一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
CS2020-65,IE2020-24(2020-11)

仮想 IoT プラットフォームを活用した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† 金井 謙治††

†金沢工業大学工学部　〒921-8501　石川県野々市市扇が丘 7-1
††早稲田大学理工学術院総合研究所 〒169-8555 東京都新宿区大久保 3-4-1

E-mail: b6900588@planet.kanazawa-it.ac.jp, {mukai.hiroaki, yokotani}@neptune.kanazawa-it.ac.jp, k.kanai@aoni.waseda.ac.jp

あらまし　近年，カメラ，センサー類，家電製品，車などのデバイスからデータを収集してクラウドで分析，可視化など行う IoT により人々の生活の利便性が高まっている．しかし，現在の IoT はアプリケーション開発者がデバイスの設置からデータの収集まで自己完結しているため，開発に時間とコストを要するという問題がある．本稿では，現在の垂直統合型 IoT プラットフォームに対して，拡張性と相互運用性を実現する水平統合型 IoT プラットフォームである仮想 IoT を紹介する．データの相互運用が実現されると，収集するデータに偶発的に個人が特定可能な情報が含まれるなどプライバシー保護が課題になる．この課題に対して仮想 IoT プラットフォームを活用し，IoT デバイスを仮想化することによる匿名性の向上を提案する．

キーワード　IoT，プラットフォーム，仮想 IoT，デバイス仮想化，プライバシー

A Study on privacy protection with the virtual IoT platform

Kazuki Shigemori† Hiroaki Mukai† Tetsuya Yokotani† and Kenji Kanai††

†Kanazawa Institute of Technology, 7-1 Ohgigaoka, Nonoichi, Ishikawa, 921-8501, Japan
††Waseda University, WISE 3-4-1 Okubo, Shinjuku-ku, Tokyo, 169-0072, Japan

E-mail: b6900588@planet.kanazawa-it.ac.jp, {mukai.hiroaki, yokotani}@neptune.kanazawa-it.ac.jp, k.kanai@aoni.waseda.ac.jp

Abstract　In recent years, the convenience of people's lives is increasing due to the Internet of Things (IoT) that collects data from devices such as cameras, sensors, home appliances, and cars, and analyzes and visualizes them in the Cloud. However, the current IoT is a vertically-integrated type in which the application developer self-completes from device installation to data collection, and there is a problem that development takes time and cost. In this paper, firstly, we introduce virtual IoT, which is a horizontally integrated IoT platform that realizes scalability and interoperability. Next, we discuss privacy issue in data interoperability. There is a possibility that collected data accidentally contains personally identifiable information. For this problem, we propose privacy protection method with the IoT device virtualization.

Keywords　IoT，platform，Virtual IoT，device virtualization，Privacy

1. はじめに

近年，センサー類，家電製品などのデバイスからデータを収集してクラウドで分析，可視化など行う IoT（Internet of Things）により人々の生活の利便性が高まっている．しかし，現在の IoT はアプリ開発者がデバイスの設置からデータの収集まで自己完結している垂直統合型であり，開発に時間とコストを要するという問題がある．本研究では，現在の垂直統合型 IoT プラットフォームに対して，水平統合型 IoT プラットフォームを，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）[1]において開発している．Fed4IoT では，各アプリケーションにおいてサイロ化された IoT プラットフォームに対して，拡張性と相互運用性を実現し，スマートシティにおけるアプリケーションの開発・展開の簡易化，持続可能性を実現することを目的としている．

IoT プラットフォームを相互運用する際，収集するデータに偶発的に個人が特定可能な情報が含まれてしまうなどプライバシーを保護に関する懸念があるが，これを仮想 IoT[2]を利用して匿名化処理を行うことによりプライバシー保護を実現する．

本稿では，現在開発中の IoT における拡張性と相互運用性を実現する仮想 IoT プラットフォームを紹介し，そこで課題となるプライバシー保護に対しては IoT デバイス仮想化の適用を提案し，試作システムを構築したので報告する．

