情報処理学会論文誌 Vol.59 No.12 2180–2190 (Dec. 2018)

地産地消型アーキテクチャによるセンサネットワークデータのプライバシ保護

干川 尚人[1,a)] 下馬場 朋禄[2] 伊藤 智義[2]

受付日 2018年3月12日, 採録日 2018年9月7日

概要：近年，カメラに代表されるネットワーク接続センサの増加と，顔認識などのデータ解析技術の発展によって，広域をサポートするセンサネットワークを介して，物理空間の人や物も，サイバー空間の情報として利用が可能になりつつある．これらは広い物理空間における人間の作業を代替する，将来の労働力不足を緩和する技術としても期待できるが，その一方で，センシングされる身の回りの情報も増加するため，プライバシデータに対する脅威も増している．センサデータを処理する主なネットワーク上のコンピューティングモデルとして，クラウドコンピューティングによる IoT プラットフォームがあるが，これは目的にかかわらず，まずデータを集約する垂直統合アーキテクチャであり，広域に点在する多数のセンサからデータを得るときに，本来の目的にかかわらない大量のプライバシデータも収集される問題がある．そこで我々は被センシング対象者とそれをとらえるセンサの位置に相関性があることに着目し，被センシング対象者の近傍にあるセンサデータのみ集約し，その場でデータ処理することで，アプリケーションの目的に関係ないデータ集約を不要にする，地産地消型アーキテクチャを提案する．また，本アーキテクチャとクラウドコンピューテイングを比較するために不要なプライバシデータの流通比を評価するための式を示し，あわせて近年研究開発が進んでいる分散アプローチのエッジコンピューティングとも比較を行う．そして，これらの結果から，提案アーキテクチャが広域なセンサネットワークデータのプライバシ保護に有用な手法であることを示す．

キーワード：プライバシ，センサネットワーク，エッジコンピューティング，Internet of Things（IoT）

Privacy Information Protection of Sensor Network Data by Local Production for Local Consumption Type Architecture

Naoto Hoshikawa[1,a)] Tomoyoshi Shimobaba[2] Tomoyoshi Ito[2]

Received: March 12, 2018, Accepted: September 7, 2018

Abstract: In recent years, person and things in physical space can also be searched as information on cyber space via a wide range of sensor networks, with the increase of network connection sensors typified by cameras and the development of data analysis technology such as face recognition. These technologies can be expected to alleviate future labor shortages by replacing human work in a wide physical space. Meanwhile, as personal information acquired by sensors also increases, the threat to our privacy data also increases. There are IoT platforms based on cloud computing as a major computing model on networks which processes sensor data. However, this model is a vertically integrated architecture that aggregates data regardless of the purpose. In addition, a large amount of privacy data irrelevant to the original purpose is also collected in the case of acquiring data from a large number of widely scattered sensors. We focus on the correlation between the target to be sensed and the position of the sensor capturing. Our research proposes an architecture type of local production for local consumption which integrates only the sensor data in the vicinity of the subject to be sensed and performs data processing on the spot so that data aggregation and distribution irrelevant to the purpose of the application are made unnecessary. Furthermore, to compare the proposed architecture with the prior art, we show the formula for evaluating these transmission rates of the unnecessary privacy data for service provider. In addition, we compare it with the edge computing of the distributed approach, which has recently advanced research and development. From these results, we show that the proposed architecture is a useful method for privacy protection of wide area sensor network data.

Keywords: privacy, sensor network, edge computing, Internet of Things (IoT)

1. はじめに

近年，センサやアクチュエータを搭載した電子機器をインターネットに接続可能にする，いわゆる Internet of Things（IoT）化が進展しているが，とりわけネットワークカメラ機器の普及はめざましく，世界での普及台数は 2018 年には 2,600 万台となり，アナログ型カメラを上回ると予測されている [1]．あわせて，画像データの解析や機械学習処理に適した PaaS（Platform as a Service）クラウドも発展してきており [2]，カメラによる人や物の認知に必要な特徴量による分類 [3] と物理世界に点在するネットワークカメラ機器を組み合わせることで，広域にわたってローカル性の高い対象の追跡が可能になる．このカメラなどの認知対象をより個人や地域コミュニティに適用できれば，少子高齢化・労働力不足が進む今後の社会における，地域コミュニティの見守り，監視・防犯の自動化・省力化などに役立てることが期待できる．

しかし，クラウド上のサーバへ情報集約を行うシステムでは，情報の利用目的にかかわらず認識に必要なプライバシ情報を預ける必要がある．加えて，センサから取得されるデータに認識対象以外の情報も含まれていても区別せずに集約されてしまうため，サービス利用者，非利用者にかかわらずプライバシデータがオンライン上に流通してしまう．これはサービス事業者にとっても，管理に必要な情報が増えるため，運営コストや漏洩時の補償コストのリスクが増加する課題となる．

そこで，本研究はセンサネットワークの生成データを利用した追跡アプリケーションにおいて，追跡対象者とともにデータ処理を行う計算ノードを移動させ，発生データの集約と処理をつねにその場で行うことでプライバシデータを保護する地産地消（Local production for local consumption：以下，LPLC）型アーキテクチャを提案する．2 章では既存技術の問題点を示し，3 章では本提案方式およびシステム構成を示す．4 章で提案方式の評価を行い，5 章で実用化に向けた検討を議論し，関連研究を示す．

2. 従来技術の課題

本研究の目的は広域に配置されたセンサ機器を活用した追跡アプリケーションにおけるプライバシデータの保護であるが，ここであげる追跡アプリケーションとは，多地点に配置したセンサ群から取得した情報を使い，特定の人物や物を追いかけるアプリケーションを指す [4], [5]．このような追跡アプリケーションとして，クラウド上のサーバへ

1 国立高等専門学校機構小山工業高等専門学校
National Institute of Technology, Oyama College, Oyama, Tochigi 323–0806, Japan
2 千葉大学
Chiba University, Chiba 263–8522, Japan
a) hoshikawa.naoto@oyama-ct.ac.jp

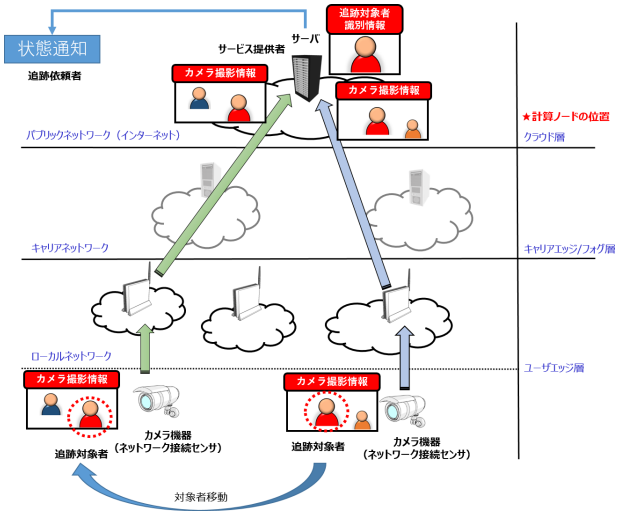

図 1 追跡アプリケーションの概要（クラウド）
Fig. 1 Overview of tracking application on cloud computing.

