用者とのインターフェースとなる管理システムから構成される本提案システムの PoC を実施し，その結果を報告した．提案システムでは，事前に収集した通信トラヒックから生成したアクセス制御を用いて，一部の IoT デバイスの特定の機能を許可／拒否することができた．今後の研究としては，他の IoT デバイスの呼び出された機能を特定し，Slack[64] などのメッセージングアプリケーションと連携させることで，通信トラヒックを監視し，現在どの機能が利用されているかをリアルタイムに利用者に通知することを計画している．また，アクセスポリシーを自動的に更新する仕組みを実装し，検証する．さらに，Wi-Fi を利用した行動認識など，他の研究手法を用いて，ネッワーク通信が意図的なものであるかどうかを特定する予定である．IoT デバイスの利用状況の可視化を通じて，利用者がセキュリティの不安を感じることなく IoT デバイスを利用できるようになることを期待している．

第 4 章

通信トラヒック分析による IoT デバイスの機能推定手法の評価

本章では，IoT 活動量計の実現のために必要な機能推定手法の評価について述べる．

4.1 はじめに

3 章で提案している IoT 活動量計の実現手段として我々は，IoT デバイスの通信トラヒックに着目し，そのパターンからデバイス及びデバイスのどのような機能が使われているかを推定し，その結果をもとに通信を制御する．また，それらの設定を，スマートフォンのパーミッション設定のように機能ごとの通信の可否を可視化し，簡単に設定できる機能を提案している．その機能を実現するうえで，どの IoT デバイスのどの機能が実行されたかを通信トラヒックから解析することが重要となる．従来の研究 [65] では，同じ種別の IoT デバイスでしか評価されていない．そのため，多数の種別の IoT デバイスでの検証と特徴量の改良が必要である．本節では，多数の種別の IoT デバイスで検証を行うため，日本国内で流通しているスマートスピーカー，スマートカメラ，スマートリモコン，スマートプラグ，4 種別の IoT デバイス各 2 機種ずつの計 8 機種の 8 種類の機能の通信トラヒックを収集し，機械学習を用いて通信トラヒックから抽出した個人を特定できる情報を含まない特徴量を用いてデバイスの分類とデバ

イスの実行した機能の分類を行いその精度を評価した．その結果，デバイスの機種と実行した機能の組み合わせの 16 通りで分類した場合，91% の精度で機能を推定できることを確認した．また，実行した機能のみの 8 通りで分類した場合，73% の精度で機能を推定できることを確認した．しかしながら，上記の手法では，機能を実行した際の通信トラヒックのすべてから特徴量を計算し推定しているため，通信の制御のために利用するためには，機能の実行と終了の検出が必要となる．そのため，数秒の通信から通信の制御を行うことは難しい．その問題を解決するために，1 秒ごとの特徴量を用いて，機械学習で IoT デバイスの機能の実行状態を推定し，その精度を評価した．また，特徴量については，従来の手法同様，通信トラヒックから通信量などを計算し，抽出した個人を特定できる情報を含まない特徴量を用いた．本研究では，数秒間隔での機能推定を行うために 8 機種の IoT デバイスについて，何も実行していない状態を含む 3 機能の推定を 1 秒ごとの特徴量を用いて機能推定を行った．その結果，8 機種中 5 機種において 83% 以上の精度で機能を推定できることを確認した．

4.2　データセット

本節では，IoT 活動量計の実現のために必要な機能推定手法に用いるデータセットについて述べる．

4.2.1　通信トラヒックの収集環境

図 4.1 に通信トラヒックの収集環境の構成図を示す．通信トラヒックの収集環境は，3 章で述べた IoT 活動量計の一部であるエッジルーターを仮想マシン上に構築し，デバイス種別 4 種の各 2 機種ずつ計 8 機種の IoT デバイスをアクセスポイントを経由してエッジルーターに接続した．これにより，IoT デバイスの通信はすべてエッジルーターを経由することとなる．表 4.1 に通信トラヒックの収集に利用した IoT デバイス一覧を示す．

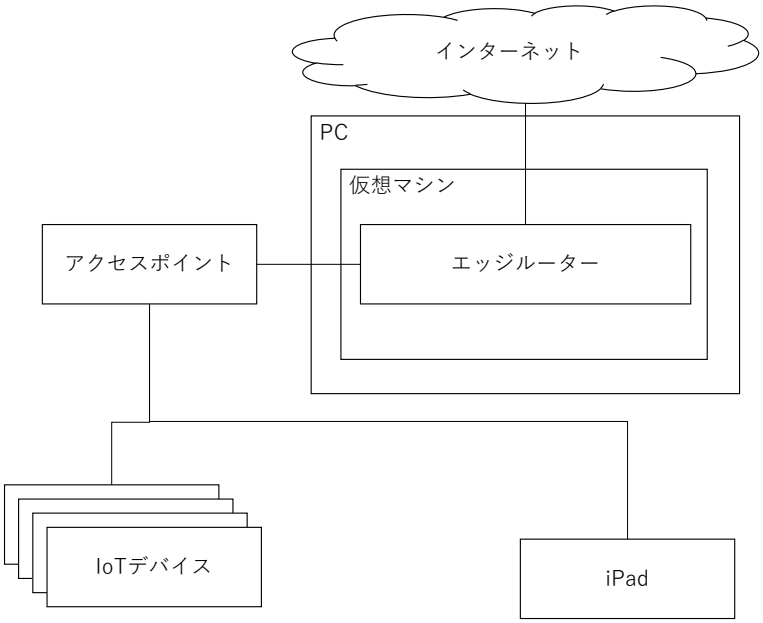

図 4.1: 通信トラヒックの収集環境の構成図

4.2.2　通信トラヒックの収集方法

4.2.1 節で述べた収集環境を用いて各デバイス種別ごとに 2 種類の機能計 8 種類の通信トラヒックを収集した．なお，各デバイス種別ごとに 2 機種ずつ用いるため収集した通信トラヒックは計 16 種別である．また，収集した 16 種別それぞれ 10 回ずつ収集を行った．表 4.2 に収集した機能一覧を示す．なお,「音楽を再生する」などの終了までに時間を要する機能については，途中で再生を止めることにより秒数の制限を行った．また，今回収集する機能の選定においては，同じデバイス種別で似た挙動をするものに絞って選定した．選定から除外した機能として，例えば，スマートスピーカーである Google Home Mini と Amazon Echo Show の「今日のニュースを聞く」という機能は，Amazon Echo Show では，毎回最初から今日のニュースが再生されるのに対し，Google Home Mini では，2 回目に今日のニュースを再生した際に途中から再生され挙動が異なるため今回は対象から除外した．

表 4.1: 通信トラヒックの収集に利用した IoT デバイス一覧

No.	デバイス種別	製品名	開発元
1	スマートカメラ	Ranger 2[66]	Imou
2		Mi 360° [67]	Xiaomi
3	スマートリモコン	SwitchBot Hub Mini[62]	SwitchBot
4		Nature Remo[68]	Nature
5	スマートスピーカー	Amazon Echo Show[3]	Amazon
6		Google Home Mini[2]	Google
7	スマートプラグ	SwitchBot プラグ [63]	SwitchBot
8		WiFi スマートプラグ [69]	TP-Link

通信トラヒックの収集の手順は，下記のとおりである．通信トラヒックの収集にはエッジルーターの IoT デバイスが接続されている側のネットワークインターフェースに対して tcpdump[70] コマンドを用いて通信パケットを収集した．

1. 通信パケットの収集を開始する．
2. 約 10 秒待機する．
3. 対象となる機能を実行する．
4. 対象となる機能の実行を確認する．
5. 約 10 秒待機する．
6. 通信パケットの収集を終了する．

4.2.3　通信トラヒックの加工方法

利用した通信トラヒックの収集環境は，すべての IoT デバイスが同じネットワーク環境に接続されているため，通信パケットを収集する際にほかの IoT デバイスの通信も混在している．今回の評価に用いるためには，対象の IoT デバイスの通信パケットのみを抽出する必要があ

表 4.2: 収集した通信トラヒックの機能一覧

No.	デバイス種別	機能
1	スマートカメラ	話しかける
2		カメラの向きを変える (左に 3 秒)
3	スマートリモコン	TV を ON にする
4		TV をミュートにする
5	スマートスピーカー	音楽を再生する (10 秒)
6		今日の天気を聞く
7	スマートプラグ	電源を ON にする
8		電源を OFF にする

る．そのため，送信先 IP 及び送信元 IP が対象の IoT デバイスの通信パケットのみを抽出し評価に用いた．

4.2.4　通信トラヒックの評価

4 章で精度の低かった Mi 360°，SwitchBot Hub Mini，Nature Remo の 3 つのデバイスの通信トラヒックを評価した．これらのデバイスは静止状態を含む 3 つの機能を持っており，それらの通信トラヒックを評価した．各通信トラフィックは，通信パケットサイズ，通信パケット数などをもとに，個人を特定できない形で評価した．評価には 1 秒間の通信トラヒックの値を使用した．なお，評価値は表 4.3 のとおりである．なお，宛先 IP アドレスや MAC アドレスなど，個人や製造元に関連する情報を用いると精度は向上するが，新機能が追加されるたびに更新する必要がある．また，それらを利用する場合には，プライバシーの問題もある．そこで，通信量から得られる情報に着目した．各 IoT デバイスの散布図マトリクスを図 4.2-図 4.4 に示す．

その結果，通信トラヒックで静止しているかどうかの分類は可能であるが，通信パケット数，通信パケットサイズなどは同じであることが多いため，機能に関しては，通信トラヒックを分

表 4.3: 評価値の一覧 (1 秒)

No.	評価値
1	送信パケット数
2	最大送信パケットサイズ
3	最小送信パケットサイズ
4	受信パケット数
5	最大受信パケットサイズ
6	最小送信パケットサイズ
7	送信先 IP 数
8	送信元 IP 数

類することは不可能であることがわかった．また，静止状態で発生する通信トラヒックは，利用者の操作とは無関係な裏側で発生するファームウェアの更新などの通信トラヒックと考えられる．これらについては今後，正確にラベル付けする必要がある．

4.3　通信トラヒック分析による IoT デバイスにおける機能推定手法

本節では参考文献 [71] を引用し，IoT 活動量計を実現するために，8 台の IoT デバイスから 2 機能ずつ，デバイス機種と実行機能の組み合わせ 16 通りの通信トラヒックを用いて通信量から得られる特徴量のうち，個人や特定の製造元を特定できる情報を含まない 28 個の特徴量を用いて，ランダムフォレストアルゴリズム [72] による分類を行い，その精度を評価した．

4.3.1　機能推定手法

3 章で述べた IoT 活動量計の IoT デバイスの通信の可否を制御するために重要となる機能としてどの IoT デバイスのどの機能が実行されたかを通信トラヒックから解析することが重要

