DX 時代における
企業のプライバシーガバナンスガイドブック
ver1.3

2023 年 4 月

総務省

経済産業省

― 変更履歴 ―

version	変更内容	変更者
1.0	・ 「DX 時代における企業のプライバシーガバナンスガイドブック」新規作成	総務省、経済産業省
1.1	・ 「３．経営者が取り組むべき三要件」及び「４．プライバシーガバナンスの重要項目」における事例の追加・見直し ※ver.1.0 公表後の企業におけるプライバシーガバナンスの実践状況を踏まえ、参考となるべき事例を充実させるための更新を実施。 ・ 参考文献の更新	総務省、経済産業省
1.2	・ 「３．経営者が取り組むべき三要件」、「４．プライバシーガバナンスの重要項目」及び「５．（参考）プライバシーリスク対応の考え方」における事例の追加 ※ver.1.1 公表後の企業におけるプライバシーガバナンスの実践状況を踏まえ、参考となるべき事例を充実させるための更新を実施。 ・ 個人情報保護法改正等を踏まえた既存表現の見直し ・ 参考文献の更新	総務省、経済産業省
1.3	・ 概念整理 ・ 「6.（参考）諸外国の法令等に係る情報収集方法」の追加 ・ 参考文献の更新	総務省、経済産業省

目次

1. 本ガイドブックの位置づけ

サイバー空間（仮想空間）とフィジカル空間（現実空間）が高度に融合された人間中心の社会である Society5.0 の実現に向けて、企業は、データの利活用によるイノベーションを創出し、製品・サービス等の高度化を通じて、経済成長と社会課題の解決を進める中心的な役割を担っている。

パーソナルデータ[1]を利活用する分野においては、イノベーションの創出による社会課題の解決等へ期待が寄せられる一方で、プライバシーに対する配慮への要請も高まっている。この要請に対して、企業は、パーソナルデータ利活用に対する消費者の意識や不安、消費者が求めている情報や取組等について理解し、その実態を把握した上で、消費者のプライバシーを守る姿勢を貫くことにより、消費者からの信頼や、企業のビジネスにおける優位性を獲得し得る。本ガイドブックは、新たな事業にチャレンジしようとする企業が、プライバシーに関わる問題について能動的に取り組み、ひいては新たな事業の円滑な実施に不可欠である信頼の獲得につながるプライバシーガバナンスの構築に向けて、まず取り組むべきことをまとめたものである。

本ガイドブックは、とりわけパーソナルデータを利活用して、消費者へ製品・サービス等を提供する中で、消費者のプライバシーへの配慮を消費者から直接要請される可能性のある企業や、そのような企業と取引をしているベンダー企業等を対象としている。

また、それら企業の中でも、以下のようなポジションの方々を主な読者として想定している。

- データ利活用やデータ保護のガバナンスに携わる企業の経営者または経営者へ提案できるポジションにいる管理職等
- データの利活用や保護に係る事柄を総合的に管理する部門の責任者・担当者

など

また、活用方法としては、以下のような活用シーンを想定している。

- 企業がデジタル・トランスフォーメーション（DX）を推進する等、大きな方向転換となる意思決定がなされたとき（大きな社会環境の変化等に伴

[1] パーソナルデータとは、個人情報保護法の個人情報だけではなく、個人に関連するあらゆる情報を指す。

い、デジタル技術を活用して、業務そのものや、組織、プロセス、企業文化・風土を変革するなど）
・プライバシー保護を通じた消費者からの信頼獲得や企業価値の向上を指向したいとき
・消費者のプライバシーへの影響が大きいと想定されるプロジェクトの検討を開始するとき・経営者または株主、投資家、親会社等の関係者から、プライバシーに関わる問題への対応強化を求められたとき
・経営者に対し、プライバシー保護に配慮した体制構築の強化を求めたい（適切な経営資源の配分を要請する）とき
・自社や業界内等において、パーソナルデータの利活用がプライバシーに関わる問題として批判を浴びるような懸念（いわゆる炎上等）を生じさせたとき[2]など

