7X-05

タクシーデータの保護と利活用に関する考察

橋本　真†　　土井　洋†

情報セキュリティ大学院大学　情報セキュリティ研究科†

1. はじめに

近年，インターネット上で様々な分野のデータ検索システム等が開発され，情報を提供している．一方，交通手段としてタクシーはよく使われており，タクシーから得られる様々なデータを活用することは有益である．平成 26 年国土交通省の調査では，タクシー業界で中小企業が多く，全事業者数の 8 割以上が個人タクシーである．本稿ではタクシーをモデルとして，タクシー利用者の個人情報やタクシー業者の企業秘密を守りながら，タクシー・データの活用システムについて基礎的な検討結果を示す.

2. システムの構造

タクシーは非常に魅力的なデータ発生源と考えられる．まず，タクシーは移動体なので位置情報を扱うことができ，移動体通信も可能である．乗車・下車する時の位置，時刻等の統計情報を安全に提供することは有益と考えられる.

タクシーに必ず設置されているデータ発生源はタクシー・メーターである．タクシーが走る時のタイヤの回転数が電気信号のパルスに変換され，メーターに入力される．メーターがこれらの信号を用いて走行距離(走行距離データ)を計算する．それを元に運賃が計算・決済され，レシートが印字される．また，これらのデータがネットワークを経由し，遠方のシステムに伝送され，集計されることも可能である.

タクシーに関してもう一つ重要な装置は GPS である．GPS を用いることで，タクシーの位置(GPS 位置データ)を把握することができる．タクシーを管理する上で非常に便利な装置であり，タクシー・メーターに直接接続し，標準搭載される場合もある.

本稿では，タクシー利用者が乗車・下車する時の時刻データ，GPS 位置データ，そして走行距離データを収集する．位置情報はタクシー利用者の自宅位置や勤め先の場所を示す可能性があり，その取り扱いには注意を払う必要がある．また，位置情報・走行距離はタクシー会社の営業活動範囲や売上に繋がる可能性があるので，安心してデータを提供してもらえるような仕組みが必要である．本稿では，タクシー・メーターで発生する走行距離（計量データ）に焦点を当てて，タクシー利用者の個人情報やタクシー業者の企業秘密を守るため，適切な処理を行い，統計情報を提供するシステムについて検討する.

3. 法律上の諸要求

3.1 計量法との関係

日本では計量法（平成４年法律第５１号）があり，計量の基準を定め，適正な計量の実施を確保し，経済の発展及び文化の向上に寄与することを目的としている.

タクシーではメーターがタクシーの走行距離を計量し，それを根拠に乗客に料金を請求しているので，計量法の対象となる．メーターは法律の要求通りに設計・製造・検査・型式申請されなければならない．また，メーターが適正に動作しているかを確認するために年一回，装置検査を受ける必要がある．なお，タクシー・メーターの性能と器差に影響を与えるパラメータやプログラムはメーター内部にあり，メーターを封印する必要がある．つまり，これらのプログラムは耐タンパー性を有する装置内で動作するとみなすことができる.

3.2 個人情報保護法との関係

表１ － 個人情報保護法の経緯とポイント

経緯	ポイント
2003 年 5 月制定	2005 年 4 月に全面施行.
2015 年 9 月改正	個人情報保護委員会の新設 匿名加工情報の導入
2020 年 5 月	仮名加工情報の導入

表 1 に示す匿名加工情報や仮名加工情報は，比較的最近導入されたものであり，個人情報ではない．匿名加工情報は本人の同意がなくても第三者への提供が可能であるが，仮名加工情報の第三者提供は基本的にできない.

一方，適切に加工された統計情報は，個人情報にも匿名加工情報にも該当しないものである．但し，統計情報という形になっていればよいと

A study on how to protect and use taxi data
† Shin Hashimoto, Hiroshi Doi,
Institute of Information Security

Copyright ©2022 Information Processing Society of Japan.
All Rights Reserved.