カメラ画像データを集約するモデルの概要を**図 1** に示す．また，追跡アプリケーションによって提供されるサービス要件を以下の項目として定義する．

- 追跡依頼者はパブリックネットワーク上にあるサービス提供者を介して追跡対象者の正常，異常などの状態通知を受け取ることができる．
- サービス提供者は地域内に分散配置された追跡に必要なセンシングを実行するためのネットワーク接続センサを利用可能とする．
- サービス提供者はセンサで取得した情報を解析処理することで，追跡対象者の状態を把握することができる．
- 追跡対象者は地域内を自由に移動できる．

このような追跡アプリケーションは，少子高齢化・労働力不足を迎える社会にとって特に有望である．たとえば，高齢者の健康寿命を延ばすために積極的な外出が推奨される [6] が，その介護サポートを広域にわたって移動する高齢者に合わせて実施することは大きな社会負担になる．そこで，ネットワークカメラと近年発展の著しい深層学習などを用いた画像認識技術 [3], [7], [8] を活用することで，本人の身体状況に合わせた見守りサービスの実現が期待できる．なお，このようなアプリケーションの対象は高齢者に限定されたものではなく，子供の登下校などの見守りや，外出している従業員の状態確認，マラソン大会の参加選手の個人識別のような，広い空間にわたる認知作業全般に適用できる．

しかし，追跡アプリケーションで扱うことになる，個人の特定性が高い情報を活用したサービスについては，利用者の不安感も大きい．総務省の調査ではクラウドサービスに対し消費者がプライバシデータを提供することについて，およそ 8 割が不安感を抱いており，特に顔画像などの生体情報はクレジットカード番号などの口座情報や公的な識別番号に次いで，不安を感じる項目としてあげられている [9]．

センサの中でも特にカメラから生成される画像情報は多数の画素や色の多次元情報を有しており，1 枚の画像からでも大量のプライバシ情報を得ることができる．加えて，カメラ画像には追跡対象者以外の人や物も写る可能性もある．このような大量のプライバシ情報を含むデータを従来のクラウドサービスのようなアプローチ同様に集約していくことは，被撮影者の不安感だけでなく，サービス提供事業者にとっても情報保護のリスク要因が増加する．

データのプライバシ保護に関する過去の研究では，カメラ撮影されたデータそのものに情報処理を施すアプローチが行われおり，サーバ側で撮影画像の一部情報を加工処理し，権限に応じて表示を可能とする手法が取り組まれている [10], [11], [12]．また，これらの表示権限は撮影を行う側のものであったため，被撮影者が監視カメラシステムに対して顔情報の秘匿有無を指示できる仕組みも提案されている [13]．しかしながら，以上の先行研究はいずれも被撮影者の情報秘匿処理を行う主体はデータを集約するサーバであるため，目的とするサービスに不要な情報も含めて蓄積され，被撮影者にとって，データ流通範囲の制御は実現しておらず，データをサービス側へ預けることの不安感は払拭できない．

これらの問題は，従来の技術がすべてのデータ処理をインターネットのようなパブリックネットワーク上のサーバに集約して行う前提としていることに起因する．しかし，送信されるすべてのデータは目的とするアプリケーション実行に必要なものばかりではない．追跡アプリケーションならば，追跡対象者とはかかわりない人や物の情報は不要である．また，その追跡対象者の情報であっても，目的にかかわらないデータは送信しない方がよい．仮に将来，クラウド集約によって有用なアプリケーションが実現した場合に，利用者がそのプライバシデータ提供を許容し，サービス提供事業者が収集データの目的外利用をしないと宣言しても，利用者と無関係な人間の情報が勝手に収集される前提では，その社会実装には理解が得られないかもしれない．

これらの課題を解決するためには，いったんすべてをまとめるのではなく，データ発生源からボトムアップ的にデータ加工をしていく仕組みが必要である．データ発生源に近い点で処理するアプローチとして，フォグ/エッジコンピューティングと呼ばれる分散コンピューティングのモデルも提案されている [14], [15], [16]．このモデルはクラウドコンピューティングと比べたとき応答遅延が小さいことが主な特徴として着目されているが，加えてインターネットのような広域ネットワークへ接続する手前でデータ処理を行う特性から，プライバシデータの制御でもメリットがあげられている．エッジコンピューティングにおける追跡アプリケーションの概要を**図 2** に示す．図 1 のクラウドと異なる点は，計算ノードの位置がキャリアエッジ/フォグ層以

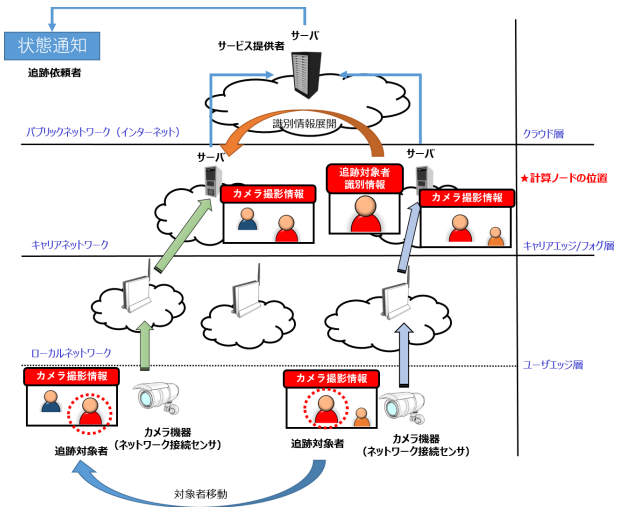

図 2　追跡アプリケーションの概要（エッジ）
Fig. 2　Overview of tracking application on edge computing.

下に配置されることである．このため，クラウド層に配置されたサーバの場合，ネットワーク接続センサが場所によらずすべて同一のサーバに接続されるのに対し，エッジ層のサーバはセンサに応じて接続サーバが分割されるため，クラウドサーバのようにデータがすべて集約することはない．しかし，特定のエッジサーバに接続可能なネットワーク接続センサは，そのセンサが接続するネットワークアクセスポイントに依存するため，追跡対象者が移動して異なる計算ノード（エッジサーバ）に接続されているセンサを活用するためには，追跡アプリケーションの解析に必要なプライバシ情報を含んだテンプレートデータ（以下，プライバシテンプレート）もその計算ノードへ展開する必要性が生じる．このようなテンプレートデータは，たとえば個人を識別するための学習済みデータのようなきわめてプライバシ性が高い情報であり，そのデータ複製には細心の注意を払う必要がある．しかし，追跡アプリケーションはその性質上，追跡対象者が自由に移動するため，その可能性のある範囲にはプライバシテンプレートを配布しなければならない．プライバシデータのトレーサビリティ確保は重要な課題で，近年では個人データ流通に関する法整備も各国で進んでいる．たとえば欧州連合（EU）では一般データ保護規則（General Data Protection Regulation：GDPR）が施行されており，提供した個人データの削除権などが明文化されている [17]．したがってデータをエッジで処理するアプローチを利用するならば拡散するテンプレートデータの管理が課題となる．

また，前述のプライバシデータの保存場所に関する法規制は国，地域を越えたプライバシデータの保存，流通についても言及されている．このような法規制は日本を始めとして世界各国で進んでおり，センサネットワークから収集したデータを無制限にクラウド上のサーバで処理している場合に規制の対象になる可能性がある．したがって，デー