上記は、本ガイドブックを手に取るきっかけとなるよう例示したものであり、関心をお持ちの方々に広く参照していただきたい[3]。

本ガイドブックの内容は、法的義務についても部分的に紹介しているが、個々の具体例については、企業の規模やリソースに応じて実施されたものであり、後述するプライバシーガバナンスの構築に当たっては個々の企業の状況に応じて活用いただきたい。

なお、プライバシーが意味するもの、あるいはプライバシーに関して起こり得る影響は、後述のとおり「変化する」という特徴を有することから、今後も本ガイドブックは、社会の動向を適切に踏まえながら更新を行っていくものである。

令和 2 年、令和 3 年に個人情報の取扱いを規定する「個人情報の保護に関する法律」（平成 15 年法律第 57 号。以下「個人情報保護法」という。）が改正

[2] ただし、本ガイドブックではいわゆる「炎上」後の対応方法に言及しているわけではない。
[3] プライバシー問題は、企業規模や法人の種類に関わらず、生じ得るものである。パーソナルデータを扱う中小企業やベンチャー企業においては、体制構築など、同じように実施することが難しい点が含まれるが、考え方や留意事項について、本ガイドブックを参照されたい。
また、令和 3 年個人情報保護法改正に伴い、個人情報保護法、行政機関個人情報保護法、独立行政法人等個人情報保護法が統合され、一部の独立行政法人等のように企業以外の組織についても、これまでの民間の個人情報取扱事業者の義務が部分的に適用されることとなった。本ガイドブックの内容は、企業を主な対象としているが、企業以外の組織（学術研究機関も含む）にとっても役に立つ内容となっているため、同改正を機に、より幅広い主体の読者にご参照いただければ幸いである。

され、データ利活用の実態の変容に伴って個人情報及びプライバシーの保護のための規制が追加され、かつ、詳細化されるなど、強化されてきた。

本ガイドブックが示していることは、法令上の個人情報に加えて、必ずしも個人情報には該当しないパーソナルデータを企業が利活用する際にも、個人情報やプライバシー保護に関する法令等遵守を前提としつつ、企業の自主的な対応を含め組織全体で能動的に取り組めるように経営者が取り組むべき事項や、構築すべき体制とその役割・機能などについて記載したものであり、個人情報保護法の改正後も、より一層活用されることが期待される。

本ガイドブックでは、はじめに前提となる基本的な考え方を第 2 章で示した上で、第 3 章で「経営者が取り組むべき 3 要件」、続く第 4 章で「プライバシーガバナンスの重要項目」を整理した後、プライバシーガバナンスに参考となる情報を第 5 章以降に記載している。

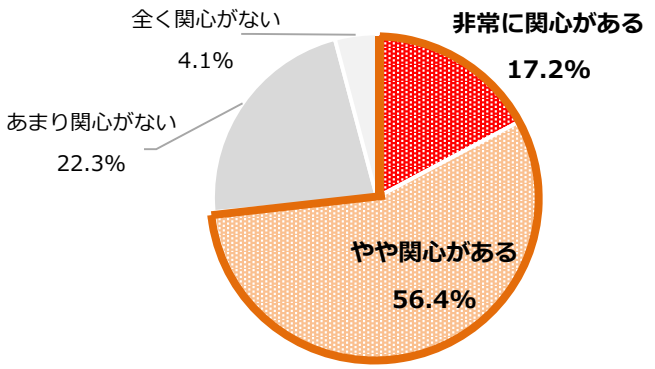
コラム -プライバシーガバナンスに関するアンケート-

「プライバシーガバナンスに関するアンケート結果（速報版）」（一般財団法人日本情報経済社会推進協会(JIPDEC)、2021 年）[4]では、プライバシーガバナンスに関し、消費者・企業に向けて、それぞれアンケート調査を実施している。その結果、企業のプライバシーガバナンスへの取組が、企業価値の向上と消費行動へ影響を与え、企業に優位性をもたらすということが明らかとなった。

