2020年代のモバイルコンピューティング
～新視点でのサイバーフィジカルシステム構成論の探究～

研究室紹介

山口弘純*

New Design Perspective for Human-Centered Cyber Physical System

Key Words：Cyber-Physical System, Artificial Intelligence, Privacy-by-Design

はじめに

筆者は2021年4月に大阪大学大学院情報科学研究科教授に就任し，モバイルコンピューティング講座という研究室を主宰する立場となった．2020年代という新たな時代を迎えて間もないタイミングでもあり，モバイル・パーベイシブコンピューティングとよばれる分野においてこれまで自身が実施してきた研究の方向性を改めて見つめなおすよい機会となった．

20年以上前の2000年代，モバイル・パーベイシブコンピューティングの分野においては，モバイル・ユビキタスな時代に向けて，モノや人をつなげて便利にするための方法論やシステムの探究が主要命題であった．私は学生であった1990年代に形式的技術に基づくプロトコル設計技術を専門としていたため，2000年代前半はその流れでアドホックネットワークや車車間・オーバレイネットワークなどのモバイル通信プロトコルの設計研究に従事した．一方，2010年代はスマートフォンを中心としたセンシングと通信の融合的かつ急速な発展により，センシングデータの取得・処理・解析に関する多様なアイディアが生み出された時代である．特に，実世界と仮想世界をカップリングし，モバイルコンピューティングで培われたセンシングや状況理解技術を駆使して実社会の課題解決に挑むサイバーフィジカルシステムの基礎概念や応用技術が多数創出された．同様に社会システムの情報化が一層進み，実世界データを扱う課題解決型の研究が一層重要視されるようになったのもこのころである．

2020年代もサイバーフィジカルシステムのコンセプトは引き続き重要視され，多くの社会情報システムはある意味ですでにサイバーフィジカルシステムであるといえる．しかし最近ではそれに加え，例えばChatGPTなど圧倒的な知識や能力を持つAIが実装されて利用されるようになり，社会に少なからぬ影響を与えるようになってきた．そういったAIはIoT機器から得られる大量のデータから意味を見出し，我々が気付かない知見や社会の効率化に向けた解を与えてくれる可能性もある．したがって，今後はAIに代表される機械と我々人間がどのように共存・共栄し，そのメリットを享受できるような社会情報システムを築けるかが重要になる．すなわちサイバーフィジカルシステムを設計する際に，そういったAIの効果や人間に与える影響，AIや人間をサイクルに含むシステムとその効率化，といった新しい視点を取り込むことが肝要であり，今後の研究者が取り組むべき大きな命題であると考える．機械が支援し人間が中心となる情報化社会における負の側面をできる限りなくすことで，Society5.0が目指す，社会のトランスフォーメーションが推進されると期待される．

本研究室ではそれらのコンセプトのもと，センシング，モデリング，状況理解，通信最適化，機械学習などを組み合わせた様々なサイバーフィジカルシステム設計論の研究開発に取り組んでいる．本稿では，科学技術振興機構（JST）の戦略的創造研究推進事業（CREST）の支援をうけて地域社会でAIやIoTデータを利活用する際のプライバシ問題を解決する情報流通基盤の設計に関する研究開発を中心に

* Hirozumi YAMAGUCHI
1971年7月生まれ
大阪大学大学院基礎工学研究科情報数理系専攻博士後期課程（1998年）
現在、大阪大学　大学院情報科学研究科情報ネットワーク学専攻　教授
博士（工学）
専門／モバイルコンピューティングと通信
TEL：06-6879-4555
E-mail：h-yamagu@ist.osaka-u.ac.jp

