データ活用次の一手

～差分プライバシーで攻めのプライバシー保護を～

株式会社第一生命経済研究所　客員研究員　水谷　俊光
（第一生命情報システム株式会社　デジタル推進部所属）

（要旨）

○　データ流通量の増大に伴うプライバシーリスクの増加と、人々のプライバシーへの関心が高まる中、企業は安全にデータを利活用することが求められる。

○　上記の背景から、データを安全に利活用するための技術群が台頭してきており、その中でも統計データを安全に外部公開するための技術である差分プライバシーが注目を集めている。

○　統計データは個人単位の情報を持たないため一見プライバシーのリスクはないように見えるが、条件が揃うと個人情報を逆算される弱点を持つことが知られている。差分プライバシーは統計データに加工を施すことにより、個人情報を逆算されるリスクを低減することができる。

○　更に差分プライバシーは従来のプライバシー保護技術にない、さまざまな攻撃手法に耐えうる性質を持っている。この性質を持つことから、2020 年、米国におけるプライバシー要件の高い国勢調査の結果を公表する際に適用された事例がある。

○　今後、差分プライバシーはプライバシー保護の文脈から社会実装が進んでいくことが予想される。差分プライバシーを含むプライバシー強化技術についての見識を深め、適切な技術選定によりデータを安全に利活用することができれば、企業はデータ活用の幅をより一層広げていくことが可能となるだろう。

1.　求められるデータ利活用の安全性

近年、データは現代における石油と喩えられ、データの利活用が企業における競争力の源泉となっている。スマートフォンや IoT デバイスの普及に伴うデータ量の増加と、AI やデータ分析技術の発展の両輪が噛み合うことによりデータの重要性は今後も増していく。

企業には競争力強化のためにデータを収集し、活用したいというモチベーションが存在し、消費者からもデータを活用した利便性の高いサービスが求められている。

その一方で、人々のプライバシーに関する意識は年々高まっており、企業は消費者のデータプライバシーを適切に保護管理することが求められる。EU における GDPR（注

1）の施行や日本における度重なる個人情報保護法の改正もこうした背景に起因している（資料 1）。

資料 1 日本・欧州における法規制の動向

（出所）筆者作成

企業におけるデータ利活用と消費者のプライバシー保護の文脈は一見相反しているように見えるが、この二つは大きなムーブメントとなっており、いずれも後戻りすることはない。企業は消費者のプライバシーに最大限配慮しながら安全にデータを利活用することが今後より一層求められることとなる。

日本では本人への十分な説明がないまま、内定辞退率や交通系 IC カードの乗車履歴などのプライバシー情報を第三者提供した事例がある。このような、データの目的外利用や漏えいなどのプライバシーに係る問題を起こした場合、一時的に非難が集まるだけでなく、消費者からの信頼を回復するために長い時間と大きな労力が必要となる。

こうした問題を避け、適切にデータを利活用するためのプライバシーに関する新技術が台頭しており、プライバシー強化技術（Privacy Enhancing Technologies：PETs）と称されている。本ジャーナルではプライバシー強化技術の中から、従来のプライバシー保護技術にない強力な性質を持つ差分プライバシーという技術を紹介したい。

2. 従来のプライバシー保護技術の限界

個人のプライバシー情報を割り出そうとする攻撃者はさまざまな手法を用いるが、従来のプライバシー保護技術は特定の攻撃に対する安全性を保証するものであり、新しい攻撃手法が生み出された場合は場当たり的な対処が要求される。

個人単位のデータのプライバシーを保護する手法である仮名化・匿名化を例に説明しよう。仮名化・匿名化は個人の識別子（注 2）を削除することによりプライバシーを保護する手法だが、準識別子（注 3）に特徴的な情報が残った場合は個人の特定リスクが残る。これに対処する方法として、K-匿名化（注 4）という技術を用いることで、同じ準識別子を含むデータを複製し、個人の特定を困難にできる。しかし、K-匿

名化を使った場合も準識別子に属さない病名などの機微情報は推定できてしまうなどの弱点があり、これに対処することはできない。

具体的な例を上げて説明しよう。資料 2 の例では、匿名加工したとしても身長が特長的であり、特定のリスクの残る 2 番目の個人の身長を K-匿名化により 180cm 以上とし、個人を一意に特定することを不可能としている。一方、個人は特定できなくとも身長 180cm 以上の人が膵臓がんを既往症に持つことは知られてしまうこととなり、機微情報を推定されるリスクが残る。

