

匿名化に関する検討について

平成25年9月27日

総務省

1. 目的

○「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会」において、事業者が積極的に多様なライフログサービスを展開し、利用者が安心してサービスを楽しむことができる環境の構築に向けた検討を行うため、「ライフログ活用サービスWG」を設置し、以下の項目を中心に検討。

(平成21年4月より検討、平成22年5月提言公表)

- (1) ライフログ活用サービスについて主にプライバシーの面からの法的課題。
- (2) ライフログ活用サービスの発展を妨げずに、利用者の不安感等を緩和する方策。

ライフログ:蓄積された個人の生活の履歴を指す。ライフログは広範な概念であり、およそ考え得る蓄積された個人に関する情報の全てが含まれる。デジタル化されたものでは、ウェブサイトの閲覧履歴、電子商取引サイトにおける購買・決済履歴、携帯端末のGPS(Global Positioning System 全地球測位システム)により把握された位置情報等々が含まれる。

ライフログ活用サービス:様々なサービスが考えられるが、本検討においては①利用者の興味・嗜好にマッチした情報を提供するサービス(行動ターゲティング広告、行動支援型サービス)、②統計情報を提供するサービスを対象とした。

2. 検討結果

○ライフログ活用サービスは、その態様によっては、プライバシーを侵害し得るし、利用者の不安感等を惹起し得る。

○よって、事業者は、ライフログの取扱いにあたって、利用者に対して一定の配慮をなすことが望ましい。

しかしながら、

- ・サービスが揺籃期にあり、事業者に過度の負担となってサービスの発展を妨げることは避けるべきこと
- ・技術革新に伴って急速に発展することが想定されること

から、規制色の強い行政等によるガイドラインではなく、事業者による自主的なガイドライン等の策定を促すべき。

その指針となる緩やかな配慮原則を策定。

○配慮原則は、

- ・個人情報保護法上の個人情報であるか否かを問わず、特定の端末、機器、ブラウザ等を識別可能な情報を対象
- ・透明性の確保、利用者関与の機会の提供等を柱とする『6つの原則』。

(①広報、普及・啓発活動の推進、②透明性の確保、③利用者関与の機会の確保、④適正な手段による取得の確保、⑤適切な安全管理の確保、⑥苦情・質問への対応体制の確保)

3. WG構成員

【主査】 上沼 紫野 虎ノ門南法律事務所 弁護士
【主査代理】 森 亮二 英知法律事務所 弁護士
石井 夏生利 情報セキュリティ大学院大学 准教授
新保 史生 慶應義塾大学 准教授
長田 三紀 東京都地域婦人団体連盟 事務局次長
藤原 まり子 博報堂生活総合研究所 客員研究員

(オブザーバー)

楠 正憲 マイクロソフト(株) 技術標準部 部長
桑子 博行 (社)テレコムサービス協会 サービス倫理委員長
下島 健彦 NECビッグロブ(株) 執行役員 ポータル事業部長
正垣 学 (株)NTTドコモ コンシューマサービス企画
コミュニケーションサービス企画担当課長
寺田 眞治 (株)オプト グループ戦略室 室長
中井 博胤 (株)ぐるなび 総合政策室 次長
別所 直哉 ヤフー(株) CCO兼法務本部長

(五十音順・敬称略)

(平成22年3月24日時点)

《個人識別性のない情報とプライバシー》

- 利用者が氏名等の個人識別情報を用いてログインせずに閲覧する場合や、匿名化された場合など、取り扱われるライフログが個人情報にあたらない場合がある。この場合、当該ライフログは、個人情報保護法制が適用されない領域であるが、プライバシーの法的な保護対象となり得るかが問題となる。

《プライバシーの法的保護対象たり得るか》

- プライバシーは、成文法は存在しないが法的に保護されるべき人格的利益として判例法理上認められてきた。我が国の最高裁判例も私人間の事例において「プライバシー」の概念を認めるに至っているが、現在では、他人にみだりに知られたくない個人に関する情報であるか否かを、もっぱら基準としている。
- 上述の個人に関する情報に、インターネット上の行動履歴のような個人識別性のない情報が含まれるか否か、つまり、個人識別性のない情報がプライバシーの法的な保護対象となり得るか否かは必ずしも明らかではない。

