

デジタル化するビジネスにおいて 考慮すべきプライバシーリスク管理(前編)

TMI総合法律事務所 TMIセキュリティ&プライバシー株式会社 弁護士 大井哲也
PwCあらた有限責任監査法人 パートナー 平岩 久人



世界経済フォーラムが公表した報告書において「パーソナルデータは新たなオイルになる」という見通しが示されたのは2011年1月のことでした¹。それ以降に私たちが経験してきたことは、この見通しが正しかったことを物語っています。「プラットフォーム」と呼ばれる事業者は、サービスやコンテンツを提供する基盤を構築・運営することを通じて、購買履歴などの個人に関連する膨大なデータを幅広く収集し、利活用しています。さらに、これらのデータを中心にさまざまな製品やサービスを提供する企業が連携することで巨大なエコシステムを形成し、圧倒的な競争力を生み出しています。今後は従来のウェブ上のデータに加えて、無線通信やセンシング技術の進展に伴いインターネットに接続することが可能になったあらゆるモノが生み出すデータの収集と利活用が、企業の競争力を左右すると考えられます。

一方、個人に関連する膨大なデータが収集・利活用されることによる個人情報の漏えいやプライバシーの侵害に対する不安も増大しています。重大な情報漏えいやプライバシー侵害を引き起こしてしまった企業や組織が、法令などに基づく行政指導や罰則の適用に加えて、社会的な批判を受けることで、事業からの撤退を余儀なくされる、あるいはレピュテーションに深刻なダメージを受けるというケースが散見されるようになってきています。そのため、データの利活用にあたっては、法令などの遵守はもちろんのこと、ビジネスパートナーや消費者などのステークホルダーに対して個人情報およびプライバシー保護の取り組みに関する情報を積極的に開示すると共に、説明および対話を通じてステークホルダーからの信頼を得ることが重要です。

本稿では前後編に分け、デジタル化する社会において存在するプライバシーに関するリスクと、プライバシーをテーマにした議論の動向、さらにはリスクを管理する上で有用なフレームワークを紹介します。前編ではプライバシーおよびプライバシーリスクについての基本的な考え方や、ビジネスへの実装が一層進むと考えられる人工知能(AI)の利用原則におけるプライバシーの取り扱いを概観していきます。

プライバシーおよびプライバシーリスク

プライバシーという考え方の始まりは、19世紀末に米国の2人の弁護士が発表した論文にさかのぼります。当時は、他人の私生活上の出来事や秘密を煽情的な記事にするメディアが隆盛していました。そのような中で「プライバシーへの権利(The Right to Privacy)」と題して「放っておいてもらう権利(right to be let alone)」が必要であると主張しました。20世紀の後半になると、コンピューターを活用した情報処理の進展に伴い、個人の情報を含む広範な情報が集積・活用されるようになったことから、プライバシーについてもより積極的に「自己情報コントロールする権利」と捉えられるようになりました。データの利活用を行う企業や組織においては、消費者などからデータを収集する代わりに、それを適切に取り扱うことが求められます。

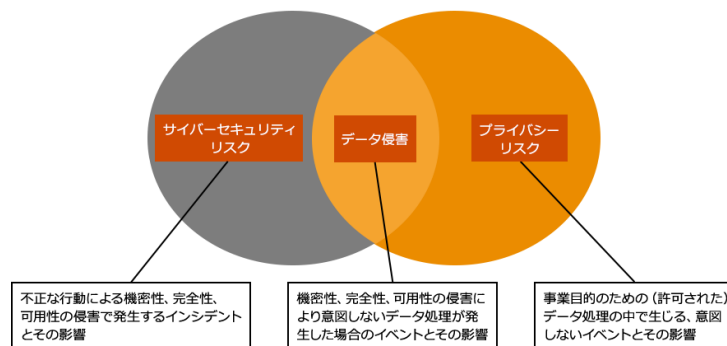
しかしながら、こうした企業や組織はデータの利活用を行う上で、常にプライバシー権を侵害するリスク(プライバシーリスク)を抱えています。米国国立標準技術研究所(National Institute of Standards and Technology: NIST)が2020年1月に公開したプライバシーフレームワーク(NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management²)を参照すると、プライバシーリスクは、事業目的のための製品やサービスにおける許可されたデータ処理の中で意図しない問題や結果が生じるリスクであると読み解くことができます。購買履歴などのさまざまなデータの分析を通じて個人の属性や性質を類推するいわゆるプロファイリングによって、センシティブ情報さえも推定されてしまうことなどが挙げられます。またプライバシーリスクとは別にサイバーセキュリティリスクについても言及されており、これについては、情報システムや情報資産の機密性、完全性および可用性を侵害する不正な行動によってインシデントが発生するリスクと考えられます。システムの脆弱性を突いた外部からの攻撃といった例が挙げられます。両者の関係は図表1の通りです。

¹World Economic Forum Report. Personal Data: The Emergence of a New Asset Class Feb. 17, 2011.

