IoT カメラサービスのプライバシ情報流出を抑制する

地産地消型システムの研究

代表研究者　　干川　尚人　　独立行政法人　国立高等専門学校機構
小山工業高等専門学校　電気電子創造工学科　講師

1 研究背景

IoT 技術の進展と共にさまざまなセンサ機器がネットワークにつながり，限られた範囲で提供されていた IoT サービスが広い物理空間でも提供可能になってきた．これに近年進化が著しい顔認識のような認知技術と連携させて，従来人の判断が必要だった地域コミュニティの防犯，見守りなどに活用できれば，労働力の大幅な省力化が期待できる．このような見守りの広域化は高齢化社会においても特に重要で，高齢者の活動領域の拡大により生活の質の向上，健康促進，そして医療費削減にも寄与できる．しかし，このような状況下では収集される身の回りの情報も増加するので，プライバシデータ流出の脅威も増す．特に，現在一般的なクラウドモデル型サービスでは，サービスの目的に関わらず無関係な情報も全て収集される問題がある．そのため将来有用なサービスが実現しても，その社会実装に理解が得られない可能性もある．代表研究者はこのような広域に渡る IoT サービス実現において，利用者が安心・安全に利用できるようにプライバシ情報の流通を制御する「地産地消型ネットワーク」を提案した[1]．この提案アーキテクチャはネットワークの仕組みを工夫することでデータ流通を制御する独自の発想に基づいており，将来のスマート社会実現に必須のセキュリティ要素技術だと考えている．本研究では，現実のセンサデータを用いたシミュレーションや実機実験を通して，提案している「地産地消型ネットワーク」の有用性を証明する．そして，本ネットワークに基づいた実装を行うことでその技術実証を実施し，実用化を目指した要素技術の開発を推進する．

2 研究報告

2-1 調査研究の動機および関連技術

（１）周辺情報を活用した見守り

建物や特定の敷地を越えた，例えば街単位の広域をサポートした見守りサービスは多くの場合，見守り対象者が保持する GNSS (Global Navigation Satellite System)センサなどを用いた位置情報の通知を以てその安全情報としていることが多い．しかし，本来見守りを依頼する側にとって重要なのは「安全な状態であること」であり，位置情報だけではその担保は不十分である．一方，見守り対象者が保持するセンサではなく，その活動する周辺環境に設置されたセンサ情報を活用したとき，そこから得られる見守り対象者の情報量は非常に豊富になる．例えば，表情，身体の体勢，そして声といった本人の情報に加え，明暗，天候，交通量，不審者の有無など，周辺の環境情報も情報の分析に使うことができる．例えば，見守り対象者の表情を識別できるテンプレートデータを組み込んだ識別システムが，見守り対象者の周辺にあるカメラ機器が撮影した画像をネットワーク経由で受信して識別することで，対象者がどこにいて，どんな状態か，などの従来の位置センサだけでは取得できなかった情報を把握することが可能になる．これは近年進歩が著しい機械学習を用いたデータ解析技術などと組み合わせることで，より確実性の高い見守りサービスの実現が期待できる．

（２）クラウドサービスとプライバシ情報保護の課題

センサデータを情報システムが取得する手段として，インターネットにつながるセンサ機器（いわゆる IoT 機器）の活用例が増えており，そしてそのデータ分析においてはクラウドサービスによるプラットフォームが多く利用されている[2－3]．前述の「表情を識別する見守りシステム」ならば，クラウド上のサーバ（以下クラウドサーバ）に識別に必要なテンプレートデータを組み込むことで，サービスの実装ができる．しかし，クラウドサーバで公共空間において収集されたセンサデータの分析を試みるとき，サービスに無関係な人物などのデータもすべてクラウドサーバへ集約してしまう問題が生じる．

公益財団法人電気通信普及財団
研究調査助成報告書　第35号　2020年度

犯罪捜査のような公共の利益を目的とする場合と異なり，特定人物の見守りのような個人用途のサービスでデータ利用する場合，そのサービス利用に無関係な人にとって，そのプライバシ情報（これを Non-related Private Data，以下 NPD と呼ぶ）が勝手に使われてしまうことに理解を得ることは難しいだろう．事実，総務省の調査によればクラウドサービス事業者に対して気づかないうちにプライバシ情報を提供していることについて多くの利用者が不安を感じている[4]．

（３）エッジコンピューティングアプローチとその課題

近年「データ発生源に近いネットワークエッジでデータ処理をする」エッジコンピューティングが注目されており，その特徴として通信応答の低レイテンシ性やデータ通信量や計算負荷の分散性，そして，データ流通の制御性が挙げられている[5]．この「制御性」の特徴は，データ発生源に近いエッジネットワークごとにデータの収集ポイントを分割できることに起因する．例えば，エッジネットワークごとに配備した計算機ノード（以下，エッジサーバ）にデータを集め，サービスに必要なデータを抽出し，無関係なものを廃棄するといった適切なデータ処理を行えば，すべてのデータが特定のクラウド事業者へ集約されるような，無秩序な流通を防ぐことができる．このような実例として，工場などの生産現場における機密情報の保護を目的としたエッジコンピューティング研究開発の事例がある[6]．しかし，公共空間で不特定多数の利用者を想定した広域見守りサービスの場合，インフラ設置と計算機リソースの 2 点で課題がある．1 点目として，サービスを提供する空間全体にエッジネットワークを構築する必要があり，そしてすべてのエッジサーバへテンプレートデータを組み込む必要がある．このとき，利用者によって変更が必要なテンプレートデータを動的に組み込むことも考慮しなければならない．2 点目として，限られた計算機リソースであるエッジサーバで，画像解析などの計算処理を複数のユーザに対して実行しなければならない．上記のように，エッジコンピューティングアプローチはプライバシデータの流通抑制の観点で優れているが，利用するユーザが頻繁に切り替わり，また複数の利用者が高負荷な演算を要求する要件において，必要なデータの配備方法や計算機リソースの確保で課題がある．