資料 2 K-匿名化のイメージ

＜匿名加工データ＞

氏名（識別子）	身長（準識別子）	既往症（機微情報）
第一 太郎	180cm	膵臓がん
第一 二郎	232cm	膵臓がん
第一 三郎	175cm	なし

＜K匿名化データ＞

氏名（識別子）	身長（準識別子）	既往症（機微情報）
第一 太郎	180cm以上	膵臓がん
第一 二郎	180cm以上	膵臓がん
第一 三郎	170~179cm	なし

（出所）筆者作成

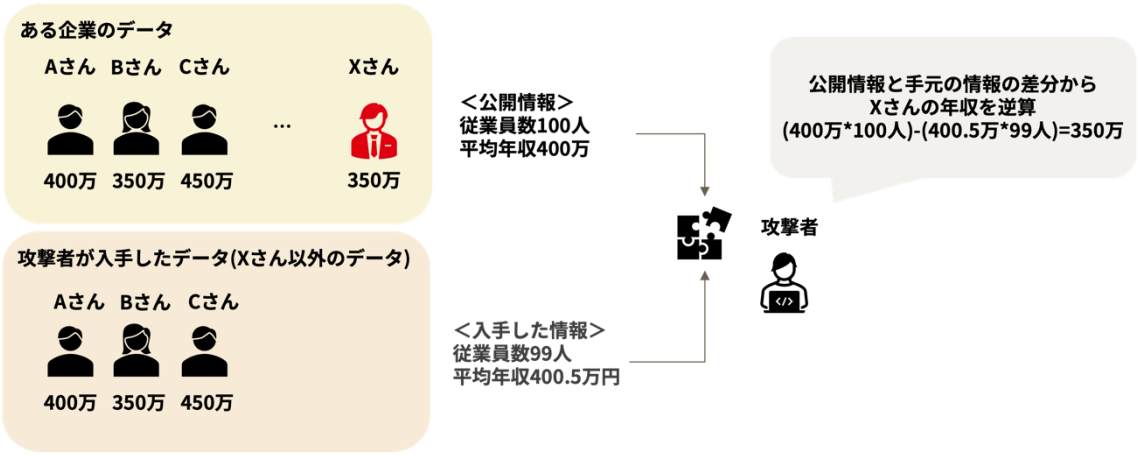
このように、K-匿名化のような従来のプライバシー保護技術は、ある特定の弱点に対する防御策であり、想定されていない他の弱点には対応できない。これを攻撃モデルに依存している状態と呼び、新たな弱点が判明した時点で別の手法により対処を行うといった後追いのプライバシー対策をすることになる。これでは攻撃者とのイタチごっこが延々に繰り返されてしまう。

3. 差分プライバシーの概要

差分プライバシーとは、平均や中央値などの統計データに対してノイズ（注 5）を加えることで、同じような有用性を持つ統計データを出力しながらも、統計データのもとになる個人に関する情報の逆算を困難にする技術である。

データを統計データとして公開する場合、個人単位の情報が集約されるため、一見プライバシーのリスクが低く見えるがそうではない。公開されているデータと攻撃者の手元にあるデータの突き合わせにより、プライバシー情報が漏えいするケースが存在する。ある企業が単純な統計データとして平均年収を公開しており、攻撃者が情報を取得したいターゲット以外の統計データを入手できた場合（注 6）を想定しよう。この場合、攻撃者は公開情報と手元のデータセットの統計データの差分からターゲットの年収というプライバシー情報をいとも簡単に特定することができてしまう（資料 3）。