タを生成する地域とその蓄積先を考慮可能なアーキテクチャを選択する必要がある．

3. LPLC アーキテクチャ

3.1 動的なセンサ選択手法

既存のクラウド技術では，最初にデータを集約してから分析する仕組みであるため，その必要有無にかかわらずプライバシデータが無秩序に集約されることは避けられない．またエッジ技術では，分析のためにデータを集めるエッジノードに対してプライバシテンプレートを配布する必要があり，サポート範囲に対するエッジノードの密度に応じてプライバシデータが拡散する．これらの問題は，アプリケーションにとって追跡対象者がどう移動するか不明であることに起因しており，仮に移動経路が完全に推測できれば「選択的にデータを集める」または「必要最低限のノードへテンプレートを配布する」という解決も可能であるが，これは追跡アプリケーションの目的上難しい．

本研究では，このような追跡アプリケーションにおいて，目的に必要なセンサの選択および無関係なデータの判断と処理をデータ発生源の近傍ですべて行う仕組みを提案する．**図 3** の概要に示すとおり，まず追跡対象者とそれをとらえるセンサは近傍にあると仮定し，その切替えは追跡対象者の携帯する計算ノードがセンサ収容ネットワークの無線アクセス接続可否によって行う．この実現にあたり，追跡対象者とこれをとらえるセンサの位置に相関性があることに着目した．まず，センサはそのセンシングに有効な範囲があるので，ここで追跡対象者をセンシング可能なセンサは追跡対象者と物理的にも近い位置に配置されていると考える．また，センサの有効範囲を内包する接続範囲を持つ無線アクセスポイントを有するローカルネットワークがあるとき，この無線アクセスポイントへ接続可能な機器も物理的に近い位置にあると見なす．ここで，追跡対象者に無線アクセスポイント接続機能を有する計算ノード（たとえばスマートフォンなど）を携帯させ，これに接続可能なローカルネットワーク上のセンサデータを収集する．これにより，必要最小限のセンサを動的に選択する仕組みを実現できる．

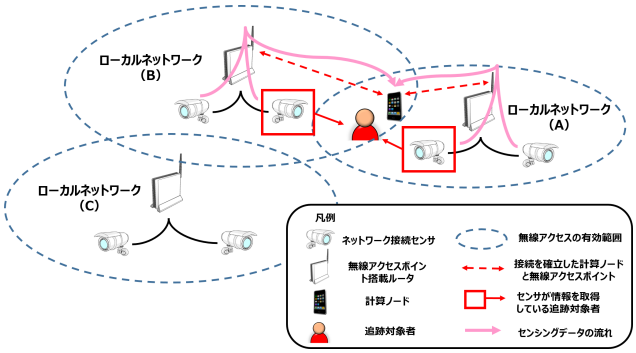

図 3　追跡対象者とローカルネットワークの相関性
Fig. 3　Correlation between tracked person and local network.

3.2 提案システムによる課題解決手法

2 章に示した課題は以下の 3 つの要件を満たすことで解決できる．

(1) センサデータの加工と識別をローカルネットワーク内で実行すること
(2) センサデータの加工と識別を行う計算ノードを 1 カ所に集約すること
(3) センサデータの発生地域内でデータ処理をすること

図 4 に追跡アプリケーションにおける提案システムの概要を示す．追跡対象者が帯同する計算ノード（サーバ）は，その移動に応じて各々のローカルネットワークに動的に接続し，センサデータ（カメラ撮影情報）を取得する．また，ネットワーク接続センサ（カメラ機器）を収容するローカルネットワークは孤立しており，計算ノード以外とは通信しないため，生成されたプライバシデータは個々のローカルネットワーク以外には流通しない．加えて，追跡アプリケーションに必要な識別，データ加工処理はこの計算ノードで行われるため，要件 (1) を満たす．また，追跡対象者が移動し，これを捕捉するセンサ（カメラ機器）が変更される場合，プライバシテンプレートデータを有する計算ノードもまた，センサと同じローカルネットワークに接続され，つねに同一の計算ノードにデータが集約されることになるので，要件 (2) を満たす．最後に，この計算ノードはつねにユーザエッジ層に位置するので，要件 (3) も満たす．

3.3 LPLC アーキテクチャの構成

LPLC アーキテクチャのモデルを**図 5** に示す．まず計算ノードである LPLC ノードが接続する 2 種のネットワークとして，地域に分散配置されているセンサ機器を収容する多数のローカルネットワークとサービス提供者へ追跡対象者の状態解析結果を通知するためのパブリックネットワークを定義する．ローカルネットワークは，センサ機

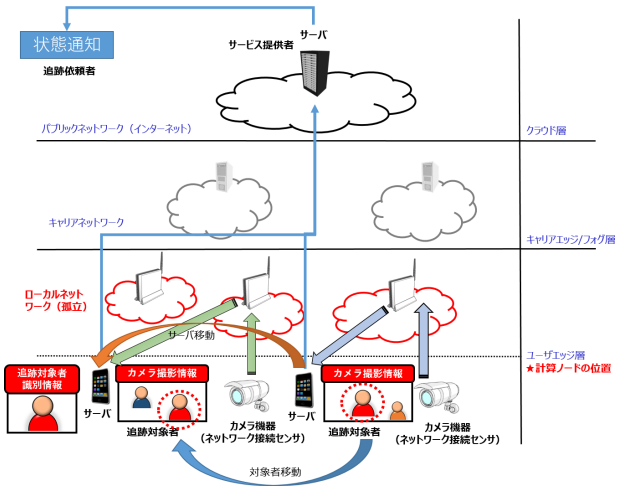

図 4　提案システムの概要
Fig. 4　Overview of tracking application on proposal system.

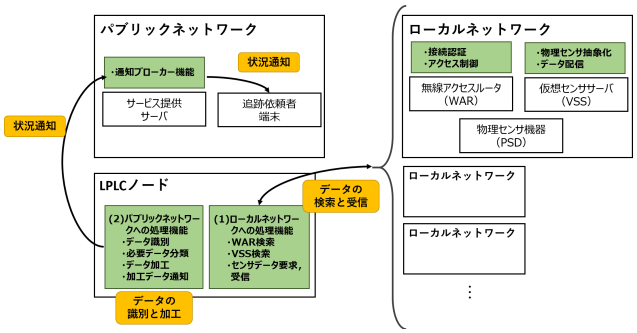

図 5 LPLC アーキテクチャモデル
Fig. 5 Model of the LPLC architecture.