2. 仮想 IoT プラットフォーム

2.1. IoT システム

図 1 に IoT システムの構成図を示す[3]. IoT システムはデバイスがデータを収集,ネットワークを通じて,プラットフォームで情報を分析し，サービスが展開される．さらに，異なるシステム間でデータを利活用する System of systems である．

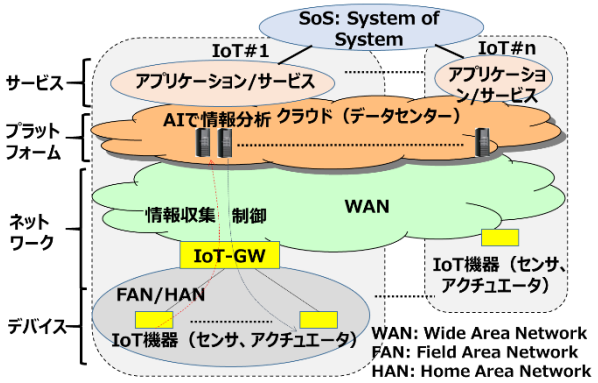

図 1　IoT システムの構成図

図 2 に示すように，現状では，IoT システムは各々が独立した垂直統合型 IoT システムとなっていることが多い．System of systems 実現には，IoT システムはデバイスとクラウド間のインタフェースは拡張性があるものであることが望ましく，また，サービス提供者と IoT デバイス提供者間でのマルチベンダ環境が実現できるよう相互運用性も求めた水平統合型 IoT プラットフォームが望ましい．

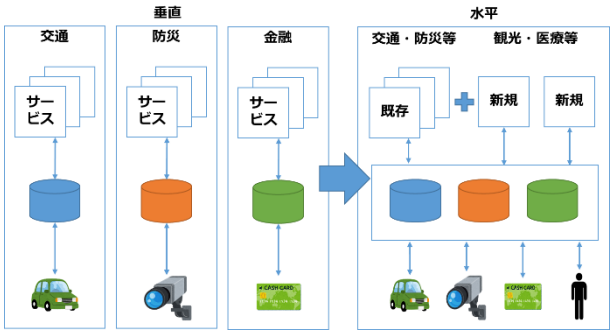

図 2　垂直統合型/水平統合型 IoT プラットフォーム

水平統合型 IoT プラットフォームに向けて，インタフェースを標準化することで，IoT のデータ流通に関連する拡張性および相互接続性の実現に向けた取り組みが行われている．これはデータ流通プラットフォームと呼ばれ，標準化団体[4]およびベンダーが開発を行なっており，異なる IoT システムでデータの利活用が可能な水平型統合型 IoT プラットフォームの実現が目標となっている．

筆者らが試作している IoT システム[5]では，データ流通プラットフォームの 1 つである FIWARE[6]を用いている．図 3 に FIWARE の基本的な構成を示す．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．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，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．アプリケーションとブローカー間，デバイスとブローカー間はネットワーク API の標準規格である NGSI[7]で定義されたデータモデルを使用している．