2-2 提案システム

本節では周辺情報を活用した広域見守りシステムの構成モデルとして，「クラウドモデル」「LPLC モデル」「MEC モデル」「MEC-MCR セントリックモデル」の 4 方式を定義した．なお，ここで「クラウドモデル」はデータをクラウドで集中管理する従来型のモデルであり，その他の 3 方式を地産地消型として分類する．

（１）クラウドモデル

監視カメラの生成する生の撮影データをクラウドサーバ上へ送信する実装案をクラウドモデルとする．この概要を図 1 に示す．各監視カメラがクラウドサーバまでデータ送信するためのネットワーク接続手段は問わない．また，テンプレートデータはクラウドサーバに配備される．サービス構成に必要な設備は非常にシンプルであり，計算機リソースも制約がないが，NPD を区別することなくデータを集約するため，個人情報の漏洩性が高い．

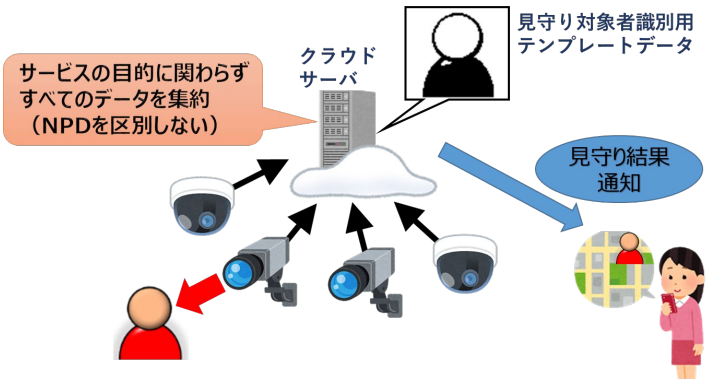

図 1 クラウドモデル

（２）LPLC モデル

当研究グループでは「ある人の見守りに必要な環境情報は，その見守り対象者の物理的な位置と相関性がある」という考えのもと，エッジコンピューティングの一形態として「データの地産地消を実現するネット

ワークアーキテクチャ（Local Production for Local Consumption Network Architecture，以下 LPLC モデル）」を提案している[1]．これは，ネットワークエッジであるローカルネットワーク上に配置された IoT カメラの情報を，見守り対象者がそのローカルなネットワークと接続可能な範囲に入ったときに，その見守り対象者が帯同している計算ノードへ送り，見守りに必要な情報（画像認識による異常検知など）を処理することで，NPD の収集を抑制するというものである（図 2）．我々はこのコンセプトに基づき無線アクセスポイント（以下 AP）搭載ルータと IP カメラから成るローカルネットワークを形成し，LPLC モデルによる見守りサービス実装の仕組みを提案している[7]．これは，カメラ画像データを用いた視覚情報に基づいて人物を追跡し，安全状態を把握するサービスで，見守り対象者とその周辺環境を撮影した画像データを処理することで，顔認識や歩容解析を行う．このとき，画像データは見守り対象者が常に携帯する Mobile Computing Resource（以下 MCR）を用いる点が，クラウドモデルと大きく異なる特徴であり，画像データ発生源に極めて近い位置で解析処理を行う，すなわちデータを地産地消することで，不要な情報をクラウド側へ送信する必要がなくなる．