器を収容する無線アクセスポイント搭載ルータ（Wireless access router：以下 WAR），同ローカルネットワーク内のセンサが取得したデータを配信する仮想センササーバ（Virtual sensor server：以下 VSS），および物理的なセンサ機器（Physical sensor device：以下 PSD）から構成される．パブリックネットワークにはサービス提供サーバを配置し，LPLC とつねに通信可能な状態とする．追跡依頼者端末はサービス提供サーバを経由して，LPLC から送信された状況通知を受信できる．

具体的に顔認識を利用した見守りサービスを例に当てはめると，ローカルネットワーク群は一定の区域ごとに監視カメラを収容している無線アクセスポイントを有する Local Area Network（LAN）の集合，パブリックネットワークはインターネット，そしてサービス提供サーバが見守りサービス提供事業者の情報通知サーバであり，見守り通知を依頼したユーザの有する情報端末が追跡依頼者端末になる．このとき，LPLC ノードは見守り対象者の識別情報である顔認識モデルを組み込んだ無線アクセス機能付きの携帯型サーバである．以降，機能ブロックごとの処理ステップを示す．

(1) **LPLC ノードのローカルネットワークへの処理**

これは追跡対象者の帯同する LPLC ノードが，近傍にあるローカルネットワーク内のセンサから，センサが取得しているデータを収集するフェーズである．まず，LPLC ノードは自分の位置からアクセス可能なローカルネットワークを提供する WAR を探索，接続し，認証を試みる．WAR はあらかじめ認証済みの LPLC ノードに対して，VSS および PSD を収容するローカルネットワークに限定したアクセスを許可する．その後，LPLC ノードはローカルネットワーク内にある VSS を検索し，センサデータの配信を要求する．VSS はセンサ機器を抽象化する仮想的なセンサデバイスとして振る舞い，センサの生成するリアルタイムデータをキャッシュし，LPLC ノードの要求に応じて配信する．

(2) **LPLC ノードのパブリックネットワークへの処理**

LPLC ノードは VSS から受信したセンシングデータをプライバシテンプレートに基づき解析し，識別処理を行う．このときの処理結果に応じて加工されたデータを，サービス提供サーバへ送信する．この通知情報の内容や頻度はサービス内容に依存し，具体的な例として定期的な正常状態通知のほか，異常検知時の緊急通知などが考えられる．なお，この識別の結果，サービスに不要なデータは破棄されるため，無関係なプライバシ情報はクラウド上に流通しない．

3.4 提案アーキテクチャの実装要件

本節では提案アーキテクチャの処理が成立するために実装で必要な基本要件について説明する．なお，セキュリティ要件，構成技術および実現に向けた課題は 5 章で述べる．

通信アクセス機能の要件

LPLC ノードが通信を行うパブリックネットワーク上のサービス提供サーバと，WAR，VSS，PSD からなるローカルネットワークのセットはそれぞれ異なる物理ネットワーク上に存在する必要がある．サービス提供サーバは LPLC ノードの物理位置によらずに通信可能なネットワーク上に存在することが要件となり，たとえばサービス提供サーバがインターネット上のアプリケーションサーバとして実装されているならば，LPLC ノードはオンラインへアクセス可能なモバイル通信機能を具備していればよい．また，各ローカルネットワークの WAR と LPLC ノードの通信は，LPLC ノードの物理位置が WAR の近傍か否かで接続・切断を行う必要があるので，前述のパブリックネットワークとは独立した専用の無線通信インタフェースを具備することが要件になる．このとき WAR は LPLC ノード以外との通信を行っても構わないが，LPLC ノードへのセンサデータ提供に関しては専用の無線通信インタフェースを非経由の場合，許可してはならない．また LPLC ノードが各 WAR に対して接続可能な無線通信機能を具備しているならば，その通信規格は 1 つに限定しなくてもよい．ただし，LPLC ノードは同時に複数のローカルネットワークの有効範囲に入る場合もありうるので，同一のインタフェースで異なるネットワークと並行して通信できる要件も求められる．そのような要件は無線通信の利用方法として一般的ではなく，標準の機能として備わっていないため，これを新たに実装する必要がある．この無線通信機能は，データ転送帯域がある程度保証され，コンシューマ向けルータやスマートフォン，シングルボードコンピュータなどの多くの小型ディジタル機器が備えている Wi-Fi 規格（IEEE802.11）インタフェースが有力だと考える．

センサデータを取得できる機器設置の要件

追跡対象者をとらえるセンサがあったとき，追跡対象者の帯同する LPLC ノードがそのセンサデータを取得するための要件として，LPLC ノードと WAR 間の無線通信範

囲は属するローカルネットワーク上の PSD が備えるセンシング有効範囲より広い必要がある．この範囲条件はセンサの種類によって大きく変わってくるが，たとえば IP カメラによる画像データを解析するような用途であれば，カメラ設置位置から追跡対象者を撮像可能な距離が必要なので，数メートルのオフセット距離があればよい．

各機能における計算機リソースの要件

LPLC ノードの処理は図 5 の (1) ローカルネットワークへの処理機能，(2) パブリックネットワークへの処理機能で示されるように 2 種類に大別される．(1) ではつねに利用可能なローカルネットワークのアクセスポイントを探索し，利用可能ならば接続してセンサデータを取得する能力を備えることが要件となる．(2) では，テンプレートデータに基づき取得したデータを解析・分類処理し，結果に応じてサービス提供者の受け入れフォーマットに合わせたデータ加工を行い，データを送信する能力を備えることが要件となる．特に (2) は解析・分類処理する内容に応じて必要な計算機リソースは大きく変動する．たとえば取得した追跡対象者の撮影画像データから，顔認識技術を用いて追跡対象者の識別やその健康状態を把握するような解析処理を行う場合は大きな演算能力が必要になる．また，LPLC ノードは携帯性が求められるため，そのハードウェアには追跡時間内に動作が可能なバッテリ機能を備える必要がある．これはスマートフォンなどの携帯デバイスの利用が考えられるが，その実現性についての考察は 5.3 節で後述する．

各ローカルネットワークにおける通信負荷は一般的なマス用途を超えることはないと考えられるので，WAR が備える無線アクセスインタフェース機能，ルーティング機能は，市販のルータ製品を利用できる．VSS の実現には PSD から取得する機器ごとに規格が異なるセンサデータを抽象化し，LPLC ノードの要求に対して配信可能なサーバ機能を実装すること，そしてその処理を実行可能な性能を有したハードウェアを備えることが要件になる．ただしその処理内容の多くはデータの転送であるので，PC やスマートフォンのような高い演算能力は不要で，サイネージ向けの小型コンピュータや IoT 向けのシングルボードコンピュータなどの演算能力でも要件は満たすことはできるだろう．ただし，地産地消のデータ流通を行うために，この計算機リソースはローカルネットワークごとに配備する必要がある．

サービス提供サーバは LPLC ノードから加工済みのデータが含まれたクエリを受け取り，その内容を分析して追跡依頼者端末へ状況通知を行う機能の実装が必要である．なお，これは一般的なオンライン上のアプリケーションサービスと大きな違いはない．

4. 提案アーキテクチャの評価

追跡アプリケーションを実行するうえで，「サービス利用にかかわらない追跡の非対象者のプライバシデータ（不要なデータ）を集めないこと」，「追跡対象者のプライバシテンプレートデータの展開先は必要最小限であること」，「データ生成域内でデータ処理されること」を評価するために，プライバシデータの管理にかかわる下記の 3 観点で検討を行った．

(1) サービス提供者への不要なデータ流通比率
(2) テンプレートデータの拡散性
(3) データの域内処理可否

比較する追跡アプリケーションは「物理空間に設置された複数の監視カメラを使い，画像から追跡対象者の状態を解析して依頼者へ通知する」ことをユースケースとして設定する．たとえば 2 km 四方程度の範囲ならば，通学路における小学生の見守りなどに適用できるし，10 km 四方ならばマラソン大会のコース範囲をサポートできる．このようなユースケースにおける主要なセンサは監視カメラであるため，以後の評価においてはセンサをカメラと呼ぶ．また，比較するアーキテクチャとして，それぞれ図 4，図 1，図 2 に該当する次の 3 モデルをあげる．