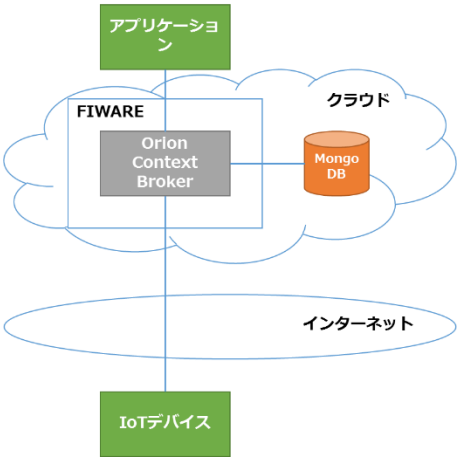

図 3　FIWARE の構成

図 4 に NGSI 形式のデータモデルの例を示す．この例は IoT デバイスが送信するデータとしてデバイスの場所と温度に関する情報を送信するものである．図中の”type”で温度計であることを示し，”location”が場所を”temperature”が温度を示す領域である．

```
{
    "id": "urn:ngsi-ld:KIT:Thermometer01",
    "type": "Thermometer",
    "dataissued": {
    "type": "TimeDate",
    "value": "2020-05-12 16:02:56.343000"
    },
    "location":{
        "type": "geo:json",
        "value": {
            "Type": "Point",
            "coordinates": [36.5313, 136.6285]
        }
    },
    "temperature": {
        "type": "Temperature",
        "value": {
            "value": "1",
            "unit": "Degree"
        }
    },
}
```

図 4　NGSI 形式のデータモデル

2.2. Fed4IoT プロジェクト

Fed4IoT プロジェクト[1]では，大規模な環境を見据え，相互作用を及ぼすデバイス，プラットフォーム，情報といった異なったレベルについて考察し，相互運用の課題に取り組んでいる．プロジェクトの目標は「斬新な IoT 仮想化技術により，拡張性に富み相互運用が可能なスマートシティアプリケーションを実現するための，IoT とクラウドインフラの連携」である．Fed4IoT プロジェクトでは図 5 のような仮想 IoT システムの開発を行っており，データ提供者とデータ利用者間の相互接続を目標とする．

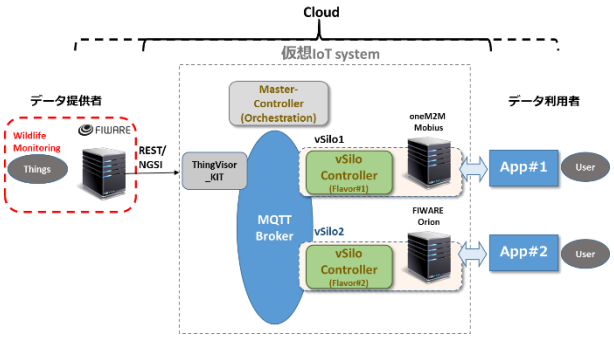

図 5　仮想 IoT システム

3. データ利活用におけるプライバシー保護に関する課題

デバイスからデータを取集する際，個人を特定可能なデータも収集される可能性がある．そのデータが異なるシステム間で利活用され，個人情報の流出から不利益を被る場合がある．IoT インタフェースの標準化が進み，拡張性および相互接続性が確保されると，データを収集している際に偶発的に個人情報混入し、その後個人情報が拡散してしまう危険性がある．

一例として，カメラがある．表 1 に IoT システムにおけるカメラの活用事例を示す．カメラの画像・映像は，街中の変化情報を把握し，地図情報の更新等や，性別や年齢の把握により，商品開発等へ活用されたりする．しかし，カメラが収集するデータには，撮影範囲内への写り込みや，設備利用上避けられない経路等があり，写る人本人が常に事前の通知を受け、個人情報の取得への暗黙の同意を行っているとは限らない状況で個人情報の取得が行われる場合がある[8]．すなわち，カメラ画像の利活用にあたって，データの利用目的やデータの漏洩による影響が分からないといった不安がある．

表 1　IoT システムにおけるカメラの活用事例

No.	分類	例
1	特定の個人を識別せず、風景のみを利活用	街中の変化情報を把握し、地図情報の更新等へ活用
2	人数を計測し、統計情報として利用	通行者数の把握により、都市計画等への活用
3	一人ひとりの人物属性を推定し、統計情報として利用	性別・年齢等の把握により、商品開発等への活用
4	一人ひとりの座標値を取得し、動線データとして利用	移動・滞留状況や棚前での行動を把握し、通路や棚の最適配置等への活用
5	一人ひとりの、来店履歴、動線データ、購買履歴、推定した人物属性を一定期間取得	一定期間、来店履歴、行動履歴、購買履歴、属性等を紐づけて把握することにより、来店客の嗜好にあった品揃えや、通路や棚の最適配置等へ活用
6	別途保有する会員情報等と紐づけ、マーケティング情報として利用	個人の購買履歴や行動履歴の把握により、個人向けサービス等への活用