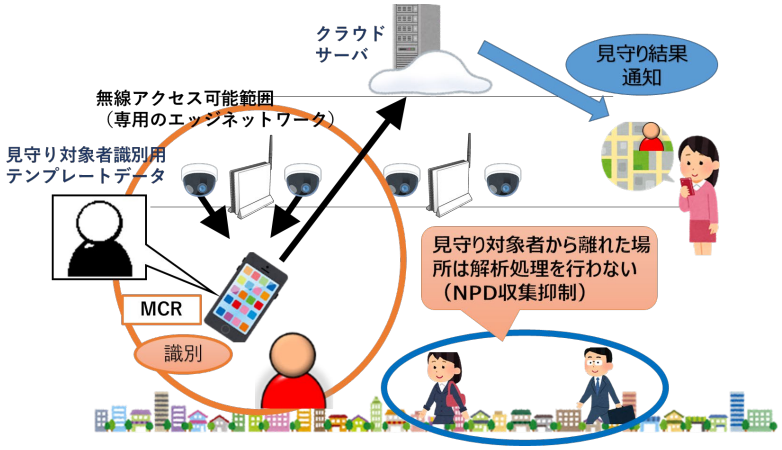

図 2 LPLC モデル

（３）MEC モデル

前述の LPLC モデルは NPD 収集の抑制に有効だが，専用のエッジネットワークを構成する必要があり，これを街中のような広域に渡って配備することは現実的ではない．しかし，近年エッジネットワークとして 5G ネットワーク網の構築が進んでいる．そこで，撮影データの処理を European Telecommunications Standards Institute（ETSI）の 5G 仕様で定義[8]されている MEC サーバで行う実装を MEC モデルとする．なお，本稿における MEC サーバは 5G の基地局範囲を最小単位としたエッジネットワークごとに 1 台配備される前提とする．MEC モデルは LPLC モデルにおける無線アクセスポイントを 5G の基地局アクセスポイントに，センサデータの抽象化と撮影データの解析を行うサービス専用の計算機リソースを MEC サーバに置き換えて構成する．見守り用のセンシングデータを収集するカメラデバイスはそれぞれ 5G 通信可能なモジュールを持つか，5G 通信可能なゲートウェイに繋げる（図 3）．5G は 4G 以前と比べ，基地局あたりの通信セル範囲が狭い点が大きな特徴である．また，5G 網のエッジネットワークには MEC サーバが組み込まれ，将来はそのカバー率も高くなることが期待できるので，これは街中のような広域な見守りサービスに非常に向いている．しかし，MEC モデルは 2 章の課題で述べたように，サービス提供範囲すべての MEC サーバにテンプレートデータを配備する問題が発生する．

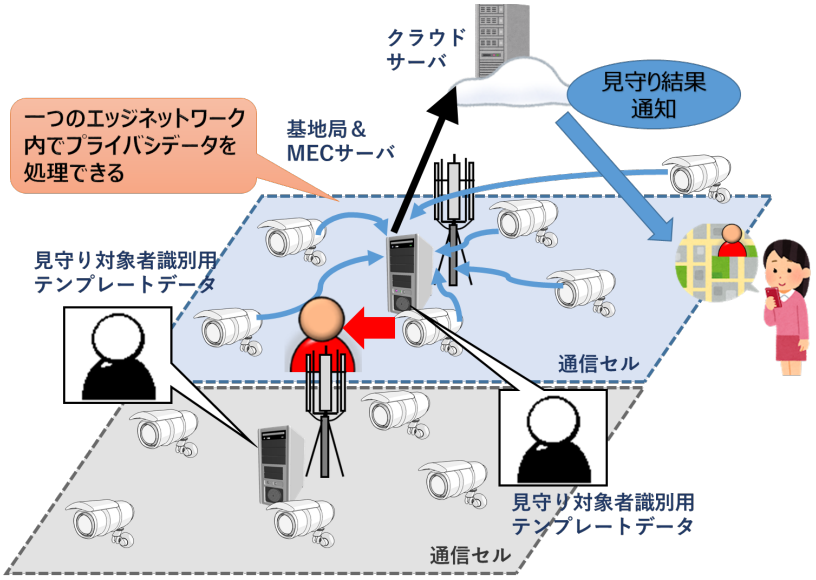

図 3 MEC モデル

（４）MEC-MCR セントリックモデル

LPLC における MCR の仕組みと 5G/MEC を用いて実装する方式を MEC-MCR セントリックモデルとする．これはテンプレートデータの配備とデータ処理を行う MCR を導入することで，前述の 2 モデルにおける課題を解決するものである．本モデルにおける MCR と MEC サーバの機能分担を（図 4）に示す．まず，MCR にテンプレートデータが配備されるため，サービス領域内のエッジサーバすべてにデータの展開が不要になる．また，MCR はサービス利用者である見守り対象者が保持する専用リソースなので，共有リソースである MEC サーバ上で利用者ごとのデータを管理する必要性がなくなる．

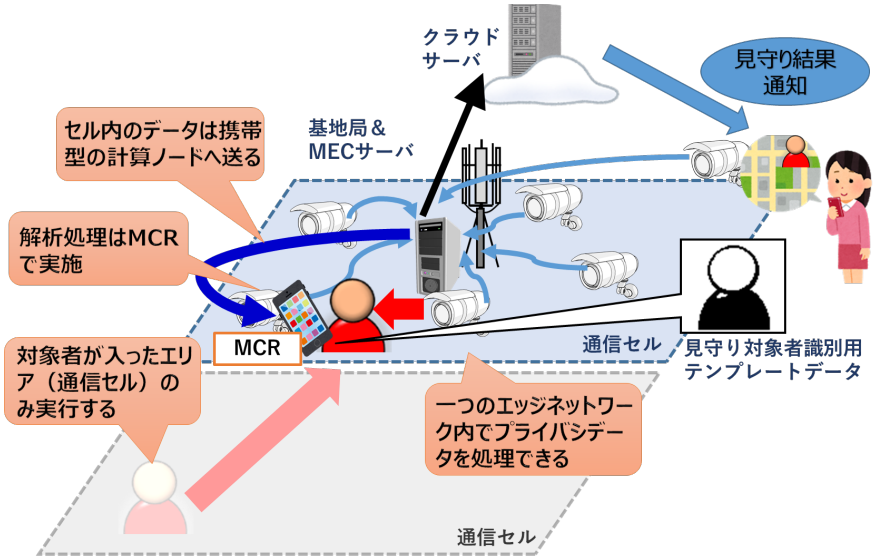

図 4 MEC-MCR セントリックモデル

2-3 システム実証結果

（１）地産地消型モデルシミュレーションによるプライバシデータ流出の定量評価

クラウドモデルに対して，地産地消型モデルがプライバシデータの流出をどの程度防ぐことができるのか，シミュレーションを行った．ここではクラウドサーバへデータ流出に対して，地産地消モデルでどの程度流出を抑制できたかを，「無関係なプライバシデータ(NPD)の流出比」で評価した．