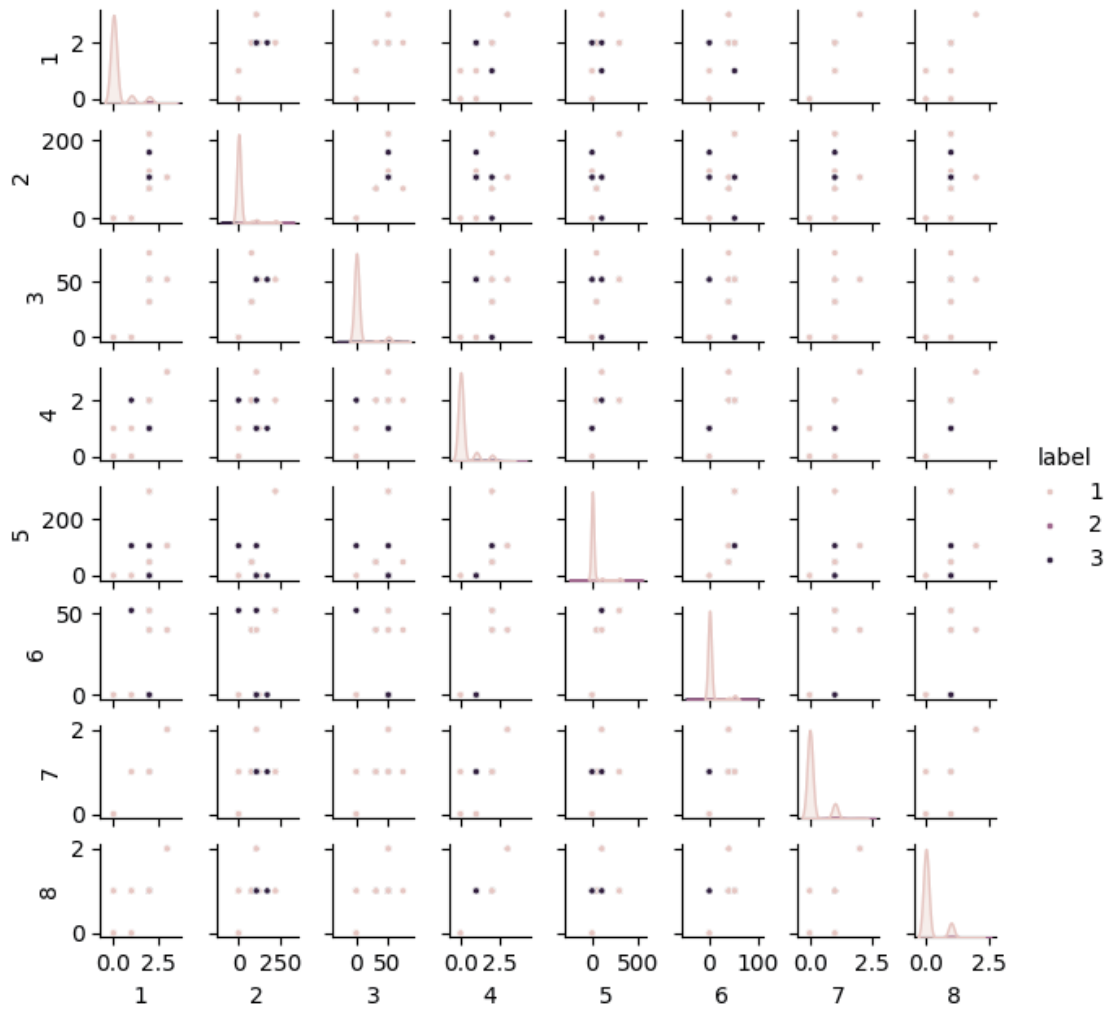

図 4.2: Mi 360° : スマートカメラの散布図マトリクス (1: 静止状態，2: 話しかける，3: カメラの向きを変える)

となる．提案方式は，IoT デバイスの機能の通信トラヒックパターンを機械学習によって学習することで機能を推定する．実際に IoT 活動量計で用いる推定機種の構築に向けて，日本国内で流通しているスマートスピーカー，スマートカメラ，スマートリモコン，スマートプラグ，4 種別の IoT デバイス各 2 機種ずつの計 8 機種の合計 16 種類の機能の通信トラヒックを用いて個人を特定できない通信トラヒックから抽出した特徴量を用いて，機械学習によりデバイスと実行機能を分類し，その精度を評価した．通信トラヒックからは，パケットサイズや宛先 IP 数などの通信量や，宛先 IP の国や宛先 IP の管理情報などの通信内容に関連する情報から特徴量を算出することができる．本手法では，通信量から得られる特徴量のうち，個人や特定の製

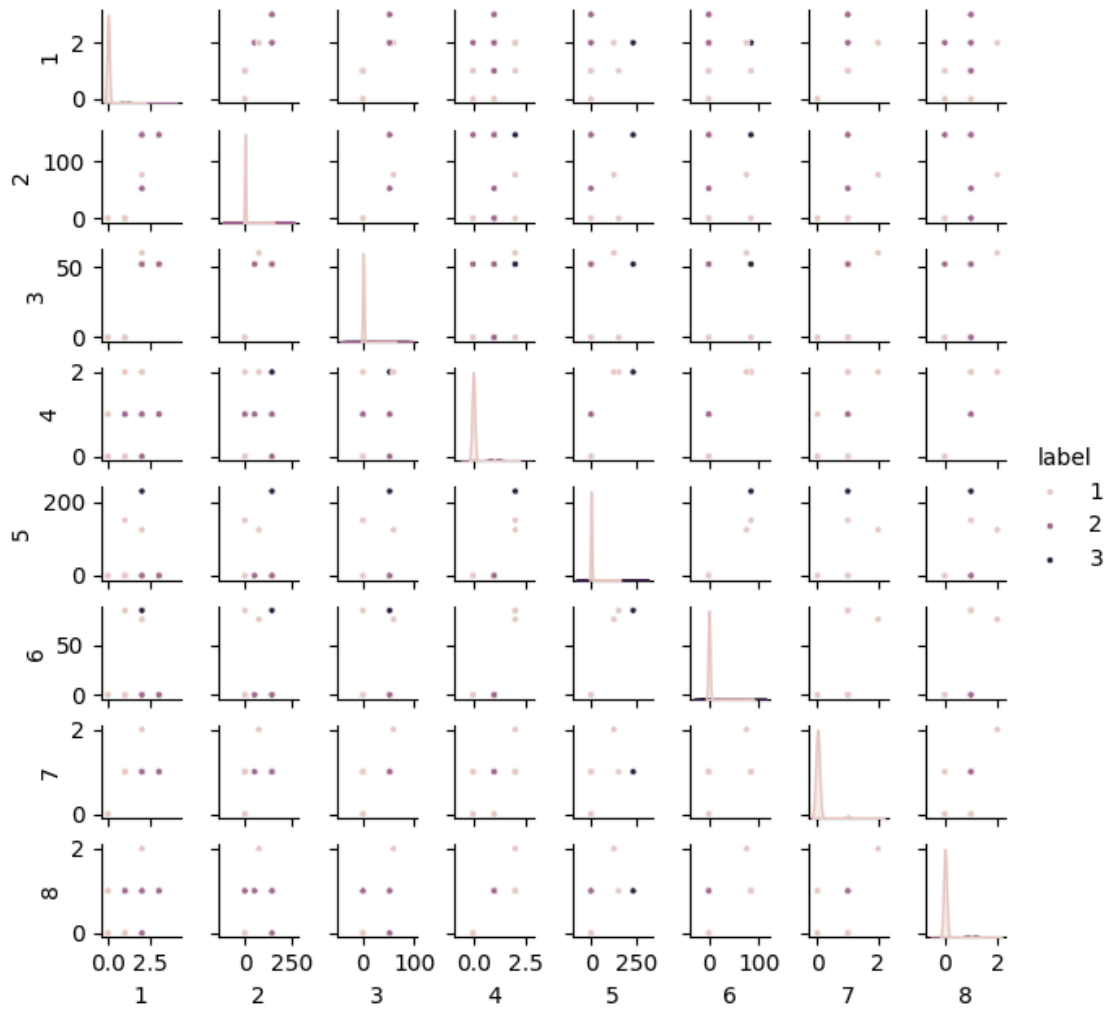

図 4.3: SwitchBot Hub Mini: スマートリモコンの散布図マトリクス (1: 静止状態,2:TV を ON にする,3:TV を OFF にする)

造業者を特定できる情報を含まない特徴量を用いた．宛先 IP や MAC アドレスなど，個人やメーカーに関連する特徴を用いれば精度は向上するが，これらを使用する場合，プライバシーの問題もある．そこで，通信量に由来する特徴量に着目した．そして，送信パケット数，送信パケットサイズ，受信パケット数，受信パケットサイズ，TCP パケット数，TCP パケットサイズ，UDP パケット数，UDP パケットサイズ，送信元 IP 数，送信先 IP 数の平均値，最大値，分散，標準偏差を 0.5 秒，1 秒，1.5 秒の時間窓で計算し，合計 120 個の特徴量を抽出した．それらの 120 個の特徴量からランダムフォレストアルゴリズムを用いて特徴量の重要度を算出し，重要度の低い特徴量は除外した．その結果，使用した特徴量は，表 4.4-4.5 の通りで

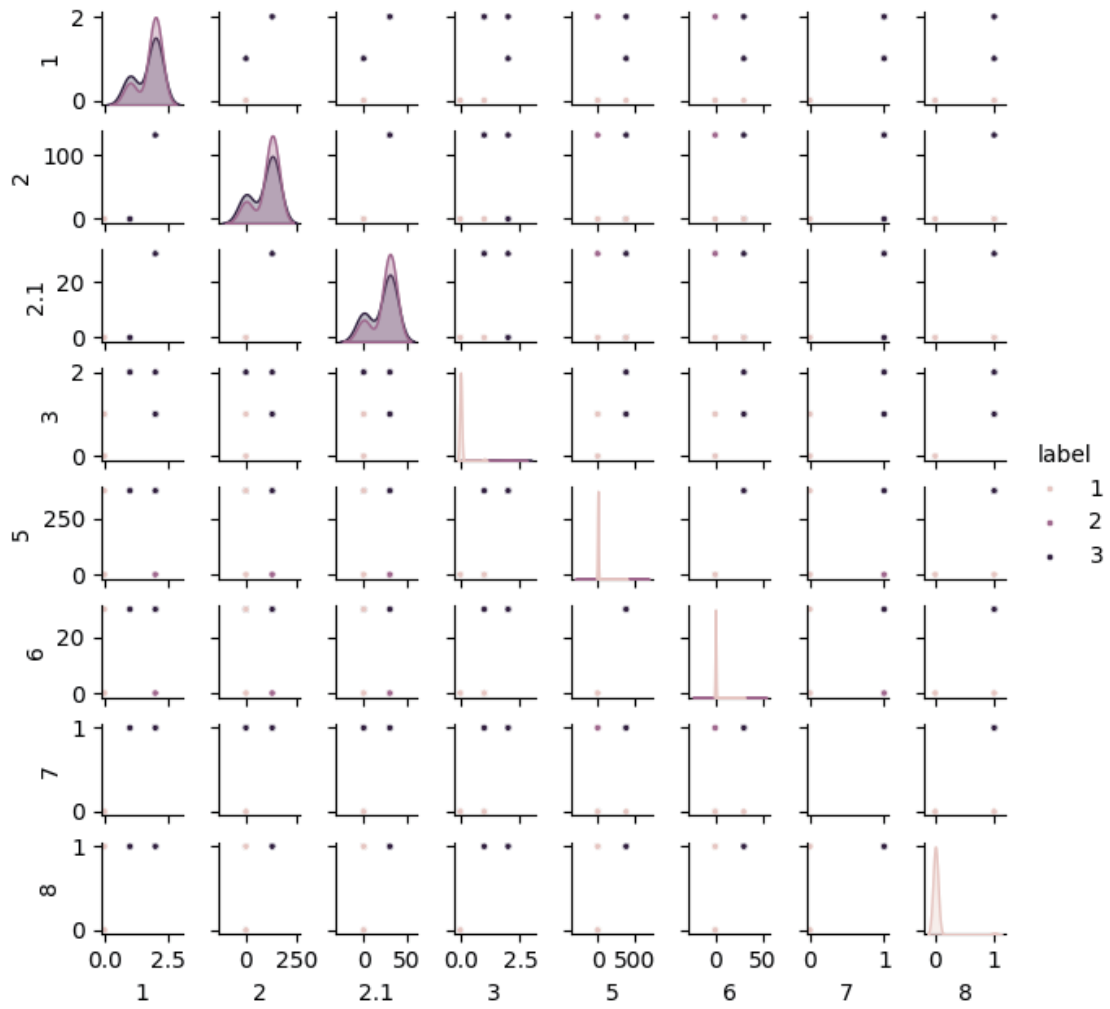

図 4.4: Nature Remo: スマートリモコンの散布図マトリクス (1: 静止状態,2:TV を ON にする,3:TV を OFF にする)