この問題に対して，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．すなわち，カメラ画像をそのまま利活用するのではなく，画像処理等を施した結果を仮想的な IoT デバイスとして仮想 IoT システム上に生成する[9][10]．例えば，通行者数の把握をしたい場合は，人やモノの数を数えるカウンターデバイスに仮想化する．また，人の移動や滞留状況などを知りたい場合は，人やモノが集まっている場所を写真として撮る設置型カメラに仮想化する．設置型カメラに仮想化する際，写真に個人情報が含まれる可能性があるので，仮想化に加え，画像処理等を施すことで利用目的は明確であるが，個人を特定される可能性がある状況をなくし，匿名性を確保することができる．以上のように，IoT デバイスの仮想化は IoT におけるプライバシー保護にも有効である．

4. デバイス仮想化を用いたプライバシー保護

4.1. 構成

図 6 にカメラの画像を，仮想 IoT を用いてプライバシー保護を行う検証系の構成と，表 2 にその構成のコンポーネントの機能説明を示す．データ流通プラットフォームに FIWARE を用いて，データを NGSI 準拠の形式とし，アプリケーションおよび IoT デバイスの相互運用を可能とした．仮想 IoT は，図 6 中の Mosquitto

MQTT Broker，Thing Visor，Virtual Silo Flavour，Master Controller，Mongo DB により構成される．PC1 はデータ提供者，PC2 はクラウド，PC3 はデータ利用者が利用する．

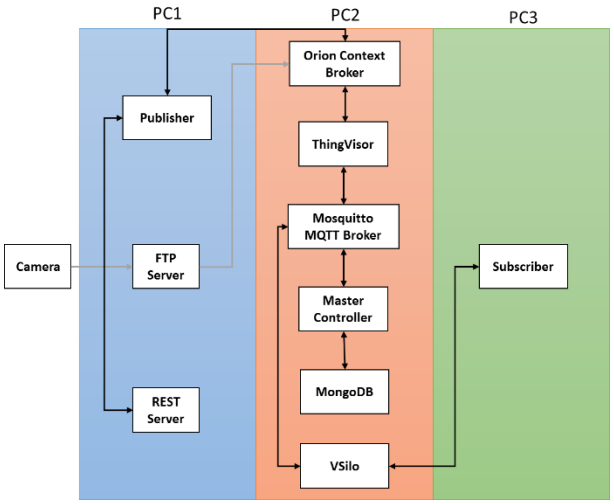

図 6　検証系の構成

表 2　各コンポーネントの機能

名称	説明
Orion Context Broker	FIWARE コンポーネントの１つである．更新、クエリ、レジストレーション、サブスクリプションなど、コンテキスト情報のライフサイクル全体を管理する．
Mosquitto MQTT Broker	パブリッシュ/サブスクライブモデルを使用してメッセージングするブローカーである．
Thing Visor	仮想デバイス（実物から来るデータを処理・制御することで得られるデータを生成する実物のエミュレーション）を実装したシステムエンティティである．今回は実物のカメラを仮想の人物カウンターにエミュレートする．
Virtual Silo Flavour	仮想サイロ（仮想デバイスと Broker によって形成される分離された仮想 IoT システム）の型を示す．例えば，Orion Flavor は Context Broker を持つ仮想サイロに関連し，MQTT Flavor は，Mosquitto MQTT Broker を持つ仮想サイロに関連する．
Master Controller	管理者やテナントからの要求に応じて，システム内の新しいコンポーネントの展開とその調整を管理する．
Mongo DB	オープンソースソフトウェアのドキュメント指向データベースである．ここでは，仮想サイロ，仮想デバイス，Thing Visor などのシステム状態情報を格納している．また，デバイスから送られてくるデータも保存される．