消費者より得た回答によると、消費者の 73.6%が、企業のプライバシー保護の取組に関して高い関心を示しており、消費者の 88.5%は、類似の商品やサービスを選択する際に、商品等を提供する企業のプライバシー保護の取組を考慮することが明らかとなっている。

他方、企業より得た回答によると、企業の 58.7%は、企業自身がプライバシー保護への取組を発信することで、少なからず消費者の消費行動に影響を与えることができると考えているといった結果が明らかになっている。

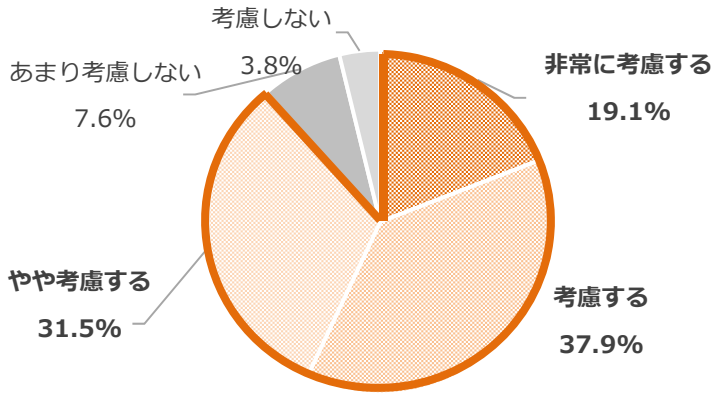
【消費者向けアンケート調査より】
Q：あなたは、プライバシー保護（例えば、個人情報、個人情報に限定されない個人の行動・状態に関するデータ、プライバシー性の高い情報などの適切な取扱い）に関して、どの程度関心をお持ちですか。
（消費者 n=314）



「非常に関心がある」「やや関心がある」の合計：73.6%

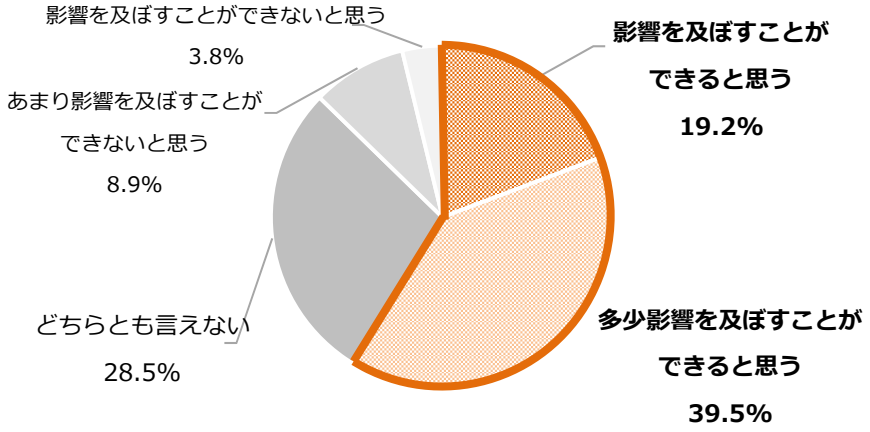
[4] 一般財団法人日本情報経済社会推進協会「プライバシーガバナンスに関するアンケート結果（速報版）」（2021 年）
https://www.jipdec.or.jp/topics/news/20211018.html

【消費者向けアンケート調査より】
Q：複数の異なる会社から、内容的に似た商品・サービスが提供されており、そのいずれか一つを購入する場合について、お尋ねします。その商品・サービスが、あなたのプライバシーに影響を与える可能性があるような情報を取り扱うとしたら、提供企業の「プライバシーへの取組」を、あなたはどの程度考慮しますか。
（消費者 n=314）