（1） －1　シミュレータの設計

ここでは，現実性の高い人の移動情報を元に評価を行うため，オープンデータを利用した．実際の移動情報としてはG空間情報センターの公表している松江駅構内人流センサデータ[9]を活用し，このデータを「学校へ登校する人の見守りサービス」としてシミュレーションを行った．ここで活用した人流センサデータはセンサ19個ごとに「センサID，日付，時刻，In，Out，In累計，Out累計」が定義されており，センシング結果は1分毎の合計である．これより，シミュレータ上でのIn，Outデータは図5のように定義する．

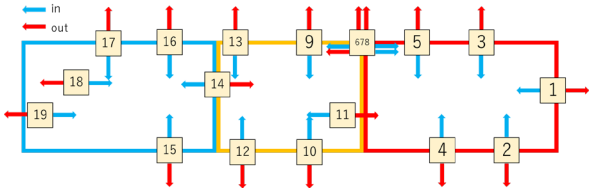

図5シミュレーションマップ上のセンサ位置図

In，Outデータを撮影するようにカメラを設置する．このカメラのセンサ有効距離は15メートルとした．また，ルータをオープンデータの人流センサと同じ位置に設定し，In，Out データを撮影するカメラの二つをルータに属するカメラとした(図6)．

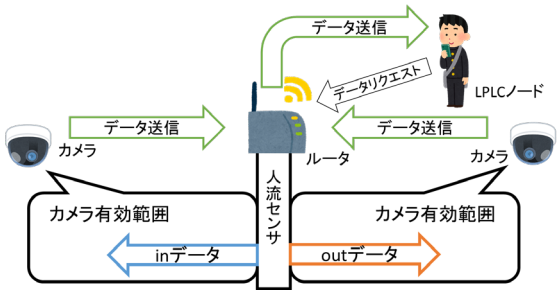

図6カメラ，ルータ位置図

本稿ではカメラのセンシング周期を1秒とする．オープンデータは1分毎に更新されているので，次に示すアルゴリズムを用いてオープンデータを1秒毎のデータへ変換した．

表1．アルゴリズムに用いる変数の定義

60の約数	*nums*[12]= {1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60}
約数毎の60分割	*vals*[12][60]
入力データ	input
出力データ	result[60]

*vals[i]*には*nums[i]*を60分割したデータが入っている．例えば 20の*vals*には{1, 0, 0, 1, 0, 0, 1, …, 1, 0, 0}と1, 0, 0が20回繰り返されるデータを格納している．このように*vals*には60個の要素の合計がnumsとなりつつ，数字が偏らないように格納されている．*input*が0になるまで次の処理を繰り返すことでresultにinputを60分割した数が格納される．

① *input*より小さい中で，最も大きい*nums*を選ぶ．選ばれた*nums*を仮に*nums[i]*とする．

② *input*から*nums[i]*を引き，*result*に*vals[i]*を足し合わせる．

ルータアクセス可能距離の値を設定し，対象者数を1人に加え，25人から200人まで25人刻みで変化させシミュレーションを行った．

（1） －2　シミュレーション結果

ルータアクセス可能距離毎の対象者人数とNPD流出比の関係をグラフにまとめた．なお比較のため，「クラウドモデル」におけるNPDを算出した結果を過去の研究[10]から採用し，これをNPD流出比の概算を追記したものが図7である．

