2 パーソナルデータコンプライアンス対策

パーソナルデータコンプライアンス設計ガイドブックの策定

NTT セキュアプラットフォーム研究所（以下、SC 研）では、パーソナルデータを利活用する技術と法の境界にある新課題の発見と解決案の提言に取り組んでおり、これまで蓄積したノウハウとして、パーソナルデータ取扱い上の法的要件と具体的な事例を解説する「パーソナルデータコンプライアンス設計ガイドブック」を策定し事業会社各社へ展開している。

――パーソナルデータの利活用に関する研究の背景と目標

SC 研では、パーソナルデータを利活用する技術と法の境界にある新課題の発見と解決策として「パーソナルデータコンプライアンス設計技術」を研究している。その成果として、NTT グループ内事業会社での利用を目的として、非公開のパーソナルデータ取扱い上の法的要件と具体的な事例を解説する「パーソナルデータコンプライアンス設計ガイドブック」を作成してきた。過去に、Ver1、Ver2 を出版し、2020 年度には、Ver3 を出版する予定である（図 1）。

その内容は、パーソナルデータの取扱いに関する法的、社会受容性に関する研究の結果を含んでいる。

2020 年 6 月の改正個人情報保護法の成立に準拠しているとともにリクナビ事件などの重要な応用事例を取り上げている。

――個人情報の取扱いに関する法規制

2011 年、世界経済フォーラムにおいて「パーソナルデータは、インターネットにおける新しい石油」といわれてから 10 年近くを経た。高度化した ICT によってパーソナルデータが大量に収集、蓄積されビッグデータとなり、IoT、AI の導入・普及によってさらにデータの収集と処理が加速し、データの新たな利活用によるさまざまなサービスが次々と生まれ、ユーザーや社会に利便性と新たな価値を提供している。

その一方で、ユーザーの想定しえない（本人の意思に反する）パーソナルデータの利活用がされ、事業者がユーザーの反発を招き、法的な処分を受け、または社会的に大きな批判を浴びる事例も後を絶たない。

NTT セキュアプラットフォーム研究所
セキュアデータ流通基盤プロジェクト
主任研究員　**亀石 久美子**氏

最近では、SNS を用いて事業内容を宣伝する場合が増えているが、SNS 炎上対策として個人情報の保護に関する事項を守る必要がある。

わが国の個人情報の保護に関する法律（平成 15 年法律第 57 号、以下、「法」という）においては、事業者は、個人情報の取得前にあらかじめ利用目的を公表、もしくは取得後に速やかに本人に利用目的を通知又は公表し（法第 18 条）、利用目的はできるだけ特定（法第 15 条 1 項）してその範囲内で個人情報を取扱わなけ

■ パーソナルデータコンプライアンス設計ガイドブックの策定状況

	2017年度	2018年度	2019年度	2020年度	2021年度	2022年度
法制度動向	△2016年改正個人情報保護法全面施行	△EUのGDPR施行	△りくなび行政処分	△2020年改正個人情報保護法成立	△委員会ガイドラインパブコメ	△改正個人情報保護法全面施行
研究活動	● パーソナルデータの取り扱いに関する法的、社会受容性に関する研究 ■ 社内PIA活動 ■ 有識者との共同研究 ■ プライバシー行動・社会受容性調査 ■ データ流通に関する法的課題・社会受容性の研究 ■ 事業会社支援活動					
ガイドブック策定	▲ V1	▲ V2		▲ V3	▲ V4（仮）	