「非常に考慮する」「考慮する」「やや考慮する」の合計：88.5%

【企業向けアンケート調査より】
Q：プライバシーへの取組を発信することで、顧客の消費行動にどの程度影響を及ぼすことができると思いますか。
（企業 n=291）



「影響を及ぼすことができると思う」「多少影響を及ぼすことができると思う」の合計：58.7%

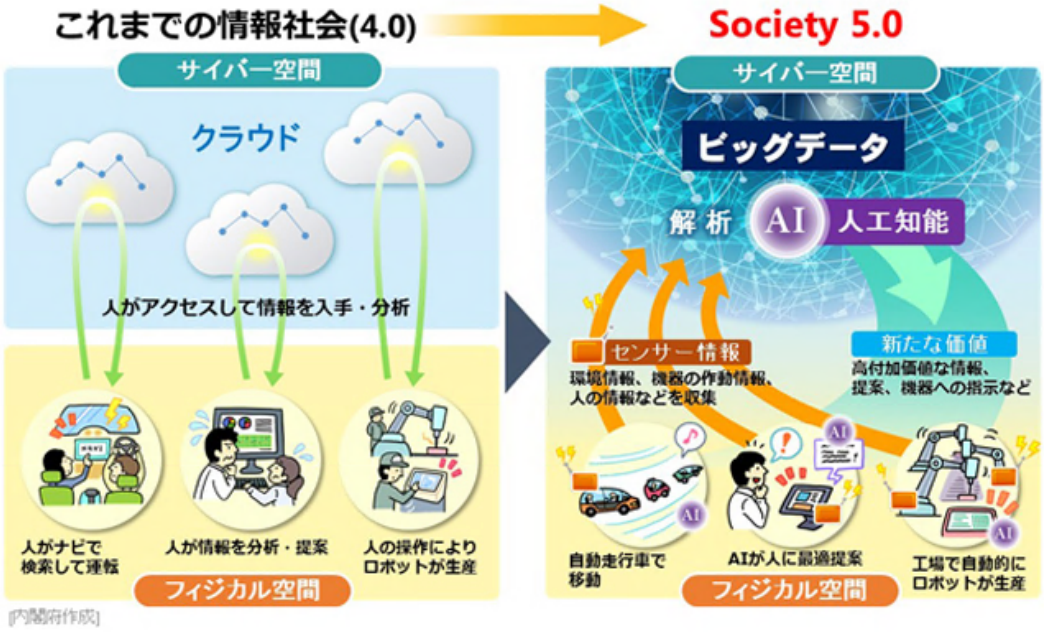
2. ガイドブックの前提

2.1. Society5.0 と企業の役割

今日、我々が生きる社会は、デジタル技術の発展とサイバー空間の拡張により、急激な構造転換を迎えている。高度に発達したセンサー、カメラをはじめとする情報取得技術や、あらゆるものをネットワークにつなげる IoT（Internet of Things）によってフィジカル空間のヒトや地上にある様々なモノがインターネットにつながり、それらの情報がクラウド等のサイバー空間で集約できるようになりつつある。また、近年、人工知能（AI）などの技術の進展により、フィジカル空間の様々な状況の推定ができるようになっている。この結果、フィジカル空間はサイバー空間においてデータとして把握・解析ができるようになり、その結果はフィジカル空間に様々な形でフィードバックされる。政府は、「サイバー空間とフィジカル空間を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する人間中心の社会」を“Society5.0”と名付け、我が国の目指すべき社会の姿として、その実現を目標に掲げている[5]。また、この Society5.0 を実現するために、企業・経営と規制・制度の両面において、デジタル・トランスフォーメーション（DX）[6]を一体的に進めることが重要であると考えられている。さらに、日本として「イノベーションと社会的信頼の双方を実現するモデル」を作るとの観点から、デジタル・ガバナンス改革も進められている。

[5] 内閣府 Society5.0（ https://www8.cao.go.jp/cstp/society5_0/index.html ）
[6] デジタル・トランスフォーメーション（DX）とは、例えば企業においては、ビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立することを指す。

図表１　これまでの情報社会と Society5.0



Society5.0 におけるサイバー空間とフィジカル空間が高度に融合した社会は、人々の生活を豊かにする革新的な製品・サービスや技術をもたらす。我々が日常的に利用している様々なデジタル・プラットフォームによるサービスや、グローバルに技術開発競争が進み、実装されつつある自動運転、環境適合的で快適・安心な暮らしを実現するスマートホーム、それらの総体としてのスマートシティはその一例である。このような社会では、これまでフィジカル空間で人間やハードウェアが担ってきた機能が、サイバー空間のデータやソフトウェアとして再定義され、頻繁に更新され、進化することになる。

