O-023

個人情報管理システムを活用した情報銀行における利用許諾自動化の試み

Towards an Automatic Authorization for Information Bank Using Personal Information Management System

寺西 司† 掛下 哲郎†
Tsukasa Teranishi Tetsuro Kakeshita

概要: 個人データ活用の仕組みとして情報銀行の取り組みが提案されている。情報銀行では、事業者が個人データに対してアクセスを行う際に個人に通知を出して同意を求めるのが一般的である。しかし、専門家でない個人が、同意の可否を的確に判断するのは難しい。そこで、本稿では法令や契約に基づく個人データの利用に対して個人による同意を自動化するシステムを構想する。本システムの構築にあたっては、著者らが提案した個人情報管理システムを活用し、OECD 8 原則に基づく個人情報保護を保証することを目指す。これにより、情報銀行の利便性向上を図るとともに個人データ利用の効率化が進むことが期待される。

1. はじめに

Web サービスには個人のデータを活用することで成り立っているものが多くある。その一方、利用者の知らないところで勝手にデータを利用していることは問題との意見が各国で挙がるようになった。近年、個人のプライバシー保護に向けた動きも活発化しており、欧州連合（EU）では一般データ保護規則 GDPR（General Data Protection Regulation）、米国カリフォルニア州では消費者プライバシー法 CCPA（California Consumer Privacy Act）がそれぞれ施行されている。しかしながら、現代社会において個人データの重要性はますます高まっている。

こうした背景の元、個人が自己情報を管理しながら効率的にデータ流通を行うための仕組みとして情報銀行が提案されている[1]。これは、原則として情報主体者から許諾を得た上で、個人情報を有益な情報源として活用する試みである。

本稿では個人情報保護の基本となる OECD 8 原則をもとにして法律や契約に基づく個人データの利用に対して個人による同意を半自動化するシステムを構想する。

2. 関連研究

日本 IT 団体連盟の情報銀行推進委員会が総務省・経済産業省による情報信託機能の認定に係る指針に基づいて、情報セキュリティ対策やプライバシー保護対策に関する認定基準に適合しているか判断している[2]。現在、サービス実施中であり認定基準に適合していると認められる「通常認定」されたサービスでは、会員登録による個人情報収集およびアンケート回答による健康や趣味などの情報収集を軸とする２つのサービスが運営されている。ただし、個人にはアンケートに回答し、個人データの入力する作業が発生する。また、個人の購買履歴等のデータは対象に含まれていない。これらはデータ流通という観点から効率的ではない。

†佐賀大学 Saga University, Saga, Japan

情報銀行の運営に関して、様々な課題が指摘されている。山岡らは現状の情報銀行の仕組みでは個人データが一か所に集約されることがリスクだと指摘している[3]。また、価値の高いデータを意図的に作り出すことも想定されデータ自体の信頼性が低くなる恐れも挙げられている。

他方、戸嶋らはデータの価値を決定する取引を自動化するための自動交渉システムを提案している[4]。これにより、データ提供者がデータの便益に対して自らの意思を反映させることが可能とされている。

3. 個人情報管理システム

著者らはこれまでに個人情報管理システム（図 1）の研究・開発を進めてきた[5]。個人情報管理システムは個人データに対してアクセスコントロールを自動化するものであり、個人情報の保護規則である OECD 8 原則（目的明確化、データ内容、個人参加、収集制限、利用制限、安全保護、責任、公開）への対応を可能としている。

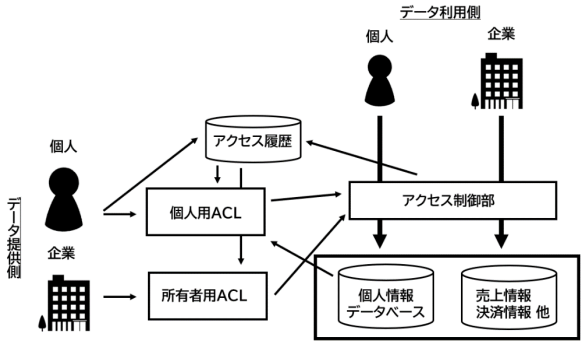

図 1：個人情報管理システム

本システムでは個人と事業者が、それぞれ複数存在する場合を想定しており、個人データは個人と事業者の取引により生じる。たとえば、個人 A が事業者 B を利用した際には、事業者 B が個人 A の利用履歴を所有することになる。図 1 のように、個人 A と事業者 B のアクセス制御リスト

（ACL，Access Control List）を分離することにより、個人と事業者を対等な関係にする。また、個人がアクセス履歴を参照できるようにすることで OECD 8 原則の個人参加の原則に適合している。

4. 提案手法

本稿では、個人情報管理システムを用いることで個人データの利用に対して個人による同意を自動化するシステムを提案する。これを利用許諾自動化システムと呼ぶ。これにより、法令などに詳しくない個人が同意の可否を自ら判断する機会を減らし個人データの利用の効率化を図る。

本システムでは、個人データ（個人情報保護法に規定する個人情報）は当人または当人がサービスを利用した企業（提供側企業）が個人データ管理システムによって管理する（図 2）。個人データの利用を希望する企業等（利用側企業）は利用許諾管理システムを通じて利用申請を出す。アクセス権限は情報銀行が管理しており、利用許諾管理システムによって可否が決定される。許諾が得られた場合、情報銀行は個人データ管理システムに利用依頼を出す。同システムは利用側企業に当該データを提供する。

