

【ポスター講演】異種サービス連携のための実空間運動型 データ管理アーキテクチャの提案

長尾 健太郎[†] 妙中雄三[‡] 永田晃^{‡‡} 田村瞳^{‡‡‡} 塚本和也^{††}

†九州工業大学大学院 情報工学府 先端情報工学専攻 〒820-8502 福岡県飯塚市川津 680-4

‡奈良先端科学技術大学院大学 先端科学技術研究科 〒630-0192 奈良県生駒市高山町 8916-5

‡‡ 株式会社 iD 〒812-0011 福岡市博多区博多駅前1丁目7-22 第14岡部ビル8F

‡‡‡ 福岡工業大学 工学研究科 電子情報工学専攻 福岡県福岡市東区和白東 3-30-1

††九州工業大学大学院 情報工学研究院 〒820-8502 福岡県飯塚市川津 680-4

E-mail: †1 nagao@infonet.cse.kyutech.ac.jp ‡ yuzo@is.naist.jp ‡‡ a-nagata@intelligent-design.co.jp

‡‡‡ h-tamura@fit.ac.jp †† tsukamoto@cse.kyutech.ac.jp

あらまし 近年、スマートシティに代表されるような、人々の生活圏内のモノ/サービスのデータや、パーソナルデータをネットワークを介して相互連携する IoT サービスが注目されている。しかし、現在パーソナルデータの利活用に関して法的制約があり、ネットワーク基盤がデータの収集範囲と対応していないため、送信者、サービス事業者はパーソナルデータ流通をしにくい状況となっている。本稿では、異種パーソナルデータ連携に必要となるデータが、地理的範囲に依存する点に着目し、多様な実空間範囲毎にデータ流通プラットフォームを設置する事で、サービス事業者の求めるデータを取得可能かつ、送信者の合意の得やすいデータ管理アーキテクチャを新たに提案する。

キーワード Internet of Things, パーソナルデータ, IPv6, データ管理, ネットワークアーキテクチャ, 地理空間情報

【Poster Presentation】 Proposal of Real-Spatial based data management architecture for heterogeneous service cooperation

Kentaro NAGAO[†] Yuzo TAENAKA[‡] Akira NAGATA^{‡‡} Hitomi TAMURA^{‡‡‡}
and Kazuya TSUKAMOTO^{††}

† Graduate School of Computer Science and System Engineering, Kyushu Institute of Technology
680-4 Kawazu, Iizuka-shi, Fukuoka, 820-8502, Japan ‡ Graduate School of Information Science, Nara Institute of
Science and Technology, 8916-5 Takayama, Ikoma, Nara 630-0192 Japan

‡‡ iD Corporation 1-7-22 Hakata-ekimae, Hakata-ku, Fukuoka, 812-0011 Japan ‡‡‡ Graduate School of
Engineering Fukuoka Institute of Technology, 3-30-1 Wajirohigashi, Higashi-ku, Fukuoka, 811-0925 Japan †† Faculty
of Computer Science and System Engineering, Kyushu Institute of Technology 680-4 Kawazu, Iizuka-shi, Fukuoka, 820-
8502, Japan.

E-mail: † nagao@infonet.cse.kyutech.ac.jp ‡ yuzo@is.naist.jp ‡‡ a-nagata@intelligent-design.co.jp
‡‡‡ h-tamura@fit.ac.jp †† tsukamoto@cse.kyutech.ac.jp

Abstract

Recently, IoT services that mutually cooperate with data of thing, services and personal data, within people's living area, via a network are receiving attention, such as smart city. However, there are legal restrictions on the utilization of personal data, and since the network infrastructure does not correspond to the data collection range, currently it is difficult for sender and service provider to distribute personal data. In this paper, we focus on the point that heterogeneous personal data depends on the geographical range, and propose a new data management architecture that can acquire the data required by the service providers and easily obtain agreement of the senders by constructing a data distribution platform for each range of various real spaces .