サイバー空間におけるイノベーションは、変化のスピードが速く、国境を越えるビジネス展開が容易であり、データの集積や直接・間接のネットワーク効果[7]により勝者総取りとなりやすいという特徴を有している。そのため、Society5.0 を実現していく中で、我が国が今後の経済成長を維持するためには、フィジカル空間とサイバー空間の連動を起点とする、創造的なイノベーションが不可欠である。

このようなイノベーションは、プライバシーに関わる問題を含む社会的課題に対して解決策をもたらす可能性がある一方で、イノベーションによって生じ

[7] ある人がネットワークに加入することによりその人の効用を増加させるだけでなく他の加入者の効用も増加させる効果のこと。直接的には、同じネットワークに属する加入者が多ければ多いほど、加入者の効用が高まる効果。間接的には、ある財とその補完財が密接に関係している場合に、ある財の利用が進展すればするほど、それに対応した多様な補完財が多く供給され、それにより効用が高まる効果。

る新たなリスクもある。そのリスクにはプライバシーに係る新たな問題が含まれる場合もある。こうしたリスクを放置すれば、イノベーションそのものが受容されなくなる恐れがある。イノベーションが社会に定着し、持続的な経済発展を可能にするためには、イノベーションがもたらすリスクを社会が適切に管理し、生命・心身・財産の安全、プライバシー、民主主義、公正な競争といった様々な社会的価値を実現する社会システムが必要である。この観点から、イノベーション促進の中心的存在として期待される企業は、社会的価値と経済的価値の両方を創造する取組を積極的に推進するとともに、イノベーション自体から生じるリスクの低減を図っていかなければならない。すなわち、個人の権利や利益を守り、社会からの信頼（トラスト）を獲得しながら事業を推進することが肝要である。また、従来、プライバシーに関わる問題を含めて社会的課題への対応は、企業にとってコストとして扱われることが多かったが、こうした課題に能動的に取り組み、その解決を図ることは、消費者を含む社会からみると、その企業の製品・サービス等の品質を高めているのと同じであり、顧客満足度を高め、他社との重要な差別化要素となり得る。今後、企業にとってプライバシーに関わる問題に取り組むことは、コストではなく、商品やサービスの品質向上のためであり、それは企業にとっても、個人にとっても、ポジティブサム[8]になると発想を切り替えて、取り組むことが求められる。

本ガイドブックでは、このような企業の重要な役割を念頭に置いたうえで、特に、パーソナルデータの利活用と深く関わるプライバシーに注目する。

2.2. プライバシーの考え方

Society5.0 実現の中核となるデータの高度な利活用は、これまでとは質・量ともに大きく異なる。とりわけパーソナルデータの利活用は、個人の嗜好やニーズにより的確にアプローチすることを可能とし、企業にとってビジネスの源泉となる。さらに、個人への的確なアプローチを駆使した様々な取組は最終的に社会的課題の解決にもつながり得ることから、社会全体にとっても非常に重要である。

一方で、パーソナルデータの利活用の進展は、個人のプライバシーに対する影響の多様化と深く関連している。

[8] トレードオフの関係を作ってしまうゼロサムアプローチではなく、全ての正当な利益及び目標を収めるアプローチのこと。本ガイドブック「7.（参考）プライバシー・バイ・デザイン」も参照されたい。

例えば、データ収集の局面においては、デジタルサービスの提供者により、精密かつ膨大な個人のデータが収集されることによって人物の行動履歴や健康状態、思想・信条、趣味嗜好等が詳細に把握可能になるといったように、個人のプライバシーに影響を与える可能性が高くなっている。個人のパーソナルデータが政治的なターゲティング広告などに利用されるなど、民主主義が成立する前提が脅かされる可能性も生じている。

