電磁・通信・家電情報に基づくIoT活動量計の検討

張 志華[1,a)]　松井 智一[1]　上田 浩行[1]　高野 誠也[1]　藤本 大介[1]　林 優一[1]　安本 慶一[1]　荒川 豊[2]

概要：近年，音声認識やカメラを備えたIoT機器が一般家庭に普及し始めている．これらのデバイスはブラックボックスであり，設置後，どのようなデータをどこに送っているのかを知る手段はない．一方で，こうした機器からのプライバシー情報の流出や機器に対する不可聴音を使った攻撃などが報告されている．本稿では，急速に広がるIoT機器を安心して利用するために，これまで考えられてこなかった，情報機器に対するトラスト，という考え方と，その実現手段を提案する．実現手段として，機器から観測される情報のみを利用してその動作を推定する手法と，消費電力などから人の行動を認識する手法を組み合わせることで，意図した通信か否かを判定する手法を提案する．特徴的な点は，機器から観測可能な情報として，通信情報と電磁情報という異なるレイヤの情報を縦断的に活用する点である．通信パケット計測，行動認識，電磁波計測の3つのサブシステムからなる提案システムのプロトタイプを試作し，予備実験としてそれぞれのデータを収集し簡易解析した結果を報告する．

1. はじめに

総務省によると2018年の世界のIoTデバイスの数は約307億台となり，2021年には約448億台にのぼると予測されており[1]，今後も一般家庭にIoTデバイスが普及していくことは確実である．最も普及しているIoTデバイスは，GoogleやAmazonから発売されているスマートスピーカーである．時計や音楽再生といった機能に加え，他のIoT機器のゲートウェイとしても用いられる．例えば，筆者の居室では，Switchbotというボタン IoTを組み合わせ，VUI（Voice User Interface）を通じて，“Alexa, エアコンを付けて”と伝えると，エアコンのOn/Offが可能になっている．他にも防犯カメラとの連携やIoT温度計との連携など，さまざまなIoT機器との連携が可能である．

このスマートスピーカーをハブとした連携は，家庭内に閉じているものではなく，常時，クラウドを介して行われる．具体例として，先述したSwitchbotとの連携について説明する．物理的には，操作する人も操作されるエアコン，仲介するAmazon Echoも同一の部屋に存在する．しかしながら，論理的には，音声コマンドを受け取ったEchoは，クラウド上にあるSwitchbotのAPIに対して命令を発信する．Switchbotも同様にクラウドに接続されており，APIを通じて命令が来た場合は，スイッチを操作する．

家庭内の機器同士であれば，わざわざインターネットを介する必要もないように思えるが，このようなアーキテクチャとする事で，外出先からスマートフォンで操作することや他のサービスとの連携，といったIoT機器ならではの利便性が生み出されており，インターネット接続は必須と言える．加えて，販売後に，ファームウェアのアップデートが疎かになるという問題もあり，IoT機器はハッキング対象にもなりやすく，種々のプライバシー流出事件が起きている．例えば，スマート掃除機に付属するカメラが簡単にハッキング可能であることが判明したこと[2]や，カジノの水槽に設置されたスマート水温計からカジノの顧客情報が盗み出された事件[3]，IPカメラがハックされ全世界のカメラにアクセス可能になった事件[4]などが実際に起きている．そのため，我々は，新しく家庭内にIoT機器を導入する際の安全性をどのように担保するかが重要な課題であると考えている．

スマートフォンにおいては，アプリケーションごとに，端末のリソース（ネットワーク，カメラ，ストレージ，位置情報など）単位でアクセス権の制御が可能となっており，ダウンロードしたアプリが勝手に位置情報を取得したり，カメラを使用したりできない仕組みが構築されている．一方，IoT機器は，ブラックボックスであり，使わないときにどのような動作をしているのかは不明である．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[5]．IoT機器に対して，ウイルス対策ソフトウェアのようなものを追加することは

1 奈良先端科学技術大学院大学
Nara Institute of Science and Technology
2 九州大学
Kyushu University
a) zhang.zhihua.yn2@is.naist.jp