Keywords Internet of Things, Personal data, IPv6, Data Management, Network architecture, Geospatial information

1. はじめに

近年、スマートシティに代表されるような、人々の生活圏内のモノ/ヒト等のデータ(異分野データ)をネットワークを介して相互連携を行い、人々/地域の生活品質を向上させる IoT サービスが注目されている[1]。異分野データを連携させるにあたって、周囲の全てのモノに自身の位置情報を把握させ、近接しているモノ同士がデータを通信し合うことは機器の設置コストや計算コストの観点で困難である。そのため、データの送信端末と、データを収集/分析する機器はネットワーク的に異なる位置に存在する。ある地理範囲内の端末から送信されたデータを、その種類、送信先にかかわらず、1箇所に集めることができれば、人々の生活圏内のデータの収集も容易となるが、現在のネットワーク基盤がサイロ型の構造になっており、現実世界の構造と対応づいていないため、地理空間連携に必要な端末がどこに存在しているのか分からず、様々な宛先に送信されたデータを1箇所に集めることができない。

これに対し[2]では、IoT サービスの多くが特定の地理範囲内のデータを収集、利活用している点に着目し、多様な地理空間範囲ごとにデータを収集するために、多様な空間範囲を識別するメッシュコードを IP アドレスに埋め込むことで IP ルーティングを利用して多様な地理空間範囲内のデータを収集可能なネットワーク基盤、Geo-Centric Network (GCN) 基盤を提案した。

次に、交換されるヒト/モノのデータ(異分野データ)に着目すると、個人を識別可能なデータはパーソナルデータと定義されており、この取扱いに関して課題が残る。パーソナルデータは漏洩することで個人の特定が可能になるため、個人情報保護法[3]や EU 一般データ保護規則[4]等の法律により、データの取得や利活用にはパーソナルデータ送信者(以下送信者)の利用合意が必要となる。しかし、送信者は、パーソナルデータ収集者(以下収集者)、サービス事業者(以下事業者)が提示する利活用目的を完全に把握/制御するのは困難である。このため、収集者/事業者は、送信者からの利用合意を取りにくく、パーソナルデータ流通促進の妨げとなっている。故に、地理空間に基づいたデータ収集の機能だけでなく、パーソナルデータを利活用範囲内で取得、及び利活用するための「送信者の合意取得」を考慮したパーソナルデータ管理方式が必要である。

そこで、本稿では、異分野データ連携の中でも、多様な分野から送信される異種パーソナルデータの取扱について着目し、データ管理アーキテクチャを新たに提案することで、送信者が自身の生活圏内において自由に利活用できる事を目指す。2 章では、パーソナルデータ利活用にあたっての制約、異種パーソナルデータ利活用の現状、要件について述べる。3 章でパーソ

ナルデータ利活用の要件を満たすまでの技術的課題について議論を行う。4 章では、新たに提案する実空間毎のデータ収集/流通を可能とするデータ管理アーキテクチャについて説明し、その有効性について定性的に評価する。5 章で提案したアーキテクチャのユースケースを述べ、6 章でまとめと今後の検討を示す。

2. 異種パーソナルデータ取扱の制約、要件

パーソナルデータ取扱に関する法的拘束の度合いや適応範囲は、国によって異なるが、その要件自体は各国共通している。本章では、EU 一般データ保護規則(GDPR: General Data Protection Rules)[4] より、送信者の権利、事業者の義務を説明し、事業者がパーソナルデータを収集する際の制約について述べる。

2.1. GDPR

送信者は、事業者からの情報を得ることが出来る権利や、パーソナルデータの保有期間や情報源を知ることが出来る権利等、パーソナルデータの収集先がどういった相手なのか、パーソナルデータがどのように扱われるかについて把握し、管理者の持つ、自身のパーソナルデータを取得出来ることを保証されている。また事業者は送信者の権利を保証するため、特定の目的を超えてパーソナルデータを収集、管理してはならない。以上より、送信者の権利を保証するためには、事業者は利用に当たる用途を明確に提示した上で本人の合意を得る必要がある。

上記の点から、事業者がパーソナルデータの取得、利活用する際に、必要となる本人の合意は以下の 2 点となる。

1. パーソナルデータの取得
2. 利用するデータが個人を識別可能な場合、パーソナルデータの利活用目的についての承諾

特に、パーソナルデータを収集した後に他のサービスに利活用する場合は、利活用時に個別に送信者の合意を取るか、パーソナルデータ取得時に利活用されうる項目に対して、送信者の合意を取る必要がある。

2.2. 異種パーソナルデータ利活用例

異種パーソナルデータの利活用については、匿名加工されたデータの利活用と、パーソナルデータのままでの利活用の 2 つの形態が挙げられる。本章では、それぞれの利用用途について紹介する。