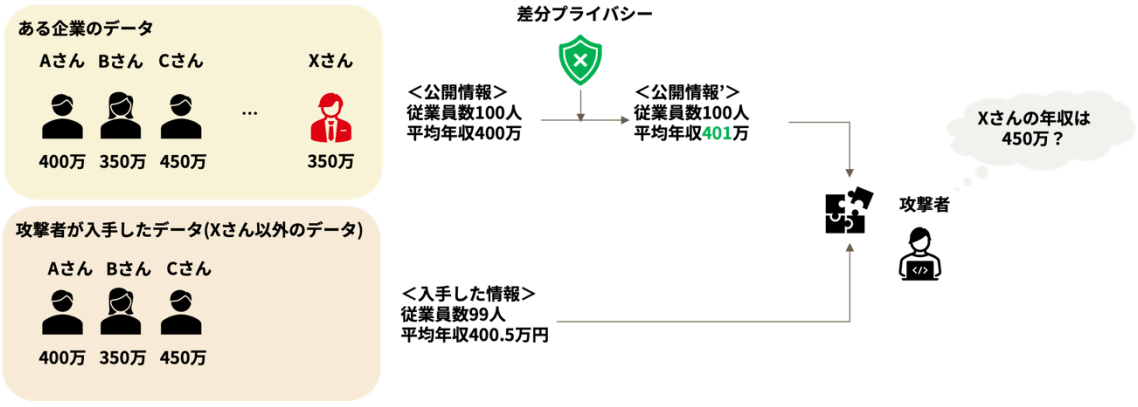
資料 3 統計量公開の弱点



（出所）筆者作成

差分プライバシーは出力のデータにプライバシーを保護するためのノイズを加えることにより、その名の通り統計データの差分から個人の情報を逆算する攻撃を困難にする。公開する統計データが差分プライバシー適用済みであると宣言することにより、攻撃者はターゲットの情報の真の値にたどり着くことが困難になるため、攻撃のモチベーションも削ぐことが可能となる。

資料 4 差分プライバシーのイメージ



（出所）筆者作成

資料 4 のケースでは、統計データである平均年収にノイズを加えることにより、攻撃者からターゲットが知られたくない年収の真の値を秘匿することが可能だ。1 万円というわずかなノイズだが、差分から算出したターゲット年収の真の値は 100 万円ずれることとなり、プライバシーが十分に保護される。また、母集団が大きい場合はさ

らに微量なノイズであっても同等のプライバシーを確保することが可能となる。

差分プライバシーは統計データにノイズを加えることにより安全性を向上させる技術だが、ノイズを加えるということは元の統計データとの誤差が発生する分、有用性が低下するということでもある。実業務に適用する場合はこのトレードオフの調整を、有用性が失われることに配慮しながら、データそのものが持つプライバシーリスクや公開範囲によるリスクなどを踏まえて適切に行う必要がある。

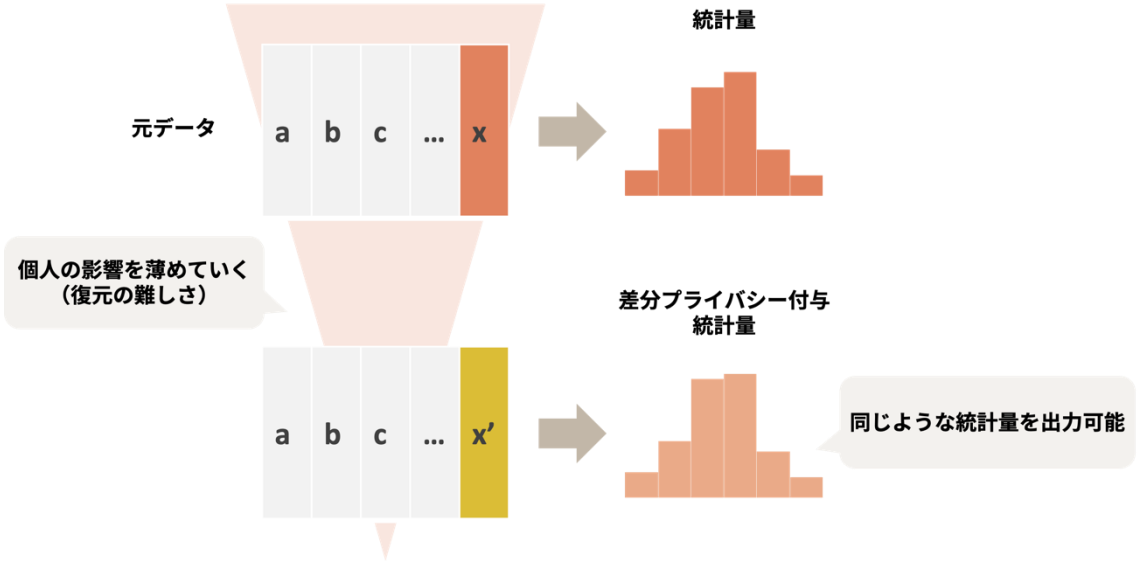
4. 差分プライバシーの特性

差分プライバシーが求められる背景には、昨今のデータ量の増加に加え、コンピューター処理能力の向上が挙げられる。これにより、今までは難しかった複数のデータの重ね合わせにより、個人のプライバシー情報を復元するデータベース再構築攻撃が現実的になっているなど、データを悪用しようとする攻撃者有利な状況になっている。

2 章で述べた通り、従来のプライバシー保護技術は特定の攻撃に対する安全性を保証するものであったが、差分プライバシーは攻撃モデルに依存しない安全性を持ち、データベース再構築攻撃も含めた任意の攻撃に対する安全性を保証することができる。

