博士論文を要約したもの

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

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，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(CDP)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．