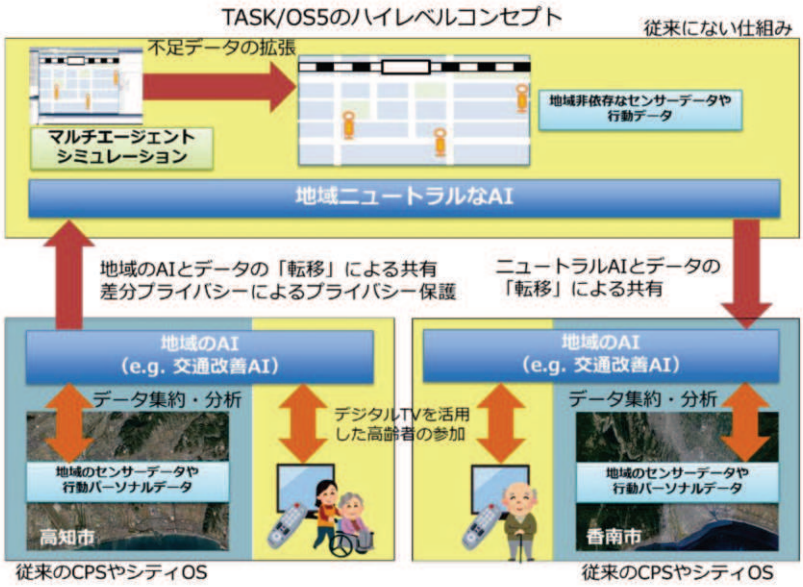

図1　知のデジタライゼーションの基本構想

紹介する．

地域を支える知のデジタライゼーションと共有基盤

JST CREST においては，文部科学省の選定した戦略目標「Society 5.0 時代の安心・安全・信頼を支える基盤ソフトウェア技術」に基づき，2021 年度に「基礎理論とシステム基盤技術の融合による Society 5.0 のための基盤ソフトウェアの創出」という新領域が発足した．日本が目指す Society 5.0 を実現するためには，IoT や AI を駆使し，人の幸福や Well-being，人間社会の高度化や成熟化のための新たな価値を生み出し，それらをデータや知として流通させることが求められる．しかしその一方で，セキュリティ・プライバシーリスクの増大が懸念されている．同領域では，その課題を解決し，原理的に安心・安全で信頼できるオープンな基盤ソフトウェアの創出を目標としている．

これに対し，本研究室が推進する課題「地域を支える知のデジタライゼーションと共有基盤」[1] では，2021 年 10 月～2027 年 3 月の 5 年 6 か月で，災害時避難支援 AI など，地域で開発される様々な AI を地域間でセキュアに共有し活用する情報基盤の実現に向けた研究を実施する．

大阪大学情報科学研究科の矢内直人准教授，人間科学研究科の稲場圭信教授，近畿大学経済学部の新井圭太准教授，および讀賣テレビ放送（株）の矢野 健太郎チーフ・エキスパートが参画し，文理融合的な視点も取り入れながら理論確立と実践的な実証を目指している．

サイバーフィジカルシステムでは，空間・人・モノの IoT/ センシングにより実世界をデジタル空間に再現し，AI で都市や地域の課題解決を図るスマートシティ OS の導入促進が期待されている．そういった AI，特に成功事例の AI は地域間で共有し，相互活用することで地域のインフラコストを下げることにつながるものの，AI を直接共有することにより個人情報やパーソナルデータを推測されるリスクが指摘されている．また地域社会は地形や人口・世帯分布などが多様であり，公共交通など社会サービスも地方自治体の規模や保有インフラなどで異なるため，ある地域のデータ集約・活用・解析型アプローチを他地域で単純に展開できない．スマートシティ OS が，データや AI を地域間の差異を超えてセキュアかつ安全に集約・転移・活用する機能を有し，高齢者がシステムに参加しやすい機能を実現すれば，それらの障壁を取り除き，地域社会の維持発展に大きく寄与できる．

これに対し，本研究では，地域社会の知をデジタライゼーションし，セキュアに共有するための S5 基盤ソフトウェア TASK/OS5（Transformation, Adaptation and Sharing of Knowledge for Open Society5.0）を開発している．キーコンセプトは，個々の地域で得られる「地域依存」のデータや機械学習モデルを「地域ニュートラル化」したデータや

図2　TASK/OS5のコンセプト

機械学習モデルに転移してから共有する点である（図1）．個人特定につながるリスクのある地域依存のモデルやデータが，地域ニュートラルモデルからは得られないことを形式的に示すことで，パーソナルデータを含むデータやモデルを安全に他地域に転移し活用する方法論を構成する．それらを実現するための都市OSであるTASK/OS5基盤を実装し，Society5.0の重点応用事例である地域交通改善や災害時支援の事例において，自治体と協力した実証実験を実施する（図2）．