その要因は、差分プライバシーの本質がキーとなっている。差分プライバシーの本質は、“ある個人がいない場合でも同じような統計データを出力すること”であり、有用性が保たれる範囲で個人の影響を薄めることを目標としている（資料 5）。

資料 5 差分プライバシーの概念



（出所）筆者作成

差分プライバシー適用後の統計データは、攻撃者が個人の情報を逆算しようとしてもその確証を得ることができない。つまり、他のデータと重ね合わせること自体が無

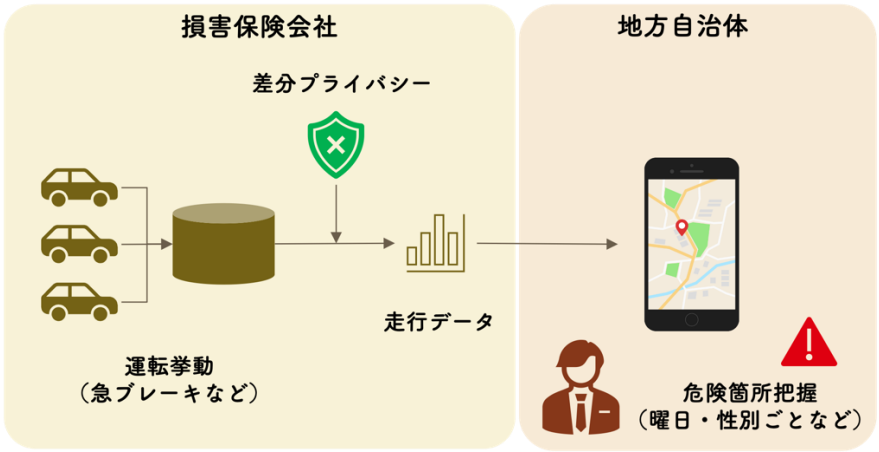
意味となるため、データが大量に出回っている昨今であっても攻撃者が保有するデータに依存しない安全性を保証できるのだ。さらにこの安全性は、差分プライバシー適用後の統計データそのものが持つ、情報復元の難しさを指標にした安全性であり、特定の攻撃に対する安全性ではない。以上が、差分プライバシーが攻撃者が保有するデータと攻撃手法に依存しない安全性を持つとされるゆえんである。特定の攻撃から守るために場当たり的な対策を行わざるを得なかった従来のプライバシー保護技術と比較して、これがいかに強力な性質であるかがわかるだろう。差分プライバシーは、攻撃者とのイタチごっこを終わらせる可能性を秘めている。

5. 差分プライバシーの事例と活用方法

差分プライバシーは、巨大 IT 企業や政府機関などで実例があり、2020 年の米国における国勢調査公表には差分プライバシーが用いられた。国勢調査局には人種や民族などの重大なプライバシーを保護しながらも、正確な人口統計データを提供しなければならないという二律背反する要件があったが、差分プライバシーによりこれを実現している。

日本においても、大手損害保険会社にて自動車走行データに差分プライバシーを用いた事例が存在する。同社はこれまでも運転挙動を分析して、地方自治体への提供を行っていたが、これを曜日や性別などの詳細な属性での分析を可能とするために差分プライバシーを用いた。詳細な情報を活用することで、個人の居場所や行動履歴などが読み取られるリスクを守っている。この事例では、曜日や性別などのメッシュごとの傾向がわかれば良いため、指標の有用性を傾向がつかめる範囲とし、分析への影響が出ない範囲でプライバシーの度合いを調整したという（資料 6）。

資料 6 差分プライバシーの活用イメージ



（出所）PRTIMES のプレスリリースより筆者作成

差分プライバシーは平たく言ってしまえば「データを外部に安全に公開するための技術」であるが、外部とは必ずしも社外とは限らない。社内においても、プライバシー性が高く、他部門にすら公開することが難しいデータに差分プライバシーを用いることで､専門組織のリソースや他部門のデータと合わせての分析が可能となるだろう。

近年では情報漏えいなどの事故そのものではなく、管理体制の不備なども GDPR の制裁対象になるなど、社内におけるデータの取扱も厳格化されている。社内におけるデータ分析であってもデータサイエンティストがプライバシー情報に触れることがないように、差分プライバシーを用いて分析することが当たり前になる未来があるかもしれない。