データ解析の局面では、機械学習等を用いたAIを含む、人を介さないアルゴリズムによる判断が社会において大きな役割を担うのに伴い、その安全性や適切性についても問題が大きくなっている。例えば、機械学習は、既存状況のデータを統計的に処理したモデルを通じて、対象に関する推定や判断をすることから、新規の対象には対処することが難しく、また状況が変化した場合もその推定や判断精度は落ちることになる。このため、常に揺れ動くフィジカル空間に関する推定や判断においては間違いが生じる可能性があり、その結果として対象やその特徴を間違えたり、あるいはサイバー空間での間違った推定や判断がフィジカル空間にフィードバックされると、その間違いが、結果として個人に対する差別や偏見を助長したり、事故につながるリスクがある。また、機械学習のモデルの元となる既存状況のデータに偏りがあった場合や統計処理が不適切な場合も、間違った推定や判断となりやすいことが知られている。

図表 2　参考：IoT と AI の利活用とプライバシーに関わる問題の例

IoT 機器等の利用	IoT 機器等により消費者からデータを取得する場合、消費者がデータ取得されていることを認識しにくく、認識したとしても、データ取得に関して自らの意思を反映させる機会がないという問題が発生しやすい。また、IoT 機器等によって取得するデータは、そもそも当該消費者以外を巻き込んでしまう（カメラであれば映り込んでしまう）性質があることにも注意が必要である。 ・計測されるデータ（What）：IoT 機器がどのようなデータを計測するかわかりにくい ・計測の場所と時間（Where&When）：いつどこで計測されているのかわかりにくい ・計測されたデータの解釈（How）：計測されたデータがどう解釈されるか、わからない ・計測の主体（Who）：データ取得主体が誰なのかわからない ・計測の目的（Why）：計測の利活用の目的を消費者に伝えることが難しい
AI を利活用して特定の個人を推測	データを利用するという観点においては、消費者から直接取得したデータが限定的である場合に、AI 等を用いて本人の行動等から本人に関する属性等を類推し、機械的に判断すること（いわゆるプロファイリングを含む）について、推定や判断の間違い、さらにはプライバシーに関わる問題が発生しやすい[9]

[9] 「OECD Principles on AI」（OECD、2019 年）、「人間中心の AI 社会原則」（総合イノベーション戦略推進会議、2019 年）、「AI 利活用ガイドライン」（総務省、2019 年）なども参考となる。

ところで、従来、プライバシーは「私生活をみだりに公開されない法的保障ないし権利」や「放っておいてもらう権利」として考えられていたが[10]、情報通信技術が発展し、情報プライバシーという概念が生まれてからは、個人の権利を尊重することが必要だとの考えが浸透してきたことも相まって「自己情報のコントロール」などの考え方へ発展していった。近年は、IoT や AI などの技術革新やそれを利活用したサービス等の変化は速く、例えば、データ解析の結果、機械的に不当な差別的扱いを受ける、あるいは多数の有権者の政治的選択に対して介入される可能性が生じる[11]、といったプライバシーに関わる新しい問題も顕在化している。

他方で、国内における商店街や商業施設、公共交通機関等への従来型の防犯カメラ（撮影した映像を記録するだけのカメラ）の設置は、一定の配慮の下で設置されることに対する肯定的な評価もある一方で、個人の識別（顔識別）機能を有する防犯カメラの設置に対しては慎重な意見や懸念もある。欧州や米国ではそのような利活用に係るルール整備が進み、日本においても犯罪予防や安全確保のためのカメラ画像の利用について、報告書が公表された[12]

このように、個人へのプライバシー侵害から、個人に影響を与えた結果生じる社会的な悪影響（社会の分断など）、例えば選挙に対する操作の可能性を生じてしまうことまで、急速な技術の変化も相まって、プライバシーに関して生じる悪影響は多様化している。さらに、個人個人の感じ方の相違によって、また社会受容性がコンテキストや時間の経過によって変わり得るなど、プライバ

---

[10] 元外務大臣有田八郎が、三島由紀夫の小説『宴のあと』によりプライバシーを侵害されたとして謝罪広告と損害賠償を請求した事件（宴のあと事件）では、東京地方裁判所は、私生活をみだりに公開されないという法的保障ないし権利として理解されるから、その侵害に対して侵害行為の差し止めや精神的苦痛による損害賠償請求権が認められるべきとした。