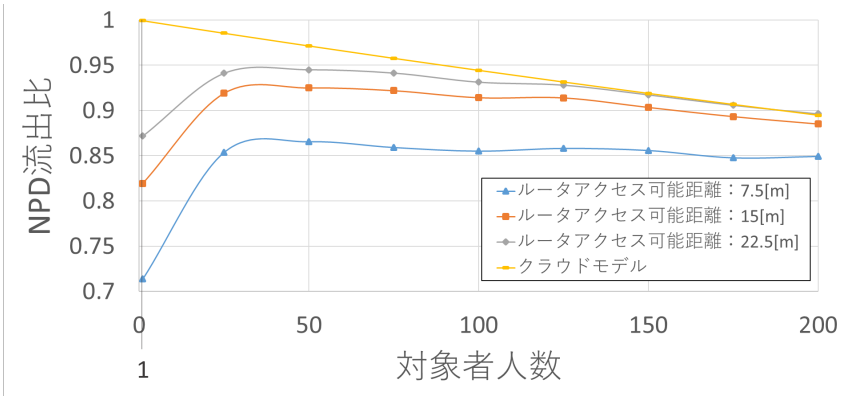

図 7 シミュレーション結果

NPD 流出比が小さいほどプライバシ保護能力が高いといえるので，ルータアクセス可能距離に依らず，クラウドモデルよりも地産地消型モデルの方が優れている．クラウドモデルを最悪値としているので，この結果は妥当である．対象者の人数を増やすと，プライバデータを生成する全体のカメラにおいて，「無関係でないデータ」の割合が増えていくので，地産地消モデルに流出比が近づく結果も妥当である．ルータアクセス可能距離がセンサ有効距離より短いと追跡サービスとして不十分であるが，反対にアクセス可能距離があまりに長いと，NPD センシング過多の原因となる．よって，センサ有効範囲を内包しつつルータアクセス可能距離を短くすることにより，プライバシに配慮した追跡サービスが実現できる．

このデータは現実性の高いシミュレーションを再現するために実際の駅ビル内の人流情報に基づくオープンデータを採用しているが，結果を見るとその流出比はルータの無線アクセス有効距離のようなネットワークトポロジーの構成条件に概ね依存してることがわかる．

（２）地産地消モデルの定性評価

カメラ型見守りサービスシステムを実装するための 4 つのモデル（クラウド，LPLC，MEC，MEC-MCR セントリック）について，その実現性を定性評価する．

（２）－１　評価観点

本研究は実用化を踏まえた評価を行うために，事業者視点での「サービス管理における情報保持リスク」と「実装可能性」の 2 観点から評価する．サービス管理における情報保持リスクはサービス運用において，事業者がパブリックネットワーク上に収集したデータに起因するリスクと定義する．具体的には，一般利用者がアクセス可能なインターネット上の事業者サーバに最終的に収集される個人データの種類や量が多ければ高リスクとなる．逆に，不必要なデータをなるべく収集しない方式であれば低リスクである．これは実現方式に依存する機能面の評価である．

実装可能性は実用化の容易さを指標とする．各方式の実装には前提となるインフラ配備が必要となるが，インフラ配備に必要なコストはサービスの実現可能性に反比例する．そこで，この観点ではコスト低減に寄与する以下の 3 点を比較対象として挙げる．

1. インフラ流用性
2. 利用者データ配備性
3. 無関係データの除外性

1 は既存または将来のインフラを活用できるか，2 は個人ごとの利用者データ（例えば見守り対象者を識別するための固有のテンプレートデータなど）を容易に配備できるか，3 はサービス利用者と無関係な情報（NPD）を絞り込むこと，つまりいかに見守り対象者に関わらない撮影データを除くことができるか，以上をそれぞれの方式で評価する．

（２）－２　評価観結果

4 つのモデルごとに定性比較評価を行った結果を表 2 に示す．本稿では総合評価として MEC-MCR セントリックモデルが最適と結論付けた．以下，評価理由を説明する．

表２　４モデルごとの比較評価

評価項目		クラウド	LPLC	MEC	MEC-MCR セントリック
サービス管理における情報保持リスク		×	○	△	○
実装可能性	インフラ流用性	○	×	△	△
	利用者データ配備性	○	△	×	△
	無関係データの除外性	×	○	×	○

クラウドモデルの場合，識別に利用するテンプレートデータや収集した識別データは最終的にパブリックネットワーク上の事業者サーバに集約・保持されるため，リスク大である．一方，エッジコンピューティングの特性を持つその他のモデルは，ネットワークエッジで事業者サーバへ送信するデータを取捨選択可能なので，リスクを低減できる．その中でも特に LPLC モデルおよび MEC-MCR セントリックモデルは，サービス実行に必要な個人情報（主に見守り対象者を識別するためのテンプレートデータ）を見守り対象者の保持する端末（MCR）へ渡しているため，サービス提供事業者観点では管理リスクを利用者に移転できる利点がある．

インフラ流用性の観点では，既存のネットワークインフラ上でサービスを実装可能なクラウドモデルが最も優れている．そして，5G/MEC インフラを利用できる MEC モデルおよび MEC-MCR セントリックモデルは次点となる．海外では 5G サービスが開始され[11]，日本でも 2020 年より始まった[12]．現時点では MEC のリソースを利用したサービスは公表されていないが,今後 5G 設備が普及し,MEC サーバを利用可能になったとき，その具体的なアプリケーションとして実装が期待できる．LPLC モデルは独自のエッジネットワークとアクセスポイントを敷設する必要があり，もっとも困難である．

利用者データの配備性はすべての利用者データを一カ所に集約可能なクラウドモデルが最も優れている．特にデータセンタ上に計算機リソースを配備できるクラウドプラットフォームの場合，サービス利用者の増減に依存するデータ数に応じたリソース管理も容易である.次点は LPLC モデルおよび MEC-MCR セントリックモデルで，見守り対象者の識別に必要なテンプレートデータを見守り対象者が保持する MCR の一カ所に配備するだけで良いため，サービスの管理性に優れる．例えば，サービス利用者が増えたとしても，その利用者用に渡す MCR に見守り対象者のテンプレートデータを組み込むだけなので，サーバのような共用を前提とする装置に対して識別に必要な計算機リソースの割り当てを管理する必要がなくなる.対して,MEC モデルは，見守りアプリケーションを実行するサービス領域全体に配備されていた MEC サーバに利用者ごとのテンプレートデータを組み込む必要があり，実行環境を整えるまでの負担が大きい．