提案モデル

提案モデルにおける計算ノードは追跡対象者が帯同する 1 台であり，プライバシテンプレートデータを保持し，これを用いて収集するすべてのセンサデータを処理する．また，1 つのローカルネットワークに属するカメラが追跡対象者をセンシングの有効範囲に納めているとき，そのローカルネットワークの WAR に対して計算ノードが必ず接続可能とする．本モデルによれば，センサから収集したデータはサービス提供者へ送信される前に処理されるため，不要なデータは流通しない．また，プライバシテンプレートの拡散性については，1 つに集約されるため，最小である．最後に，データの域内処理については，データ発生源の物理的近傍で処理されるので，問題にならない．

クラウドモデル

クラウド層に計算ノードを配置した場合をクラウドモデルとする．これはサービス提供者と同レイヤのインターネットのようなアクセスに地域制約のないパブリックネットワーク上にある 1 つの計算ノードであり，プライバシテンプレートデータを保持し，これを用いて収集するすべてのセンサデータを処理する．また，追跡対象者の位置によらず，常時すべてのカメラをサポートできる．この計算ノードはクラウドサーバ上にカメラデータを集約し，データ解析処理を行う PaaS サービスなどで構成したサーバを想定している．なお，テンプレートデータは 1 カ所に集約されるため，その拡散性の観点では提案モデルと同様である．

エッジモデル

キャリアもしくはユーザのエッジ層に計算ノードを配置した場合をエッジモデルとする．各エッジは計算ノードご

とにプライバシテンプレートデータを保持し，計算ノードのサポートするカメラ群が収集するセンサデータを処理する．このとき追跡対象者の行動範囲をサポートするエッジ計算ノードすべてにプライバシテンプレートデータを配置しなければならない．なお，データはサービス提供者へ送信される前に処理されるため，不要なデータ流通比率の観点は，提案モデルと同様である．また，データの域内処理に関しては，上述のとおり現在示されている妥当なエッジモデルならば同国（地域内）で完結するため問題にならない．

4.1 サービス提供者への不要なデータ流通比率

提案モデルおよびエッジモデルと比較したとき，クラウドモデルではアプリケーションサービスを利用する人間（追跡対象者）と目的に無関係な人間（非対象者）のデータ流通が発生する．ここでは無関係なデータがどの程度サービス提供者へ流通しているかを定量評価するために，不要なデータ流通比率としてモデル化する．

まず，全プライバシデータ流通量ならびに不要プライバシデータ流通量比を定義する．アプリ有効範囲を長方形で内包し，それを $x \times x$ の正方形のセルを敷き詰め内包する．セルは縦横に n 個 $\times$ m 個配置し，セルの境目は考えない．セルの持つ追跡対象者，非対象者，センサの有無といった情報を行列に対応させモデル化する．各セルに追跡対象者 h_n がいる全期間を対応させ，行列 H_n とし，その総和（$H_1 + H_2 + \cdots$）を H 行列と呼ぶ．同様に非対象者 a_n につき行列 A_n を用意し，その総和（$A_1 + A_2 + \cdots$）を S 行列と呼ぶ．各セルにその内部を網羅するセンサ数を対応させ，この行列を C 行列とする．以上より不要プライバシデータ流通比は以下の式になる．

$$\frac{\sum_{i=1}^{n}\sum_{j=1}^{m}(C_{ij}S_{ij})}{\sum_{i=1}^{n}\sum_{j=1}^{m}(C_{ij}S_{ij}) + \sum_{i=1}^{n}\sum_{j=1}^{m}(C_{ij}H_{ij})} \qquad (1)$$

ここで分子は不要データ流通量，分母は不要データ量と追跡対象者をとらえたデータ量の和である．

この定量評価を行うため，不要なデータの流出性が問題になるクラウドモデルにおいて，約 60 m の行程からなる「公園から学校までの児童見守りモデル」について栃木県小山市内の実際の地図をもとにモデル化し，シミュレーションを行った（**図 6**）．このモデルではマップ上のすべての人の歩行速度を 1.25 [m/sec]，1 つのセンサがデータを生成する周期（カメラのフレームレート）を 1 [fps]，セル 1 辺を 1.25 [m] とした．また，追跡対象者は赤線に示す固定のルートを，非対象者は青矢印に示す 15 カ所の流入口からランダムに 1 つ選びそこからのルートを立ち止まることなくランダムウォークする．なお，センサはすべての交差点に設置し，時刻 t の時点でセンサ有効範囲内に存在する歩行者はフレームレートに応じたデータを取得され，サービス

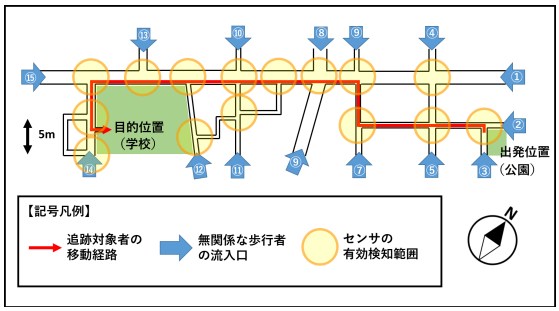

図 6 公園から学校までの児童見守りモデル
Fig. 6 Model of surveillance for children from park to school.

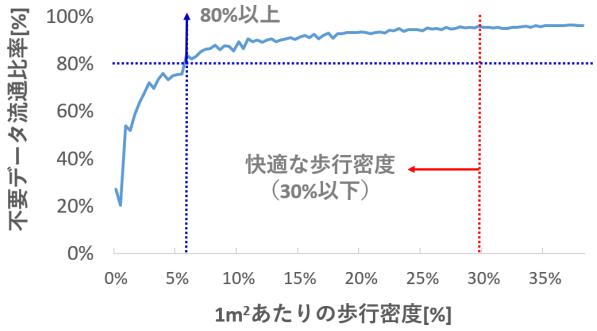

図 7 不要プライバシデータ流通比率
Fig. 7 Unnecessary privacy data transmission rate.

提供者へ転送される．また，データを収集する時間は追跡対象者が移動完了する時間として，60 [秒] としている．以上の条件から非対象者の作る行列 A_n をランダムに生成し，不要なデータ流通比を算出するシミュレーションを一試行あたりの人流量を 1 から 100 までの範囲で増加させて実行した．その結果を**図 7** に示す．なお，歩行量の指標で一般的な歩行密度を設定するため，横軸はシミュレータ上の歩行路総面積 262.5 m^2 を人流量で割った比率を置いている．

4.2 テンプレートデータの拡散性

提案モデルおよびクラウドモデルと比較したとき，多数の計算ノードを利用する可能性があるエッジモデルではテンプレートデータの拡散性が問題になる．このとき，テンプレートデータ配布の必要性が生じるノード数は追跡対象者の行動範囲と，その範囲内にあるエッジ計算ノードの集積率に依存する．そこで，追跡対象者のある行動範囲において，エッジ計算ノードの種類に応じてどの程度テンプレートデータが拡散するか比較評価する．

エッジコンピューティングは計算ノードの配置点についても，通信キャリアの設備や，Wi-Fi アクセスポイントや IoT ゲートウェイのようなユーザ寄り設備といった，様々な提案がなされている [18] ため，明確に 1 つのモデル設定を置くことは難しいが，ここでは現実の公開設備データをもとに，東京都千代田区（面積 11.66 km^2）におけるエッジ計算ノードの台数を下記に示す 3 種のエッジノードで分類・定義し，それぞれの値を推定する．