ある．機械学習アルゴリズムは，教師あり機械学習であるランダムフォレストを用い，10 分割交差検証により評価を行った．

4.3.2　評価

機能推定手法の妥当性を検証するため，ランダムフォレストアルゴリズムを用い，10 分割交差検証による評価を行った．評価は，IoT デバイスの機種と実行機能の組み合わせ 16 種類と，実行機能のみの組み合わせ 8 種類の計 2 種類を実施した．その結果，デバイス機種と実行関数の組み合わせ 16 種類に分類した場合，91% の精度で分類できることを確認した．その混

表 4.4: 利用した特徴量一覧

No.	特徴量
1	1.5 秒間の送信パケットサイズの最大
2	1.5 秒間の受信パケットサイズの最大
3	1.5 秒間の TCP パケットサイズの平均
4	1.5 秒間の送信パケットサイズの平均
5	1 秒間の受信パケットサイズの平均
6	1 秒間の受信パケットサイズの最大
7	0.5 秒間の送信パケットサイズの最大
8	1.5 秒間の TCP パケットサイズの最大
9	1 秒間の TCP パケット数の平均
10	1 秒間の TCP パケットサイズの最大
11	1 秒間の送信パケットサイズの平均
12	1.5 秒間の受信パケット数の最大
13	1 秒間の UDP パケットサイズの平均
14	1 秒間の TCP パケットサイズの平均

同行列を表 4.6 に，クラスラベル一覧を表 4.7 に示す．いずれの IoT デバイスも，通信量の多い「音楽を再生する (10 秒)」や「今日の天気を聞く」を分類できた．SwitchBot プラグの「電源を ON にする」や Nature Remo の「TV をミュートにする」のような通信の少ない機能は，他の機能よりも精度が低く，類似した機能として誤分類される．これらは，そもそも機能を実行するための通信が数回しか発生していないため，今後 IoT デバイスや機能が追加され評価されるようになると，さらに精度が低下することが予想される．

実行された機能のみの 8 つの組み合わせで分類した場合，73% の精度で分類できることを確認した．その混同行列を表 4.8 に，クラスラベル一覧を表 4.9 に示す．この場合も，通信量の多い 「音楽を再生する (10 秒)」や「今日の天気を聞く」が正しく分類されている．一方，通信があまり発生しない「TV を ON にする」「TV を OFF にする」の精度は低い．特に「TV

表 4.5: 利用した特徴量一覧 (続き)

No.	特徴量
15	0.5 秒間の UDP パケットサイズの平均
16	1.5 秒間の受信パケットサイズの平均
17	1 秒間の送信パケットサイズの最大
18	1 秒間の UDP パケット数の最大
19	1 秒間の UDP パケットサイズの最大
20	1 秒間の受信パケット数の最大
21	0.5 秒間の TCP パケットサイズの最大
22	0.5 秒間の送信パケットサイズの分散
23	1.5 秒間の TCP パケット数の最大
24	1 秒間の送信パケットサイズの分散
25	1 秒間の TCP パケット数の最大
26	1 秒間の UDP パケット数の平均
27	0.5 秒間の送信パケットサイズの標準偏差
28	1.5 秒間の UDP パケットサイズの最大

を ON にする」「TV を OFF にする」はスマートリモコンを使って行うものであり，指示を受けたスマートリモコンは当該機能の赤外線信号を送信する．したがって，実際の通信はほとんど同じであり，通信回数も少ないことから，通信トラヒックの情報のみで分類することは困難であると考えられる．

4.3.3　議論

この項では，IoT デバイスの設定の影響，IoT デバイスのファームウェアの更新の影響，通信トラヒックが似た機能など，いくつかの重要な問題について議論する．

表 4.6: 機能推定結果の混同行列 (IoT デバイスの機種と実行機能の組み合わせの 16 通り)

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	10	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	10	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	10	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	9	0	0	0	0	1	0	0	0	0	0
6	0	0	0	0	0	1	8	1	0	0	0	1	0	0	0	0
7	0	0	0	0	0	1	0	9	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	7	3	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	2	8	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	9	0	1	0	0	0
11	0	0	0	0	0	0	0	0	0	0	2	8	0	0	0	0
12	0	0	0	0	0	0	1	0	0	0	0	0	9	0	0	0
13	0	0	0	0	0	0	0	1	0	0	0	0	1	8	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	10	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	10

IoT デバイスの設定による影響

本研究では，日本国内に流通している IoT デバイスを対象としていたため，言語設定は日本語として通信トラヒックを収集し評価した．しかし，IoT デバイスは様々な国で流通しており，同様の機能でも言語設定や設置されている位置情報などによって特徴が異なる可能性がある．そのため，IoT デバイスの設定による影響も検討していく必要がある．

表 4.7: 機能推定結果の混同行列 (IoT デバイスの機種と実行機能の組み合わせの 16 通り) である表 4.6 のクラスラベル

クラスラベル	内容
0	音楽を再生する (10 秒)(Amazon Echo Show)
1	今日の天気を聞く (Amazon Echo Show)
2	音楽を再生する (10 秒)(Google Home Mini)
3	今日の天気を聞く (Google Home Mini)
4	カメラの向きを変える (左に 3 秒)(Ranger 2)
5	話しかける (Ranger 2)
6	カメラの向きを変える (左に 3 秒)(Mi 360°)
7	話しかける (Mi 360°)
8	TV をミュートにする (Nature Remo)
9	TV を ON にする (Nature Remo)
10	電源を OFF にする (SwitchBot プラグ)
11	電源を ON にする (SwitchBot プラグ)
12	TV をミュートにする (SwitchBot Hub Mini)
13	TV を ON にする (SwitchBot Hub Mini)
14	電源を OFF にする (WiFi スマートプラグ)
15	電源を ON にする (WiFi スマートプラグ)

IoT デバイスのファームウェアの更新による影響

IoT デバイスは，定期的にファームウェアの更新が発生する．その際に通信先や通信量などに変化が生じる可能性がある．また，スマートスピーカーなどの第三者が提供するアプリケーションを追加で導入することが可能な IoT デバイスではアプリケーションの更新も考慮する必要がある．

表 4.8: 機能推定結果の混同行列 (実行機能のみの 8 通り)

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	15	3	1	0	0	1	0	0
1	5	15	0	0	0	0	0	0
2	0	0	15	0	4	1	0	0
3	0	0	0	20	0	0	0	0
4	0	0	2	0	18	0	0	0
5	0	0	1	0	0	7	12	0
6	0	0	1	0	0	13	6	0
7	0	0	0	0	0	0	0	20

表 4.9: 機能推定結果の混同行列 (実行機能のみの 8 通り) である表 4.8 のクラスラベル

クラスラベル	**内容**
0	電源を OFF にする
1	電源を ON にする
2	カメラの向きを変える (左に 3 秒)
3	音楽を再生する (10 秒)
4	話しかける
5	TV をミュートにする
6	TV を ON にする
7	今日の天気を聞く

同じ機能を持つ異なる IoT デバイスの機種の通信トラヒックの類似性

同じ機能であっても，IoT デバイスの機種が異なれば，通信トラヒックの特徴が異なる場合がある．例えば，IoT デバイスの製造元が異なれば，接続先や実装方法が異なるため，通信トラヒックの特徴も異なる．そのため，これらを分類するためには，まず IoT デバイスを分類

し，次に機能を分類することが有効であると考えられる．ただし，例えばスマートスピーカーの「音楽を再生する」は，IoT デバイスの機種が異なっても，IoT デバイス上で動作するアプリケーションの接続先が同じであれば，同様の通信トラヒックの特徴を持つことになる．

通信トラヒックが似た機能

多くの IoT デバイスの通信は，HTTPS で行われており JSON などの形式で内容の受信や送信を行う．例えば，スマートリモコンの場合，JSON で命令を送るとしても，数回の通信でかつ内容もあまり差異がない．そのため通信トラヒックのみから分類することは難しいと考えられる．そのため，実際にこれらの機能を検知するためには，既存の行動認識の技術と連携し，部屋の在室状況などと連動し検知を行う必要がある．

デバイスや機能の増加による影響

本研究では，16 種類の IoT デバイスと機能の組み合わせを検証した．今後も組み合わせを追加し，検証を進めていく予定である．本検証の結果から，4.3.3 で述べた IoT デバイスの機能を除けば，識別は良好である．そのため，スマートリモコンなど各機能の通信が類似している IoT デバイスを追加した場合，精度が低下することが予想される．スマートスピーカーなど，機能ごとに通信が異なる IoT デバイスは，機能やデバイスの数が増えても識別がうまくいくことが期待される．

4.3.4　まとめ

本研究では，IoT 活動量計に用いられる IoT デバイスが実行する機能単位での通信制御を実現するために，IoT デバイスの通信トラヒックを解析することで，IoT デバイスにおける機能推定手法を提示した．実際に日本国内で流通しているスマートスピーカー，スマートカメラ，スマートリモコン，スマートプラグ，4 種別の IoT デバイス各 2 機種ずつの計 8 機種の 8 種類の機能の通信トラヒックに対して，個人を特定できる情報を含まない通信トラヒックから抽出した特徴量を用いて，機械学習によりデバイスと機能を分類し，その精度を評価した．その結

果，デバイスの機種と実行機能の 16 種類の組み合わせで分類した場合，91% の精度で機能を推定できることを確認した．また，実行機能のみの 8 種類の組み合わせで分類した場合，73% の精度で機能を推定できることを確認した．今後は，IoT デバイスの種類や実行機能の数をさらに増やし，特徴量の値を改善することで精度を向上させる．また，既存の行動認識技術と連携し，利用者の意図した通信かどうかの識別，結果の可視化，通信制御を行うことで，利用者がより安心して IoT デバイスを利用できる世界の実現を目指す．

4.4　通信トラヒック分析による数秒間隔での IoT デバイスの機能推定手法

従来の方法では，機能実行時の全通信トラヒックから特徴量を計算・推定するため，通信制御に利用するためには実行時の実行・終了を検出する必要がある．そのため，数秒間の通信に対して通信制御を行うことは困難である．本節では参考文献 [73] を引用し，この問題を解決するために，機械学習を用いて 1 秒あたりの特徴量を用いて IoT デバイスの機能の実行状態を推定し，その推定精度を評価した．特徴量については，従来の手法と同様に，通信トラヒックの量に関する特徴量を抽出し個人を特定できる情報を含まない特徴量を用いた．

4.4.1　機能推定手法

4.3.1 節の手法では，機能を実行した際の通信トラヒックのすべてから特徴量を計算し推定しているため，通信の制御のために利用するためには，機能の実行と終了の検出が必要となる．そのため，数秒の通信から通信の制御を行うことは難しい．本節では，その問題を解決するために，1 秒ごとの特徴量を用いて，機械学習で IoT デバイスの機能の実行状態を推定し，その精度を評価した．また，本稿では，1 秒ごとの状態を推定するために，4.2 節で述べた通信トラヒックを 1 秒ごとに静止状態を含む発動機能のラベルを付与した．特徴量は，各秒の 3 秒前までの通信トラヒックを用いて計算し，従来の手法同様，個人や特定の製造業者を特定できる情報を含まない特徴量を用いた．宛先 IP や MAC アドレスなど，個人やメーカーに関連する

特徴を用いれば精度は向上するが，これらを使用する場合，プライバシーの問題もある．そこで，通信量に由来する特徴量に着目した．算出した特徴量を表 4.10-表 4.12 に示す．特徴量の中からランダムフォレストアルゴリズムを用いて重要度を算出し，重要度の高い順に 39 番目までの特徴量を用いた．機械学習アルゴリズムは，教師あり機械学習であるランダムフォレストアルゴリズムを用い，また，静止のラベルの通信トラヒックが非常に多いためアンダーサンプリングを行い，ラベルごとの数を揃えたのち，10 分割交差検証により評価を行った．