いうものではなく，個人との対応関係が十分に排斥できるような形で統計化されていることが重要である．また，個人履歴情報に含まれる位置情報（緯度，経度情報）の扱いには配慮が必要である[1]．

アメリカニューヨーク市では New York City (NYC) taxi trips data set という公開データセットがある．それには NYC のすべてのタクシー運用記録を含まれている．[2]によれば，ナンバープレート番号の加工に不適切なハッシュ値を用いたことにより，すべてのナンバープレート番号が復元された．ドライバの個人情報が漏洩され，彼らの収入も簡単に抽出された．

本稿のシステムで収集するデータ（走行距離や乗車下車時の GPS 位置）は，個人を特定できるクレジットカード番号などは含まれないので，一見個人情報とは無関係に見える．しかし，サンプリング数が極端に少ない場合，その他の情報と組み合わせて，結果的に個人を特定できる可能性がある．そのため，データを第三者に提供する前に適切に加工する必要がある．

4. 技術面からの検討

ここまでの議論を基に，タクシー利用者の個人情報やタクシー業者の企業秘密を守りながら，タクシー・データを処理・活用システム(図 1)について検討する．

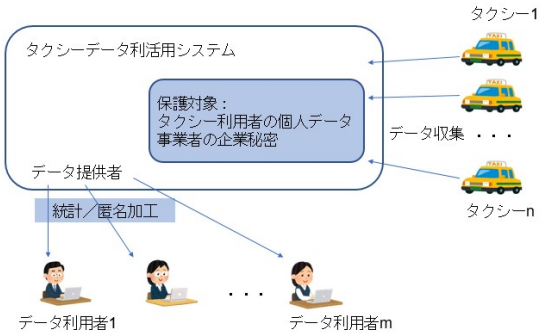

図 1 - 利活用システムの概念図

4.1 通信データの守秘と認証

無線通信の内容の第三者への漏洩を防ぐため，守秘技術(公開鍵暗号等)を利用し，メーターとシステム間で安全な通信を確立する．そのため，（耐タンパー性を有する）タクシー・メーター内部に秘密鍵や公開鍵を設定する．その後，双方が暗号化通信を行う．

4.2 秘密計算の導入

様々なタクシー業者がシステムに参加できるように，提案するシステムでは秘密計算の導入を試みる．その前段としての秘密分散法としては，(2,3)秘密分散法を用いる．システム内にサーバを 3 台設けるが，1 台のサーバでは秘密の復元はできず，2 台のサーバが協力して秘密を復元できるようにする．秘密分散技術は国際基準（ISO/IEC 19592-2:2017）によって標準化されている．

秘密計算では理論上，加算と乗算ができれば，任意の計算が組み合わせることによってできる．秘密計算は通常の計算より遥かに複雑であるが，近年実用できるレベルまで発展してきた[3][1]．これらは(2,3)秘密分散法を用いる．秘密計算を用いることで，統計データのみを出力することが可能となり，タクシー業者の企業秘密を守りつつ，タクシー・データの活用システムを用いることが可能となる．

4.3 匿名加工の実施

個人情報保護委員会[1]は，匿名加工についての具体例をいくつか示している．例えば，ID の場合，ハッシュ関数を利用して ID を置き換える．車の移動履歴の場合，始点・終点から数%の位置情報を削除するようにするなどである．本稿のシステムでは，タクシー・データを第三者に提供する前に，このような匿名加工を行う必要がある．

5. 今後の課題

タクシー業界では中小規模の事業者，特に個人タクシーが多いのが特徴である．個人タクシーの事業者に本システムに参加する場合の，データの取り扱い方法等について，法制度と技術の両面から検討を継続したい．

謝辞

本研究の一部は JSPS 科研費 JP18K11306 の助成を受けたものである．

参考文献

[1] 個人情報保護委員会，匿名加工情報－パーソナルデータの利活用促進と消費者の信頼性確保の両立に向けて (2017)

[2] Dan Goodin, ″Poorly anonymized logs reveal NYC cab drivers' detailed whereabouts.″ Ars Technica (2014).

[3] 菊池亮，五十嵐大，秘密計算の発展－データを隠しつつ計算する仕組みとその発展,電子情報通信学会 基礎・境界ソサイエティ Fundamentals Review,12 巻 1 号 (2018).

[4] 千田浩司，五十嵐大，濱田浩気，高橋克巳，エラー検出可能な軽量３パーティ秘匿関数計算の提案と実装評価，情報処理学会論文誌 Vol.52, No.9, pp.2674-2685 (2011).

Copyright ©2022 Information Processing Society of Japan.
All Rights Reserved.