積極的なデータ活用を見据えた『攻め』と『守り』のプライバシー

TMI総合法律事務所／PwC

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（後編）

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

本稿では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。後編では、AIネットワーク社会推進会議が公表した「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～」1から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、概観していきます。さらに、企業や組織がプライバシーリスク管理を実現する際に参考になると思われるフレームワークなどを紹介します。なお、各フレームワークなどの詳細については、本シリーズで法的観点と共に解説していきます。

「AI利活用ガイドライン」におけるプライバシーに関する原則

「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～」において、プライバシーの原則は「利用者及びデータ提供者は、AIシステム又はAIサービスの利活用において、他者又は自己のプライバシーが侵害されないよう配慮する」と定義されています。また、その前提として、日本においては個人情報保護法の遵守が必要であるとされています。その上で、主な論点が3つ提示され、次のように解説されています。

1. AIの利活用における最終利用者及び第三者のプライバシーの尊重

「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～」において、プライバシーの原則は「利用者及びデータ提供者は、AIシステム又はAIサービスの利活用において、他者又は自己のプライバシーが侵害されないよう配慮する」と定義されています。また、その前提として、日本においては個人情報保護法の遵守が必要であるとされています。その上で、主な論点が3つ提示され、次のように解説されています。

- AIサービスプロバイダ及びビジネス利用者は、AIを利活用する際の社会的文脈や人々の合理的な期待を踏まえ、AIの利活用において最終利用者及び第三者のプライバシーを尊重する。
- また、最終利用者及び第三者のプライバシーを侵害した場合に講ずるべき措置について、あらかじめ整理しておくことが期待される。
- 加えて、当該措置について、最終利用者及び第三者に対し、必要な情報提供を行うことが期待される。

2. パーソナルデータの収集・前処理・提供等におけるプライバシーの尊重

- AIサービスプロバイダ、ビジネス利用者及びデータ提供者は、AIの学習等に用いられるパーソナルデータの収集・前処理・提供等において、また、それらを通じて生成された学習モデルの提供等において、最終利用者及び第三者のプライバシーを尊重する。

3. 自己等のプライバシー侵害への留意及びパーソナルデータ流出の防止

- AIサービスプロバイダ、ビジネス利用者及びデータ提供者は、AIの判断により本人同意なくパーソナルデータが第三者に提供されることがないよう、同意が得られていないデータはシステム上第三者に提供できないこととするなど、適切な措置を講ずることが期待される。

pwc

TMI PRIVACY AND SECURITY

図表1：プライバシーの原則と主な論点、期待される措置

プライバシーの原則	利用者及びデータ提供者は、AIシステム又はAIサービスの利活用において、他者又は自己のプライバシーが侵害されないよう配慮する

主な論点		期待される措置（主な論点（1）の解説より）
（1）	AIの利活用における最終利用者及び第三者のプライバシーの尊重	最終利用者及び第三者のプライバシーを侵害した場合に講ずるべき措置について、あらかじめ整理しておくことが期待される。
（2）	パーソナルデータの収集・前処理・提供等におけるプライバシーの尊重	加えて、当該措置について、最終利用者及び第三者に対し、必要な情報提供を行うことが期待される。
（3）	自己等のプライバシー侵害への留意及びパーソナルデータ流出の防止	

（1）で言及されている「プライバシーを侵害した場合に講ずるべき措置」とは、どのような措置が想定されているのでしょうか。パーソナルデータを利用するさまざまなシーンでのプライバシーの尊重や流出の防止は当然のこととして、次の2つが例示されています2。

プライバシー侵害時に講ずるべき措置の例

- 最終利用者及び第三者のプライバシーを侵害する情報を誤って取得した場合における、当該情報の消去、AIのアルゴリズムの更新 等
- 最終利用者及び第三者のプライバシーを侵害する情報を拡散した場合における、保存先への消去の依頼、AIのアルゴリズムの更新 等

プライバシーを侵害された被害者の救済のためにも必要かつ重要な措置であることに異論はないと筆者は考えます。その一方、システム管理者などの立場からすると、当該情報の「消去」は実務上、とても大きな困難を伴うことも事実です。「消去」を当該情報の物理的な削除と想定すると、当該情報の消去によってシステム内でデータの不整合が発生し、最悪の場合、システムが停止する恐れがあるからです。また、バックアップデータなどを含めて当該情報を網羅的に洗い出し、「消去」するためには、相応の労力が必要になります。そのため、データ利活用を含むサービスや製品においては、データ主体の消去・訂正・開示請求に応じる場面を含めプライバシーに関わる情報を取り扱うあらゆる側面で適切な対応ができるよう、その設計段階から、プライバシー保護のために必要となる措置をあらかじめ考慮しておくプライバシー・バイ・デザインの考え方が、今後ますます重要になると考えられます

