6Y-09

モノのインターネットにおけるプライバシー保護に関する検討

重森 一槻　　向井 宏明　　横谷 哲也

金沢工業大学工学部　〒921-8501　石川県野々市市扇が丘 7-1

1. はじめに

近年，ヘルスケアやコネクテッドカーなどモノのインターネット（IoT：Internet of Things）を活用することで人々の生活の利便性が高まってきている．一方で，個人を特定可能な情報の流出事例の報告もあり，今後はプライバシー保護が重要である．しかしながらプライバシー保護を強化しようとすると情報サービスの利便性を低下させてしまうという，トレードオフの関係にある．そこで，本研究では IoT のプライバシー面に注目し，利便性とプライバシーを両立するデータ転送方式の確立を目標とする．

2. IoT における個人情報流出に関する課題

IoT は異なるシステム間でデータを利活用する System of system であり，利活用を効率的に行うために，様々なベンダーや標準化団体により IoT プラットフォームの開発が進んでいる．しかし，データを集める際，個人情報も含むものもあり，どのようにデータを扱うかが問題となっている．

IoT における個人情報が問題となった事例の 1 つとして，2013 年にイギリスで起きたものがある．ある企業がロンドンの街角に無線 LAN 基地局機能を持つ「スマートゴミ箱」を複数台設置し，そのゴミ箱で通行人らが所有するスマートフォンやタブレットなどの携帯端末の MAC アドレスを収集する実験を行われた．このゴミ箱は広告が表示できるディスプレイが備え付けられ，広告収入によってゴミ箱管理の費用を軽減しようというものであった．しかし，MAC アドレスは個人にひもづくもので、そのデータがトラッキングされることがプライバシー上の懸念となるということからこの実験は中止された．[1]

3. IoT におけるデバイス仮想化によるプライバシー保護

前述の課題を解決するために，デバイスの情報をそのまま伝達するのではなく，情報を加工し仮想的なデバイスとしてデータを利活用することが有効であると考えられる．[2][3]

A Study on privacy protection in IoT
Kazuki Shigemori, Hiroaki Mukai and Tetsuya Yokotani
Kanazawa Institute of Technology, 7-1 Ohgigaoka, Nonoichi, Ishikawa, 921-8501, Japan

図 1 に，IoT デバイスの仮想化のイメージを示す．IoT デバイスの仮想化とは，物理 IoT デバイスを仮想化し，デバイスから生成されるデータやコンテキスト情報，またその処理機能をサービスとして提供する Things as a Service を実現する技術である．

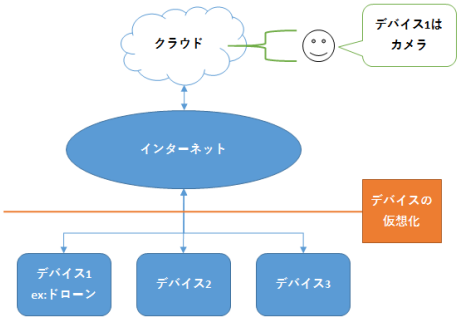

図 1 IoT デバイスの仮想化

前述のスマートゴミ箱の事例は，MAC アドレスを収集し，それを利用して広告を表示していた．ここで問題とされているのが，収集された MAC アドレスまでも利活用され，個人情報が流出する可能性があるという点である．企業が収集したいデータは，広告を何度表示したか，視認されたかという情報であった．

そこで IoT デバイスの仮想化の技術であるデバイスから収集したデータを加工し，個人を特定できる可能性があるデータを隠蔽する．図の例では，ドローンを仮想化し，1 つ，または，複数の特定の位置に移動できる非常に遅い速度で写真を撮るカメラにする．これはドローンの経路を制御して，テナントが選択した場所を定期的に駆動し，それによって写真を撮影することによって実現される．

前述の事例においては，デバイスから収集した MAC アドレスを元に人数をカウントする別のデバイスに見せる．実際のデバイスが収集する情報自体は MAC アドレスに変わりはないが，クラウドでは仮想化された他のデバイスにより人数に関する情報が利活用されることになる．

4. 仮想 IoT システムの概要

図 3 に検証した仮想 IoT システムの構成を示す．今回検証したシステムでは，Orion Context Broker と IoT Agent の 2 つの FIWARE コンポーネントと，Mosquitto MQTT Broker，MongoDB を使用する．