(1) 固定キャリアネットワークに収容
(2) 移動体キャリアネットワークに収容
(3) ホットスポット規模のネットワークに収容

まず，(1) は東京都千代田区内でサービスを提供している固定キャリア事業者に，1 つの局ビルに 1 つのエッジノードが収容されると仮定し，千代田区の局ビル数を算出した [19]．(2) は第 5 世代移動通信システム（5G）において実用化検討が進んでいる Multi-access Edge Computing（MEC）モデルをあげる [20]．この計算ノードは移動通信キャリアの設備である屋外型無線基地局（eNodeB）に配置される想定であるため，都市部の場合は 1 km^2 あたり 30 局配置されることから [21]，これを千代田区の面積を掛けて算出した．(3) のホットスポット規模には Wi-Fi ネットワーク程度の範囲をサポートする仕組みとして提案された Cloudlet モデル [16] のエッジを想定する．その台数は Wi-Fi ホットスポットサービスを提供する事業者が千代田区内に提供するスポット数から算出した [22]．以上のデータをグラフ化したものが**図 8** である．

4.3 既存技術との比較

以上の結果をもとに**表 1** で既存技術との比較を定性評価した結果を示す．まずクラウドモデルの短所である不要なデータの流出比は歩行密度が増加するに従い増加していることが分かる．1 m^2 あたりの快適な歩行密度は 30%以下であるといわれているが [23]，これに対し，シミュレーションモデルでは 6%を超えた時点ですでに不要なデータが 80%以上を占めている．これは，追跡対象者が移動を完了するわずかな時間（1 分）に限定してセンサを動作させたとしても，送信される大半の情報が無関係な情報となってしまうことを示している．このように，クラウドモデルでサービスを実現する限り，不要なデータが収集されてしまうことは避けられない．国・地域によらずデータアクセスが可能なクラウドの特徴から，追跡対象者の場所によらずテンプレートデータが拡散しない利点はあるが，しかしこの特徴はデータ保存の地域リスクも発生させる．

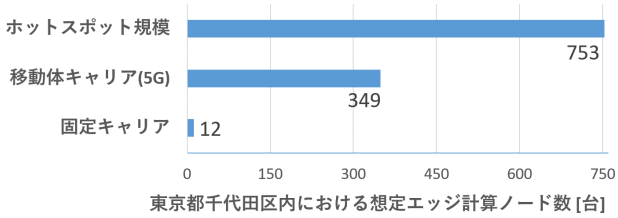

図 8 千代田区内におけるエッジ計算ノード台数
Fig. 8 Number of edge computation nodes in Chiyoda-ku.

表 1 既存技術との比較評価
Table 1 Comparative evaluation with existing technologies.

	提案モデル	クラウドモデル	エッジモデル
不要なデータ流出性	**小**（その場で処理）	大（全センサ集約）	**小**（エッジで処理）
テンプレートデータ拡散性	**小**（1 ノード）	**小**（1 ノード）	大（複数のノード）
データ保存の地域リスク	**影響なし**（データ源とほぼ同じ）	影響あり（地域ごとに物理サーバを分割要）	**影響なし**（同地域内）
総合評価	**最適**	不適	条件によって選択可

エッジモデルの短所であるプライバシテンプレートの拡散性は，将来エッジコンピューティング実用化の際に問題になる．もちろん拡散したテンプレートデータも適切にデータ管理がなされていれば問題にはならないので，たとえば暗号化領域で認識などの処理を実行する手法 [24] を用いればこれも選択肢にはなりうる．しかし，このような暗号化に加えて適切なデータ配置・削除を行う仕組みの導入も必要になり，設備のスケールに比例してセキュアな管理体制維持コストも拡大する．また，エッジのサポート規模に応じたプライバシテンプレートデータの拡散は，図 8 の結果から，(2)，(3) において拡散が顕著であり，(1) は比較的緩和されていることが分かる．しかし，千代田区内は 3 km 程度の歩行でほぼ区内を横断できることを考えると，どのケースでも計算ノードが切り替わる可能性があり，適切なデータ制御機能の具備が必要になる．なお，データ保存の地域リスクに関しては，どのような規模のエッジであっても，問題にならない．

提案技術はネットワークエッジでのデータ処理とテンプレートデータの集約管理が可能であり，クラウドおよびエッジ両モデルの長所を持つので，追跡型アプリケーションのプライバシデータ保護で優れた特徴を有するといえる．提案技術の実用性について他のサービスとの比較は次節にて議論する．

4.4 既存サービスとの比較

追跡型サービスはスマートフォンやカーナビなどの主に Global Positioning System を用いた機器と連動したサービスとして多くの実用例があげられる [25]．また，加速度や心拍などの生体情報を取得するセンサ機能を携帯機器や着衣に実装する技術も発展しており [26]，携帯型センサ単体でも，高度な状態推定を行う環境が整いつつある．ただし，これらは追跡対象者が携帯するデバイスの機能であるため，基本的に密着した状態から得られる情報に限られる．また，センサ機能の増加にともないコストも増加するので，これらを導入しサービスを享受できるユーザの格差につながる問題がある．これに対し，外部のセンサネットワークを利用した地産地消型アーキテクチャは下記の利点がある．

(1) 相対的な空間情報を利用可能
ビジョンセンサ，赤外線センサ，超音波センサなどの相対的な距離を要するセンサを活用できるため，対象者の顔表情，動作，周辺状態などの全体像を俯瞰した

情報を取得できる．特に昨今では，対象者が意識せずに撮られたような低解像度画像であっても高精度に解析を行う技術も発展しているが [27]，この種の情報利用は携帯型センサでは難しい．

(2) オープンな IoT インフラ活用によるコスト低減
現状の IoT サービスはその目的のために作られたセンサ，計算リソースなどの専用インフラに支えられたサイロ構造が主流であるが，公共の空間にも敷設されるインフラを各サービス専用に整備していくことは現実的ではない．そこで，サービス，基盤，規格によらず接続可能にする IoT のオープン化の必要性も主張されており [28]，産業界においても IoT 基盤の標準化・デファクト化が進められている．個々人の保持する機器の性能に依存せず，このようなオープン化されたインフラを活用できれば，低コストで均質なサービス品質が期待できる．

(3) 設備の共用によるコスト削減
専用型センサと異なり，1 つの LPLC ノード機器には複数の追跡対象者のプライバシテンプレートをインポート可能であるため，ユースケースによっては共用利用によってコスト低減も可能である．しかし，LPLC ノードに求められる機器の性能も増大するので，コストの観点ではそのトレードオフの検討が必要である．たとえば小学校の集団登下校はその有望なユースケースである．

ただし，センサネットワークと携帯型センサは互いに競合するものではなく，技術的に相互補完可能である．たとえば携帯型機器が取得する詳細情報を LPLC ノードが参加するローカルネットワーク経由で情報提供することによって，地産地消のプライバシ情報制御の特徴を活かしつつ，これと連携したより高度なサービスも可能になるだろう．