4.4.2　評価

機能推定手法の妥当性を検証するため，ランダムフォレストアルゴリズムを用い，10 分割交差検証による評価を行った．また，本研究では実行機能の分類に重点を置いているため，デバイスの分類は行っていない．そのため，機能推定方法については，デバイスがすでに分類されているものとして評価した．各機種において，重要度の高い順に 39 番目までの特徴量を用いた．各機種における特徴量の重要度を図 4.5 と図 4.8 に示す．UDP 関連の特徴量については，全機種で寄与がなかった．通信量の多いスマートスピーカーは 1 秒に関する特徴量の寄与が大きく，スマートプラグは送信パケットサイズに関する特徴量の寄与が大きい．

その結果，8 機種のうち 5 機種は 83% 以上の精度で分類できたが，3 機種は 60% 台の精度でうまく分類できなかった．各機種の混同行列を表 4.13-表 4.20 に，クラスラベルを表 4.21 に示す．表 4.22 に各機種の実行機能の分類精度を示す．特に，両スマートリモコンの精度は，他の 2 つの機種よりも低い．これは，機能実行に必要な通信回数が少ないことも影響しているが，スマートリモコンは指示を受けた機能に対して赤外線信号を送信しており，実際の通信はほぼ同じであるため，通信トラヒックだけで分類することが難しい．スマートカメラ Mi 360° も実際の通信にほとんど差がないため，精度が低いと考えられる．Ranger 2 と Mi 360° の精度の差は，開発元が異なる 2 つのカメラの通信の違いによるものである．静止状態を誤認識している部分については，IoT デバイスは静止していても何らかの通信を行っている可能性があるため，誤認識が発生していると考えられる．

4.4.3　議論

この項では，IoT デバイスの設定の影響，IoT デバイスのファームウェアの更新の影響，通信トラヒックが似た機能など，いくつかの重要な問題について議論する．

IoT デバイスの設定の影響

本研究では，日本国内で流通する IoT デバイスを対象としたため，日本を対象に通信トラヒックを収集・評価した．しかし，IoT デバイスは様々な国で流通しており，同じような機能であっても言語設定や位置情報などによって特性が異なる場合がある．そのため，IoT デバイスの構成による影響も考慮する必要がある．

IoT デバイスのファームウェアの更新による影響

IoT デバイスは，定期的にファームウェアの更新が発生し，その際に通信先や通信量などに変化が生じる可能性がある．また，スマートスピーカーなどの第三者の提供するアプリケーションを追加で導入することが可能な IoT デバイスではアプリケーションの更新も考慮する必要があり，更新後の通信トラヒックを収集して学習を行う仕組みを構築する必要がある．

利用者の行動に関わらず実行される機能

今回推定を行った機能は，利用者が指示を出すことにより，実行されるものと利用者が何も行っていない状態を推定している．しかしながら，IoT デバイスは，利用者が指示を出さなくともファームウェアの更新などで通信を行っている．利用者の指示により実行される機能と異なり，任意の時点で機能を実行することができないため通信トラヒックの収集が難しいが，それらの機能も考慮して推定していく必要がある．

通信トラヒックが似た機能

多くの IoT デバイスの通信は，HTTPS で行われており暗号化されている．本手法では，通信の中身を確認しないため，送信時の通信パケットサイズや受信時の通信パケット数などの特

徴量を用いている．また，多くの IoT デバイスの通信は，JSON などの形式で内容の受信や送信を行っており，通信も数回しか発生せず，内容もあまり差異のないものがある．特にスマートリモコンの場合は，いずれの機能を使うにせよ基本的に赤外線の発信機に対して命令を送るためあまり内容に差異がない．そのため通信トラヒックのみから分類することは難しいと考えられる．実際にこれらの機能を検知するためには，既存の行動認識の技術と連携し，部屋の在室状況などと連動し検知を行う必要がある．

IoT 活動量計の実現に必要な精度

我々が提案する IoT 活動量計は，通信トラヒックのパターンの解析に基づき，IoT デバイスの実行機能の通信を一時的または恒久的に遮断する機能を持っている．IoT 活動量計で実際に通信トラヒックを制御するためには，正常な通信を妨げてはならないため，高い精度が要求される．そのため，実環境で利用するためには，本研究の結果以上の精度が必要となる．

4.4.4　まとめ

本稿では，我々が提案する IoT 活動量計に用いる IoT デバイスの実行した機能単位での通信の制御の実現に向けて，IoT デバイスの通信トラヒック分析による IoT デバイスの数秒間隔での機能推定手法を示し評価した．実際に日本国内で流通しているスマートスピーカー，スマートカメラ，スマートリモコン，スマートプラグ，4 種別の IoT デバイス各 2 機種ずつの計 8 機種中，5 機種において，1 秒ごとの特徴量を用いて静止を含む 3 種類の機能の推定について 83% 以上の精度で分類することができたが，3 機種については，60% 台の精度であり，うまく分類できていない．IoT 活動量計で実際に通信トラヒックを制御するためには，正常な通信を妨げてはならないため，高い精度が求められる．今回，83 %以上の精度で識別できた IoT デバイスもあったが，実際の環境に導入するためには，さらなる精度向上が必要である．

今後は，さらに IoT デバイスの種別と実行する機能を増やしての評価を行うとともに特徴量の改善を行い精度の向上を図る．また，実際に IoT デバイスと開発中の IoT 活動量計を設置したスマートホーム環境を用意し，実環境で IoT 活動量計が特定機能の通信制御を行えるか検

証する予定である．通信トラヒックのみで推定が難しいものについては，既存の行動認識の技術と連携して制御する方法を検討する．通信が利用者の意図したものかどうかを識別し，結果の可視化と通信の制御を行うことにより，利用者がより安心して IoT デバイスを利用できる世界の実現を目指す．

表 4.10: 計算した特徴量

No.	特徴量
1	1 秒間の送信パケット数
2	1 秒間の送信パケットサイズの最大
3	1 秒間の送信パケットサイズの最小
4	1 秒間の受信パケット数
5	1 秒間の受信パケットサイズの最大
6	1 秒間の受信パケットサイズの最小
7	1 秒間の TCP パケット数
8	1 秒間の UDP パケット数
9	1 秒間の TCP パケットサイズの最大
10	1 秒間の TCP パケットサイズの最小
11	1 秒間の UDP パケットサイズの最大
12	1 秒間の UDP パケットサイズの最小
13	1 秒間の送信先 IP 数
14	1 秒間の送信元 IP 数
15	1 秒間の送信パケットサイズの平均
16	1 秒間の送信パケットサイズの分散
17	1 秒間の送信パケットサイズの標準偏差
18	1 秒間の受信パケットサイズの平均
19	1 秒間の受信パケットサイズの分散
20	1 秒間の受信パケットサイズの標準偏差
21	1 秒間の TCP パケットサイズの平均
22	1 秒間の TCP パケットサイズの分散
23	1 秒間の TCP パケットサイズの標準偏差
24	1 秒間の UDP パケットサイズの平均
25	1 秒間の UDP パケットサイズの分散
26	1 秒間の UDP パケットサイズの標準偏差
27	2 秒間の送信パケット数
28	2 秒間の送信パケットサイズの最大

表 4.11: 計算した特徴量 (続き)

No.	特徴量
29	2 秒間の送信パケットサイズの最小
30	2 秒間の受信パケット数
31	2 秒間の受信パケットサイズの最大
32	2 秒間の受信パケットサイズの最小
33	2 秒間の TCP パケット数
34	2 秒間の UDP パケット数
35	2 秒間の TCP パケットサイズの最大
36	2 秒間の TCP パケットサイズの最小
37	2 秒間の UDP パケットサイズの最大
38	2 秒間の UDP パケットサイズの最小
39	2 秒間の送信先 IP 数
40	2 秒間の送信元 IP 数
41	2 秒間の送信パケットサイズの平均
42	2 秒間の送信パケットサイズの分散
43	2 秒間の送信パケットサイズの標準偏差
44	2 秒間の受信パケットサイズの平均
45	2 秒間の受信パケットサイズの分散
46	2 秒間の受信パケットサイズの標準偏差
47	2 秒間の TCP パケットサイズの平均
48	2 秒間の TCP パケットサイズの分散
49	2 秒間の TCP パケットサイズの標準偏差
50	2 秒間の UDP パケットサイズの平均
51	2 秒間の UDP パケットサイズの分散
52	2 秒間の UDP パケットサイズの標準偏差
53	3 秒間の送信パケット数
54	3 秒間の送信パケットサイズの最大
55	3 秒間の送信パケットサイズの最小
56	3 秒間の受信パケット数

表 4.12: 計算した特徴量 (続き)

No.	**特徴量**
57	3 秒間の受信パケットサイズの最大
58	3 秒間の受信パケットサイズの最小
59	3 秒間の TCP パケット数
60	3 秒間の UDP パケット数
61	3 秒間の TCP パケットサイズの最大
62	3 秒間の TCP パケットサイズの最小
63	3 秒間の UDP パケットサイズの最大
64	3 秒間の UDP パケットサイズの最小
65	3 秒間の送信先 IP 数
66	3 秒間の送信元 IP 数
67	3 秒間の送信パケットサイズの平均
68	3 秒間の送信パケットサイズの分散
69	3 秒間の送信パケットサイズの標準偏差
70	3 秒間の受信パケットサイズの平均
71	3 秒間の受信パケットサイズの分散
72	3 秒間の受信パケットサイズの標準偏差
73	3 秒間の TCP パケットサイズの平均
74	3 秒間の TCP パケットサイズの分散
75	3 秒間の TCP パケットサイズの標準偏差
76	3 秒間の UDP パケットサイズの平均
77	3 秒間の UDP パケットサイズの分散
78	3 秒間の UDP パケットサイズの標準偏差

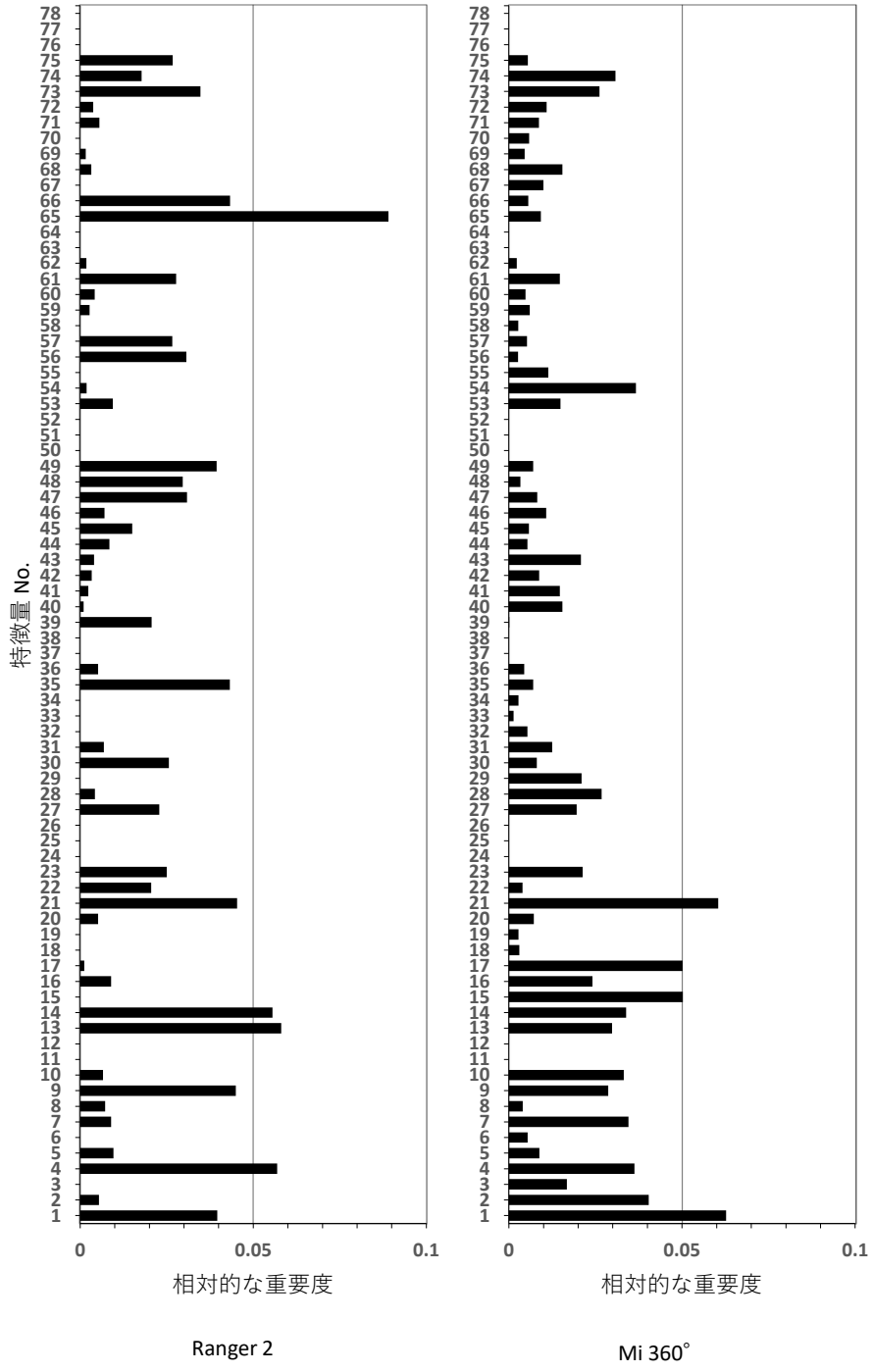

図 4.5: 各機種の特徴量の重要度 (スマートカメラ)