無関係データの除外性は，見守り対象者の周辺の撮影データのみを利用する仕組みを具備している LPLC モデルおよび MEC-MCR セントリックモデルが最も優れている．クラウドモデルおよび MEC モデルの場合，収集する撮影データを絞り込むために，見守り対象者の位置情報を獲得する仕組みが必要な点が課題である．

（３）実装モデルの設計と評価

シミュレーション結果によって，地産地消モデルのプライバシデータの流出抑制効果を確認し，その性能を上げる調整はネットワークトポロジーの設定に依存することが判明したので，次に本コンセプトのフィージビリティを確認するための実装モデルを設計し，評価を行った．ここで採用したモデルは前述の定性評価結果で最も優れていた（４）MEC-MCR セントリックモデルである．ただし，インフラの配備性以外の点では（２）LPLC モデルとネットワークトポロジーは変わらないため，本実証のフェーズでは高価な 5G および MEC インフラを用いない，LPLC モデルで実装した．以下，これを提案モデルと表し，説明する．

（３）－１　実装モデルの設計

物理機能図を図８に示す．仮想カメラサーバ(Virtual Camera Server: VCS)は IP カメラからの画像データを抽象化して保持し，要求に応じてそれを送信する．MCR は常に無線アクセスルータ(Wireless Access Router: WAR)を探し，接続後は VCS から画像データを取得し見守りに必要な情報だけを取り出す．そしてサービス提供サーバを通して見守り依頼者に通知される．MCR は WAR のアクセスポイント（Access Point: AP）に入った時，その AP 内のカメラのデータのみを取得する．そのため，見守り対象者の情報を含まないデータの取得を削減することができる．

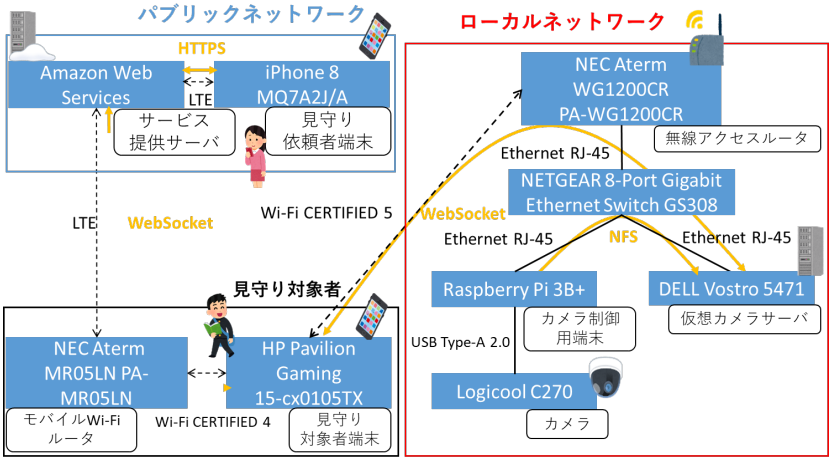

図 8 MCR セントリックモデルの物理機能図

本モデルを実現するには以下の要件を満たす必要がある.

1)カメラにより撮影された画像データはローカルネットワーク外に流出しない.
2)AP の範囲はカメラの撮影範囲を内包しつつ，かつ大きすぎない.
3)MCR はパブリックネットワークとローカルネットワーク両方に接続する.
4)MCR は AP を常に検索し，接続する.
5)接続後は VCS にデータを要求する.
6)MCR は取得したデータをリアルタイムに処理し，その結果を見守り依頼者に通知する.
7)MCR 搭載の同一ネットワークインターフェースで異なる複数の AP に入る場合がある.

以上の要件を満たすように実装されたシステム構成の使用機器を表 3 に示す.

表 3 実装システム構成の使用機器

システム構成要素	使用機器
IPカメラ	Logicool C270, Raspberry Pi 3B+
仮想カメラサーバ(VCS)	DELL Vostro 5471
レイヤ2スイッチ	NETGEAR 8-Port Gigabit Ethernet Switch GS308
無線アクセスルータ(WAR)	NEC Aterm WG1200CR PA-WG1200CR
見守り対象者端末(MCR), モバイル無線アクセスルータ	HP Pavilion Gaming 15-cx0105TX, NEC Aterm MR05LN PA-MR05LN
サービス提供サーバ	Amazon Web Services
見守り対象者端末	iPhone 8 MQ7A2J/A

IP カメラは通常のカメラとその制御用デバイスで構成し，撮影された画像データは NFS(Network File System)を通して VCS に送信される．また，WAR は他の用途で使われる AP と区別がつく記号列と，見守りシステム用の他の WAR による AP と区別がつく識別子を合わせた SSID(Service Set Identifier)を持つ．MCR はその記号列のみをあらかじめ記憶し，見守りシステム用の WAR を検索する．そして，最も電波強度の強い WAR にあらかじめ記憶しているパスワードを用いて認証，接続する．VCS はどの WAR でも同じ固定 IP アドレスを保持しているため，MCR は WAR 接続後，VCS に画像データを要求することができる．MCR は VCS との通信を，WebSocket を用いて行い，画像データ取得後は画像処理によって見守り対象者の情報を取り出し，その結果をサービス提供サーバに送信する．見守り依頼者はサービス提供サーバの公開する Web サイト上で見守り対象者を見守ることができる.本実装では見守り対象者が持つ色マーカを画像処理ライブラリ OpenCV を用