5. 将来課題および関連研究

本章では本論文の提案概念について，実用化に向けた将来課題としてセキュリティ性の考慮事項および実装に向けた技術動向と課題を述べ，あわせて現状の関連研究を示す．

5.1 システムのセキュリティ性検討と課題

提案アーキテクチャにおけるセキュリティ性を検討するため，「機密性」，「完全性」，「可用性」[29] の観点で，本システムに必要な対応技術を示す．まず，提案システムを構成する LPLC ノード，サービス提供サーバ，WAR および VSS における機密性の確保は，適正な利用者の接続認証を行うことで担保できる．このとき LPLC ノードからの認証はパブリックネットワーク側ではサービス提供サーバが，ローカルネットワーク側では WAR が行う．また，データ通信路の機密性は Secure Sockets Layer（SSL）[30] プロトコルなどを用いた Virtual Private Network（VPN）で暗号化することで担保可能である．この場合，LPLC ノードとの VPN 終端先は不特定多数の無線端末から接続が要求される WAR で行うことが望ましい．LPLC ノードの可用性については，ノードが機能せず定期的な正常状態通知が失われることを，異常状態通知として見なせば，サービス提供サーバが担保していると見なせる．しかし，クラウドモデルやエッジモデルは計算ノードそのものの冗長構成やデータレプリケーション性を有しているので，同様に運用上の信頼性を上げるための可用性機能の検討が必要である．

5.2 実装技術の検討と課題

LPLC ノードの構成技術について述べる．無線アクセスポイントを選択する機能の接続規格は Wi-Fi 規格（IEEE1394.11）に限定されず，Bluetooth Low Energy [31]，ECHONET LITE [32]，ZigBee [33] などの通信プロトコルを利用してもよい．追跡対象者の識別機構では，機械学習済みのデータを LPLC ノードへ組み込むことが考えられる．過去の研究にはローカルネットワークに配置したサーバへ学習済みデータをつど選択配信して動的に画像識別を切り替えた実装例もある [34]．LPLC ノードからローカルネットワーク側のセンサ機器検索は既存の規格として OSGi [35]，Universal Plug and Play（UPnP）[36]，Multicast DNS [37] などの活用が考えられる．ただし，LPLC ノード側ですべてのプロトコルを対応させることは現実的ではないので，ローカルネットワーク側の VSS が物理センサとの接続を抽象化する必要がある．このような抽象化サーバ機能は Hypercat [38]，OMA GotAPI [39] などの IoT 向け接続規格およびプラットフォームの活用が有望である．

5.3 実現に向けた課題

3.4 節で示した要件について，今後基本動作の実証において特に考慮が必要な点を考察し，以下に課題として示す．

まず，機器設置の要件における課題を述べる．センサ機器と無線有効範囲のオフセット距離はセンサ機器の種類によって大きく変わるので，たとえば IP カメラ機器などの具体的なユースケースを置いて，要件を満たす具体的な設計を行い，実現性を検証する必要がある．また，要件を満たした場合でもオフセット間隔が広すぎるとその分多くのデータ量を LPLC ノードが収集することになり，後述の計算機リソースにも影響するので，あわせてそのバランス調整も課題になる．加えて，現実の無線通信能力は障害物の有無，通信チャネルの利用状況などの環境状況に応じて変動するため，その点も検証が必要である．

計算機リソースの要件では，処理の重いデータ処理が集中する LPLC ノードの実装における十分なリソース確保が課題である．特に LPLC ノードには携帯性が求められるため，非常に限定された計算機リソースで実行する必要があ

る．昨今はスマートフォン上で機械学習による視覚認識技術を適用するモデル [40] も提案されているので，動作を確認するための限定した解析・分類の条件下ならば現在のモバイルハードウェアでも成立しうる．しかし，本提案は相対的な空間情報を利用した多様な解析を行えることが，既存の携帯型センサを用いた追跡サービスと比べた優位点である．たとえばユースケース例の広域見守りを想定すると，顔認識だけでなく，対象者の表情，動き，体勢，また周辺の状況解析など，多くの解析処理を LPLC ノードで逐次行うことが求められる．このようなリアルタイム処理や画像などの非構造化データの解析処理には大きな計算機リソースが必要であるが，この解決には電力比性能の優れたヘテロジニアスプロセッサの活用が考えられ，GPU を搭載したスマートフォンやシングルボードコンピュータに FPGA を組み込んだ実装などの解決アプローチの検討が必要になる．これは電力，演算性能の限られた計算機リソース環境において GPU などの特化型プロセッサを活用する研究事例があるように [41]，処理の重くなる顔認識などの認知知能処理などに特化したシステムを実装することによって解決できる可能性がある．その具体的なハード設計およびソフト設計は将来の課題である．

6. おわりに

労働力不足・少子高齢化社会に向けて IoT 技術を活用した社会支援アプリケーションの研究開発は大きな期待を受ける一方で，ますます増大していくプライバシデータの脅威に対する対策が求められている．この研究の貢献は，広域で展開されるセンサネットワークで有望な追跡アプリケーションにおけるプライバシデータ保護技術として，データの地産地消を行うアーキテクチャを示したことである．また，サービス利用者と無関係な人のプライバシデータがサービス事業者に収集される不要データの流通比率や，サービス利用者のプライバシ性の高いテンプレートデータが拡散する問題について定量化し，既存技術であるクラウドモデル，エッジモデルと比較することで，提案アーキテクチャの有用性を示した．今後は実用モデルの構築へ向けた計算機リソースの検討とコンセプト実証を行っていく．

参考文献

[1] IP カメラ国内市場に関する調査を実施（2016 年）：株式会社矢野経済研究所，入手先 ⟨https://www.yano.co.jp/press/press.php/001599⟩（参照 2018-02-20）.

[2] PaaS で誰もがデータ分析：日経コンピュータ，入手先 ⟨http://tech.nikkeibp.co.jp/it/atclact/active/15/010700161/010700003/⟩（参照 2018-02-20）.

[3] Taigman, Y., Yang, M., Ranzato, M.'A. and Wolf, L.: DeepFace: Closing the Gap to Human-Level Performance in Face Verification, *CVPR* (2014).

[4] 西岡潔郁，山崎俊彦，相澤清晴：ネットワーク化されたカメラを支える諸技術とその応用，映像情報メディア学会誌，Vol.62, No.7, pp.997–1002 (2008).

[5] Morris, B.T. and Trivedi, M.M.: A Survey of Vision-Based Trajectory Learning and Analysis for Surveillance, *IEEE Trans. Circuits and Systems for Video Technology*, Vol.18, No.8, pp.1114–1127 (2008).

[6] 竹内孝仁：寝たきり老人の成因—「閉じこもり症候群」について，老人保健の基本と展開，pp.148–152, 医学書院 (1984).

[7] Hinton, G.E., Osindero, S. and Teh, Y.: A fast learning algorithm for deep belief nets, *Neural Computation*, Vol.18, pp.1527–1544 (2006).

[8] Le, Q.V., Ranzato, M., Monga, R., Devin, M., Chen, K., Corrado, G.S., Dean, J. and Ng, A.Y.: Building high-level features using large scale unsupervised learning, *ICML* (2012).

[9] 総務省：特集データ主導経済と社会変革，平成 29 年版情報通信白書 ICT 白書 2017，第 1 部，第 2 章，p.79 (2017).