2.2.1 匿名加工されたパーソナルデータ利活用

匿名加工されたパーソナルデータは個人を識別出来ないため、自由に利活用することができ、多様な分野で利活用されている。匿名加工されたデータは、それ単体で利活用することは難しく、複数の匿名加工データ/環境情報等を組み合わせることで新たな価値創造を実現している。ロンドンにおけるオープンデータ[5][6] では、ロンドン市行政が主導となり、市民の戸

籍情報を用いた市民の年代の分布や地域による人口密度等の統計情報や、電車やバスなどの公共交通機関の乗降データの統計や道路の工事に関するリアルタイム情報を公開している。公開されたデータを用いて、スマートシティサービスへの利活用が行われている。

しかし、複数の匿名加工データを組み合わせることで個人情報を識別することが可能となる[7][8]ため、利活用に関する送信者の合意を得ずにデータ流通を行う際には、個人を特定しにくくするために、パーソナルデータの粒度をより粗くする必要がある。粒度を粗くすることにより、データから読み取れる情報は少なくなり、データの有用度は下がる[9]。IoTサービスの発展のためには、匿名加工されたデータだけでは、事業者が求める粒度のデータを取得できない恐れがあるため、サービスの要求する粒度に応じてパーソナルデータのままの情報流通が必要となってくる。

2.2.2 パーソナルデータのままの利活用

パーソナルデータのままの流通は、法的制約により、本人に対してデータ毎にどのサービスを利用するか、に関する同意を取る必要があるため、送信者が主体的にパーソナルデータを提供するような利用形態が検討されている。以下に、現在検討されているPDS(Personal Data Store)型、情報銀行型の2つのパーソナルデータ流通形態について述べる。

PDS型では、送信者がパーソナルデータを管理しているサービス事業者から自身のパーソナルデータを取得し、送信者にサービスを還元する他の事業者に提供するといった流通形態である。事業者はより個人の趣向にあったサービスを実現することができ、送信者は、自身の趣向や健康状態を分析してもらうことで、生活の質の向上に繋がる。PDS型の流通は、どのサービス事業者が信頼できるか、自分にメリットのあるサービスを提供してくれるか、といった判断を送信者自身が行わなければならないため、パーソナルデータ保護、サービス利用に関する高いリテラシーが求められる。

情報銀行型の流通は、PDS型で取得したパーソナルデータを情報銀行と呼ばれる信頼できる機関に委託し、データ流通を行う方式である。情報銀行はパーソナルデータ保護が一定の水準を満たし、送信者、または送信者の生活圏内に対してメリットを還元する事業者を選定し、委託されたパーソナルデータを提供する。これにより、本人は、パーソナルデータを提供する事業者の選定に必要なリテラシーを持たなくても、信頼できる相手へのパーソナルデータ流通が可能となる。また、事業者はより多くのパーソナルデータを取得でき、多くの提供者への還元が可能となる。

2.3. 異種パーソナルデータ利活用の要件

2.2節での考察の結果、本節では、異種パーソナルデ

ータ利活用の要件を纏める。

IoTサービスにおけるパーソナルデータ流通形態は、PDS型のような流通形態では、利活用してほしいデータをユーザーが自身で選択的に適応させる必要があり、全ての人が自身情報を選択的に利活用することは難しかったため、情報銀行のような、信頼できる機関にパーソナルデータを委託するような形態が望ましい。現在、情報銀行型流通は、現在検討段階であり、実現のためには、以下の2点の要件を満たす必要がある。

要件1. 利用者に信頼される機関の設立

日本におけるパーソナルデータ流通普及における本人の情報の提供に関する障壁として、情報の流出、不正利用に介する不安、パーソナルデータの利用用途が不明確、といった要素が挙げられている[10]。このことから、情報銀行となる機関は、利用目的やどの程度のパーソナルデータ保証を行っているのか、といったことを透明化させる必要がある。

要件2. 利用者へのメリットの提示

信頼できる機関が作られたとしても、利用者にどのようなメリットがあるかということを提示しなければ利用者はパーソナルデータ流通を利用しない。IoTサービスの発展のためには、提供される異種パーソナルデータが、送信者/送信者の生活圏内にメリットとして還元されるパーソナルデータ流通が必要である。