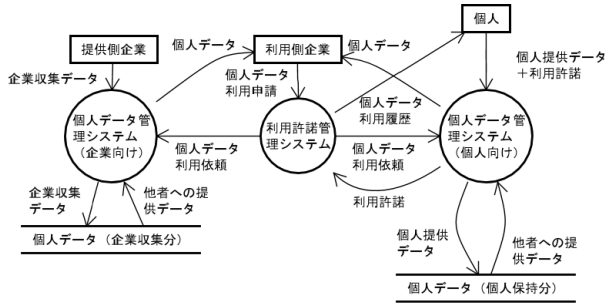

図 2：個人データ収集・提供システムの DFD

個人は本システムから個人データの利用履歴を取得できる。また、本システムが自動判定できない場合は、個人に利用許諾の可否を問い合わせる仕組みも有する。この点を考慮した利用許諾管理システムの詳細な構成を図 3 の灰色部分に示す。

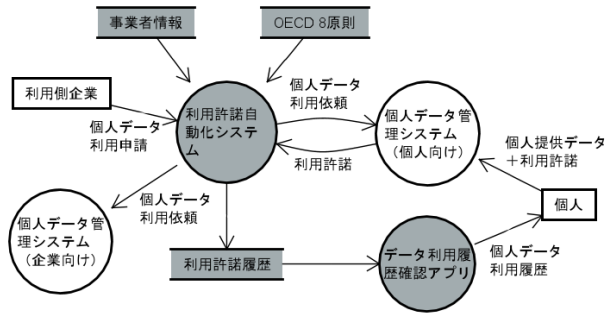

図 3：利用許諾管理システムの DFD

利用許諾の可否を判定する際には、OECD 8 原則の中でもデータ利用先や責任の所在および利用目的に合致した内容の収集であるかが重要である。ただし、個人はいつでも許諾履歴やデータの提供履歴を閲覧可能とし、問題がある場合は異議を申し立てることができる。これにより、過去のデータに対してもデータ内容の保証および個人参加の原則を担保できる。

個人に対する利用許諾の可否の問い合わせは、通知が必要だと利用者があらかじめ設定したデータへの利用申請が出されたときに行われる。この場合は個人に通知を出した上でその情報主体から許諾が得られない限り個人データが提供されることはない。また、このとき得られた利用許諾の可否は過去の経験として蓄積する。過去の事例を活用することで、将来の判定の自動化に役立てる。

利用許諾管理システムは、個人に対してデータ利用履歴確認アプリを提供している。このアプリケーションでは許諾申請の通知の他、許諾履歴やデータの提供履歴を閲覧できる。こうすることで、完全な自動化が達成できない場合でも、利用可能なデータが増える可能性が見いだせる。さらに、個人に通知を出す際にもデータ利用拒否および許諾の推奨オプションを提供できる。完全自動化を目指すのではなく個人の参加を重視するところに意義がある。

5. 今後の展望

本稿では、個人情報管理システムを活用し、個人データの利用許諾の半自動化を提案した。システムの構想に当たっては、利用者と事業者を公平に扱う点を特に考慮した。データ利活用に対する社会的なニーズの高まりを考えると判定の自動化率を高めることが望まれる。個人の参加が増えると当然ながらデータ利活用の効率性が阻害される可能性はある。ただ、個人の権利は保証すべきであることはすでに多くの国において共通認識である。それらを両立させることが本システムの目標である。

また、将来的にはディープラーニングなどの技術を活用し利用許諾の自動化精度を高めたいと考えている。具体的には、多数の利用者から得られたデータ利用許諾状況の情報を基に法令や規制面からだけでなく人間の感情や世論を参考にすることで自動化が強化できる。

6. おわりに

本稿では、個人情報管理システムを活用し、情報銀行の取り組みに関連してデータの利用に対して個人による同意を自動化するシステムを構想した。

情報銀行の取り組みに関してはまだ課題が残っており、多くの人が利用するようなサービスには至っていない。しかし、現代社会にとってデータの利活用は不可欠である。本稿のように利便性向上を目指す取り組みにより個人データの利用効率化や高度化が進むことを期待したい。

参考文献

[1] 砂原秀樹, 山内正人, 金杉洋, 柴崎亮介, 「情報銀行」構想とその技術的課題, マルチメディア・分散・協調とモバイルシンポジウム（2014）.
[2] 一般社団法人日本 IT 団体連盟 情報銀行推進委員会: 「情報銀行」認定制度について（2021）, < https://www.tpdms.jp/system/index.html> .
[3] 山岡裕司, 前田若菜, 「情報銀行」自己情報コントロールと権限分散を両立するパーソナルデータ流通方式の提案, Computer Security Symposium October 2018 （2018）.
[4] 戸嶋丈士, 高橋晶子, 阿部亨, 菅沼拓夫, 情報流通においてデータ提供への対価を決定する第三者エージェントを用いた自動交渉, 情報処理学会論文誌, Vol.62, No.2, 508-517 （2021）.
[5] 掛下哲郎, 新井康平, 大月美佳, 吉田豊昭, 個人情報管理システム, 特願 2004-4779 号, 2004 年 1 月.