[11] データを解析した予測結果が企業に利活用され採用プロセスに影響を与えた可能性が取り沙汰される例や、海外においては、SNS の個人情報から心理プロファイリングを行った結果が、SNS を通じて投票行動へ影響を与えたのではないかとされる例も出ている。

[12] 欧州では、2020 年 1 月に「ビデオ機器を通じた個人データ処理に関するガイドライン第 2.0 版」が採択された。これは GDPR（EU 一般データ保護規則）の下でのカメラ画像や顔認識技術の取扱いに関する指針であるが、提案された当時は事業者の立場から見ると厳しい内容の規制も含まれていた。2020 年 2 月に公表された欧州の人工知能戦略のホワイトペーパー「On Artificial Intelligence - A European approach to excellence and trust」の制定の過程では、顔認証の利用の可否に関する記述が変遷するなどし、その位置づけは揺れ動いてきた。米国では、2019 年 6 月に、警察など市の 53 の機関での顔認識技術の利用や顔認識技術で取得された情報の利用を禁止する条例が施行された。顔認識ソフトウェアの提供中止を表明する企業も現れた。日本においても、2021 年度より個人情報保護委員会の「犯罪予防や安全確保のためのカメラ画像利用に関する有識者検討会」にて検討が進められ、2023 年 3 月に「犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用について」が公表された。

シーという概念を固定して考えられない点に、プライバシーに関わる問題への対応の難しさがある。

このような時代においては、個人や社会から「これはプライバシー侵害ではないか」との問いかけがなされる中で、プライバシーについての考え方が変わったり、プライバシーに関して問題とされる類型が広がってくる[13][14]。プライバシーに関する問題が個人や社会において生じるリスク（以下「プライバシーリスク」という。）に、パーソナルデータを利活用する企業が適切に対応できなければ、その結果が、経営上の悪影響につながる経営リスクとして、企業に跳ね返ることになる。

パーソナルデータを利活用する企業は、プライバシーリスクは企業のリスクである前に個人のリスクであること、そしてそれが社会全体に影響を及ぼす可能性があることを認識し、プライバシーに関する検討や取組を、企業活動に常に組み込むことが重要となる。

本ガイドブックにおいては、上記のような、個人へのプライバシー侵害から社会的な悪影響まで、プライバシーに関して生じる悪影響をプライバシー問題

---

[13] プライバシー問題については「5.2.プライバシー問題の洗い出し」を参照のこと。

[14]本ガイドブック ver.1.0（2020 年 8 月公表）から同 ver.1.3（2023 年 4 月公表）の期間においても、プライバシーに関わる社会的状況は目まぐるしく変化している。
膨大なデータを取り扱うデジタル・プラットフォーム等によるプライバシー侵害への危機感が高まり、欧米においては、利用者情報の取扱いに関する透明性の確保やアカウンタビリティ向上のための法制度の整備や適用が進んでいる。欧州では、2022 年 7 月、オンライン・プラットフォームに対してオンライン広告の透明性確保等の義務を課す「デジタルサービス法（Digital Services Act：DSA）」、及び、マーケットプレイス等を提供する事業者のうち一定の要件を満たす「ゲートキーパー」に対して、不当な条件の設定やデジタル市場の開放性を損なう行為を規制（複数サービス間の個人データの組み合わせ等の抑制、データポータビリティの提供、プロファイリング技術についての監査等の規制を含む）する「デジタル市場法（Digital Markets Act：DMA）」の修正案が、欧州議会にて採択された。また、米国では、2020 年 11 月、同年 1 月から施行されている「カリフォルニア州消費者プライバシー法（California Consumer Privacy Act）」を改正する「カリフォルニア州プライバシー権利法（California Privacy Rights Act）」が住民投票で可決され、2023 年 1 月に全面施行される予定である。CPRA は、個人データの（販売のみならず）共有に対するオプトアウト権も認めるなど、プライバシー保護を一層強化する内容となっている。
一方でプラットフォーム事業者等も、プライバシー意識の高まりを背景に、クロスサイトトラッキングをブロック又は抑制する方向に進んできた。モバイル市場で大きなシェアをもつ Apple は、Safari において Third Party Cookie の活用に対する制限を段階的に進め、2020 年には Third Party Cookie を完全にブロックしていたが、さらに 2021 年 4 月 26 日以降は、Apple の提供する広告 ID である IDFA（Identifier For Advertisers）についてもユーザの同意取得なしでは利用できなくなり、アプリ上のトラッキングも大きく制限されることとなった。Google も Chrome における Third Party Cookie の段階的廃止を計画（2024 年後半より順次廃止の見込み）していることを発表している。（「Expanding testing for the Privacy Sandbox for the Web」（Google LLC、2022 年 7 月）
https://blog.google/products/chrome/update-testing-privacy-sandbox-web/）

