通信トラヒック分析に基づく数秒間隔でのIoTデバイスの機能判定手法

服部 祐一[1]　荒川 豊[2]　井上 創造[1]

概要：近年，一般家庭にも様々な IoT デバイスが普及し，家庭での様々な場面で活用されている．しかし，現在の IoT デバイスは動作がブラックボックスであり，IoT デバイスが不審な通信を行っていた場合に気づく術がない．そこで，我々は 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アクセス制御の機能と 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ユーザが 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システム (IoT 活動量計) の実現を目指している．その実現のためには，機能推定手法において数秒間の通信トラヒックで推定する必要がある．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行った．その結果，8 機種中 5 機種において，それぞれ 80%以上の精度で機能を推定できることを確認した．

Functional Estimation Methods in IoT Devices at Intervals of a Few Seconds by Communication Traffic Analysis

Yuichi HATTORI[1]　Yutaka ARAKAWA[2]　Sozo INOUE[1]

1. はじめに

近年，一般家庭にも IoT デバイスが普及し，リモコンや照明，ドアロック，コンセントなど様々な機能を持つ IoT デバイスが販売され，家庭での様々な場面で活用されている．これらのデバイスは今後さらに普及することが予想され，日本の総務省の調査によると，2021 年の世界の IoT デバイスの数は約 292 億個であり，2024 年には約 400 億個に達すると予想されている [1]．例えば，家庭で使われる IoT デバイスとしてよく知られているのは，Google Home や Amazon Echo などのスマートスピーカーである．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）が搭載されており，インターネット検索や家電製品の操作，音楽再生など，音声でさまざまな機能を実行することができる．また，カメラを搭載し，他の IoT 機器やスマートフォンとビデオ通話ができる機器もある．また，それらと連携できるネットワークカメラやスマートリモコンは家電量販店等で容易に購入することができるほど普及している．これらの IoT デバイスは，基本的にクラウドとの連携を前提としており，その機能によりスマートフォン等との連携を実現している．利用者は，スマートフォンからこれらのシステムにアクセスし，機器の操作や情報の閲覧を行うことができる．国立研究開発法人情報通信研究機構が行っている無差別型サイバー攻撃の大局的な動向を把握することを目的としたサイバー攻撃観測・分析システムの NICTER[2] の 2022 年度の観測レポートによると IoT ボットの感染活動は，昨年に続き，Mirai 亜種等の活発な活動が観測され，日本国内ではピーク時には約 5000 ホストまで増加している [3]．IoT 機器は，外部のネットワークに接続することを前提としているため，情報セキュリティの面で多くの問題があり，様々な不正アクセス事案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データを送信する事案が発生している．例えば，国土交通省近畿地方整備局が管理する 337 台の河川監視用のカメラが，不正アクセスを受けた疑いで運用を休止したり [4]，家庭用ルーターがサードパーティー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，サードパーティー宛に

[1] 九州工業大学大学院生命体工学研究科
[2] 九州大学大学院システム情報科学研究院

データを送信していることが確認されている [5].

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アップデート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や企業自体の倒産などの要因により，ファームウェアのアップデートやサポートが受けられなくなる可能性がある．

(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，デバイスがどのデータをどこに送信するかというユーザが把握することはできない．セキュリティ上の問題からデータをどのようなデータをどこに送信するかは重要な問題である．テレビ会議システム Zoom の問題のように，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 [6].

(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ユーザがインストールすることができない．

そこで，我々は，それら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や理解することを可能にする動作状況の可視化システム（IoT 活動量計）を提案している [7]．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 [8] では，4 種別の IoT 機器各 2 機種ずつの計 8 機種の合計 16 種類実行機能の推定で 91%，実行機能のみの 8 種類の推定で 73%の精度であった．しかしながら，従来の手法では，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．本稿では，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 機器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 80%以上の精度で機能を推定できることを確認した．使用した通信トラヒックは，従来の研究 [8] で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を用いた．

本稿の構成は以下の通りである．2 章では IoT の通信トラヒック分析の関連研究を述べ，3 章では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を示し，その評価 4 章で示す．5 章で議論を述べ，最後に 6 章でまとめとする．

2. 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，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．

2.1 スマートホームのエンドユーザセキュリティとプライバシーの懸念を示す研究

Zeng ら [9] は，スマートホームを利用するエンドユーザ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，ユーザ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，エンドユーザのデバイス関連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．

我々の研究は，不正な通信を検知するだけでなく，デバイス情報の可視化も提供することにより，ユーザ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．

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 [10] 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，暗号化されたトラヒックの送受信レートからユーザ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ユーザに与えることを警鐘している．攻撃者からユーザの行動を推定できないようにトラヒック情報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，ユーザに報告することも重要なことである．

Dong ら [11] 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，パケット間の時間的関係を利用した機器識別のフレームワークを提案し，高い精度で機器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モーフィングされている場合でもユーザ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．

IoT デバイスの通信トラヒックを解析することで活動情報をユーザに提示するこれらの研究は，不審なネットワーク通信の検知に役立てることができる．

2.3 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 [12] 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 [13] 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 週間のトラヒックデータを収集した．そして，通信トラヒック（トラヒック負荷，信号パターン，アクティブ時間とスリープ時間の分布など）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 [14] 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 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 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 [15].