3. 異種パーソナルデータ利活用における課題

現在のインターネットはサイロ型の構造をとっており、現実の地理空間と対応付いた構造となっていなかったため、異種パーソナルデータ連携に必要な地理範囲内のデータを保有している管理者/送信端末がインターネット上に分散して存在している。故に、現在の異種パーソナルデータ収集は、様々な地理範囲上に存在している、匿名加工されたデータ/パーソナルデータ/パーソナデータへのリンクを、クラウド基盤上に集約する方法で実現されている[11]。このような利活用形態においての課題を、送信者と、事業者/収集者の二者の視点から議論する。

3.1. 送信者側の課題

現在、一つの収集者(クラウド)に対して様々な利活用目的の事業者が情報を取得する形態を取っており、パーソナルデータがどのような用途で使われるのか、不透明である。そのため、送信者が提供する情報が自身に還元されるのかといった判断をするには、送信者は利用する用途、地理範囲、保存時間等を、全て把握する必要があるが、それは送信者にとって容易では無いため要件1を満たすことは難しい。

また、要件2を満たすためには、送信者が主体的にパーソナルデータ利活用を許可する範囲を制御し、自身の生活圏内に還元できることが望ましい。しかし、

現状は収集者/事業者側が提示したプライバシポリシーに同意するか拒否する、という選択しか出来ず、要件 2 を十分に満たしていない。

3.2. 収集者/事業者側の課題

事業者は、収集者が集約する、サービスに利用する、特定の地理範囲内に存在する利活用に合意が取れている異種パーソナルデータを検索し、収集する必要がある。しかし、収集者の元には、様々なデータフォーマット/送信地域/種類 のパーソナルデータや、パーソナルデータ保護や知的財産保護の制約のため、データのリンクが集約される。故に、収集者は全てのデータの粒度や、どの用途の利活用に合意されているかを把握した上でデータを整理することが難しく、集約した全てのパーソナルデータの利活用範囲を把握することは難しい。そのため事業者はデータを取得する際には利用するパーソナルデータの選定に精査をする必要があり、送信者にメリットの高いサービスを提供できず、要件 2 を満たせない恐れがある。

4. 地理に基づくデータ管理アーキテクチャ

3 章で述べた課題の解決のため、送信者は、自身の生活圏内での利活用のみ許可するといった、地理を意識した公開制御が出来ることが望ましい。また、事業者にとっては、収集者が持つデータが、人々の生活圏内の異種パーソナルデータが整理されており、ある程度共通した利用用途に合意されていることが望ましい。

そこで本稿では、[2] で提案した GCN 基盤を用いて、送信者が、地理を意識した公開制御を可能にするデータ管理アーキテクチャを新たに提案する。

4.1. 収集/利活用する地理空間の指定方法

IoT サービスによって、収集したい空間は異なるため、収集対象となる地理範囲を柔軟に指定できることが必要となる。そこで、空間を緯線、経線に基づいてメッシュ状に分割していく、階層構造をもたせて表現する[12][13]。実空間の分割イメージと、九州工業大学付近の各次数のメッシュコードを図 1 に示す。1 次メッシュは 1 辺が 80km 四方の区間であり、2 次メッシュは 1 次メッシュを緯度、経度方向に 8 等分した 64 区間で、10km 四方の空間である。3 次メッシュ以降は、n 次メッシュ ($2 \leq n \leq 9$) を、緯度、経度方向に 2 等分した 4 区間を $(n+1)$ 次メッシュと定義する。分割した空間の識別子は、可変長の 1 次元コード(メッシュコード)を用いて表現し、1 次メッシュでは 4 枠、2 次メッシュでは 1 次メッシュに 2 枠を追加した 6 枠、3 次メッシュ以降では、次数が増加する毎に 1 枠追加され、39m 四方の空間である 10 次メッシュまで定義する。

