〔短期在外研究〕

研　究　者	東京都市大学 講師　Surantha Nico	2246002
研究課題名	IoT ベースのヘルスケアシステムにおけるサイバーセキュリティの課題の緩和に関する研究	
共同研究者／所属，職名	Diep N. Nguyen/University of Technology Sydney, Associate Professor, Director of Transnational Education	
在留地域	シドニー/オーストラリア	
渡航期間	2024 年 7 月 24 日～2024 年 8 月 28 日（35 日間）	

［在外研究の目的・意義］

モノのインターネット（IoT），ウェアラブルセンサー，クラウドコンピューティング，人工知能の出現は，IoT ベースのヘルスケアシステムを構築する有望な機会を提供している。IoT ベースの医療システムは，社会に対する医療サービスの向上と医療費の削減を同時に実現できる。IoT は遠隔患者モニタリングと遠隔医療を可能にする。そのため，患者は自宅からケアにアクセスすることができ，通院や再入院の必要性を減らすことができる。また，自宅から患者データを定期的にモニタリングできるため，医師が記録されたデータを分析することで病気の診断に役立てることができる。

しかし，IoT ベースのヘルスケアは，環境の複雑さと配置されたデバイスの性質により，いくつかのセキュリティ問題に悩まされている。この IoT システムは，データの完全性，ユーザーの機密性，サービスの可用性といったサイバーセキュリティの問題に対して脆弱である。そのため，IoT を利用した医療システムを商業的に開始する前に，そのセキュリティを管理することが非常に重要である。セキュリティ対策は，無線ネットワークを介したデータ伝送とクラウド・コンピューティング・インフラストラクチャへのデータ保存において必要である。患者の個人データや健康データへの不正アクセスを防止することが重要である。

この共同研究では，IoT ベースのヘルスケアシステムにおけるサイバーセキュリティの課題を軽減することを提案する。この研究では，サイバーセキュリティと通信ネットワークの専門知識を持つ Diep N. Nguyen（University of Technology Sydney, Australia）と協力し，安全で信頼性の高い IoT ベースのヘルスケアシステムを提案。

［得られた成果・効果と今後の発展性］

以前，我々はデータの処理と保存にクラウド・コンピューティングを利用した健康モニタリング・システムを開発した。しかし，このような実装は信頼できるネットワーク状況に大きく依存する。ネットワーク接続の信頼性が大都市ほど高くない地方で実装する場合，問題となる。本研究では，ハイブリッド・エッジとクラウド・コンピューティングを用いた健康モニタリング・システムを開発した。ハイブリッド・エッジとクラウド・コンピューティング・システムに関する我々の成果は，メルボルンで開催された 2024 IEEE Annual Congress on Artificial Intelligence ofThings（IEEE AIoT）で発表された。

University of Technology Sydney を訪問した際，ディエップ・グエン教授（Prof. DiepNguyen）とハイブリッド・エッジ・クラウド・ヘルス・モニタリングのセキュリティ方法について議論した。その一つが，Federated Learning（FL）についてのアイデアだ。FL は，ウェアラブルセンサーを使った健康モニタリングにおける新たなパラダイムであり，機密性の高い健康データを一元管理することなく機械学習モデルの開発を可能にする。統合学習の実装を図 1 に示す。

このアプローチでは，データは個々のデバイスに残り，ローカルでトレーニングされたモデルの更新のみが中央サーバーと共有される。これらの更新はグローバルモデルを作成するために集約され，ユーザーのウェアラブルデバイス上で生データを安全に保つことでプライバシーを確保する。FL は，個人の健康情報の保護と，異なるデバイス間でのデータの不均一性の克服という 2 つの課題に対処するため，ウェアラブルセンサーに特に適している。この分散型アプローチは，データ漏洩に関連するリスクを低減し，General Data Protection Regulation（GDPR）や Health Insurance Portability and Accountability Act（HIPAA）などの厳格なプライバシー規制に準拠している。

ヘルスモニタリングの場合，FL は，ウェアラブルがプライバシーを損なうことなく連携できるようにすることで，パーソナライズされた健康推奨と早期異常検知をサポートする。このトピックに関する今後の研究としては，リソースに制約のあるデバイスに対する FL の最適化，軽量アルゴリズム，通信効率，敵対的攻撃に対するセキュリティに焦点を当てるなど，いくつかの具体的なトピックに取り組むことができる。さらに，差分プライバシーやセキュアなマルチパーティ計算などのプライバシー保護技術と FL を統合することで，FL の堅牢性が向上する。FL は，ウェアラブルセンサーのエコシステムを強化し，ユーザーのプライバシーを尊重しながら，多様で分散したデータセットから学習し，ヘルスケアを改善するためのスケーラブルなソリューションを提供する。

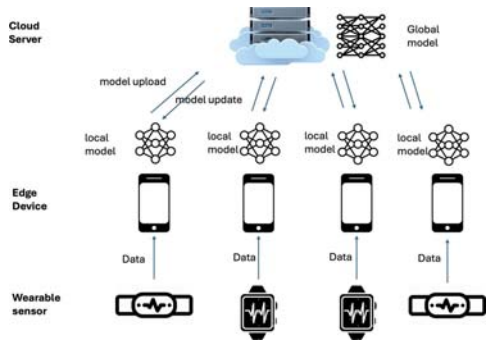

図 1　ベースのヘルスケアシステムのための Federated Learning（FL）の実装