プライバシーリスク管理のためのフレームワークなど

企業や組織がプライバシーリスクを適切に管理しながらデータを利活用するためには、具体的にどのような取り組みが求められるのでしょうか。多くの企業や組織では、従来の情報セキュリティや個人情報保護法などへのコンプライアンスを主管する部門が中心となり、情報システム部門といった関係部門と連携しながらプライバシーリスク管理を実施しているものと思われます。関係者間の利害や立場の違いを超えて、企業や組織として適切にプライバシーリスクを管理しデータの利活用を推進できるよう、参考になると思われるフレームワークなどを紹介して、本稿を締めくくります。なお、各フレームワークなどの詳細は、リンク先のインサイトをご参照ください。

■NISTプライバシーフレームワーク

NISTが2020年1月にVersion 1.0を公開したこのフレームワークは、プライバシー保護のために企業や組織が遵守すべきベースラインとして、次の3つを目的に策定されています。

製品やサービスなどの設計や開発において、プライバシー保護の合理的な説明責任を果たすこと

プライバシー保護活動の情報発信やコミュニケーションをしやすくすること

評価結果をもとに経営層、法務部門、IT部門などの間で、部門横断的なコラボレーションを実現できること

セキュリティ領域におけるデファクトスタンダードとなっている「NIST Cyber Security Framework」の姉妹版ということもあって、日本でも普及が想定されるフレームワークの1つです。

「**NISTプライバシーフレームワークを日本企業はどう活用するべきか-部門横断的なコラボレーションの必要性**」

■ISO/IEC 29100:2011（JIS X 9250:2017）プライバシーフレームワーク

この規格は情報通信技術（ICT）システムにおける個人識別可能情報（PII）の保護のためのフレームワークであり、企業や組織がICT環境におけるPIIに関連するプライバシー安全対策要件を定義するための一助となることを目的として，プライバシー安全対策要件の説明などを提供しています3。

また、2019年8月に発行されたISO/IEC27701:2019 Security techniques – Extension to ISO/IEC 27001 and ISO/IEC27002 for privacy information management – Requirements and guidelinesも本規格と整合して策定されていることから、既存のISMSに基づいてプライバシー情報マネジメントを確立したい企業や組織にとっては、本規格の理解が有用です。

プライバシーに関連する主な国際規格を図表2に示します。

図表2：プライバシーに関連する主な国際規格

プライバシーに関連する主な国際規格	
ISO/IEC 29100:2011 (JIS X 9250:2017)	プライバシーフレームワーク（プライバシー保護の枠組みおよび原則）
ISO/IEC 29101:2018	プライバシー・アーキテクチャ・フレームワーク
ISO/IEC 29134:2017	プライバシー影響評価のガイドライン
ISO/IEC 29151:2017	個人識別可能情報（Personally Identifiable Information：PII）保護の実践規範
ISO/IEC 29184:2020	オンライン・プライバシー通知と同意
ISO/IEC 27018:2019	パブリッククラウドコンピューティング環境における個人情報（PII）保護のための管理目的および管理策

■プライバシー・バイ・デザイン

製品やサービスの企画・設計段階から、プライバシーに関連する情報を取り扱うことが想定されるビジネスプロセス全般においてプライバシー保護の施策を事前的・予防的に組み込んでおこうというコンセプトで、次の7つの原則が示されています4。

このコンセプト自体は1990年代の半ばに提唱されたものですが、データの利活用に伴うプライバシー保護が企業や組織にとって喫緊の課題となりつつある今、あらためて注目されている考え方です。

図表3：プライバシー・バイ・デザインの7原則

プライバシー・バイ・デザインの7原則	
(1)	事前的・予防的であること
(2)	デフォルトの設定でプライバシーが保護されること
(3)	プライバシー対策が企画・設計時に組み込まれること
(4)	ゼロサムではなくポジティブサムであること
(5)	ライフサイクル全体を通じて保護されること
(6)	可視化され透明性が確保されていること
(7)	個人のプライバシーが尊重されていること

■プライバシー影響評価（Privacy Impact Assessment：PIA）

上述のプライバシー・バイ・デザインの考え方に基づき、製品やサービスの企画・設計段階でプライバシーへの影響を事前に分析・評価するリスク管理手法として、プライバシー影響評価が知られています。国際標準規格としては、ISO/IEC 29134：2017 Guidelines for privacy impact assessmentが2017年6月に発行されています。本規格は、プライバシー影響評価の実施プロセスとその報告書の構成と内容についてのガイドラインを提供しています。

企業や組織が製品やサービスの企画・設計段階でプライバシー影響評価を実施することで、プライバシーリスクを適切に管理することができるのはもちろんのこと、その実施や結果をステークホルダーに対して積極的に開示し、自らのプライバシー保護への取り組みに対する説明と対話を行うことで、ステークホルダーからの信頼を得るリスクコミュニケーションツールとして用いることも考えられます。

[1]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～ AIネットワーク社会推進会議 令和元年8月9日
[2]AI利活用原則の各論点に対する詳細 AIネットワーク社会推進会議 令和元年8月9日
[3]JIS X 9250：2017 情報技術―セキュリティ技術―プライバシーフレームワーク（プライバシー保護の枠組み及び原則）
Information technology -- Security techniques -- Privacy framework
[4]堀部政男、一般財団法人日本情報経済社会推進協会編（2012）プライバシー・バイ・デザイン プライバシー情報を守るための世界的新潮流