図 1: 電磁・通信・家電情報に基づく IoT 活動量計のコンセプト

できないため，機器から出力される情報から動作を推定する必要があり，まず，WiFi 通信のトラヒックパターンから機器と発動機能を推定する手法を提案した [5], [6]．この手法では，家庭内の WiFi アクセスポイントに，IoT 活動量計の機能を追加することを想定している．

本稿では，IoT 機器から出力されるもう 1 つの情報として，“電磁波” を用いた発動機能推定に関する初期評価について報告する．通信トラヒックを利用した攻撃検知は，パケットキャプチャの手法や分析手法が確立されており，比較的取り扱いやすいといえる．しかしながら，IoT 機器に対する攻撃として，正規の通信チャネル以外を用いた情報漏えいや機器へのコマンド発行などが実行される可能性があり，これらの攻撃をパケットキャプチャのみから検出することは難しい．一方で，電磁波を利用した攻撃検知に関しては，現状では計測に専用の機器が必要であり，得られるデータも膨大であるものの，機器の内部処理に応じて副次的に生ずる電磁波などのサイドチャネル情報を取得・解析することで，上述した攻撃を検出できる可能性が高い．

2. 関連研究

本研究では主な IoT 機器として，宅内に存在する家電などの機器を想定する．技術の発展に伴い，家電製品もよりスマート化されており，スマート化された家電と IoT 機器とセンサを利用し，宅内の行動認識を行う研究が多数存在する．Cook ら [7] や Matsui ら [8] は，一般の住宅に後付可能な人感センサやドアセンサ，照度センサなどの設置型センサを利用して，住民の行動を認識するためのスマートホームキットを提案している．Yassine[9] らや Nakagawa ら [10] は，宅内に設置するセンサだけでなく，宅内で消費される家電の消費電力情報などから居住者の行動認識を行う手法を提案している．その他，水道管に水が通過する音を利用した行動認識に関する研究 [11] や，独自に開発したウェアラブルデバイスを利用した行動認識に関する研究 [12] が行われている．これら家に設置される IoT 機器，提供されるサービスは増えているが，IoT 機器への不正操作，不正情報取得を検知する方法に関して，標準となる技術は確立されていない．

さらに，このような IoT 機器からは電磁波を通じて情報の漏えいが生ずることが報告されている．Fukushima[13], [14] らはスピーカーフォンやスマートスピーカの動作に伴って発生する電磁波が空間に放射，または給電ケーブルを伝搬され，これを傍受されることにより音声情報の漏えいが発生する危険性を指摘している．このような電磁波の漏えいが発生する原因はスイッチングレギュレータを用いた電源回路の動作に伴い発生する強力な電磁ノイズに音声信号処理時の情報が重畳されたからであると述べられている．

また，システムに必要な複数の機能を一つのチップに統合した MSoC(Multiple System on Chip) デバイスからの放射電磁波を測定することで，音情報の取得を可能とすることも確認されている [15]．こちらもスピーカーフォンやスマートスピーカーと同様，回路に組み込まれたスイッチングレギュレータが原因であると指摘されている．

3. 提案システム

3.1 IoT 活動量計の概要

筆者らが提案する IoT 活動量計というコンセプトを図 1 に示す．家庭内の IoT 機器は，内部にウィルスチェックソフトウェアのようなものを追加することはできないものの，必ず電源とネットワークに接続されることから，その両方から得られる外形的な情報から機器の動作を推定し，利用者に対して可視化するというものである．

IoT 活動量計を実現するにあたり，本研究では，大きく 3 つの研究を並行して進める．1 つ目は，通信情報に基づく IoT 機器の識別および発動機能検知システムである．IoT