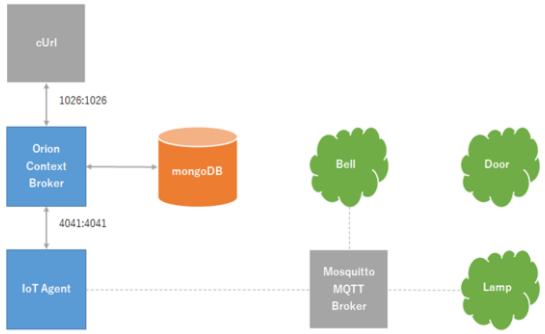

図 3 仮想 IoT システムの構成

FIWARE は，拡張された OpenStack ベースのクラウド環境とオープンスタンダード API セットを提供する．[4]

IoT システムに接続し，ビッグデータとリアルタイムメディアを処理・分析したり，ユーザの操作のための高度な機能を組み込むことができる．また，コンテキスト情報を大量に生成・収集・公開・消費する手段を提供する．

Orion Context Broker は，標準の REST API を実装することにより，コンテキスト情報を大規模に処理できる．ここでは，NGSI を使用してリクエストを受信する．

IoT Agent は，モジュラアーキテクチャを備えたいくつかの IoT プロトコルをサポートする．ここでは，NGSI を使用してサウスバウンドを受信し，MQTT Broker 用の JSON のトピックに変換する．登録されたトピックについて MQTT Broker をリッスンし，測定値をノースバウンドに送信する．

Mosquitto MQTT Broker は，必要に応じて MQTT トピックを IoT Agent と IoT デバイスの間でやりとりする中央通信ポイントとして機能する．

MongoDB は，Context Broker が，データエンティティ，サブスクリプション，レジストレーションなどのコンテキストデータ情報を保持するために使用する．IoT Agent がデバイスの URLs や Keys などのデバイス情報を保持するために使用する．ここでは，保持している情報の永続性を保つために 2 つの FIWARE コンポーネントが用いる．また，Mosquitto のインスタンスを追加する．

5. 検証

今回の検証では，デバイスを作成し，パブリッシュ・サブスクライブ（Publish-Subscribe）方式で仮想化されたデバイスが生成するデータを送受信する．

curl コマンドを使用して新しいデバイスを作成する．ここでは温度と輝度を測定できるカメラがあることを想定する．Temperature（温度）と Luminance（輝度）の 2 つのアクティブな属性を宣言し，デバイスの作成を行う．

IoT Agent は測定値が要求されると，Context Broker にその値を問い合わせる．それらを収集すると，”/sensor01/attrs”のサフィックスを持つトピックのデバイスに送信する．仮想化されたデバイスでこのオペレーションを確認するために図 4 のコマンドを実行する．

```
$ mosquitto_sub -t /1234/sensor01/attrs
```

図 4 サブスクライブ

デバイスから測定値を仮想化する．今回設定したデバイスは，DeviceID は sensor01，API Key は 1234 であるので，図 5 のコマンドを実行する．Temperature を 31.5 と Luminance を 4 と設定する．

```
$ mosquitto_pub -t /1234/sensor01/attrs -m '{"l":4,"t": "31.5"}'
```

図 5 パブリッシュ

図 6 に，仮想化されたデバイスの出力データを示す．Temperature が 31.5，Luminance が 4 となっていて，これはデータとしてクラウドに提供される．

```
$ mosquitto_sub -t /1234/sensor01/attrs
{"l":4,"t": "31.5"}
```

図 6 仮想化されたデバイスのデータ

6. おわりに

今回，仮想化された IoT デバイスを生成し，データを利活用できることを検証した．これにより個人を特定可能な情報の流出を避けることができると考えられる．しかし，必要ない場合でも情報自体は取得できるので，今後は，個人を特定可能な情報については，利便性を損なわず，かつ，匿名性を確保できる方式を検討する．

謝辞

本研究成果は，戦略的情報通信研究開発推進事業（国際標準獲得型）「スマートシティアプリケーションに拡張性と相互運用性をもたらす仮想 IoT クラウド連携基盤の研究開発(Fed4IoT)」によるものである．

参考文献

[1] https://www.dekyo.or.jp/info/2017/07/security/28/
[2] https://fed4iot.org/index.php/japan-home
[3] 金井 謙治, 吉田英聖, 金光永煥, 中里秀則, 横谷哲也,向井宏明, 中村健 一, 上杉充, ” Things as a Service を実現する Fed4IoT プラットフォームの研究開発”, 信学技報, vol. 119, no. 256, CS2019-69, pp. 39-44, 2019 年 10 月
[4] https://www.letsfiware.jp/