4.2. 物理位置調和型通信

メッシュコードに基づくネットワークプロトコルを新しく定義することはネットワークを実社会に適応

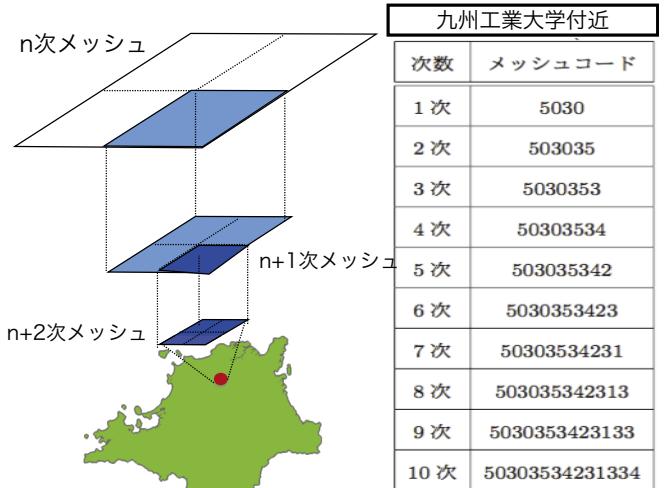


図 1 メッシュコードの構造

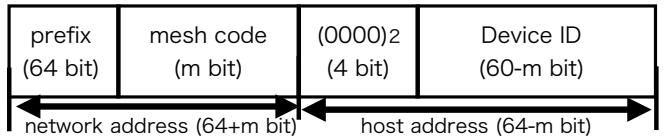


図 2 物理位置調和型 IPv6 アドレス

(グローバルユニキャストアドレス)

するための設置/開発コストが高く、実現性の観点から難しいため、既存のネットワーク基盤上に適応し、物理的な変更を最小限に抑えることが望ましい。

そこで本稿では、既存のネットワーク技術であり、アドレス空間が十分に存在する IPv6 アドレスの一部にメッシュコードを埋め込む形で GCN を実現する物理位置調和型通信技術を活用する[2]。図 2 に、物理位置調和型通信技術に用いる IPv6 アドレスフォーマットを示す。複数の IoT 機器/情報通信端末からの異分野データを収集するため、グローバルユニキャストアドレスを採用している。前半の 64bit は既存の IPv6 グローバルユニキャストアドレスとの重複を避けるため、物理位置調和型通信固有の Prefix を定める。また、メッシュ上の端末を識別するために Device ID を Mesh Code の下位ビットに付与する。また、Mesh Code と Device ID を識別するため、Mesh Code と Device ID の間に 4 ビットのパディングを含める。

Mesh Code と IPv6 サブネットは同様に階層構造を有しているため、地理空間と、ネットワークサブネットを対応付ける事が可能となる。故に、IPv6 の Longest Match アルゴリズムを用いると、次数の高い(地理空間的に狭い)メッシュから次数の低い(地理空間的に広い)メッシュへルーティングすることができ、地理を意識したルーティングが実現される。

これにより、次数の高いメッシュに所属している端末から、次数の低いメッシュに接続されているクラウド上のサーバに向けてデータ送信をする場合、経路上に存在するルータには、地理に基づいてルーティング

されているため、宛先がクラウド上のどのサーバかに関係なく、それぞれのルータの所属しているメッシュ内の全てのデータが自律的に集まる。

4.3. 地理に基づくデータ管理アーキテクチャ

[2] では、実ネットワーク上でどの機器にデータ収集させることができ有効かという点や、パーソナルデータ利用承諾をどのようにして取得するか、といった点については未考慮であった。本項では、GCN 基盤上でデータ管理アーキテクチャを提案し、2.3 節で述べた要件 1, 2 の一部を満足することを目指したデータ管理アーキテクチャを新たに提案する。図 3 に物理位置調和型通信上でのデータ収集アーキテクチャを示す。

データの収集地点は、交換局を想定する。交換局は複数のキャリアの収束点であり、キャリアを跨いだ地理ベースの異種パーソナルデータ収集が可能となる。

データ流通プラットフォーム(収集者)の管理者は人々の生活圏内に密接に関係している区役所や市役所等の自治体が行い、収集範囲は、それぞれの自治体を包含しているメッシュ(1~4 次メッシュ)が望ましい。事業者は、自治体が所属しているメッシュ上に存在し、データ流通プラットフォームの情報を取得する。

IoT 機器/情報通信端末は AP 等の無線環境を想定する。AP が所属するメッシュの範囲は、カバレッジを考慮して 39m 四方の 10 次メッシュを割り当てる。

情報通信端末から送信されるデータは、利活用しても良い異種パーソナルデータ以外にも、連携に必要な無いデータや利活用してほしくないパーソナルデータも送信することが考えられるため、物理位置調和型ネットワークと既存の IPv6 ネットワークの両方に接続されることを想定している、そのため、送信者が送信するデータによって、経由するネットワークを制御する機能が必要となる。この機能は、既存ネットワーク技術である IPv6 ソースアドレスルーティングを用いて、送信データの送信アドレスに物理位置調和型 IP アドレスまたは既存 IP アドレスを指定し、経由するネットワークを選択することで実現される。