いて認識することで見守り対象者を認識し，画像データから取り出した時刻と位置情報をサービス提供サーバへ送信する．また，今回使用した WAR は AP 範囲の調整が不可能であったため，MCR で電波強度を測定し，ある閾値を上回ったら接続，下回ったら切断をすることでカメラの撮影範囲を適切に内包する半径 5m の AP を擬似的に作成した．

（３）－２　実装モデルの評価

実装システムを用い，クラウドモデルに対する提案モデルを評価する．表 4 の条件，図 9 の学校内の環境で AP を 2 往復した時，MCR セントリックモデルとクラウドモデルで見守り対象者が写る画像(これを必要データと呼ぶ)の枚数を比較する．クラウドモデルでは，画像データは常にクラウドコンピュータに送信される．見守り対象者は AP を約 7 秒で渡り，それを 2 往復するため，クラウドコンピュータは約 140 枚の必要データを取得すると予測できる．また，提案モデルでは，WAR の認証後に VCS から画像データを取得するため，Wi-Fi の接続時間が発生する．事前実験で Wi-Fi 接続時間は約 2.3 秒とわかっていたので，それを考慮すると MCR が取得する必要データは約 94 枚と予測できる．よって，提案モデルはクラウドモデルの 67%ほどの必要データを取得すると予測できる．実験では，上記の Wi-Fi の接続時間による必要データ減少を確認する．クラウドモデルが取得した必要データ 120 枚，MCR セントリックモデルでは 52 枚であった．よって，MCR セントリックモデルはクラウドモデルの 43%ほどの必要データを取得した．100%を下回るため Wi-Fi 接続時間によるデータ数の減少は確認できた．しかし，予測の 67%と大きな差があるため Wi-Fi 接続時間以外に MCR セントリックモデルにおいて必要データの取得を減少させる要因があると考えられる．この結果に最も影響を与えている要因の 1 つは，MCR で範囲を調整した擬似的な AP の精度の悪さであると考えられる．実装で使用した WAR は AP 範囲を調整する機能を搭載しておらず，AP 範囲を調整できる WAR を新たに導入するか，別の要素で補整する必要があった．本システムが実際に導入される際，全ての WAR が AP 範囲を調整する機能を持つとは限らず，WAR 以外の要素でこの問題を解決しなければならない．そのため，MCR で Wi-Fi 接続を切り替えることにより擬似的に半径 5m の AP を作成するという手法をとった．結果，今回の手法は MCR セントリックモデルの必要データ取得の確実性を欠いた．すなわち，WAR 以外の要素でこれを解決する新たな手法が必要である．

表 4 実装システムの設定条件

パラメータ	条件
見守り対象者人数	1人
見守り対象者端末(MCR)台数	1台
無線アクセスルータ(WAR)台数	1 台
アクセスポイント(AP)半径	5 m
カメラ台数	2 台
カメラ視野	60 °
カメラの撮影速度	5 fps
見守り対象者の歩行速度[2]	約 1.4 m/s

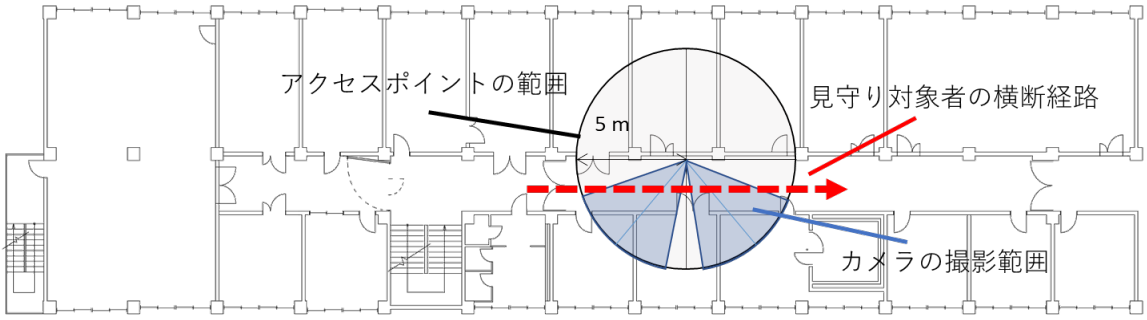

図 9 実験実施環境（小山高専 電気物質工学棟 2F）

2-4 実用化に向けた考察と課題

カメラ型見守りシステム実装において，MEC モデルに関わる諸課題は，主に情報管理機能に関するもので，特に課題となる利用者データ配備性は MEC サーバの十分なリソース配分と動的なデータ更新機構が備わっていれば解決できる．これらは 5G/MEC インフラ設備機能に強く依存するため，インフラを保持する通信キャリアが実装する場合では，この方式が選択肢になり得る．対して，MEC-MCR セントリックモデルは，カメラ機器と MEC サーバをつなぐアクセスネットワークを担う 5G/MEC インフラ部分と，アプリケーション機能への依存性が高い MCR およびサービス提供サーバ部分が機能分担されているため，通信キャリアをバックヤードに置く Business to Business to Consumer 型で実装する場合は特に有望である．