同プロジェクトにおいては，まず地域ニュートラルという概念を明確化するため，介護タクシー配車システムの実データなどをもとに検討した．その結果，プライベートとすべき地域データは，ユーザ（居住者などの人間）の識別子に相当する情報，ユーザの属性に関する情報，ユーザやオブジェクト（車両）などの位置やトレースといった位置行動データ，およびPoI（Point of Interest）や具体的な地域名といった地理情報，などであると結論付けた．例えば，行動履歴はユーザの出発地点が高確率で自宅であると推定され，特定地点での滞在履歴が含まれれば，ユーザ間の関係性も類推される．地域名やPoIが暴露されれば，ジェンダー嗜好や既往症特定につながる滞在場所の特定も可能となり，行動履歴からの推定も可能となる．

ユーザ識別子や地域名はいわゆる匿名化で隠蔽できる．また，属性データについては属性名を隠蔽することも匿名化となり得る．位置行動データについては，純粋な位置情報や軌跡情報の匿名化アプローチは様々なプライバシーリスクモデルのもとで提案されている．いずれの方法においても，データそのものの特徴量がそのまま残されるため，匿名化が安全性につながる保証はない．しかし，そういった特徴量は人間の可読性・可用性の維持を意味するアプローチである点で極めて有用である．例えば匿名化したデータを用いたマルチエージェントシミュレーション等により，データを合成できる可能性がある．もう一つの方法は，データを別のデータに転移させる，いわゆる仮想化である．これについては安全かつ，利用者（ここではAI）にとってのデータの意味（特徴量）を損なわないマッピング関数を開発することが主題となる．ここでは，研究室で開発した仮想化の方法[2]について紹介する．

近年では例えばAI顔認識において，性別や年齢といった人間が理解できるプライバシー特徴量を希薄化し，一方でAIにはそれらが区別可能な特徴量を残す技術が敵対的生成ネットワークなどを用いて提案されつつある．このアイディアに基づき，データ利用者であるAIが元の地域データとの差異を区別不可能な合成地域データを生成するGANを活用するアプローチを採用した．具体的には，まずGPS座標や時刻，IDなどを含む軌跡データを，GANが扱いやすい統一した形式に変換する．例えばGPS座標は基準位置からの相対位置，時刻は曜日と24時間のタイムスロットで表現する．次に，GANの生成器を用いて合成軌跡を生成するため，GANを訓練し，入力軌跡のパターンを学習させる．この目的のため，生成された軌跡が本物か偽物かを