[10] 福岡直也，伊藤義道，馬場口登：観察者に応じたプライバシー保護映像を生成可能な映像配信手法，第 10 回情報科学技術フォーラム，RK-006, pp.97–100 (2011).

[11] Zhang, W., Cheung, S.S. and Chen, M.: Hiding privacy information in video surveillance system, *ICIP* (2005).

[12] Sohn, H., Neve, W.E. and Ro, Y.M.: Privacy Protection in Video Surveillance Systems: Analysis of Subband-Adaptive Scrambling in JPEG XR, *IEEE Trans. Circuits and Systems for Video Technology*, Vol.21, No.2, pp.170–177 (2011).

[13] 小林健人，稲村勝樹，金田北洋，岩村恵市：プライバシ保護と犯罪防止を両立させる監視カメラシステム，情報処理学会論文誌，Vol.57, No.1, pp.172–183 (2016).

[14] Bonomi, F.: Connected vehicles, the internet of things, and fog computing, *VANNET 2011* (2011).

[15] Jaraweh, Y., Doulat, A. and AlQudah, O.: The future of mobile cloud computing: Integrating cloudlets and Mobile Edge Computing, *ICT2016* (2016).

[16] Satyanarayanan, M., Bahl, P., Caceres, R. and Davies, N.: The case for vm-based cloudlets in mobile computing, *IEEE Pervasive Computing*, Vol.8, No.4, pp.14–23 (2009).

[17] 総務省：特集データ主導経済と社会変革，平成 29 年版情報通信白書 ICT 白書 2017，第 1 部，第 2 章，pp.89–99 (2017).

[18] 丸山　宏：エッジ・ヘビー・データとそのアーキテクチャ，情報管理，Vol.56, No.5, pp.269–275 (2013).

[19] NTT 東日本企業情報：収容局毎のカバーエリア，入手先 ⟨https://www.ntt-east.co.jp/info-st/info_dsl/area.html⟩（参照 2018-07-07）.

[20] ETSI: MEC Deployments in 4G and Evolution Towards 5G, ETSI White Paper, No.24 (2018), available from ⟨http://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp24_MEC_deployment_in_4G_5G_FINAL.pdf⟩ (accessed 2018-02-20).

[21] 総務省：「新世代モバイル通信システムに関する技術的条件」のうち「LTE-Advanced 等の高度化に関する技術的条件」，情報通信審議会情報通信技術分科会新世代モバイル通信システム委員会報告概要，平成 29 年 (2017). 入手先 ⟨http://www.soumu.go.jp/main_content/000485376.pdf⟩（参照 2018-02-20）.

[22] ドコモ Wi-Fi エリア検索サイト，入手先 ⟨https://sasp.mapion.co.jp/b/mzone/⟩（参照 2018-02-20）.

[23] 中村俊行，大西博文，恒岡伸幸，時　政宏：道路空間の安全性・快適性の向上に関する研究，国土技術政策総合研究所プロジェクト研究報告 (2006).

[24] Erkin, Z., Franz, M., Guajardo, J., Katzenbeisser, S., Lagendijk, I. and Toft, T.: Privacy-Preserving Face

Recognition, *Proc. 9th International Symposium on Privacy Enhancing Technologies*, pp.235–253 (2009).
[25] NTT ドコモイマドコサーチ，入手先 ⟨https://www.nttdocomo.co.jp/service/imadoco/⟩（参照 2018-07-07）.
[26] 桑原　啓，高河原和彦：「hitoe」生体情報計測ウェアと超小型血流センサの技術と応用展開，エレクトロニクス実装学会誌，Vol.18, No.6, pp.417–421 (2015).
[27] 鈴木武志：動画顔認証を中心とした生体認証技術：現状と，安全・安心な社会の実現に向けて，情報管理，Vol.60, No.8, pp.564–573 (2017).
[28] 坂村　健：オープン IoT—考え方と実践，パーソナルメディア (2016).
[29] 日本工業標準調査会：JIS Q 27002，p.5 (2006).
[30] Freier, A., Karlton, P. and Kocher, P.: The Secure Sockets Layer (SSL) Protocol Version 3.0, RFC6101 (2011).
[31] Bluetooth SIG Regulatory Committee: BLUETOOTH LOW ENERGY REGULATORY ASPECTS (2011).
[32] ECHONET Lite 規格書 Ver.1.12（日本語版）：ECHONET Consortium, 入手先 ⟨https://echonet.jp/wp/wp-content/uploads/pdf/General/Download/echo_brochure_en_1702.pdf⟩（参照 2018-02-20）.
[33] ZIGBEE SPECIFICATION: ZigBee SIG-Japan, 入手先 ⟨http://www.wirelessdesign.jp/doc/zigbee-spec_081209.pdf⟩（参照 2018-02-20）.
[34] Kataoka, M., Hoshikawa, N., Noguchi, H., Demizu, T. and Yamato, Y.: Tacit Computing and its Application for Open IoT Era, *CCNC 2018*, pp.12–16 (2018).
[35] OSGi and the Enterprise Business White Paper Revision 1.3: OSGi Alliance, available from ⟨https://www.osgi.org/wp-content/uploads/OSGiAndTheEnterpriseBusinessWhitepaper2.pdf⟩ (accessed 2018-02-20).
[36] MAKING THE SMART HOME SMARTER WITH UPnP TECHNOLOGIES, UPnP FORUM, available from ⟨http://upnp.org/resources/whitepapers/UPnP_SmartHome_Whitepaper_2015.pdf⟩ (accessed 2018-02-20).
[37] Cheshire, S. and Krochmal, M.: Multicast DNS, RFC6762 (2013).
[38] Hypercat 3.00 Specification: Hypercat Limited (2016), available from ⟨http://www.hypercat.io/⟩ (accessed 2018-02-20).
[39] OMA GotAPI Generic Open Terminal API Framework: oma, available from ⟨https://cdn2.hubspot.net/hubfs/183757/OMA_GotAPI_White_Paper.pdf?t=1435857783749⟩, 2015 (accessed 2018-02-20).
[40] Howard, A.G., Zhu, M., Chen, B., Kalenichenko, D., Wang, W., Weyand, T., Andreetto, M. and Adam, H.: MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications, arXiv.org:1704.04861 (2017).
[41] Qiu, H. and Memm, G.: Fast selective encryption method for bitmaps based on GPU acceleration, *2014 IEEE International Symposium on Multimedia* (2014).

千川 尚人

2009 年名古屋大学大学院情報科学研究科博士課程単位取得退学．同年東日本電信電話株式会社入社．2013 年日本電信電話株式会社 NTT ネットワークサービスシステム研究所．2018 年小山工業高等専門学校電気電子創造工学科助教．IoT サービスのネットワークシステム研究に従事．博士（情報科学）．

下馬場 朋禄

2002 年千葉大学大学院自然科学研究科博士課程修了．同年理化学研究所基礎科学特別研究員．2005 年山形大学工学部助教授．2007 年同大学大学院理工学研究科准教授．2009 年より千葉大学工学研究科准教授．ホログラフィ応用技術の研究に従事．博士（工学）．

伊藤 智義 （正会員）

1992 年東京大学大学院総合文化研究科博士課程中退．同年群馬大学工学部助手．1994 年同大学助教授．1999 年千葉大学工学部助教授．2004 年より同大学教授．専用計算機による数値計算の高速化の研究に従事．博士（学術）．