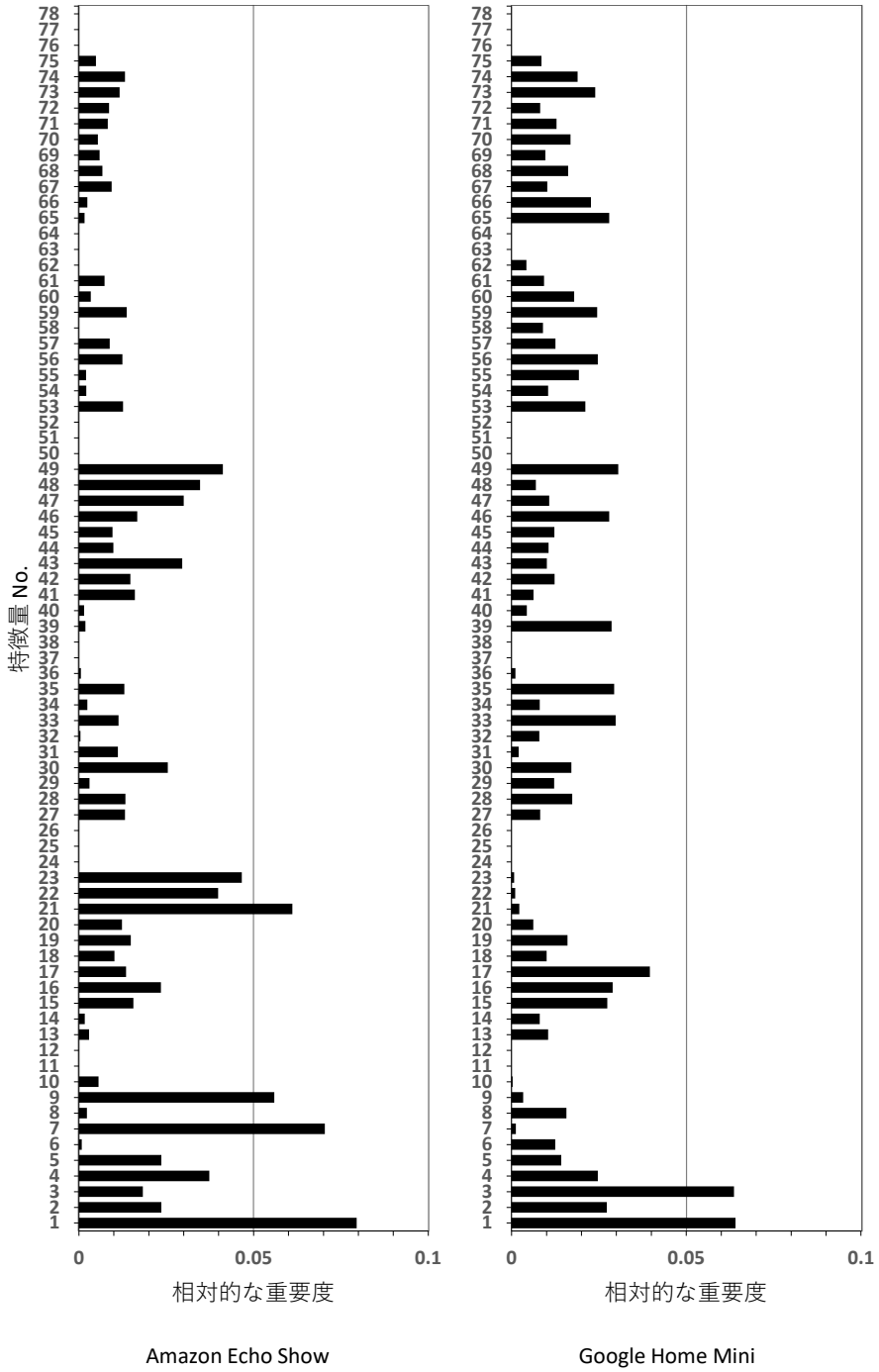

図 4.6: 各機種の特徴量の重要度 (スマートスピーカー)

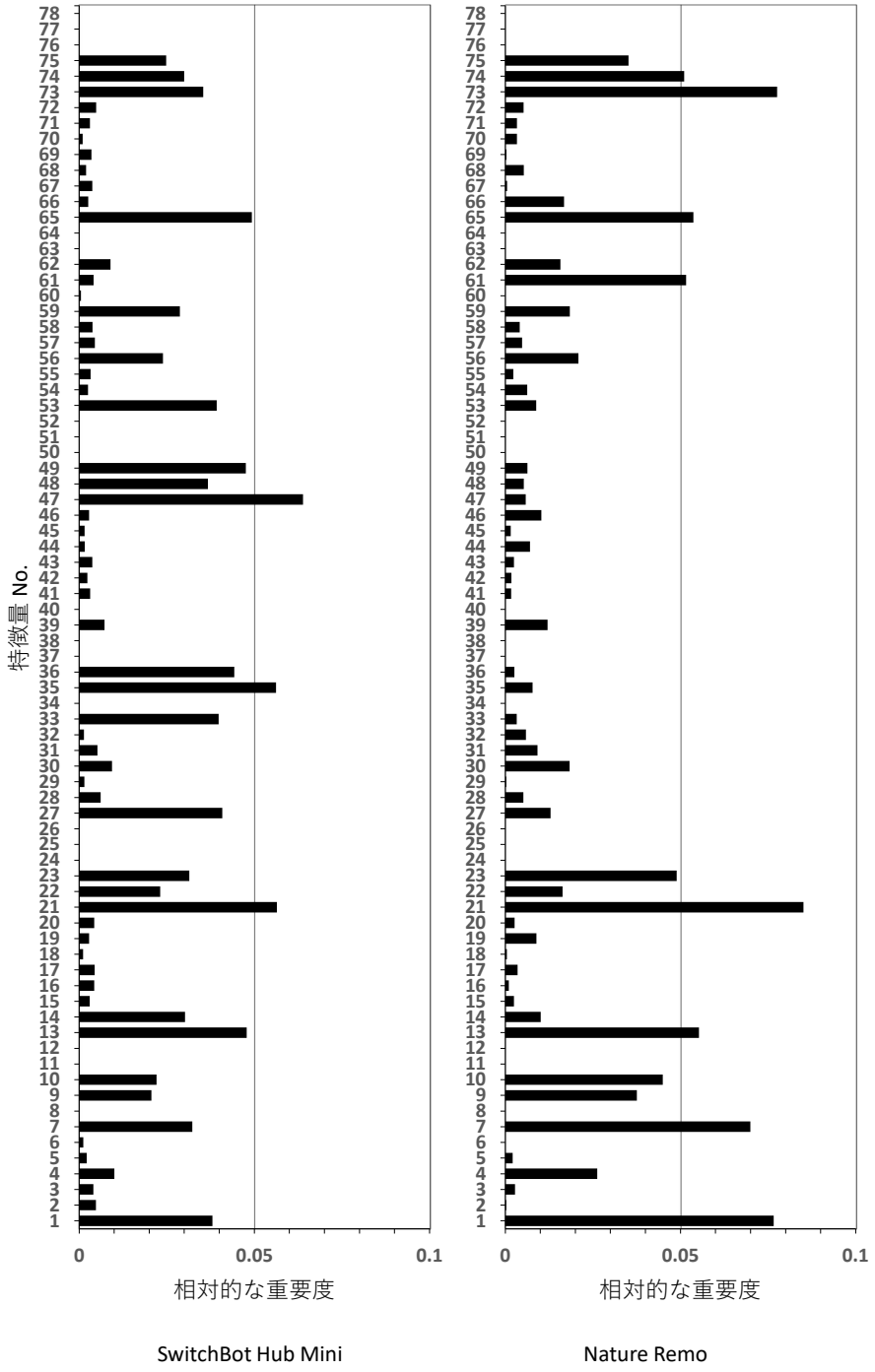

図 4.7: 各機種の特徴量の重要度 (スマートリモコン)

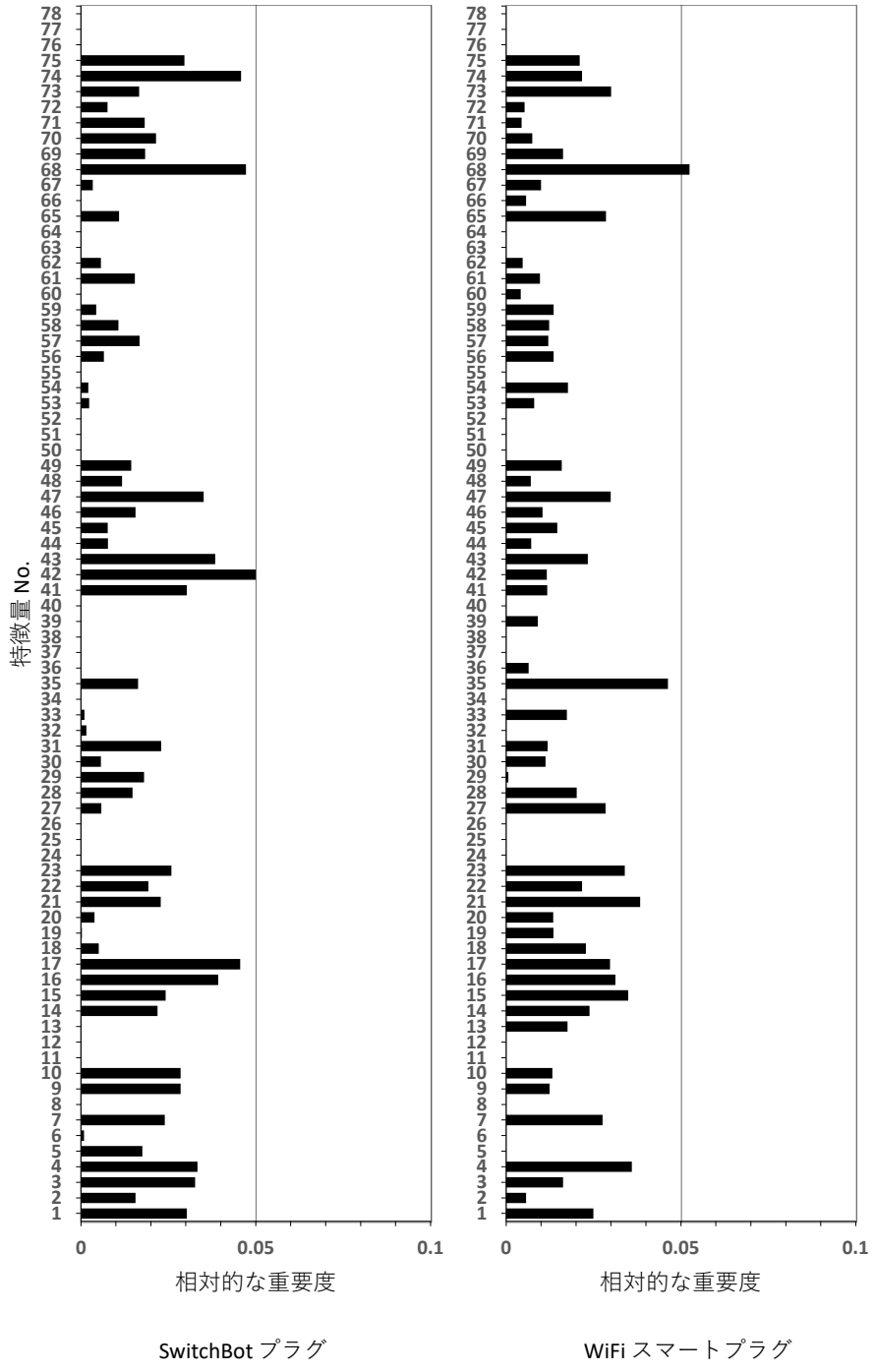

図 4.8: 各機種の特徴量の重要度 (スマートプラグ)