²NIST Releases Version 1.0 of Privacy Framework Jan16,2020

³NIST Privacy Framework: A Tool for improving privacy through enterprise risk management, version 1.0 Jan16,2020 P.3 Figure2: Cybersecurity and Privacy Risk Relationship

⁴報告書2019概要 AIネットワーク社会推進会議 令和元年8月9日





図表1: プライバシーリスクの位置づけ³

プライバシーリスクとサイバーセキュリティリスクが重なり合った時に生じるのが、データ侵害です。故意または過失による個人情報の漏えいといったセキュリティインシデントが挙げられます。データの利活用は企業や組織に多くの恩恵をもたらしますが、同時にこうしたリスクと常に隣り合わせであることを自覚しておく必要があります。

AIの利用原則におけるプライバシー

ここからは、AIの利活用においてプライバシーがどのように扱われているかを紹介します。急速に社会への実装が進むAIを正しく有効に活用するため、その利用原則に関する議論が、これまで精力的に行われてきました。日本を含む多くの国際機関や各国・地域で、その結果がAI利活用原則として取りまとめられています。2019年6月のG20茨城つくば貿易・デジタル経済大臣会合においては「人間中心」の考えを踏まえたAI原則が採択されるなど、「AI原則の項目については、国際的にほぼコンセンサスが得られつつ」⁴ある状況です。図表2に代表的なAIの利活用原則を示します。

図表2: 代表的なAIの利用原則（例）⁵

国際機関／国／地域	概要
 OECD	AIに関するOECD原則（一部抜粋） ・人権等を尊重するように設計され、また公平公正な社会を確保するために適切な対策が取れる → 例えば必要に応じて人的介入ができるようにすべき ・人々がどのような時にそれと関わり結果の正当性を批判できるのかを理解できるようにするために、透明性を確保し責任ある情報開示を行うべき など
 日本	人間中心のAI社会原則（一部抜粋） ・プライバシー確保の原則 → 個人の自由、尊厳、平等が侵害されないようにすべき → パーソナルデータを利用するAIは、当該データのプライバシーにかかわる部分については、正確性・正当性の確保及び本人が実質的な関与ができる仕組みを持つべき → パーソナルデータは、その重要性・要配慮性に応じて適切な保護がなされなければならない。利活用と保護のバランスについては、文化的背景や社会の共通理解をもとにきめ細やかに検討される必要がある など
 米国	米商工会議所：AI原則（一部抜粋） ・強固かつ柔軟なプライバシーレジームの追求 → 明確で一貫したプライバシー保護は信頼に足るAIに必須の構成要素である など
 EU	AIの倫理指針（一部抜粋） ・プライバシーおよびデータガバナンス → プライバシーの侵害を未然に防止するためには、使用されるデータの品質と整合性を確保するデータガバナンスが求められる など

日本では上述の「人間中心のAI社会原則」を踏まえ、AIネットワーク社会推進会議が「AI利活用ガイドライン～AI利活用のためのプラクティカルリファレンス～」を公表しています⁶。当該ガイドラインは、適正利用、適正学習、連携、安全、セキュリティ、プライバシー、尊厳・自律、公平性、透明性、アカウントビリティからなるAI利活用原則を定めると共に、同原則を実現するための具体的方策について取りまとめています。

本稿の後編で、プライバシーに関する原則および具体的方策を取り上げます。

³OECDニュースルーム 42か国がOECDの人工知能に関する新原則を採択 2019年5月22日
 人間中心のAI社会原則 統合イノベーション戦略推進会議決定 平成31年3月29日
 U.S. Chamber of Commerce U.S. Chamber Releases Artificial Intelligence Principles Sep.23, 2019.
 European Commission Futurium Ethics Guidelines for Trustworthy AI
⁶総務省 AIネットワーク社会推進会議 報告書2019の公表