これらの研究では，高い精度でデバイスを特定し，また，デバイスの行動の変化を検出を行っているが，デバイスの機能の特定は行っていない．本研究では，デバイスの機能の特定を行う．

2.4 ネットワークゲートウェイを用いた IoT デバイス向けのセキュリティシステム

Miettinen ら [16] 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ったが，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．

2.5 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，センサー，外部ストレージ等）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 [17]． 過去に，ユーザの同意なしにアプリ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ユーザの許可なくサードパーティ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 [5]．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 デバイスごとに利用するリソースを制御することが必要である．

3. 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

本章では，提案する IoT 活動量計と推定に使用したデータセット，数秒間隔での IoT デバイスの機能推定手法について述べる．

3.1 IoT 活動量計

図 1 に我々提案する IoT 活動量計を示す．太い黒枠で示す部分が IoT 活動量計の提供する部分となり，エッジルーターとマネジメントシステムから構成される．IoT 活動量計は一般家庭で使用することを想定しており，複数の IoT デバイスが有線もしくは無線でルーターに接続されている環境で用いられることを想定している．つまり，接続されたすべての機器から送受信される通信トラヒックがルーターに収集される環境を想定している．このルーターの部

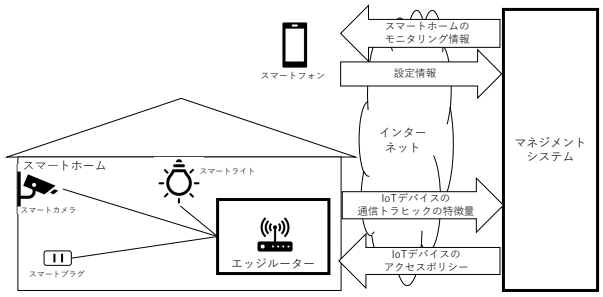

図 1 IoT 活動量計の概要

表 1 使用した通信トラヒックの IoT デバイス一覧

	デバイス種別	製品名	開発元
1	スマートカメラ	Ranger 2	Imou
2		Mi 360°	Xiaomi
3	スマートリモコン	SwitchBot ハブミニ	SwitchBot
4		Nature Remo	Nature
5	スマートスピーカー	Amazon Echo Show	Amazon
6		Google Home Mini	Google
7	スマートプラグ	SwitchBot プラグ	SwitchBot
8		WiFi スマートプラグ	TP-Link

分を IoT 活動量計ではエッジルーターと呼ぶ．このエッジルーターで収集した通信トラヒックをもとに利用状況の可視化や，スマートホームに設置された IoT デバイスの通信の可否に関する設定を利用者がスマートフォン等で行い，その設定をエッジルーターに反映させることができるシステムが Web アプリケーションとして提供される．クラウド上に設置されたこれらの機能を提供する Web アプリケーションを IoT 活動量計では，マネジメントシステムと呼ぶ．

3.2 使用したデータセット

使用したデータセットは，従来の研究で収集した 4 種別の IoT 機器各 2 機種ずつの計 8 機種の合計 16 種類の通信トラヒックのデータセットを用いた [8]．今回使用した通信トラヒックは，4 種別の IoT 機器各 2 機種ずつの計 8 機種の合計 16 種類を用いており，IoT デバイスの一覧は表 1，機能の一覧は表 2 の通りである．

3.3 数秒間隔での IoT デバイスの機能推定手法

3.1 節で述べた 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．従来の研究 [8] では，4 種別の IoT 機器各 2 機種ずつの計 8 機種の合計 16 種類実行機能の推定で 91%，実行機能のみの 8 種類の推定で 73%の精度であった．しかしながら，従来の手法では，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．また，機能を実行していない状態を考慮していない．本稿では，その問題を解決するために，1 秒ごとに機械学習を用いて IoT 機器の機能の実行状態を推定手法を提案する．実際に IoT 活動量計で用いる推定モデルの構築に向けて，3.2 節で述べた日本国内で流通している IoT デバイスの通信トラヒックを用いて機器ごとに精度の評価を行った．本稿では，1 秒ごとの状態を推定するために，3.2 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，1 秒ごとに 3 秒前までの通信トラヒックを用いて計算し，表 3 の個人を特定できる情報を含まないのみを用いた．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を用い，また，静止のラベルのデータが非常に多いためアンダーサンプリングを行い，ラベルごとのデータ数を揃えたのち，10 分割交差検証により評価を行った．