表 4.13: 実行機能推定結果の混同行列

(Ranger 2: スマートカメラ)

	0	**1**	**2**
0	10	0	0
1	0	10	0
2	0	0	10

表 4.14: 実行機能推定結果の混同行列

(Mi 360°: スマートカメラ)

	0	**1**	**2**
0	10	0	0
1	2	5	3
2	0	5	5

表 4.15: 実行機能推定結果の混同行列

(SwitchBot Hub Mini: スマートリモコン)

	0	**3**	**4**
0	18	0	1
3	0	15	4
4	0	15	4

表 4.16: 実行機能推定結果の混同行列

(Nature Remo: スマートリモコン)

	0	**3**	**4**
0	10	0	0
3	1	5	4
4	0	5	5

表 4.17: 実行機能推定結果の混同行列

(Amazon Echo Show: スマートスピーカー)

	0	**5**	**6**
0	70	0	2
5	0	59	13
6	0	6	66

表 4.18: 実行機能推定結果の混同行列

(Google Home Mini: スマートスピーカー)

	0	**5**	**6**
0	33	3	2
5	1	27	7
6	2	2	30

表 4.19: 実行機能推定結果の混同行列

(SwitchBot プラグ: スマートプラグ)

	0	**7**	**8**
0	10	0	0
7	0	9	1
8	0	0	10

表 4.20: 実行機能推定結果の混同行列

(WiFi スマートプラグ: スマートプラグ)

	0	**7**	**8**
0	10	0	0
7	0	7	3
8	0	2	8

表 4.21: 実行機能推定結果の混同行列である表 4.13-表 4.20 のクラスラベル

クラスラベル	内容
0	静止
1	カメラの向きを変える (左に 3 秒)
2	話しかける
3	TV をミュートにする
4	TV を ON にする
5	音楽を再生する (10 秒)
6	今日の天気を聞く
7	電源を OFF にする
8	電源を ON にする

表 4.22: 各デバイスの分類精度一覧

	機種	デバイス名	精度
1	スマートカメラ	Ranger 2	100%
2		Mi 360°	67%
3	スマートリモコン	SwitchBot Hub Mini	65%
4		Nature Remo	67%
5	スマートスピーカー	Amazon Echo Show	90%
6		Google Home Mini	83%
7	スマートプラグ	SwitchBot プラグ	97%
8		WiFi スマートプラグ	83%

第 5 章

議論と今後の展望

本研究では，家庭内の IoT デバイスを安心・安全に利用するための IoT 活動量計を提案し，その PoC を行い一部の IoT デバイスについて想定する動作が実行できることを確認した．また，IoT 活動量計の実現のための通信トラヒックから抽出した個人を特定できる情報を含まない特徴量での IoT デバイスの実行機能の推定手法について提案と評価を行い一定の精度で IoT デバイスの実行機能を推定することができた．本章では，これらの評価結果から考察される課題と今後の展望について述べる．

5.1 議論

今後，さらに IoT デバイスや実行機能の対象を増やしていくにあたって実行機能の分類に用いる特徴量の追加も検討していく必要がある．IoT デバイスのファームウェアの更新による影響は，IoT デバイスがクラウド上のサーバーと接続され定期的にファームウェアの更新が実行される以上，避けることができない課題である．本研究では，利用者の行動に基づくビデオ通話や家電の操作といった実行機能を対象に行ったが，実行機能の評価の際に静止状態と誤認識している結果がいくつかあり，これは時刻同期などの利用者の行動に関わらず実行される機能が影響していると考えられる．実行機能の評価の際にスマートリモコンは特に実行機能が違う場合でも通信機能が似ているため，今回の評価に用いた手法だけでは，分類することが難し

い．また，IoT 活動量計を実際の家庭に導入する場合，正常な実行機能を妨害してはならないため，高精度な実行機能の分類が必要となる．そして，IoT 活動量計は，管理システムをクラウド上のサーバーに構築する想定で設計されており，実際に運用する際には運用する組織が必要となる．これらの課題を解決することで家庭内の IoT デバイスを安心・安全に利用するための IoT 活動量計の実現につながる．以下ではそれらの考察される課題について述べる．

5.1.1　実行機能の分類に用いる特徴量

本研究では，特徴量として個人を特定できる情報を含まないものを用いるために通信トラヒックから得られるパケット数やパケットサイズといった量に関する特徴量を用いた．また，特徴量の重要度に関する評価を行い，4.4.2 節で述べた通り，今回の対象の実行機能においては，UDP 関連の特徴量については，全機種で寄与がなく，通信量の多いスマートスピーカーは 1 秒に関する特徴量の寄与が大きく，スマートプラグは送信パケットサイズに関する特徴量の寄与が大きいという結果を得た．また，今後さらに IoT デバイスや実行機能の対象を増やしていくにあたっては，IoT デバイスの種別や実行機能によって特徴が異なる可能性がある．そのため，対象を増やしていく際には，新しい特徴量の検討を行い評価していく必要がある．

5.1.2　IoT デバイスのファームウェアの更新による影響

IoT デバイスは，定期的にファームウェアの更新が発生し，その際にクラウド上のサーバーとの通信内容が変更されることにより，通信先や通信量などに変化が生じる可能性がある．また，スマートスピーカーなどの高機能な IoT デバイスについては，第三者が提供するアプリケーションを追加で導入することが可能であり，それらのアプリケーションの更新も考慮する必要がある．そのため，今後更新後の通信トラヒックを収集して学習を行う仕組みを構築する必要がある．

5.1.3　利用者の行動に関わらず実行される機能

今回 4.4 節にて推定を行った機能は，利用者が指示を出すことにより，実行されるものと利用者が何も行っていない状態を推定している．しかしながら，IoT デバイスは，利用者が指示を出さなくともファームウェアの更新や時刻同期などで通信を行っている．利用者の指示により実行される機能と異なり，任意の時点で機能を実行することができないため通信トラヒックの収集が難しいが，それらの機能も考慮して推定していく必要がある．

5.1.4　通信トラヒックが似た機能

多くの IoT デバイスの通信トラヒックは，HTTPS で行われており暗号化されている．これは，暗号化せずに通信を行った場合，通信経路で通信トラヒックに含まれる重要情報などが漏えいする可能性があるためである．本手法では，個人を特定できる情報を使わない形をとっており，通信の中身を確認しないため，送信時の通信パケットサイズや受信時の通信パケット数などの特徴量を用いている．また，多くの IoT デバイスの通信は，WebAPI を用いて JSON などの形式で内容の受信や送信を行っており，通信も数回しか発生せず，内容もあまり差異のないものがある．特にスマートリモコンなどの場合は，いずれの機能を使うにせよ基本的に赤外線の発信機に対して命令を送るためあまり通信内容に差異がない．そのため通信トラヒックのみから分類することは難しいと考えられる．実際にこれらの機能を検知するためには，既存の行動認識の技術と連携し，部屋の在室状況などと連動し検知を行うことなどを検討していく必要がある．

5.1.5　IoT 活動量計の実現に必要な精度

我々が提案する IoT 活動量計は，通信トラヒックのパターンの解析に基づき，IoT デバイスの実行機能の通信を一時的または恒久的に遮断する機能を持っている．IoT 活動量計で実際に通信トラヒックを制御するためには，正常な通信を妨げてはならないため，高い精度が要求さ

れる．4.4 節の手法では，日本国内で流通しているスマートスピーカー，スマートカメラ，スマートリモコン，スマートプラグ，4 種別の IoT デバイス各 2 機種ずつの計 8 機種のうち 5 機種において，1 秒ごとの特徴量を用いて静止を含む 3 種類の機能の推定について 83% 以上の精度で分類することができた．しかし，実環境で利用するためには，本研究の結果以上の精度が必要となる．

5.1.6　IoT 活動量計を運用の問題

IoT 活動量計は，管理システムをクラウド上のサーバーに構築する想定で設計されている．そのため，実際に多くの利用者に利用してもらうためには，そのクラウド上のサーバーを誰かが運用していく必要がある．その運用を誰が行うかについては，IoT デバイスの製造元が運用すると競合他社との関係性などのために対応が偏る可能性があるので，IoT デバイスを製造していない中立的な機関が運用することが望ましい．また，参考となる IoT デバイスに関する認定では，クラウドサービスである AWS に限定されるが AWS と連携するための AWS デバイス認定プログラム [74] や国内では，経済産業省にて IoT 製品に対するセキュリティ適合性評価制度構築に向けた検討 [75] が進められている．

5.2　今後の展望

本節では，本研究の結果と議論から家庭内の IoT デバイスを安心・安全に利用するための IoT 活動量計を実際の環境で実現するために必要となる今後の展望について述べる．

5.2.1　IoT デバイスの種別と機能を増やしての評価

本研究では，日本国内で流通しているスマートスピーカー，スマートカメラ，スマートリモコン，スマートプラグ，4 種別の IoT デバイス各 2 機種ずつの計 8 機種の合計 16 種類の機能の通信トラヒックを用いて精度の評価を行った．しかし，その他にも家庭向け IoT デバイスは多く存在しており，より多くの IoT デバイスとその機能を含めた評価を行う必要がある．ま

た，日本国内での利用を想定し，日本語設定で操作を行っているため，言語設定による通信への影響も調査する必要がある．本研究では，我々が通信トラヒックを収集してデータセットを作成して評価している．もし，IoT デバイスの開発元の協力が得られるのであれば，5.2.2 項で述べている利用者の行動と関係ない機能も含めて通信トラヒックのサンプルなどを得ることができる可能性がある．そのような協力体制を築くためにも IoT デバイスの評価を行うため必要な項目をひな形として用意し，より多くの IoT デバイスを評価できる仕組みを構築する必要がある．

5.2.2　利用者の行動と関係ない機能の推定

4.2 節で述べた今回 IoT デバイスの機能推定に用いたデータセットは，利用者の行動に紐づいた実行機能である．IoT デバイスは，自動更新やバックアップなどの利用者の行動に紐づかない実行機能が多々ある．これらの実行機能は，ビデオ通話や家電の操作と違い，利用者の行動によって実行される機能ではない．利用者の行動に紐づく実行機能であれば，4.2.1 項で述べた収集方法でデータセットを作成することができるが，利用者の行動に紐づかない実行機能は同じ方法では収集することができない．利用者の行動に紐づかない実行機能の評価を行うために，その通信トラヒックの収集も含めて検討する必要がある．