機器は必ずクラウドに接続されており，何らかの通信を行っている．また，過去に発生した IoT 機器からの情報流出においても，不正アクセスや許可を得ないデータのアップロードに起因しており，通信情報の監視は重要となる．2 つ目と 3 つ目は，いずれも電源から得られる情報である．まず，消費電力情報は，スマート配電盤やスマートタップを用いて取得可能な情報である．IoT 機器の消費電力は機能や状態によって大きく変化することはないと考えられるが，他の一般家電の動作などから居住者の行動を認識することができる [16] ため，誤検知や未検知の低減に活用できると想定している．次に，電磁情報は，電源ケーブルや配電盤から漏れ出る電磁波の情報である．特殊な装置を用いて計測する必要があるものの，IoT 機器内部のハードウェアの動作が変わることにより，消費電力的には殆ど変わらない場合でも，電磁波の変化を通じて動作を検知することが可能になると考えている．

3.2　通信パケット監視サブシステム

図 2 に，文献 [5], [6] において発表済みの，通信情報に基づく機器と機能の識別の流れについて示す．提案システムは，WiFi ルータ内に実装されることを想定し，そこを通過するパケットの宛先や種類，量に基づき，家庭内のどの IoT 機器がどんな機能を発動しているかを識別する．まず，IoT 機器なのか，スマートフォンやパソコンなのか，データを分離する必要があり，我々は，宛先 IP アドレスの多様性に基づいた分離手法を提案している [6]．これは，IoT 機器が出荷時に設定されている特定のサーバへのアクセスに偏っているのに対して，スマートフォンやパソコンではさまざまな IP アドレスにアクセスするという特徴に基づいている．データを分離したあと，IoT 機器・機能ごとにデータを収集し，機械学習によって，発動機能識別システムを構築した．

図 2: 通信情報に基づく機器と機能の識別

Amazon のスマートスピーカーである EchoSpot, EchoDot，EchoFlex という 3 機種を用いて実験を行ったところ，パソコンやスマートフォンなどの背景トラヒックを含む通信トラヒックデータから，発動した 8 種類の機能をそれぞれ 74.34%, 73.19%, 73.55%で推定できることを確認した．

3.3　行動認識・家電制御システム

実験を行うスマートホームには，インターネット接続可能な Echonet Lite 規格に対応したテレビ・エアコンなどのスマート家電と，人感・ドア・環境センサなどの設置型センサ，宅内の電力消費を確認できるスマート分電盤などが設置されている．各オブジェクトから得られるデータはゲートウェイを介してサーバ PC へ送信され，データベースへ格納される．IoT 機器の異常を検出するためには，居住者が現在どのような行動をしているかが重要であると考えられる．そのため，居住者の行動認識を行う際には，これらの家電情報・センサ・電力データを基に学習した，機械学習モデルを利用する．

Echonet Lite 規格に対応した家電をスマートスピーカーで制御するために，ゲートウェイとして Jetson nano を使用する．スマートスピーカーがユーザから家電制御の音声コマンドを受けたとき，スキルと呼ばれるプログラムを起動し，クラウドサーバへコマンドの内容を送信する．クラウドサーバは受けた内容によって，ターゲットである家電の状態を取得する．次に，クラウドサーバは取得した家電の情報によって，状態を変更するかどうかを判断する．家電状態を変更する必要がある場合（例えば：オフからオンにする），Jetson nano を経由して，家電を制御する．

3.4　電磁波測定システム

スマートスピーカー内部では, 音声信号などの情報が時間的に変動する電気信号として処理されており，この処理過程において，サイドチャネル情報 [17] [18] として電磁波が機器外部に放出される．本項ではこのように機器から漏れ出た電磁波としてのサイドチャネル情報の評価方法を示す．

3.4.1　電磁的情報漏えいの評価系

電磁波として機器外部に漏えいするサイドチャネル情報は，機器内部の信号が電磁界を通じて周囲の導体と電磁的に結合・伝搬することによって発生する．過去の検討において，スピーカーフォンに接続された給電/通信ケーブルを通じた機器内部の音声情報の漏えいが報告されている [13]．こうした過去の検討より，スマートスピーカーからも同様に電磁波を通じたサイドチャネル情報が漏えいする可能性が考えられる．