しかし，両方式においても，撮影データの解析などの主なデータ処理を担う十分な計算機リソースの確保が大きな課題となる．MEC サーバは基地局ごとの据え置き型である分，演算・電力リソースの面でやや有利だが，動的に変更されるサービス利用者数に応じた割り当てをする必要が生じるので，そのリソース割り当てのプロビジョニング手法が課題である．一方で，MEC-MCR セントリックモデルの計算機サーバである MCR はモバイル機器であるため演算能力や電力について大きな制限がある．特に，画像解析・認識処理などの負荷の高いプログラム処理を可能にする計算機リソースおよび電力源の確保は難しいため，この課題を解決するための電力性能比の高いハードウェアや効率的な処理アルゴリズムなどの実現が課題である．

また，実装を通したフィージビリティ実験から，既存の無線アクセスポイントの切り替え速度が大きな影響を及ぼすことが分かったため，この改善も課題である．この点については，本研究において有望なモデルとして評価された MEC-MCR セントリックモデルの実装によって，5G および MEC サーバの特徴である低遅延性，多接続性を導入できれば改善が期待できる．インフラ整備の観点も踏まえ，今後は 5G インフラを軸とした実証評価が必要である．

2-5 結論

本研究では，地産地消型ネットワークを用いたプライバシデータの流出を抑制した，新たな見守りシステムの検討を行った．そして，シミュレーション評価，定性評価，フィージビリティ評価を通して，5G によるエッジコンピューティングの機構を利用したカメラ型の広域見守りサービス実装方式が有望であることを示した．今後はこの方式に基づく MEC-MCR セントリックモデル実証システムの実装を推進し，その定量評価を行う．そして，より具体的かつ実践的なユースケースを元に社会実装を行っていく．

【参考文献】

[1] 干川尚人，下馬場朋禄，伊藤智義, “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”, 情報処理学会論文誌, Vol.59, No.12, 2180-2190, Dec. 2018.

[2] “AWS IoT Core features”, amazon.com Inc, https://aws.amazon.com/iot-core/features/（参照:12-24-2019）.

[3] “Internet of Things (IoT) technologies and solutions: PaaS and SaaS”, Microsoft Corporation, https://docs.microsoft.com/ja-jp/azure/iot-fundamentals/iot-services-and-technologies（参照:12-24-2019）.

[4] 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.

[5] 干川尚人“知っておきたいキーワード エッジコンピューティング”, 映像情報メディア学会誌, 73(4), 707-709, 2019 年 7 月.

[6] 柳生 理子, 高橋 雄一, 大谷 治之, “製造業における IoT の活用例と将来像-e-F@ctory を例として-”, 日本オペレーションズリサーチ学会 ORSJ, pp.205-209, Apr. 2018.

[7] Keisuke Komatsubara, Naoto Hoshikawa, Takashi Nishitsuji, Tomoyoshi Shimobaba and Tomoyoshi Ito, “Proposal of the Implementation of a Camera-Type Wide-Area Surveillance System that Suppresses the Flow of Irrelevant Private Data”, in Proc. 2019 Taiwan and Japan Conference on Circuits and Systems (TJCAS 2019 at Nikko), Japan, 4C-10, 19-21, August, 2019.

[8] ETSI, "MEC Deployments in 4G and Evolution Towards 5G", ETSI White Paper, No. 24 (2018), https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp24_MEC_deployment_in_4G_5G_FINAL.pdf
[9] 社会基盤情報流通推進協議会，人流解析チーム，“松江駅構内人流センサデータ”, https://www.geospatial.jp/gp_front/ （参照:6-25-2020）
[10] 田村 崚，干川 尚人，下馬場 朋禄，伊藤 智義 "多地点カメラを用いた見守りサービスにおける第三者のプライバシデータ流出比の定量評価"，電子情報通信学会，第 18 回ネットワークソフトウェア研究会，分散クラウドの実現に向けたネットワークソフトウェア技術＋一般, Jan, 2019
[11] ” 米 Verizon、1 週間前倒しで 5G サービス開始　韓国から世界初の座を奪う”, engadget 日本語版, 4-5, 2019, https://japanese.engadget.com/2019/04/04/verizon-5g-1/
[12] ” 20 年春 5G 開始　ドコモ・KDDI、5 年内で全国 9 割に”，日本経済新聞,4-10, 2019, https://www.nikkei.com/article/DGXMZO43552430Z00C19A4MM0000/

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
プライバシ情報の流出を抑制するカメラ型広域見守りシステムの提案	電子情報通信学会(IEICE) 通信ソサイエティ 第 19 回ネットワークソフトウェア研究会 Society5.0 に向けたネットワークソフトウェア＋一般, 03_05	2019 年 6 月 6 日
5G/MEC による個人情報の漏洩を抑制するカメラ型見守りシステムの提案	電子情報通信学会 信学技報, vol. 119, no 383, NS2019-162, pp. 7-12	2020 年 1 月 23 日