図 7 にデータ利用者へ Orion Context Broker を介して画像を提供する構成を示す．①カメラから得た画像を FTP Server で受け取って，②Orion Context Broker へ画像のリソースを Publish する．その後，③実際の画像へのアクセスを REST で受けつけ，④実際の画像を取得し，保存する．データ利用者は GET のリクエストを送ると，画像を得ることができる．

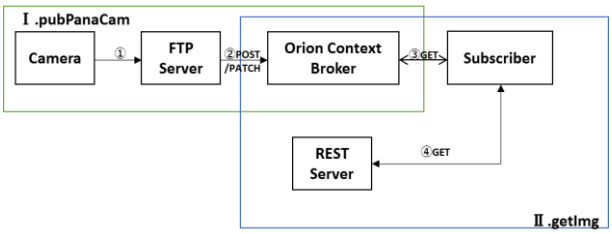

図 7　画像をデータ利用者へ提供する構成

図 8 にデータ利用者へ人物検知の情報を提供する構成を示す．データ提供者が画像を入手するまでは図と同じ手順である．データ提供者が画像を得た後，Object Counter で人や物を検知させ，その結果を Orion Context Broker へ POST する．⑥データ利用者は GET のリクエストを送ると,その結果を得ることができる．

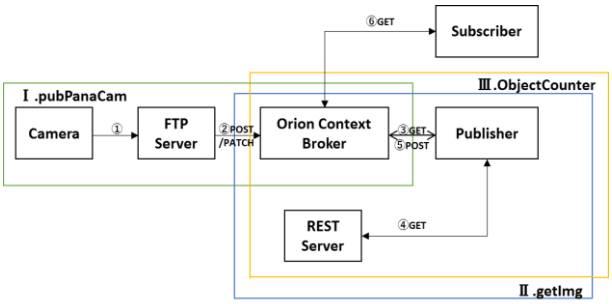

図 8　人物検知情報をデータ利用者へ提供する構成

図 9 にデータ利用者へ仮想 IoT を介して人物検知の情報を提供する構成．図 8 が実物のカメラで撮った画像を物体検知したデータを得るものに対し，図 9 は仮想 IoT システムを用いて，実物のカメラを仮想的なカウンターとして，データを得るものとなっておりデータの利活用を可能とするものである．ObjectCount まで図 8 と同じ手順である．⑦検知したデータを ThingVisor によって仮想的なデバイスにした後，データ利用者はそのデバイスからデータを得る(⑧～⑫)．

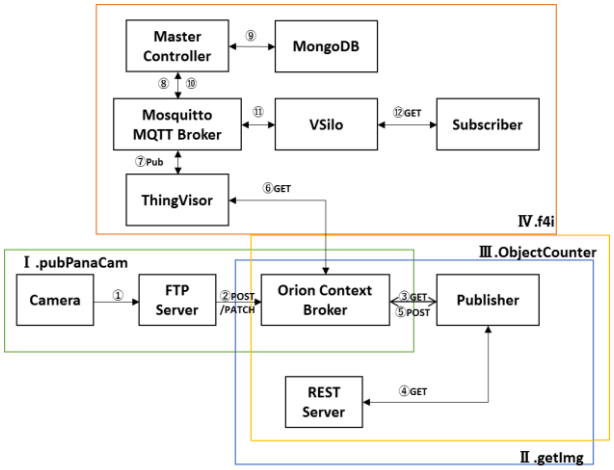

図 9　仮想 IoT を経由して人物検知情報をデータ利用者へ提供する構成

図 10 に仮想 IoT を経由して人物検知情報をデータ利用者へ提供する手順を示す. データ提供者は, Master Controller にログインし，Thing Visor を追加する．その後，データ提供者が設置したデバイスから収集しているデータを Context Broker へ POST する. Thing Visor は Context Broker からデータを GET し，Mosquitto へパブリッシュする.