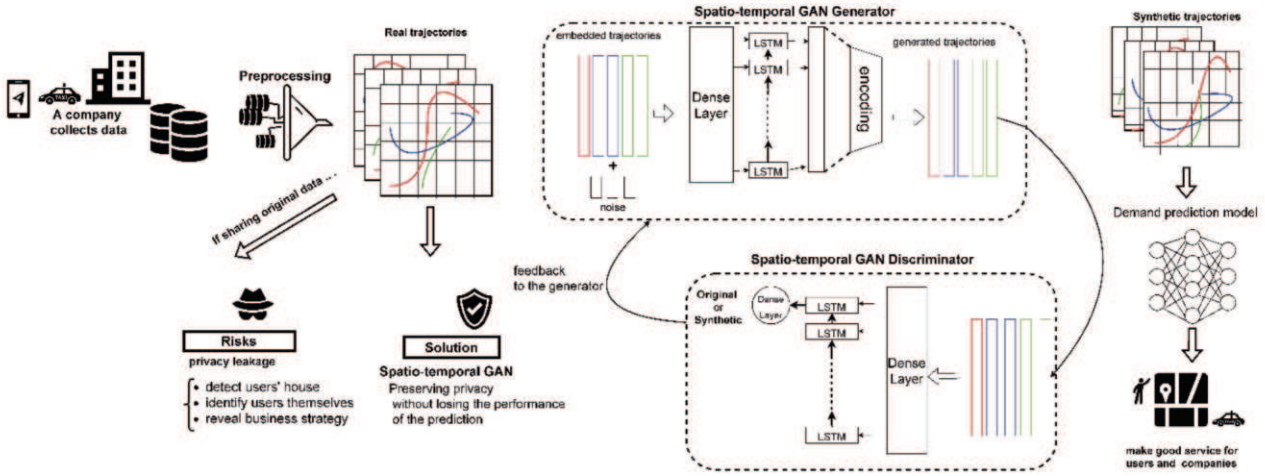

図3　プライバシー安全な移動軌跡の生成

識別する識別器とLSTMを組み合わせたネットワークを構成する．図3に上記手順の概略を示す．

合成された軌跡を用いて，軌跡の発生地点と時刻を予測する移動需要予測器を構成する．予測器のモデルとしてサポートベクターマシン（SVM），ランダムフォレスト（RF），XGBoost（XGB），フィードフォワードニューラルネットワーク（NN）を用いる．ここで，合成された軌跡（別の言い方では，ニュートラル化された軌跡）の集合を T_{synth} とし，これを用いて訓練される予測器を P_{synth} とする．P_{synth} が，元の軌跡集合（すなわちプライバシー機敏な情報）T_{priv} を用いて訓練された 移動需要予測器 P_{priv} に対し，どの程度の攻撃耐性を有し，かつどの程度の予測精度を達成するかが評価指標となる．

評価では約 30 km × 55 km の範囲の約 15,000 の実軌跡を T_{priv} とした．P_{priv} および P_{synth} のいずれも，元の軌跡集合 T_{priv} の部分集合を用いて予測した結果を評価している．その結果，合成軌跡集合 T_{synth} で学習した P_{synth} は，テスト対象である T_{priv} に対し，78.0% の精度で正しい移動需要を予測できた．P_{priv} は 81.2% であり，これはパーソナル情報を保護しながら移動需要予測精度の低下を最大でも 3.2 % に抑制できたことを意味する．この結果は，合成された T_{synth} がパーソナルデータなどの秘密情報を保持することなく元データ T_{priv} の意味的情報量を保持できていることを示唆する．

図4は元の軌跡データとGANによって生成された軌跡データを示したものである．図においては時刻は示していないが，GANが生成したデータは，

図4　元の軌跡データ（左）と合成された軌跡データ（右）

概ね元の軌跡の形状を維持しつつ，出発・到着位置のずれあるいは時刻のずれのいずれかを実現し，元データが推測されないようにしている．T_{priv} の軌跡の始点および終点と，それに対応する T_{synth} の軌跡のそれらとの差は，距離にして3〜4000m（多くの場合2000m），時間にして0〜5時間である．これにより，T_{priv} と T_{synth} のデータ間の不一致率は88%になり，最新のプライバシー保護手法より30%改善されている．さらに，メンバーシップ推論攻撃を施行する実験も行った．この攻撃は，学習データに含まれるデータを推測し漏えいさせることを目的とする．施行の結果，P_{synth} は最新のプライバシー保護手法で構成した移動需要予測器 $P_{geomask}$，および元データで学習した移動需要予測器 P_{priv} に対し，攻撃成功率をそれぞれ31.9%および11.0%低減させている．

この取り組みが地域多様性やプライバシーの垣根を越えてAIが共有され地域社会に貢献する未来を実現する取組みとなるよう，精力的に研究開発を進めていきたい．

おわりに

今回紹介したプロジェクトの他にもスマートシテ

ィ・スマートホーム，スマートビルディング[3]，高度交通システム，ヘルスケア，ユビキタスコンピューティングなどの分野における行動把握や状況理解，無線センシング，プライバシー保護，位置推定やエッジコンピューティングなどの技術の研究を実施している．ご興味のある方は研究室のWEBページ[4]をご覧いただきたい．

参考文献

1) 地域を支える知のデジタライゼーションと共有基盤
https://mc.net.ist.osaka-u.ac.jp/ja/projects/crest/

2) R. Ozeki, H. Yonekura, H. Rizk, and H. Yamaguchi, Sharing without caring: privacy protection of users' spatio-temporal data without compromise on utility. In Proc. of ACM SIGSPATIAL '22) pp.1−2

3) M. Ohno, R. Ukyo, T. Amano, H. Rizk and H. Yamaguchi, Privacy-preserving Pedestrian Tracking using Distributed 3D LiDARs, Proc. of IEEE PerCom2023, 9 pages, March 2023 (in press)

4) 大阪大学大学院情報科学研究科山口研究室
https://mc.net.ist.osaka-u.ac.jp/