家庭内に設置されるスマートスピーカーは常時電源を入

図 3: 取得信号から音声を再構築するまでの流れ

れておくことを想定されているため，常時通電が必要な機種が多く，電源線への接続が求められるため，電源線を通じてサイドチャネル情報が漏えいする可能性がある．

以上の点を考慮し，本測定システムではスマートスピーカーの主要な接続線路である電源線を対象としたサイドチャネル情報の評価を行う．

3.4.2 電磁波を通じたサイドチャネル情報取得の流れ

サイドチャネル情報の評価のため，背景ノイズのパワースペクトルを取得後，スマートスピーカー内部で音声処理が行われている状態で電源線を伝搬する電磁波のパワースペクトルを取得する．両パワースペクトルを比較することで，スマートスピーカーの音声処理の有無による電磁波の漏えい強度の変化について検討する. パワースペクトルの比較において差が観測された場合，動作時にサイドチャネル情報が電磁波として漏えいしている可能性がある．

本実験では，スマートスピーカーからの漏えい電磁波の中に音声情報がどの程度含まれているかを評価するため，既知の音声信号をスマートスピーカーに処理させ，その処理に応じて漏えいした電磁波としてのサイドチャネル情報を図 3 の流れに沿って既知の音声信号を再構築し，再構築した音声データをスペクトログラムに変換する．スペクトログラムを使用したサイドチャネル情報の評価では，背景ノイズと復元した音声信号の強度の差が大きい場合，電磁波をサイドチャネル情報として機器内部の動作を推定できる可能性がある．

4. 評価シナリオと予備実験

4.1 実験のシナリオ

IoT 機器への攻撃の一例として，非可聴域の音波を利用したドルフィンアタックへの対処を検証するためのシナリオを検討した．具体的には，日常生活のルーティングに基づいて 4 つのシナリオ（帰宅，寝る直前，起きた直後，外出）を設計した．これによって，人が部屋に存在しないときの IoT 機器の異常と，人が部屋にいる間の IoT 機器の異常をテストすることが可能である．

4.1.1 帰宅

初期状態として，家電の使用状態は「オフ」で，ユーザは家にいないこととする．ユーザが家に帰宅したとき，以下の行動を行う（L はリビングにある家電のことを指す）：

(1) 帰宅
(2) リビング（L）へ移動する
(3) スマートスピーカーを経由し，家電を操作する
　(a) 照明（L）をつける
　(b) テレビ（L）をつける
　(c) エアコン（L）をつける
(4) リビングで休憩する

4.1.2 寝る直前

初期状態として，家電の使用状態は「オン」で，ユーザはリビングにいることとする．ユーザは寝る直前に以下の行動を行う（L はリビングにある家電のことを指す；B は寝室にある家電のことを指す）：

(1) リビング（L）で PC を操作している
(2) スマートスピーカーを経由し，家電を操作する
　(a) 照明（L）を消す
　(b) テレビ（L）を消す
　(c) エアコン（L）を消す
(3) 寝室（B）へ移動する
(4) 照明（B）を消す
(5) 寝る

4.1.3 起きた直後

初期状態として，家電の使用状態は「オフ」で，ユーザは寝室にいることとする．ユーザが起きた直後に以下の行動を行う（L はリビングにある家電のことを指す）：

(1) 起きる
(2) リビング（L）へ移動する
(3) スマートスピーカーを経由し，家電を操作する
　(a) 照明（L）をつける
　(b) テレビ（L）をつける
　(c) エアコン（L）をつける
(4) リビング（L）で休憩する

4.1.4 外出

初期状態として，家電の使用状態は「オン」で，ユーザはリビングにいることとする．ユーザが外出するとき，以下の行動を行う（L はリビングにある家電のことを指す）：

(1) リビング（L）で PC を操作している
(2) スマートスピーカーを経由し，家電を操作する
　(a) 照明（L）を消す
　(b) テレビ（L）を消す
　(c) エアコン（L）を消す
(3) 玄関へ移動する
(4) 家から出る

表 1: 4.2 で使用した機器の型番

Device	Product Model
Current Probe	FCC F-2000-12mm
LNA	COSMOWAVE LNA270WS
Spectrum Analyzer	Tektronix RSA306B
Receiver	USRP X310