図 1　ガイドブックの策定状況

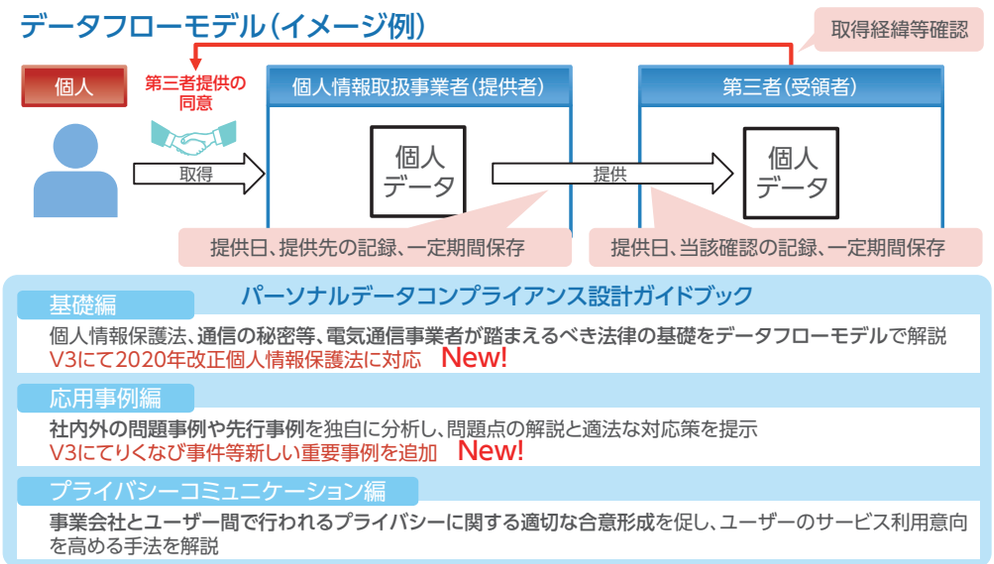

図2　ガイドブックの特徴と構成

ればならず、原則としてあらかじめ本人の同意を得ずに利用目的の達成に必要な範囲を超えて取り扱うことは禁止されている(法第16条1項)。これにより、本人は自分の個人情報がどのように事業者に利用されるか確認し、事業者に提供するかどうか選択することができる（Notice and Choice)。

EU の General Data Protection Regulation（以下､「GDPR」という）も「特定され、明確であり、かつ、正当な目的のために収集されるものとし、かつ、その目的に適合しない態様で追加的取扱いをしてはならない」(GDPR 第5条1項（b)）と定めている。その他、米国、アジア諸国などにも個人情報の利用目的の特定と制限について、わが国や GDPR の定めと概ね同様の定めがある。

――ガイドブックの特徴と構成

本ガイドブックは、パーソナルデータを利活用するサービス／システムの開発者が情報処理の適法性を判断できるように、開発者に分かりやすくデータフローモデルを用いてプライバシー・個人情報保護などの法的要件を解説している点において一般の法律の書籍と一線を画す。

ガイドブックの構成は、「基礎編」「応用事例編」「プライバシーコミュニケション編」からなる。「基礎編」では、個人情報保護法、通信の秘密など、電気通信事業者が踏まえるべき法律の基礎をデータフローモデルで解説している。最新の改正個人情報保護法に対応している。

「応用事例編」では、社内外の問題事例や先行事例を独自に分析し、問題点の解説と適法な対応策を提示しており、リクナビ事件などの新しい重要事例も追加している。

また、「プライバシーコミュニケション編」では、事業会社とユーザー間で行われるプライバシーに関する適切な合意形成を促し、ユーザーのサービス利用意向を高める手法を解説している（図2)。

――「スマートシティ実証実験」のプライバシー対策の事例

以下では、NTT 西日本との取り組み事例を紹介する。グランフロント大阪の「スマートシティ実証実験」のプライバシー対策の事例である[1]。この実証実験では、カメラ、音センサー、Wi-Fi センサー、扉の開閉センサー、温度センサーを設置し、映像による混雑度、音による危険と賑わい度、Wi-Fi センサーによる人の動きを把握し、これらのセンシングデータを利用した都市サービスの効率化を想定して、人流情報と温度変化を基にした空調管理によるエネルギー効率化の有効性を検証した。

ここでは、一般利用者の不安感を低減するための説明会など、事前の説明を行うことが大事である。特に、カメラなどセンサーの存在を事前説明することが重要である。これらのことで、レストラン共用部とトイレの空き情報や混雑度を見える化することが可能になり、都市のスマート化のモデルとしてその有効性が検証できる。

つまり、利便性の告知だけでなく、カメラ画像などのデータの取扱いに

図３　来街者への説明例（ステッカー）

ついて紙面を割いて説明することが求められる。センシングを望まない来街者が取りうる手段についても一例を周知する必要がある。例えば、各センサー周辺に告知を行い、データ取得対象となることを望まない来街者がとりうる手段を周知するなど、リスク発生を未然に防止する必要がある。すなわち、実験の目的・来街者への効用を明確に設明するとともに、「すること／しないこと」を明確に説明し、誤解を生む表現を避ける必要がある（図３）。