表 2 使用した通信トラヒックの機能一覧

	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 の電源を 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

4. 評価

3.3 節で述べた機能推定手法の有効性を検証するためにランダムフォレストを用いて，10 分割交差検証により評価を行った．用いた特徴量は，表 3 の通りであり，機種ごとに発動機能の推定を行った．

その結果，8 機種中，5 機種においては 80%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．機種ごとの混同行列を表 4-表 11 に，そのクラスラベルの一覧を表 12 に示す．また，機種ごとの機能推定結果の分類精度一覧を表 13 に示す．特にスマートリモコンについては，2 機種とも他に比べ精度が低く，これは実行するための通信の回数が少ない点もあるがスマートリモコンは，指示を受けた当該機能の赤外線信号を送信しているものであり，実際の通信はほとんど差異がないため通信トラヒックの情報だけでは分

表 3 利用した特徴量一覧

	特徴量
1	1 秒間送信パケット数
2	1 秒間の送信パケットサイズの平均
3	1 秒間の送信パケットサイズの最大数
4	1 秒間の送信パケットサイズの分散
5	1 秒間の送信パケットサイズの標準偏差
6	1 秒間の受信パケット数
7	1 秒間の受信パケットサイズの平均
8	1 秒間の受信パケットサイズの最大数
9	1 秒間の受信パケットサイズの分散
10	1 秒間の受信パケットサイズの標準偏差
11	1 秒間の TCP パケット数
12	1 秒間の UDP パケット数
13	1 秒間の送信元 IP 数
14	1 秒間の送信先 IP 数
15	2 秒間送信パケット数
16	2 秒間の送信パケットサイズの平均
17	2 秒間の送信パケットサイズの最大数
18	2 秒間の送信パケットサイズの分散
19	2 秒間の送信パケットサイズの標準偏差
20	2 秒間の受信パケット数
21	2 秒間の受信パケットサイズの平均
22	2 秒間の受信パケットサイズの最大数
23	2 秒間の受信パケットサイズの分散
24	2 秒間の受信パケットサイズの標準偏差
25	2 秒間の TCP パケット数
26	2 秒間の UDP パケット数
27	2 秒間の送信元 IP 数
28	2 秒間の送信先 IP 数
29	3 秒間送信パケット数
30	3 秒間の送信パケットサイズの平均
31	3 秒間の送信パケットサイズの最大数
32	3 秒間の送信パケットサイズの分散
33	3 秒間の送信パケットサイズの標準偏差
34	3 秒間の受信パケット数
35	3 秒間の受信パケットサイズの平均
36	3 秒間の受信パケットサイズの最大数
37	3 秒間の受信パケットサイズの分散
38	3 秒間の受信パケットサイズの標準偏差
39	3 秒間の TCP パケット数
40	3 秒間の UDP パケット数
41	3 秒間の送信元 IP 数
42	3 秒間の送信先 IP 数

類が難しいと考えられる．スマートカメラである Mi 360° に関しても，実際の通信はほとんど差異がないため低い精度になったと考えられる．もう一つのスマートカメラある Ranger 2 の精度と差が出た点については，開発元が違うため，実装が異なり，Ranger 2 に関しては通信の差異が見られたため精度が高かったものと考えれる．また，静止状態を誤認識している部分については，静止状態とはいえ IoT 機器は何らかの通信を行っている場合があるため，誤認識が発生したと考えられる．

表 4 機能推定結果の混同行列 (Ranger 2: スマートカメラ)

	0	1	2
0	9	0	1
1	0	9	1
2	0	0	10

表 5 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	4	4
2	0	5	5

表 6 機能推定結果の混同行列 (SwitchBot ハブミニ: スマートリモコン)

	0	3	4
0	18	0	1
3	0	15	4
4	0	14	5

表 7 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	6	4

表 8 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	5	67

表 9 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	26	8
6	5	3	27

表 10 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 11 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	3	7

表 12 表 4-表 11 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 13 機器ごとの機能推定結果の分類精度一覧

	デバイス種別	機器名	分類精度
1	スマートカメラ	Ranger 2	93%
2		Mi 360°	63%
3	スマートリモコン	SwitchBot ハブミニ	67%
4		Nature Remo	63%
5	スマートスピーカー	Amazon Echo Show	91%
6		Google Home Mini	80%
7	スマートプラグ	SwitchBot プラグ	97%
8		WiFi スマートプラグ	80%

5. 議論

本章では，評価結果から考察される課題について述べる．

5.1 IoT デバイス等のアップデートによる影響

IoT デバイスは，定期的にソフトウェアアップデートが発生し，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等のサードパーティーのアプリケーションを追加でインストールすることが可能な IoT デバイスではアプリケーションのアップデートも考慮する必要があり，アップデート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．

5.2 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アップデート等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，任意のタイミング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．

5.3 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，送信時のパケットのサイズや受信時のパケットの数等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 などの形式でデータ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等の場合は，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．

6. 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 80% 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．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，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等を検討する．通信がユーザ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，ユーザがより安心して IoT デバイスを利用できる世界の実現を目指す．

謝辞 本稿で示した研究の一部は, 科研費 (JP19KT0020) の助成で行われた．

参考文献

[1] 総務省：総務省 | 令和 4 年版 情報通信白書 | データ集（第 3 章関連データ） (2023). https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r04/html/nf3r1000.html.