4.2 予備実験

前節のスマートスピーカーによる家電の操作に着目し，電磁波を計測する実験を行った．本実験では，スマートスピーカーの内部処理に関連する情報がサイドチャネル情報として漏えいするかどうかを検討する．そこで，その基礎的検討として，既知の音声信号をスマートスピーカーに処理させた場合，漏えいするサイドチャネル情報として考えられる電源線を伝搬する電磁波について評価した．以下に実験環境と評価結果を示す．

実験では，Amazon Echo Dot（第 2 世代）を対象としてサイドチャネル情報の取得を行った．ここで，実験環境を図 4，実験で使用した機器の型番を表 1 に示す．スマートスピーカーに入力として与える既知の音声信号には図 5 に示すチャープ音を使用した．なお，スマートスピーカーはコンセントから給電を行い，同室に設置したラップトップから Bluetooth 接続でチャープ音を連続再生した状態で実験を行った．電源タップから測定用のカレントプローブまでの距離は 150 mm とし，アルミ板のサイズは 500 mm × 300 mm × 5 mm のものを使用した．

まず，スマートスピーカー動作時の電源線の伝導ノイズを測定したパワースペクトルを図 7 に示す．ここで，青線は背景ノイズ，橙線はチャープ音を再生した場合のパワースペクトルである．両者の比較では，広い帯域でパワーが上昇していることが確認でき，音声情報が漏えいしている可能性がある．

次に図 5 のチャープ音をスマートスピーカーから再生した場合において，再構築された音声のスペクトログラムを図 6 に示す．ここで，音声の再構成には，チャープ音再生時にパワースペクトルの上昇が最大となる周波数の 140 MHz を選択した．図 6 より，スペクトログラムにチャープ音及びその倍音が現れたことから，音声信号が再構築可能であるといえる．さらに，音声のスペクトル強度が背景ノイズと比べて高い値で観測されており，漏えいした電磁波から音声信号は鮮明に再構築することがわかる．

これらの実験結果から，対象のスマートスピーカーに対して既知の音声信号を入力として与えた場合，この信号は電源線を伝搬する電磁波をサイドチャネル情報として漏えいすることが確認できた．また，漏えいした信号はカレントプローブ及び計測器を利用することで音声への再構築が可能であることも確認された．

図 4: スマートスピーカーからの情報漏えい評価実験環境

図 5: スマートスピーカーで再生した音声ファイルのスペクトログラム

5. おわりに

本論文では，一般家庭に設置される IoT 機器に対するトラストを実現するために，電磁情報，通信情報，そして家電情報という 3 つの情報を組合せ，IoT 機器の動作を可視化し，ユーザに提示する IoT 活動量計というコンセプトを提案した．これまでに行った通信情報に基づく，IoT 機器の識別および発動機能推定に加え，本稿では，IoT 機器から出力される，もう 1 つの情報として，“電磁波” を用いた発動機能推定に関する初期評価について報告した．電磁波というサイドチャネル情報を取得・解析することで，通信情報だけでは検出できない不正動作やハッキングを検知できる可能性がある．

さまざまな IoT 家電が設置されている奈良先端大のスマートホーム環境内に，電磁波計測環境を構築し，Amazon Echo Dot（第 2 世代）を対象とした電磁波計測を行ったところ，音声情報（マイク素子）が漏洩しており，観測した電磁波情報から再構築可能であることが判明した．

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. Iot デバイスの急速な普及. https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r01/html/nd112120.html.

[2] Forbes. Time to update your vacuum cleaner

図 7: Amazon Echo Dot（第 2 世代）動作時の電源線の伝導ノイズを測定したパワースペクトル

図 6: スマートスピーカーの電源線を伝搬する電磁波から再構成された音声のスペクトログラム

– hack turns lg robot hoover into a spy, 2017. https://www.forbes.com/sites/thomasbrewster/2017/10/26/lg-hom-bot-robot-hoover-hacked-into-surveillance-device/#71ccc44bf042.