提案手法にどのようなメリットがあるのかを、送信者と、事業者/収集者、の二者の視点で述べる。

4.3.1 送信者側のメリット

- ・送信者が公開制御出来る機能

送信データ毎に経由するネットワークを制御する機能を活用することで、送信者は、物理位置調和型通信を利用する際に、データの取得と利活用を許可するメッシュエリアを指定することで、地理的範囲を指定したパーソナルデータの公開制御が可能となる。これにより自身/自身の生活圏内に直接還元されるようなサービスであれば利活用しても良い、といった公開制御が新たに可能となり、要件 2 を満たすことに寄与する。

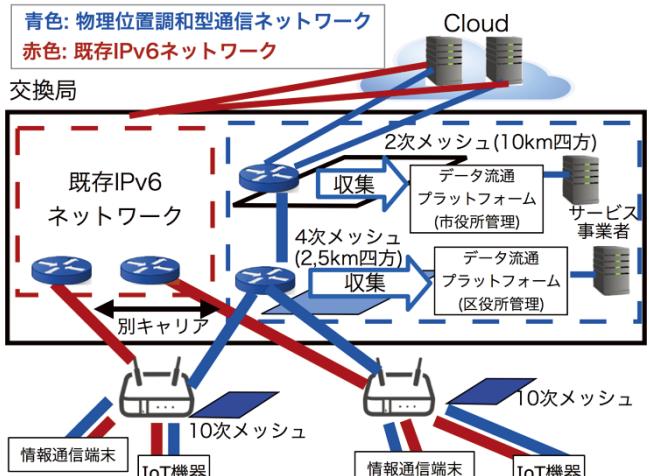


図 3 地理空間に基づく異分野データ管理

アーキテクチャ

- ・利活用用途について把握の容易化

データ流通プラットフォームに収集された異種パーソナルデータは、公開する地理範囲を限定し、送信者/送信者の生活圏内に利益のある用途にのみ用いるため、既存手法と比較して利活用用途の把握が容易となり要件 1 の達成に寄与する。

- ・パーソナルデータ提供への障壁の緩和

自治体は既に、戸籍情報やマイナンバーなどのパーソナルデータを管理しているため、利用者は、パーソナルデータを提供する心理的障壁が低いと考えられ、要件 1 を満たすことに寄与する

4.3.2 事業者/収集者側のメリット

- ・パーソナルデータの合意内容把握の容易化

事業者は、利活用したい地理範囲内の、利活用合意の取れた異種パーソナルデータを収集する必要がある。収集者は、交換局にデータ流通プラットフォームを設置し、メッシュ上のルータを経由するデータを収集することで、交換局を包含するメッシュ上の異分野データの収集が可能となる。また、収集されたパーソナルデータは、収集した地理範囲内に還元される用途での利活用に合意されているため、事業者はパーソナルデータ毎に合意内容を精査する必要がなく、利活用の促進へつながり、要件 2 の達成に寄与する。

4.3.3 定性的評価と課題

表 1 に既存ネットワーク基盤上でのクラウドでのデータ管理と、提案した地理に基づくデータ管理の定性的評価をまとめたものを示す。表 1 より、提案手法の方が既存手法より要件 1, 2 を満たしている項目が多く、異種パーソナルデータ流通に適していると言える。

一方で、要件 2 を十分に満たすには、公開する地理範囲の制御だけでなく、特定の分野/サービスの利活用のみを許可する、といったより詳細な公開制御機能が必要である。しかし、現状提案手法では地理範囲による

公開制御しか出来ないため、提案手法を拡張し、より詳細な公開制御機能を実現する必要がある。

尚、要件 1 を満たすためにはパーソナルデータ保護技術やセキュリティの保証といった点も達成する必要があるが、それらはデータ流通プラットフォーム上の機能とし、本稿の範疇を超えるため議論しない。

表 1 既存手法(既存ネットワーク上でのクラウドによるパーソナルデータ管理)と提案手法(地理に基づいて分割されたパーソナルデータ管理)の定性的評価

要件	評価項目	既存手法	提案手法
1	送信者の利活用用途把握	困難	容易
1	送信者のデータ提供する際の心理的障壁	事業者に依存	低い
2	送信者の地理範囲に基づく公開制御	×	○
2	事業者が取得するパーソナルデータの同意内容把握の容易性	×	○