5.2.3　他の行動認識技術との連携

5.1.4 項で述べた通り，通信トラヒックの特徴だけでは分類することが難しい実行機能が存在する．スマートリモコンなどの通信トラヒックが少なくかつほぼ差異がないものについては，通信トラヒックのみからの分類を行うことが難しい．そのため，既存の行動認識技術と連携し，部屋の在室状況などの情報を用いることにより，それらの実行機能を分類する必要がある．スマートホームの研究では，温度センサや照度センサなどの様々なセンサや Wi-Fi の電波を使い，利用者の行動認識などの研究がおこなわれている．それらの研究成果と連携することにより，通信トラヒックから分類することが難しい実行機能についても分類することができる

ようになると考えられる．

5.2.4　実際の環境での IoT 活動量計の評価

本研究では，IoT 活動量計について，いくつかの IoT デバイスを接続した検証環境で PoC を実施し評価した．今後の，さらに 2 段階の評価を行っていく必要がある．次の段階は，5.2.3 項で述べた他の行動認識技術との連携を行っていくために，他の研究で行っているスマートホームを模した環境での実験 [34] のような実験形態を検討していく必要がある．その次の段階は，スマートホームを模した環境での実験の後に，実際の家庭環境に IoT デバイスを設置し，IoT 活動量計が実際の家庭環境で動作するかを検証していく必要がある．また，実際の家庭環境に設置を行って実験を行う際には，設置する IoT デバイスやセンサの選定も同時に行う必要がある．

第 6 章

まとめ

本論文では，家庭向けの IoT デバイスに関するセキュリティ上の問題を解決し IoT デバイスを安心・安全に利用するために，通信トラヒックを用いて IoT デバイスの実行機能を分類し，通信トラヒックを制御する IoT 活動量計を提案し，IoT 活動量計の実現のための通信トラヒックから抽出した個人を特定できる情報を含まない特徴量での IoT デバイスの実行機能の推定手法について述べた．以下，各章で得られた成果について述べる．

1 章では，本研究の背景と目的について述べ，課題である IoT デバイスがどのような通信を行っているかを検知し，それをもとに適切な通信のみ許可し通信トラヒックを制御することと通信トラヒックから抽出した個人を特定できる情報を含まない特徴量での IoT デバイスの実行機能を推定することについて，概要と貢献を述べた．

2 章では，ユビキタスコンピューティングに関わる研究について述べるとともに，関連研究と本研究の立ち位置について述べた．

3 章では，家庭内の IoT デバイスを安心・安全に利用するための IoT 活動量計と呼ばれるフレームワークを提案し，PoC を実施しその結果を報告する．提案システムでは，事前に収集した通信トラヒックから生成したアクセス制御を用いて，一部の IoT デバイスの特定の機能を許可／拒否することができ，本提案が有益であることを示した．

4 章では，IoT 活動量計の実現のために必要な通信トラヒックの分析のために収集した日本国内で流通しているスマートスピーカー，スマートカメラ，スマートリモコン，スマートプラ

グ，4 種別の IoT デバイス各 2 機種ずつの計 8 機種の 8 種類の機能の通信トラヒックとその収集方法について述べ，そして，その通信トラヒックを用いた 2 種類の機能推定手法についての評価結果を述べる．一つは，機能実行時の全通信トラヒックから特徴量を計算し，個人や特定の製造元を特定できる情報を含まない 28 個の特徴量を用いて，ランダムフォレストアルゴリズムによる分類を行い，その精度を IoT デバイスの機種と実行機能の組み合わせ 16 種類と，実行機能のみの組み合わせ 8 種類の計 2 種類で評価した．その結果，デバイスの機種と実行した機能の組み合わせの 16 通りで分類した場合，91% の精度で機能を分類できることを確認した．また，実行した機能のみの 8 通りで分類した場合，73% の精度で機能を分類できることを確認した．しかしながら，この手法では，機能を実行した際の通信トラヒックのすべてから特徴量を計算し推定しているため，通信の制御のために利用するためには，機能の実行と終了の検出が必要である．一つは，8 つの IoT デバイスに対して静止を含む 3 種類の機能の推定を 1 秒ごとの特徴量を用いて，ランダムフォレストアルゴリズムで IoT デバイスの機能の実行状態を推定し，その精度を評価した．そして，8 機種のうち 5 機種は 83% 以上の精度で分類できた．また，残りの 3 機種については，通信トラヒックのみからの分類は難しいということを考察として述べ，提案手法において，5 機種において一定の精度で IoT デバイスの実行機能が分類できることを示した．

5 章では，得られた知見から，今後 IoT 活動量計を実現させていくうえで考慮していく必要がある考察を行い，今後の展望と課題について述べた．今後，家庭内の IoT デバイスを安心・安全に利用するための IoT 活動量計の実現に向けて，IoT デバイスの種別と機能を増やしての評価や既存の行動認識技術と連携することによる通信トラヒックから分類することが難しい実行機能に対する分類の検討を行い，そして，スマートホームを模した環境などの実際の環境に近い形での実験を行い IoT 活動量計が実際の環境で動作するかを検証していく必要がある．

以上のように本研究では，家庭内の IoT デバイスを安心・安全に利用するための IoT 活動量計を提案し，その PoC を行い一部の IoT デバイスについて想定する動作が実行できることを確認した．また，IoT 活動量計の実現のための通信トラヒックから抽出した個人を特定でき

る情報を含まない特徴量での IoT デバイスの実行機能の推定手法について提案と評価を行い 8 機種のうち 5 機種は 83% 以上の精度で分類できたが，残りの 3 機種については，通信トラヒックのみからの分類は難しいということが分かった．そして，その結果から得られた知見から，今後 IoT 活動量計を実現させていくうえで考慮していく必要がある考察を述べた．

謝辞

本研究を進めるにあたって，実に多くの方のご理解とご協力賜り，心より感謝申し上げます．

まず，指導教員である九州工業大学井上創造教授には，修士論文，博士論文と長きにわたりご指導いただきましたことを心より感謝申し上げます．特に社会人博士後期課程として受け入れて頂き，ここまで研究を続けてこれたのは，井上創造教授のご指導のおかげです．

共同研究先である九州大学荒川豊教授には，ご多忙の中丁寧にご指導いただき助言を頂きましたことを深く感謝しております．ユビキタスコンピューティングに加えセキュリティに関わる研究を進めることができたのは荒川豊教授のご指導があってのことです．

また，研究にあたり貴重な議論をして頂きました井上創造研究室のメンバーに感謝申し上げます．

研究にあたる事務処理をご支援して頂きました内田美貴氏に深く感謝申し上げます．特に国際学会に関する事務手続き等，社会人学生ですので普通の学生と違いイレギュラーなものもあったかと思いますが対応していただき感謝しております．

そして，研究に対して理解していただいた株式会社セキュアサイクルの方々にも感謝申し上げます．

最後に，これまで私をあたたかく応援してくれた両親，妻と 3 人の娘達に心から感謝します．

参考文献

[1] 総務省. 情報通信白書令和 5 年版. https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/index.html. (2024 年 6 月 6 日閲覧).

[2] Google LLC. Best Google Home Devices: Smart Gadgets & Products for Your Home — Google Home. https://home.google.com/welcome/. (2024 年 6 月 6 日閲覧).

[3] Amazon.com, Inc. Amazon.com: Echo Smart Speakers & Displays: Amazon Devices & Accessories: Smart Speakers, Smart Displays & More. https://www.amazon.com/smart-home-devices/b?ie=UTF8&node=9818047011. (2024 年 6 月 6 日閲覧).

[4] Cathy Pearl. *Designing voice user interfaces*. O'Reilly Media, December 2016.

[5] Forbes. Time To Update Your Vacuum Cleaner – Hack Turns LG Robot Hoover Into A Spy. https://www.forbes.com/sites/thomasbrewster/2017/10/26/lg-hom-bot-robot-hoover-hacked-into-surveillance-device/. (2024 年 6 月 6 日閲覧).

[6] XDA. TP-Link Deco X68 Review: A good mesh router ruined by bizarre software. https://www.xda-developers.com/tp-link-deco-x68-review. (2024 年 6 月 6 日閲覧).

[7] Guoming Zhang, Chen Yan, Xiaoyu Ji, Tianchen Zhang, Taimin Zhang, and Wenyuan Xu. DolphinAttack: Inaudible Voice Commands. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, CCS ' 17. ACM, October 2017.

[8] Anirban Chakraborty, Manaar Alam, Vishal Dey, Anupam Chattopadhyay, and Deb-

deep Mukhopadhyay. Adversarial attacks and defences: A survey. *arXiv preprint arXiv:1810.00069*, 2018.

[9] Jian Mao, Shishi Zhu, Dai Xuan, Qixiao Lin, and Jianwei Liu. Watchdog: Detecting ultrasonic-based inaudible voice attacks to smart home systems. *IEEE Internet of Things Journal*, 2020.

[10] Cloudflare, Inc. マルウェアとは？ — Cloudflare. https://www.cloudflare.com/ja-jp/learning/ddos/glossary/malware/. (2024 年 6 月 6 日閲覧).

[11] JPCERT/CC. JVNTA#95530271 Mirai 等のマルウェアで構築されたボットネットによる DDoS 攻撃の脅威. https://jvn.jp/ta/JVNTA95530271/. (2024 年 6 月 6 日閲覧).

[12] JPCERT/CC. Mirai 亜種の感染活動に関する注意喚起. https://www.jpcert.or.jp/at/2017/at170049.html. (2024 年 6 月 6 日閲覧).

[13] NICT. NICTERWEB - Dark net observation — National Institute of Information and Communications Technology Cybersecurity Laboratory. https://www.nicter.jp/en. (2024 年 6 月 6 日閲覧).

[14] NICT. NICTER Observation Report 2023. https://csl.nict.go.jp/report/NICTER_report_2023.pdf. (2024 年 6 月 6 日閲覧).

[15] NICTER. Survey Scanner List. https://github.com/nict-csl/survey-scanner. (2024 年 6 月 6 日閲覧).

[16] JPCERT/CC. 注意喚起「ネットワークに接続されたシステム・機器の設定には注意を」. https://www.jpcert.or.jp/pr/2016/pr160001.html. (2024 年 6 月 6 日閲覧).

[17] アイティメディア株式会社. 家のカギが「サービス終了」で物議 その後の対応は？ スマートロックの Qrio に聞く（1/2 ページ） - ITmedia NEWS. https://www.itmedia.co.jp/news/articles/2305/17/news113.html. (2024 年 6 月 6 日閲覧).

[18] JPCERT/CC. JVNVU#94260088 エレコム製ルータにおける認証不備および OS コマ

ンドインジェクションの脆弱性. https://jvn.jp/vu/JVNVU94260088/. (2024 年 6 月 6 日閲覧).

[19] JPCERT/CC. JVN#82074338 NEC Aterm シリーズにおける複数の脆弱性. https://jvn.jp/jp/JVN82074338/index.html. (2024 年 6 月 6 日閲覧).

[20] JPCERT/CC. JVNVU#90274525 バッファロー製の複数のネットワーク機器においてデバッグ機能を有効化される問題. https://jvn.jp/vu/JVNVU90274525/. (2024 年 6 月 6 日閲覧).

[21] Yahoo. Zoom admits some calls were routed through China by mistake. https://techcrunch.com/2020/04/03/zoom-calls-routed-china/. (2024 年 6 月 6 日閲覧).

[22] Mark Weiser. Some computer science issues in ubiquitous computing. *Commun. ACM*, 36(7):75–84, jul 1993.

[23] 井上 創造. ウェアラブルセンサを用いたヒューマンセンシング. **知能と情報**, 28(6):170–186, 2016.

[24] 徳田 英幸. センサネットワーク総論. **計測と制御**, 46(2):71–76, 2007.

[25] Yuichi Hattori and Sozo Inoue. A Large Scale Gathering System for Activity Data using Mobile Devices. *Journal of Information Processing*, 20(1):177–184, 2012.

[26] Nattaya Mairittha and Sozo Inoue. Gamification for high-quality dataset in mobile activity recognition. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, 240:216–222, 2018.