[3] Forbes. Criminals hacked a fish tank to steal data from a casino, 2017. https://www.forbes.com/sites/leemathews/2017/07/27/criminals-hacked-a-fish-tank-to-steal-data-from-a-casino/#7faff4e832b9.

[4] Techcrunch. 世界中の無防備な web カメラを見せる insecam…パスワードに無関心なアドミンが多い, 2014. https://jp.techcrunch.com/2014/11/08/20141107insecam-displays-insecure-webcams-from-around-the-world/.

[5] 小池大地, 石田繁巳, 荒川豊. 通信トラヒック分析に基づく iot デバイスの発動機能推定手法の検討. マルチメディア，分散，協調とモバイル (DICOMO2020) シンポジウム, pp. 933 – 939, 2020.

[6] Yutaka Arakawa Daichi Koike, Shigemi Ishida. Called function identification of iot devices by network traffic analysis. In *The 36th ACM/SIGAPP Symposium On Applied Computing (SAC2021)*, pp. 737–743, 2021.

[7] Diane J Cook, Aaron S Crandall, Brian L Thomas, and Narayanan C Krishnan. Casas: A smart home in a box. *Computer*, Vol. 46, No. 7, pp. 62–69, 2012.

[8] Tomokazu Matsui, Kosei Onishi, Shinya Misaki, Manato Fujimoto, Hirohiko Suwa, and Keiichi Yasumoto. Salon: Simplified sensing system for activity of daily living in ordinary home. *Sensors*, Vol. 20, No. 17, p. 4895, 2020.

[9] Abdulsalam Yassine, Shailendra Singh, and Atif Alamri. Mining human activity patterns from smart home big data for health care applications. *IEEE Access*, Vol. 5, pp. 13131–13141, 2017.

[10] Eri Nakagawa, Kazuki Moriya, Hirohiko Suwa, Manato Fujimoto, Yutaka Arakawa, and Keiichi Yasumoto. Toward real-time in-home activity recognition using indoor positioning sensor and power meters. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 539–544. IEEE, 2017.

[11] Patrice Guyot, Julien Pinquier, and Régine André-Obrecht. Water sound recognition based on physical models. In *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 793–797. IEEE, 2013.

[12] Xenofon Fafoutis, Balazs Janko, Evangelos Mellios, Geoffrey Hilton, R Simon Sherratt, Robert Piechocki, and Ian Craddock. Spw-1: A low-maintenance wearable activity tracker for residential monitoring and healthcare applications. eHealth 360° , pp. 294–305. Springer, 2017.

[13] 福嶋章悟, 藤本大介, 林優一. リモートワーク環境におけるスピーカーフォンからの電磁波を通じた情報漏えい評価. 2021 年暗号と情報セキュリティ シンポジウム（SCIS2021）, pp. 2D2–2, 2021.

[14] 福嶋章悟, 藤本大介, 林優一. 設置環境の異なるスマートスピーカーからの電磁的情報漏えい評価と対策. ハードウェアセキュリティ研究会 (HWS), pp. HWS2020–66, 2021.

[15] Jieun Choi, Hae-Yong Yang, and Dong-Ho Cho. Tempest comeback: A realistic audio eavesdropping threat on mixed-signal socs. CCS '20, p. 1085–1101. Association for Computing Machinery, 2020.

[16] 上田健揮, 玉井森彦, 荒川豊, 諏訪博彦, 安本慶一ほか. ユーザ位置情報と家電消費電力に基づいた宅内生活行動認識システム. 情報処理学会論文誌, Vol. 57, No. 2, pp. 416–425, 2016.

[17] Stefan Mangard, Elisabeth Oswald, and Thomas Popp. *Power analysis attacks : revealing the secrets of smart cards*. Springer Science Business Media, 2008.

[18] Yu-Ichi Hayashi, Naofumi Homma, Takashi Watanabe, William O. Price, and William A. Radasky. Introduction to the special section on electromagnetic information security. *IEEE Transactions on Electromagnetic Compatibility*, Vol. 55, No. 3, pp. 539–546, 2013.