データ利用者は，Master Controller にログインし，Virtual Silo Flavour を登録する．その後，仮想デバイスのエンティティである vThing のリストを確認し, その中から必要な vThing を追加する．追加その際，Virtual Silo Flavour は Mosquitto へサブスクライブを行い，Mosquitto は Virtual Silo Flavour へパブリッシュを行う．パブリッシュを受けた Virtual Silo Flavour は Context Broker へデータを POST し，データ利用者は Context Broker からデータを GET する.

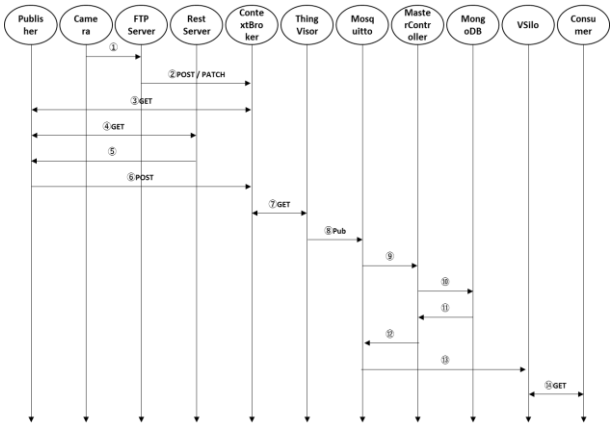

図 10　仮想 IoT を経由して人物検知情報をデータ利用者へ提供する手順

4.2. 試作システムの検証

試作システムによりカメラで撮影した画像を人物検知デバイスとして仮想化し,個人情報が含まれないデータとしてクラウドで利活用する具体例を示す.

図 11 に図 7 中の pubPanaCam の動作を示す. pubPanaCam は，カメラから得た画像を FTP Server で受けとり，Orion Context Broker へ画像のリソース（タイムスタンプ）を Publish するソフトウェアである.

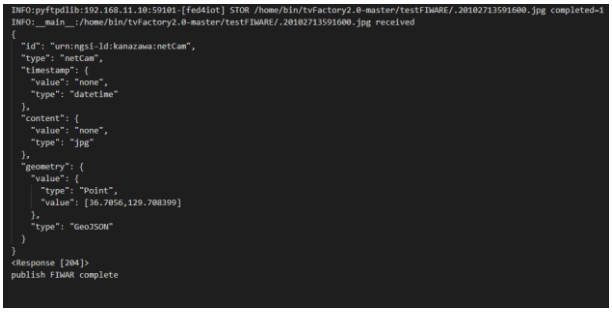

図 11　pubPanaCam の動作

図 12 に図 7 中の getImg の動作を示す．getImg は，Orion Context Broker からの画像ファイルの URI を取得し，画像ファイルの URI を指定して，REST サーバから画像データを GET する．その後，画像ファイルをカレントディレクトリに保存する．図 12 中の URI が画像ファイルの格納先である.