[2] 国立研究開発法人情報通信研究機構：NICTERWEB - ダークネット観測 — 国立研究開発法人情報通信研究機構 サイバーセキュリティ研究室 (2023). https://www.nicter.jp/.

[3] 国立研究開発法人情報通信研究機構：NICTER 観測レポート 2022 (2023). https://csl.nict.go.jp/report/NICTER_report_2022.pdf.

[4] 国土交通省：報道発表資料：配信を停止している簡易型河川監視カメラの再開について - 国土交通省 (2023). https://www.mlit.go.jp/report/press/mizukokudo03_hh_001168.html.

[5] XDA: TP-Link Deco X68 Review: A good mesh router ruined by bizarre software (2022). https://www.xda-developers.com/tp-link-deco-x68-review.

[6] Yahoo: Zoom admits some calls were routed through China by mistake (2020). https://techcrunch.com/2020/04/03/zoom-calls-routed-

china/.

[7] Hattori, Y., Arakawa, Y., Koike, D., Ishida, S. and Inoue, S.: Function-level Access Control System for Home IoT Devices, *Sensors and Materials, Volume 34, Number 6(2)*, Sensors and Materials, pp. 2125–2139 (online), available from ⟨https://doi.org/10.18494/SAM3901⟩ (2022).

[8] Yuichi Hattori, Yutaka Arakawa, S. I.: Function Estimation of Multiple IoT Devices by Communication Traffic Analysis, *The 4th International Conference on Activity and Behavior Computing (ABC2022)*, (online), available from ⟨https://arakawa-lab.com/wp-content/uploads/2022/11/ABC2022$_0$7$_h$*attori.pdf*⟩ (2022).

[9] Zeng, E., Mare, S. and Roesner, F.: End user security and privacy concerns with smart homes, *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*, pp. 65–80 (online), available from ⟨https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng⟩ (2017).

[10] Apthorpe, N., Reisman, D. and Feamster, N.: A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic, *arXiv preprint arXiv:1705.06805*, (online), available from ⟨https://arxiv.org/abs/1705.06805⟩ (2017).

[11] Dong, S., Li, Z., Tang, D., Chen, J., Sun, M. and Zhang, K.: Your Smart Home Can't Keep a Secret: Towards Automated Fingerprinting of IoT Traffic, *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, ASIA CCS '20, New York, NY, USA, Association for Computing Machinery, p. 47–59 (online), DOI: 10.1145/3320269.3384732 (2020).

[12] Meidan, Y., Bohadana, M., Shabtai, A., Guarnizo, J. D., Ochoa, M., Tippenhauer, N. O. and Elovici, Y.: ProfilIoT: a machine learning approach for IoT device identification based on network traffic analysis, *Proceedings of the symposium on applied computing*, pp. 506–509 (online), available from ⟨https://dl.acm.org/doi/10.1145/3019612.3019878⟩ (2017).

[13] Sivanathan, A., Sherratt, D., Gharakheili, H. H., Radford, A., Wijenayake, C., Vishwanath, A. and Sivaraman, V.: Characterizing and classifying IoT traffic in smart cities and campuses, *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 559–564 (online), available from ⟨https://ieeexplore.ieee.org/abstract/document/8116438⟩ (2017).

[14] Sivanathan, A., Gharakheili, H. H. and Sivaraman, V.: Inferring iot device types from network behavior using unsupervised clustering, *2019 IEEE 44th Conference on Local Computer Networks (LCN)*, IEEE, pp. 230–233 (2019).

[15] Sivanathan, A., Gharakheili, H. H. and Sivaraman, V.: Detecting behavioral change of IoT devices using clustering-based network traffic modeling, *IEEE Internet of Things Journal*, Vol. 7, No. 8, pp. 7295–7309 (2020).

[16] Miettinen, M., Marchal, S., Hafeez, I., Asokan, N., Sadeghi, A.-R. and Tarkoma, S.: Iot sentinel: Automated device-type identification for security enforcement in iot, *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, IEEE, pp. 2177–2184 (2017).

[17] Google: Change app permissions on your Android phone - Android Help (2022). https://support.google.com/android/answer/9431959.