5. ユースケース

ここで、提案手法を用いたユースケースを紹介する。

5.1. 地域に還元されるデータ利活用

パーソナルデータの収集者(自治体)の元には、地理範囲に基づいて、一定の範囲での利活用許可のされたパーソナルデータが自律的に収集される。自治体は、取得したパーソナルデータを用いて、自治体内に還元される用途のみで許可された、データの粒度の細かい情報を公開することができ、地域のデータ流通の促進につながる。これにより、サービス事業者は、利用用途に応じて、クラウド上に存在する広範囲から収集されたデータの粒度の粗いオープンデータと、粒度の細かい自治体が公開するデータを選択的に指定できる。また、事業者は要求する様々な地理範囲内の匿名加工済データを収集/利活用することが可能となる。これにより、自治体内に存在する様々な課題の分析がより容易となり、送信者は、自身の生活圏内のデータを用いたサービスを享受でき、生活の質の向上につながる。

5.2. 個人に還元されるデータ利活用

提案手法は、送信者が主体的に連携させるパーソナルデータを指定できるため、情報銀行のようなパーソナルデータの今までの流通にも有効だと考えられる。連携情報銀行をどの機関が担うかについては、自治体による管理を進めることを提案する。自治体は現状で既にマイナンバーや戸籍情報等の個人情報を取り扱っていることから、パーソナルデータの委託に関する障壁が薄いと考えられる。また、自治体側も、パーソナルデータのままの利活用による市民の生活品質の向上

に寄与することができるメリットがある。また、自身の生活圏内のみを利活用の対象に指定できるためユーザの合意が得られやすい。パーソナルデータ流通が自治体内で活発になることにより、データ提供者のリアルタイムなニーズに沿った新たなサービスが誕生すると考えられる。

6. まとめと今後の検討

本研究ではパーソナルデータを含む異分野データ連携を行う IoT サービスにおいての課題である、データ収集、データ流通の解決のために、地理に基づいたデータ管理アーキテクチャを提案し、その有効性について定性的に評価を行い、ユースケースを示した。

今後は、地域ごとに存在する特有課題(ニーズ)がどういったものなのか調査し、判明した課題の解決に対しての、GCN 基盤や提案手法の有効性を実証実験等を通して行い、解決できない機能については研究開発を行う。また、GCN の定量的評価のために収集するデータの価値や、流出される個人情報の定量化を行う。

謝 辞

本研究は JSPS 科研費 JP18H03234、及び公益財団法人電気通信普及財団 研究調査助成を受けたものです。

文 献

- [1] スマート IoT 推進フォーラム異分野連携プロジェクト，“異分野データ連携 H28 年度技術報告書～データでつなぐ人・モノ・コト～スマート IoT 推進フォーラム異分野データ連携プロジェクト”，2017 年 3 月。
- [2] 永田晃,中村勝一他,”物理位置調和型アドレスに基づく Geo-Centric Networking の検討”2018 年電子情報通信学会総合大会,pp.51,B-6-51,2018 年 3 月。
- [3] 個人情報保護委員会, “個人情報の保護に関する法律(平成 15 年法律第 57 号)”, 2017 年 6 月。
- [4] The European parliament and of the council, “General Data Protection Regulation : GDPR”, 2016 年 4 月。
- [5] “London Datastore”. <https://data.london.gov.uk/>
- [6] “Keeping London moving - Transport for London”. <https://tfl.gov.uk/>
- [7] N. Li, T. Li, and S. Venkatasubramanian, “t-closeness: Privacy beyond k-anonymity and l-diversity,” in ICDE, pp. 106–115, April 2007
- [8] X.Xiao and Y.Tao, “Personalized privacy preservation,” Proc. ACM SIGMOD, pp. 229–240, June 2006.
- [9] M.H. Afifi, Kai Zhou, “Privacy Characterization and Quantification in Data Publishing” IEEE Transactions on Knowledge and Data Engineering pp.(99):1-1 , January 2018.
- [10] 総務省, “データ流通・利活用における課題” 平成 29 年度情報通信白書, 第 2 章, 第 2 節, pp. 63–88, 2017 年 7 月。
- [11] “ G 空間情報センター ” . https://www.geospatial.jp/gp_front/.
- [12] 行政管理庁告示第 143 号(総務省統計局統計センター), “統計に用いる標準地域メッシュおよび標準地域メッシュコード” 1973 年 7 月。
- [13](株)NTT ドコモ,「オープン i エリア 説明書 第 5.7 版」, 2012 年 4 月。