パーソナルデータの取扱いに関しては、その方針を決定することでリスク低減できる。つまり、個人情報を取り込まず、かつ属性情報も取り扱わない、センサーが個人情報を取得する場合には、データを解析し個人情報が破棄されるまで適切に管理し、第三者への提供も行わない、実験終了後には速やかに破棄するなど、指針を示すべきである。

カメラで撮影した映像は推定データの生成後に破棄されるため、映像情報は保存されない、顔や容貌などの特徴検出は行わないなどを、事前に説明するべきである。

――利用目的の再編統合を可能にする内包的枠組み

事業者は、ユーザー本人に対し利用目的を明確に示しその範囲内でパーソナルデータを取扱わなければならないが、事業分野やサービス毎に別々に利用目的を定めると個々の業務との関係は極めて複雑となる。複雑さを解消し、合目的的なシステム実装・運用とユーザーの分かりやすさの向上のため、利用目的の再編統合が必要となることがある。私たちは、そのような場合にも適用できる、利用目的を共通の性質（内包）によって分類・整理する枠組みを考案した。

内包は、事業者にとってもユーザーにとっても分かりやすいものであることが重要で、「契約履行上の必要性」（その利用目的がサービス提供上必須かそうでないか）と「利用行為の方向性」（その利用行為がユーザー自身に直接向けられたものか、サービス･商品か）で、ユーザーにとって関心の高い軸である。[2]

NTT ドコモは、本利用目的の内包的枠組みを採用し、パーソナルデータの利用目的を再編統合し、表現を分かりやすく記載し直し、既存の利用目的も併記した。

「サービス・商品などの提供に必要なこと／お客さまへの提案や企画開発・調査などにかかわること」は契約履行上の必要性の軸に対応し、「一人ひとりのユーザーにかかわること／サービス・商品などにかかわること」は利用行為の方向性の軸に対応している（図４）。

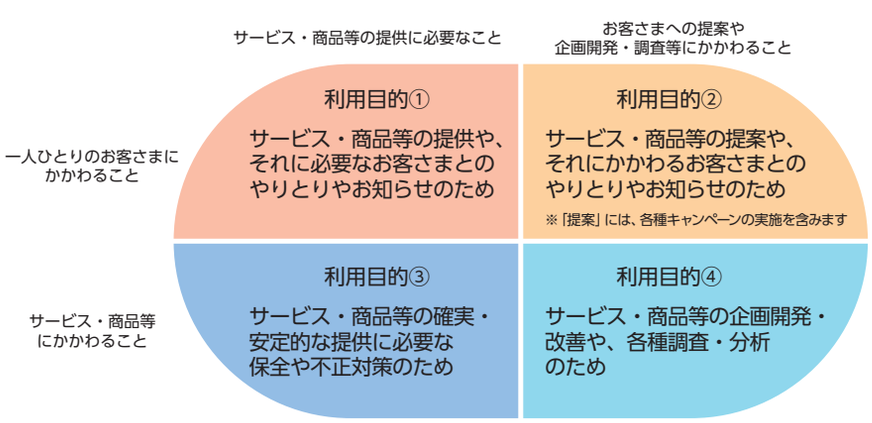

図４　NTT ドコモの再編後の個人情報の利用目的 [3]

[1] 一般財団法人アジア太平洋研究所『自主研究「都市におけるＩｏＴの活用」「スマートシティ実証実験」実施報告書』，2019 年 8 月 .https://www.apir.or.jp/wp/wp-content/uploads/APIR_REPORT_FY2019_IoT_SmartcityTrial.pdf
[2] 間形文彦ほか「個人情報の利用目的のシステム実装を最適化する内包的枠組み～NTT ドコモのプライバシーポリシー再編への適用～」、『情報処理学会研究報告』Vol.2019-EIP-85 No.3.
[3] NTTドコモ「パーソナルデータの利用目的」https://www.nttdocomo.co.jp/utility/privacy/?icid=CRP_common_footer_to_CRP_UTI_privacy