[27] 南石 晃明, 谷口 倫一郎, 竹田 正幸, 星 岳彦, 岡安 崇史, 平井 康丸, 坂内 英夫, 長原 一, 金子 邦彦, 有田 大作, 竹内 重吉, 畑埜 晃平, 島田 敬士, and 長命 洋佑. 低コスト・省力化, 軽労化技術等の開発—農家の作業技術の数値化及びデータマイニング手法の開発—第 1 章「農匠ナビ」全体システム設計・開発・評価 1「農匠ナビ」全体システム設計・実証および農作業連続計測・可視化・データマイニング基盤技術の研究開発. **農林水産省農林水産技**

術会議事務局研究成果, (543):14–18, 3 2016.

[28] 井上 吉雄 and 横山 正樹. ドローンリモートセンシングによる作物・農地診断情報計測とそのスマート農業への応用. **日本リモートセンシング学会誌**, 37(3):224–235, 2017.

[29] 松木 萌, 井上 創造, and 清田 陽司. 介護施設紹介コールセンタ記録のアンサンブル学習による将来予測と傾向分析. **情報処理学会論文誌**, 59(10):1837–1852, 10 2018.

[30] Nattaya Mairittha, Tittaya Mairittha, and Sozo Inoue. A mobile app for nursing activity recognition. In *Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers*, UbiComp '18, page 400–403, New York, NY, USA, 2018. Association for Computing Machinery.

[31] Sozo Inoue, Naonori Ueda, Yasunobu Nohara, and Naoki Nakashima. Recognizing and understanding nursing activities for a whole day with a big dataset. *Journal of Information Processing*, 24(6):853–866, 2016.

[32] Sozo Inoue. Activity recognition and future prediction in hospitals. *ACM International Conference Proceeding Series*, 28-:59–65, 11 2016.

[33] 佐々木 渉, 藤原 聖司, 藤本 まなと, 諏訪 博彦, 荒川 豊, and 安本 慶一. スマートホームデータの時系列分析に基づく宅内行動生起タイミングの予測. In **マルチメディア，分散協調とモバイルシンポジウム** *2018* **論文集**, volume 2018, pages 1220–1226, jun 2018.

[34] 上田 健揮, 玉井 森彦, and 安本 慶一. スマートホームにおける複数のセンシングデータに基づいた生活行動データ抽出システムの提案. In **マルチメディア、分散協調とモバイルシンポジウム** *2014* **論文集**, volume 2014, pages 1884–1891, jul 2014.

[35] Lingmei Ren and Yanjun Peng. Research of Fall Detection and Fall Prevention Technologies: A Systematic Review. *IEEE Access*, 7:77702–77722, 2019.

[36] Defry Hamdhana, Haru Kaneko, John Noel Victorino, and Sozo Inoue. Improved Evaluation Metrics for Sentence Suggestions in Nursing and Elderly Care Record

Applications. *Healthcare*, 12(3), 2024.

[37] Keisuke Umakoshi, Tomokazu Matsui, Makoto Yoshida, Hyuckjin Choi, Manato Fujimoto, Hirohiko Suwa, and Keiichi Yasumoto. Non-contact person identification by piezoelectric-based gait vibration sensing. In Leonard Barolli, Isaac Woungang, and Tomoya Enokido, editors, *Advanced Information Networking and Applications*, pages 745–757. Springer International Publishing, 2021.

[38] Hikoto Iseda, Keiichi Yasumoto, Akira Uchiyama, and Teruo Higashino. Daily Living Activity Recognition with Frequency-Shift WiFi Backscatter Tags. *Sensors*, 24(11), 2024.

[39] 清威人. **スマート・ファクトリー — 戦略的「工場マネジメント」の処方箋**. 英治出版, 2010.

[40] 独立行政法人情報処理推進機構. スマートビルガイドライン. https://www.ipa.go.jp/digital/architecture/guidelines/smartbuilding-guideline.html. (2024 年 6 月 6 日閲覧).

[41] 農林水産省. スマート農業：農林水産省. https://www.maff.go.jp/j/kanbo/smart/. (2024 年 6 月 6 日閲覧).

[42] 独立行政法人情報処理推進機構. 「IoT 開発におけるセキュリティ設計の手引き」を公開 — 情報セキュリティ — IPA 独立行政法人 情報処理推進機構. https://www.ipa.go.jp/security/iot/iotguide.html. (2024 年 6 月 6 日閲覧).

[43] 一般社団法人 日本電機工業会. スマートホーム. https://www.jema-net.or.jp/Japanese/ha/smarthome/index.html. (2024 年 6 月 6 日閲覧).

[44] Gueltoum Bendiab, Stavros Shiaeles, Abdulrahman Alruban, and Nicholas Kolokotronis. IoT Malware Network Traffic Classification using Visual Representation and Deep Learning. In *2020 6th IEEE Conference on Network Softwarization (NetSoft)*, pages 444–449, Ghent, Belgium, 2020.

[45] Mehrnoosh Nobakht, Reza Javidan, and Alireza Pourebrahimi. DEMD-IoT: a deep ensemble model for IoT malware detection using CNNs and network traffic. *Evolving Systems*, 14:1–17, 10 2022.

[46] Noah Apthorpe, Dillon Reisman, and Nick Feamster. A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic. *arXiv preprint arXiv:1705.06805*, 2017.

[47] Shuaike Dong, Zhou Li, Di Tang, Jiongyi Chen, Menghan Sun, and Kehuan Zhang. Your Smart Home Can't Keep a Secret: Towards Automated Fingerprinting of IoT Traffic. In *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, ASIA CCS '20, page 47–59, New York, NY, USA, 2020. Association for Computing Machinery.

[48] Eric Zeng, Shrirang Mare, and Franziska Roesner. End user security and privacy concerns with smart homes. *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 65–80, 2017.

[49] Markus Miettinen, Samuel Marchal, Ibbad Hafeez, N Asokan, Ahmad-Reza Sadeghi, and Sasu Tarkoma. Iot sentinel: Automated device-type identification for security enforcement in iot. In *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, pages 2177–2184, Atlanta, GA, USA, 2017. IEEE.

[50] Cisco. Snort - Network Intrusion Detection & Prevention System. https://snort.org/. (2024 年 6 月 6 日閲覧).

[51] Cloudflare, Inc. DDoS 攻撃とは？ — Cloudflare. https://www.cloudflare.com/ja-jp/learning/ddos/what-is-a-ddos-attack/. (2024 年 6 月 6 日閲覧).

[52] 独立行政法人情報処理推進機構. JVN iPedia - 活用ガイド. https://jvndb.jvn.jp/nav/guide_sysadm.html. (2024 年 6 月 6 日閲覧).

[53] Cloudflare, Inc. ゼロデイエクスプロイトとは？— ゼロデイ脅威 — Cloudflare. https://www.cloudflare.com/ja-jp/learning/security/threats/zero-day-exploit/.

(2024 年 6 月 6 日閲覧).

[54] Google LLC. Change app permissions on your Android phone - Android Help. https://support.google.com/android/answer/9431959. (2024 年 6 月 6 日閲覧).

[55] Yair Meidan, Michael Bohadana, Asaf Shabtai, Juan David Guarnizo, Martín Ochoa, Nils Ole Tippenhauer, and Yuval Elovici. ProfilIoT: a machine learning approach for IoT device identification based on network traffic analysis. In *Proceedings of the Symposium on Applied Computing*, SAC '17, page 506–509, New York, NY, USA, 2017. Association for Computing Machinery.

[56] Arunan Sivanathan, Daniel Sherratt, Hassan Habibi Gharakheili, Adam Radford, Chamith Wijenayake, Arun Vishwanath, and Vijay Sivaraman. Characterizing and classifying iot traffic in smart cities and campuses. *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 559–564, 2017.

[57] Arunan Sivanathan, Hassan Habibi Gharakheili, and Vijay Sivaraman. Inferring iot device types from network behavior using unsupervised clustering. In *2019 IEEE 44th Conference on Local Computer Networks (LCN)*, pages 230–233. IEEE, 2019.

[58] Arunan Sivanathan, Hassan Habibi Gharakheili, and Vijay Sivaraman. Detecting behavioral change of iot devices using clustering-based network traffic modeling. *IEEE Internet of Things Journal*, 7(8):7295–7309, 2020.

[59] Squid Project. Squid: Optimising Web Delivery. https://www.squid-cache.org/. (2024 年 6 月 6 日閲覧).

[60] Yuichi Hattori, Yutaka Arakawa, Daichi Koike, Shigemi Ishida, and Sozo Inoue. Function-level Access Control System for Home IoT Devices. In *Sensors and Materials, Volume 34, Number 6(2)*, pages 2125–2139. MYU K.K. Sensors and Materials, 2022.

[61] vyos.io. VyOS–Open source router and firewall platform, howpublished =

”https://vyos.io/”, note = (2024 年 6 月 6 日閲覧).

[62] SWITCHBOT 株式会社. SwitchBot ハブミニ｜リモコンを一つにまとめるスマートリモコン - SwitchBot (スイッチボット). https://www.switchbot.jp/products/switchbot-hub-mini. (2024 年 6 月 6 日閲覧).

[63] SWITCHBOT 株式会社. SwitchBot 史上最高性能スマートプラグ — 今ある家電を手軽に IoT 化しよう– SwitchBot (スイッチボット). https://www.switchbot.jp/pages/switchbot-plug-mini. (2024 年 6 月 6 日閲覧).

[64] Slack Technologies, LLC. Slack はニーズに応えるプロダクティビティプラットフォーム. https://slack.com/intl/ja-jp/. (2024 年 6 月 6 日閲覧).

[65] Daichi Koike, Shigemi Ishida, and Yutaka Arakawa. Called Function Identification of IoT Devices by Network Traffic Analysis. In *Proceedings of the 36th Annual ACM Symposium on Applied Computing*, SAC ’21, page 737–743, New York, NY, USA, 2021. Association for Computing Machinery.

[66] Hangzhou Huacheng Network Technology Co., Ltd. Imou Life. https://www.imoulife.com/product/detail/Ranger2. (2024 年 6 月 6 日閲覧).

[67] 小米技術日本株式会社. Xiaomi Mi 360° 家庭用スマートカメラ 2K — Xiaomi Japan. https://www.mi.com/jp/product/mi-360-home-security-camera-2k/. (2024 年 6 月 6 日閲覧).

[68] Nature 株式会社. Nature Remo（ネイチャーリモ） – Nature 公式サイト. https://shop.nature.global/collections/nature-remo. (2024 年 6 月 6 日閲覧).

[69] TP-Link. HS105 — Wi-Fi スマートプラグ 遠隔操作 直差しコンセント Echo シリーズ Google Home 対応 音声コントロール コンパクト ハブ不要 3 年保証 — TP-Link 日本. https://www.tp-link.com/jp/home-networking/smart-plug/hs105/. (2024 年 6 月 6 日閲覧).

[70] The Tcpdump Group. the-tcpdump-group/tcpdump: the TCPdump network dissec-

tor. https://github.com/the-tcpdump-group/tcpdump. (2024 年 6 月 6 日閲覧).

[71] Yuichi Hattori, Yutaka Arakawa, and Sozo Inoue. Function Estimation of Multiple IoT Devices by Communication Traffic Analysis. In *The 4th International Conference on Activity and Behavior Computing (ABC2022)*, London, UK, 2022.

[72] Leo Breiman. Random forests. *Machine Learning*, 45:5–32, 10 2001.

[73] Yuichi Hattori, Yutaka Arakawa, and Sozo Inoue. Evaluation of Functional Estimation Methods in IoT Devices at Intervals of a Few Seconds by Communication Traffic Analysis. *International Journal of Activity and Behavior Computing*, 2024(1):5, 2024.

[74] Amazon.com, Inc. AWS デバイス認定プログラム. https://aws.amazon.com/jp/partners/programs/dqp/. (2024 年 6 月 6 日閲覧).

[75] 経済産業省. IoT 製品に対するセキュリティ適合性評価制度構築に向けた検討会の最終とりまとめを公表し、制度構築方針案に対する意見公募を開始しました. https://www.meti.go.jp/press/2023/03/20240315005/20240315005.html. (2024 年 6 月 6 日閲覧).