論 文 内 容 の 要 旨

博士論文題目　A Study on Adaptive and Robust Privacy-Enhancing Technologies for Spatio-Temporal Data Aggregation

氏　名　　笹田 大翔

（論文内容の要旨）

時空間データは都市計画、流行病学、自然災害管理など、さまざまな目的で利用されているが、収集されたデータから個人の居住地や職場などの機密情報が漏洩するリスクがある。ローカル差分プライバシ（LDP）に基づくデータ収集は、機密情報を保護する有望な手法であり、データの各位置を他と区別できないように修正することでプライバシを保護する。しかし、LDP を時空間データに適用すると、データ価値またはプライバシ保護のいずれかを損なうことがある。LDP では、データストア（データ収集者）は、全データセットの分布に基づいてプライバシ保護の強度を決定する必要があるが、時空間データは場所や時間によって異なる分布になっており、データの特性も時間経過で変化する。加えて、データ所有者は自らのデータに対する様々なプライバシ選好を持っているが、LDP では均一な保護強度でデータを修正する。さらに異なるドメインのデータと結合すると分析結果に対する参照透過性を保証できず、そのため、結果の歪曲がノイズまたは LDP 処理に起因するか不明確にする。

これらの問題に対して、本論文は、複数のプライバシ強化技術を併用するこれらの問題を解決する。データ価値の保存に向けて、類似の特性を持つデータ所有者をクラスタリングして類似のクラスタに保護強度を割り当て、各クラスタ内でノイズを追加することで、クラスタ間の特性を保持しながらクラスタ内で非識別化する。次に、プライバシ選好の問題に対処するために、統計的特性をデータ量から分離するための空間・時間データの収集方法を導入する。紛失通信プロトコル上でLDPを実装することで、統計的特性のみを分離的に収集する。最後に、参照透過性に処理するためのプライバシ保護データ集約を設計する。LDP はさまざまな組織間の分析に適していないため、この方法は LDP なしで LDP と同じ信頼モデルを達成する。具体的には、セントラル差分プライバシと準同型暗号を組み合わせ、データの暗号化を維持しながら範囲計数処理を実行する。時空間データのプライバシ保護における三つの問題を解決することで、時空間データ集約のための適応的かつ強力なプライバシ強化技術を達成した。

氏 名	笹田 大翔

（論文審査結果の要旨）

本研究は、時空間データにおけるプライバシ保護に向けてローカル差分プライバシ（LDP）適用で生じる課題を解決する手法を提案している。具体的には、プライバシモデルの拡張、プライバシ選好への適応、データ結合における参照透過性の保証を行い、適応的かつ頑強なプライバシ強化技術を実現している。これによりデータ価値保存とプライバシ保護を両立しており、時空間データの安全な利活用促進において重要な研究となる。本論文の主な成果は、以下に要約される。

1. 従来の LDP では、全データセットの分布に基づいて一律のプライバシ保護強度を決定する必要があった。本研究では、データ所有者のもつ位置・軌跡の分布に基づいて保護強度を分割し、それぞれのクラスタに適切な保護強度を割り当てることで、分散的なプライバシ保護を実現している。研究内容は国際会議で発表されており、実社会での応用が期待できる。

2. 本研究は、データ所有者のプライバシ選好に適応する方法を提案した。従来の LDP では、一律の保護強度が必要であったため、異なるプライバシ選好に合わせることが困難であり、データ増幅や改ざんといった攻撃の動機を誘発させていた。これに対して本研究では、統計的特性をデータ量から分離する手法を導入することで、データ増幅や改ざんにかかわらず時空間データを安全に収集可能な方式を実現させた。

3. 本研究は、異なる組織間でのデータ集約におけるプライバシの問題を解決する新しい集約法を提案している。従来の LDP では、異なるドメインのデータと結合する際に生じる分析結果の歪曲が問題であったが、提案集約法では、準同型暗号を組み合わせることで各組織のデータプライバシ保護を維持しつつ、異なる組織間での範囲計数処理を実行可能にしている。非時空間データにおいて時間的・空間的な情報価値をもたらすことができるため、この研究の貢献は大きい。

以上のように、本論文は高いデータ価値保存・プライバシ保護を両立可能な時空間データ収集の実現に大きく貢献している。それぞれの成果は1編の学術論文と4編の査読付き国際会議論文として発表されており、研究成果の有効性を見ることができる。よって本論文は、博士（工学）の学位論文としての価値があるものと認める。