《なぜ個人識別性のないライフログにも、配慮が求められるのか》

- しかしながら、インターネット上の行動履歴等のような個人識別性のない情報(非個人情報)については、プライバシーの法的保護の対象と解することが難しいとはいえ、
 - ① 非個人情報であっても、第三者の持つ情報と照合した結果、個人識別性を獲得する場合が考えられること
 - ② 非個人情報を大量に蓄積することで、個人を推定することが可能になる場合が考えられること
 - ③ 技術の発達により、非個人情報であっても将来的に個人識別性を獲得する場合が考えられること、
 - ④ 非個人情報であっても、利用者には、その取得・保存・利活用に不快感や不安感が存在し、事業者の円滑なサービスの発展を阻害している場合が考えられることから、事業者は自主的に一定程度の配慮を行うことが望ましいと考えられる。

匿名化に関する検討

《匿名化と個人識別性》

- 行動ターゲティング広告や統計情報提供サービス等必ずしも個人を識別する必要のないサービスにおいて、個人識別性を具備する情報に対して匿名化を行うことで個人識別性を喪失させ、流通や利活用を容易にする取組が検討されている。

個人識別性の獲得リスクを回避するため、各方面においてk-匿名化等の処理のアプローチを検討。

k-匿名化 行動履歴の一部を一般化やあいまい化することにより、組み合わせることで個人を推定できる可能性のある情報(準識別子と呼ぶ。)の組み合わせ(準識別子群)と同じ準識別子群を少なくともk個以上存在する状態を作り出す処理。

しかし、客観的に、完全に個人識別性を喪失させるのは容易ではなく、個別の判断によらざるを得ない。

《匿名化により個人識別性を喪失させる行為も、個人情報利用に当たるのか》

- ① 個人情報保護法の規定する利用目的の特定(法第15条)の趣旨は、不必要に又はみだりに個人情報を取り扱うことを制限するとともに、個人情報の取扱いの透明性を図り、本人自らが権利利益の侵害を未然に防止するために必要な対応をとることができる環境を整備しようとするものであること
 - ② 一方、匿名化を行って個人識別性を喪失させる行為は、個人の権利利益の侵害のおそれを小さくするものであり、利用目的の特定等の義務を課さない方がむしろ法の趣旨に沿うと考えられること
- から、匿名化を行って個人識別性を喪失させる行為は個人情報の利用には当たらず、個人情報取扱事業者は、匿名化を個人情報保護法上の「利用目的」として、特定する必要はないと考えられる。
- これを踏まえ、「電気通信事業における個人情報保護に関するガイドライン(平成16年総務省告示第695号)の解説」に明記。(平成22年7月29日)

「電気通信事業における個人情報保護に関するガイドライン」の解説

(利用目的の特定)

第5条 電気通信事業者は、個人情報を取り扱うに当たっては、その利用の目的(以下「利用目的」という。)をできる限り特定するものとする。
2・3 (略)

(解説)

(1) (略)

(2) (略)