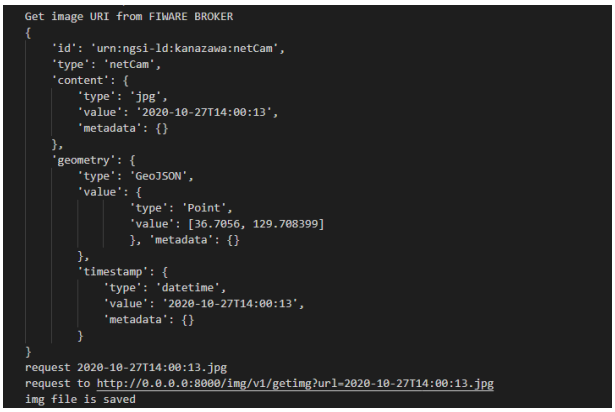

図 12　getImg の動作

図 13 に図 8 中の Object Counter の動作を示す．Object Counter は，Orion Context Broker からの画像の URI の取得し，REST サーバから画像データを GET する．その後，YOLOv3-tiny（You Look Only Onse：リアルタイムオブジェクト検出アルゴリズム）でオブジェクトを検出して、オブジェクトの数を数える．その結果を Orion Context Broker へ Publish をする．図 14 は Object Couter を動作させたもので，この画像には人物が 3 人写っているため, 図 13 の counter は人数を指すが，そのため value が 3 となっている.

```
[callYOLO] start callYOLO function
conneted from 127.0.0.1.
write image to file
complete
request.jpg: Predicted in 3.757565 seconds.
person,72,519,532,134,157
person,70,237,265,111,181
person,61,316,446,40,315
send results
complete!
{
  "content": {
  },
  "geometry": {
  },
  "timestamp": {
  },
  "object": {
  },
  "counter": {
    "type": "Property",
    "value": {
      "value": 3,
      "tag": "person"
    }
  }
}
publish to FIWARE Broker
```


図 13　ObjectCounter の動作

図 14　実際の画像

図 15 に仮想 IoT システムの動作を示す．現実のカメラを仮想化し，仮想的な人物カウンターにした．図中の ”type”で”counter”と表示されており，実デバイスはカメラであるがクラウドでは人物カウンターデバイスとしてデータを提供することがわかる．


```
"data": [{
    "id": "urn:ngsi-ld:KIT:Counter01",
    "type": "counter",
    "detectedObject": {
        "type": "Property",
        "value": "{
            "id":
            "urn:ngsi-ld:kanazawa:netCam:counter:person",
            "type": "counter",
            "content": {
                "type": "jpg",
                "value": "2020-10-27T15:47:40",
                "metadata": {}
            },
            "counter": {
                "type": "Property",
                "value": {
                    "value": 1,
                    "tag": "person"
                }, "metadata": {}
            },
            "geometry": {
            },
            "object": {
            },
            "timestamp": {
            }
        }"
    }
}],
"meta": {
    "vThingID": "counter-tv/hello"
}
```


図 15　仮想 IoT システムの動作

この仮想カウンターは実際のデバイスのデータを利用しているため，データ提供者側から見ると，どちらも同じに見えるが，データ利用者側からは，実物のデバイスは見えない．そのため，１台のカメラでなくても，複数のカメラから得たものや，カメラ以外，例えばドローンなど，他のデバイスに変更することもできる．利活用されたくないデータ，今回は画像そのものを意図的になくすことができる．

5. まとめ

仮想 IoT システムを用いて，拡張性・相互接続性が実現可能な水平型 IoT プラットフォームの構築と，それを用いたデータ利活用時のプライバシー保護について検証を行った．今回はカメラを用いたが，プライバシーの保護をする必要があるデバイスは他にも存在する．今後はそういったデバイスに対しても，匿名性を確保することを目指す．

謝　辞

本研究成果は，総務省 SCOPE（国際標準獲得型）JPJ000595「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．

文　献

[1] https://fed4iot.org/index.php/japan-home/

[2] 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

[3] ITU-T Recommendation Y.2060, "Overview of the Internet of things"

[4] https://www.onem2m.org/

[5] 重森一槻，阿蔵和馬，丸山航，向井宏明，横谷哲也，"屋外ワイヤレスセンサーネットワークに適用する IoT デバイス管理方式"，信学技報，vol.119, no.424, CS2019-109, pp.67-72, 2020 年 2 月．

[6] https://www.letsfiware.jp/

[7] https://www.etsi.org/deliver/etsi_gs/CIM/001_099/009/01.01.01_60/gs_CIM009v010101p.pdf

[8] https://www.soumu.go.jp/main_content/000542668.pdf

[9] 重森 一槻，向井 宏明，横谷 哲也，” 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”，情報処理学会 全国大会, 2020 年 3 月

[10] 重森一槻，向井宏明，横谷哲也，"仮想 IoT におけるプライバシー保護に関する検討"，信学技報，vol. 120, no. 164, CS2020-45, pp. 53-56, 2020 年 9 月