6. 差分プライバシーの今後

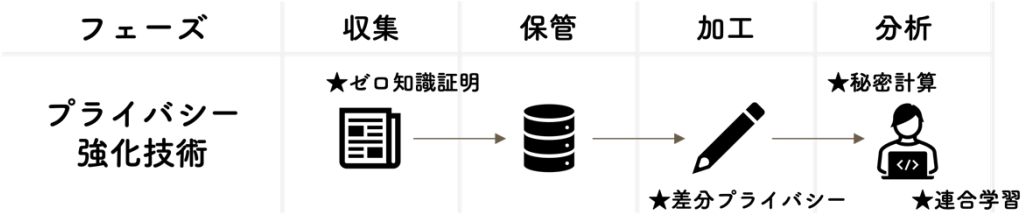
5 章で事例を挙げたが、差分プライバシーは現状ほとんどが実証実験レベルのものであり、一般企業への普及にはまだ時間がかかるだろう。Gartner 社のレポートにおいても差分プライバシーは黎明期と位置づけられており、普及までに 5～10 年を要するとされている。

差分プライバシーは統計データのプライバシーをより強固にする技術であるため、プライバシー要件の高いデータの主な特徴や傾向などの外観を分析したい場合などに適すると考えられる。逆に、単純な匿名化で要件を満たすようなプライバシー要件の低いデータや、個人単位で細かい分析をしたい場合などには適さない。このように、すべてのデータが差分プライバシーに適するわけではないため、実証実験フェーズを経ることで、適用範囲が明確になっていくだろう。

また、この手の技術は、さまざまな分析基盤やソリューションに標準搭載されるなど、誰もが手軽に利用できるようになって初めて普及してきたと言えるが、現状は差分プライバシーに精通したベンダーやエンジニアのみが触れる技術である。スタートアップ企業を中心に、分析機能も一体となった差分プライバシーソリューションが提供され始めているが、このような適用のハードルを下げるソリューションが開発されることも普及に向けた要件の一つとなるだろう。

最後に、差分プライバシーは未知の攻撃にも耐えうる安全性を持つ技術であるが、それだけですべてのプライバシーの問題を解決できるわけではない。差分プライバシーの適用領域外のプライバシーに関しては、他の技術と合わせて複合的に保護していく必要がある。企業においては秘密計算（注 7）なども含めて技術や適用領域の選定を行うスキルが求められる（資料 7)。

資料 7 プライバシー強化技術の適用領域



（出所）筆者作成

プライバシー強化技術はプライバシー保護の潮流を乗りこなし、データの活用を推進していくための強力な武器となる。これを使いこなすことができれば、企業のデータ利活用には確実な追い風となる。プライバシーの問題に尻込みして歩みを止めるのではなく、消費者に安心を与えるために使いこなすという目線を持ってプライバシー強化技術についての理解を深めていくべきだろう。

以　上

【注釈】

1) General Data Protection Regulation：一般データ保護規則。EU 域内の個人データ保護を規定する法として、「EU データ保護指令(Data Protection Directive 95)」に代わり、2018 年 5 月 25 日に施行された。
2) 個人 ID、氏名、生年月日など、データに係る個人を一意に識別するための情報。
3) 年齢や住所などの複数の属性値を組み合わせることで個人を一意に識別できる可能性が高い情報。
4) ある属性で絞り込んだときのレコードが 1 つにならないようにデータを加工することにより、個人の特定を困難にする技術。
5) 一般的には、雑音、耳障りな音といった意味。 統計学でいうノイズもこれに近い意味で、データとは関係のない誤差、ばらつきを意味する。
6) 攻撃者はターゲットの情報を抽出するために、事前に入手した属性の情報などを組み合わせ、条件を変えて複数回のクエリを実行し、ターゲットが含まれるデータセットとそうでないデータセットの入手を試みる。
7) データを暗号化したまま処理する技術。筆者レポート「秘密計算技術の活用」(2021 年 10 月）を参照（https://www.dlri.co.jp/report/ld/174276.html)。

【参考文献】

- 佐久間 淳, データ解析におけるプライバシー保護 (機械学習プロフェッショナルシリーズ), 講談社, 2016
- The Algorithmic Foundations of Differential Privacy
  https://www.cis.upenn.edu/~aaroth/Papers/privacybook.pdf
- Disclosure Avoidance for the 2020 Census: An Introduction
  https://www2.census.gov/library/publications/decennial/2020/2020-census-disclosure-avoidance-handbook.pdf
- あいおいニッセイ同和損保と LayerX、プライバシー保護技術「Anonify」を活用した自動車走行データの分析サービスの提供を開始
  https://prtimes.jp/main/html/rd/p/000000145.000036528.html
- Gartner Says Digital Ethics is at the Peak of Inflated Expectations in the 2021 Gartner Hype Cycle for Privacy
  https://www.gartner.com/en/newsroom/press-releases/2021-09-30-gartner-says-digital-ethics-is-at-the-peak-of-inflate