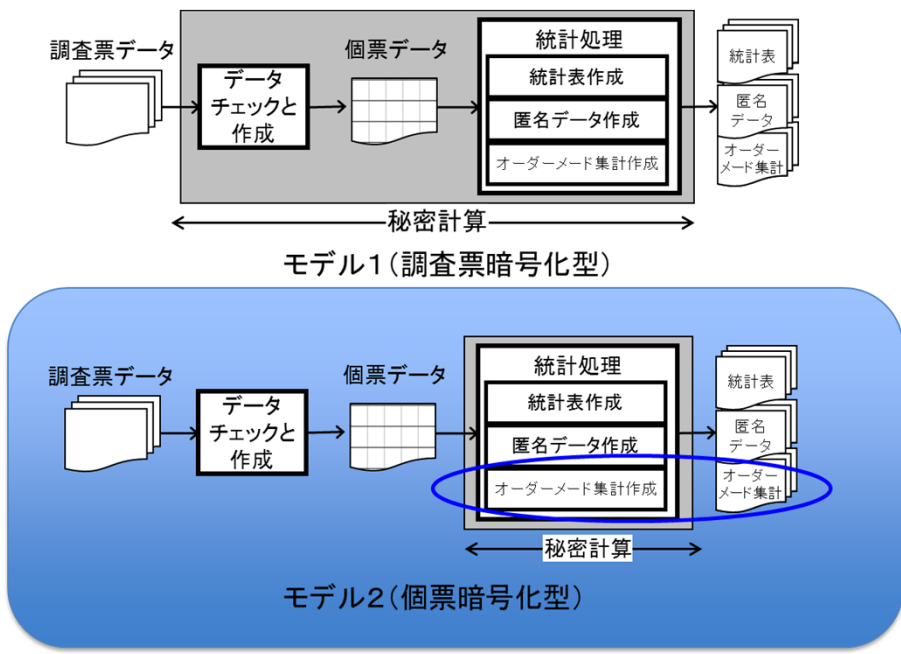
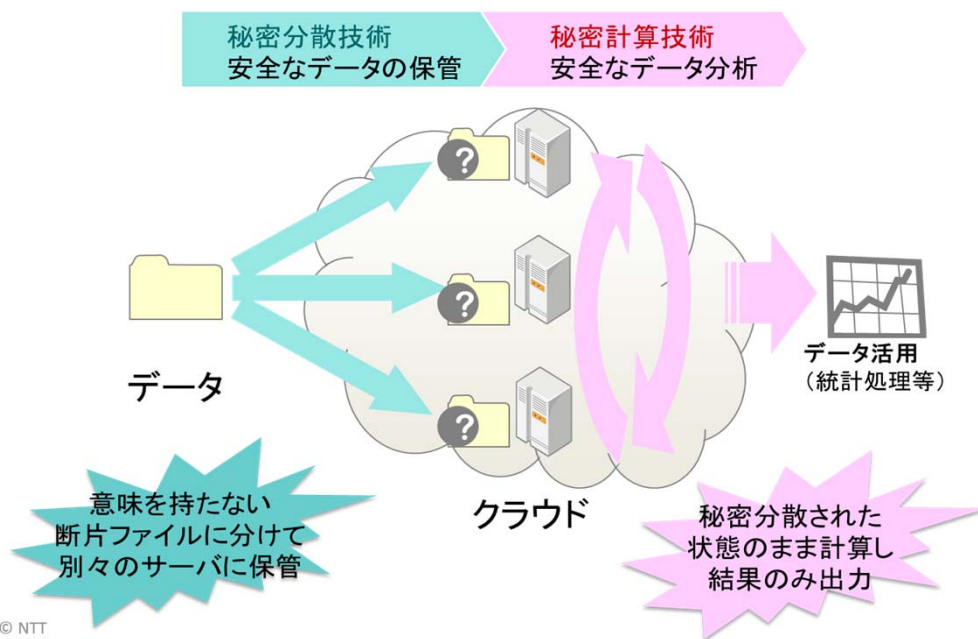
なお、個人情報に対して、特定の個人を識別できないようにする加工(いわゆる匿名化)を行うことは、個人情報の利用に当たらず、利用目的として特定する必要はない。

(3)・(4) (略)

秘密分散・秘密計算技術の統計業務への適用に関する研究

◆ 暗号化技術(秘密分散技術と秘密計算技術)を公的統計の分野に適用することにより、データの情報安全性と有用性、利用者の利便性のバランスを取って、個別データを開示することなくオフサイトでリアルタイムに集計・統計分析をする仕組みを構築することができないか。

⇒ 総務省統計研修所では、平成24年度からNTTプラットフォーム研究所と共同研究を開始。



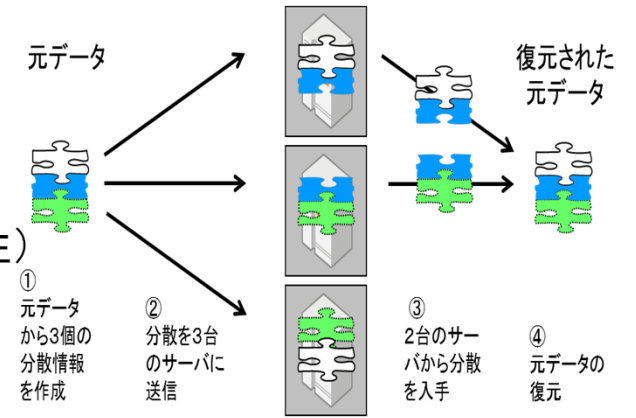
<研究成果>

- 秘密計算技術の統計業務への適用を実証
- 今後、秘密計算と汎用的な集計ソフトを要素技術として組み合わせることによる実利用を目指す

(参考)秘密分散・秘密計算技術

秘密分散技術

- データを複数の分散に分けn 台のコンピュータに分散させ保管
- k 台のコンピュータから分散を集めデータを復元
- k-1 台までのコンピュータからデータを盗んでも何の情報も得られない(機密性)
- n-k 台まで故障しても、残りのコンピュータからデータを復元できる(可用性)



秘密計算技術

- データを複数の分散に分けn 台のコンピュータに分散させ保管(秘密分散)
- コンピュータ間でデータ処理とデータの送受信を必要回数行って計算を行う(マルチパーティー計算)
- 計算過程で各コンピュータは何の情報も得られず、k-1 台までのコンピュータからのデータが集められても何の情報も漏れない
- 計算結果の分散が各コンピュータに分散配置され終了