と位置づけ、パーソナルデータを利活用する企業がこれらの問題について取り組むべきことを記している。

2.3. 企業のプライバシーガバナンスの重要性

パーソナルデータの利活用によって、イノベーションを起こし、社会に対して価値を創出する主体は、企業が担うことが多い。したがって、プライバシー問題への取組についても企業が中心的な役割を担うことが期待される。プライバシー問題の発生を抑制すべく適切に対応しなければ、個人のプライバシーを侵害することとなる。そして、人々のプライバシーリスクへの不安や懸念と相まって、社会全体にデータの利活用に対する不信感が蔓延することとなり、ひいてはイノベーションが阻害される。そのような状況があっては、Society5.0、つまり経済発展と社会課題の解決を両立する人間中心の社会の実現は覚束ない。そのため、プライバシー問題への取組は、Society5.0 の実現に欠かすことのできない重要なものといえる。プライバシー問題への取組に当たっては、企業は、サイバー空間を介していても、取り扱う対象が単なるデータではなく、フィジカル空間の生身の個人と直接向き合っているという事実を改めて認識し、個人の基本的な権利を損なうことのないよう、真剣に考えを尽くし、適切に対応することが求められる。

加えて、企業の社会的責任や「ビジネスと人権」の観点から、企業に対して人権尊重責任を求める動きが広がっている[15][16]。企業が、消費者あるいは個人

---

15 国際的には「Guidance on social responsibility」（ISO26000：2010）や「ビジネスと人権に関する指導原則」（国連人権理事会、2011 年）が策定され、日本国内においても「ビジネスと人権に関する指導原則」に基づいた「ビジネスと人権」に関する行動計画（2020-2025）がビジネスと人権に関する行動計画に係る関係府省庁連絡会議により 2020 年に策定された。企業における人権尊重の取組強化のための「ビジネスと人権に関する調査研究」報告書（法務省、2021 年）や、「責任あるサプライチェーン等における人権尊重のためのガイドライン」（経済産業省、2022 年）も策定・公表されている。「ビジネスと人権」に関する行動計画では、インターネット上の名誉棄損、プライバシー侵害、差別への対応や、AI の適正な利用等「新しい技術の発展に伴う人権」に言及されている。「ビジネスと人権に関する調査研究」報告書では、企業が配慮すべき主要な人権及び企業活動に関連する人権に関するリスクとして「テクノロジー・AI に関する人権問題」「プライバシーの権利」も挙げられ、リスクの事例も紹介されている。

16 企業への投資決定を行う際に、従来のように財務情報だけでなく、環境（Environment）、社会（Social）、ガバナンス（Governance）の要素を考慮する ESG 投資が日本でも広がっている。ESG 投資は結果として、2015 年に国連で採択された SDGs（持続可能な開発目標）達成に貢献することにもなるとされている（参考 年金積立金管理運用独立行政法人（GPIF）Web サイト https://www.gpif.go.jp/esg-stw/esginvestments/ ）。

「スチュワードシップ・コード」（金融庁、2020 年改訂）や「コーポレートガバナンス・コード」（株式会社東京証券取引所、2021 年改訂）においても、投資先企業の状況の把握や企業

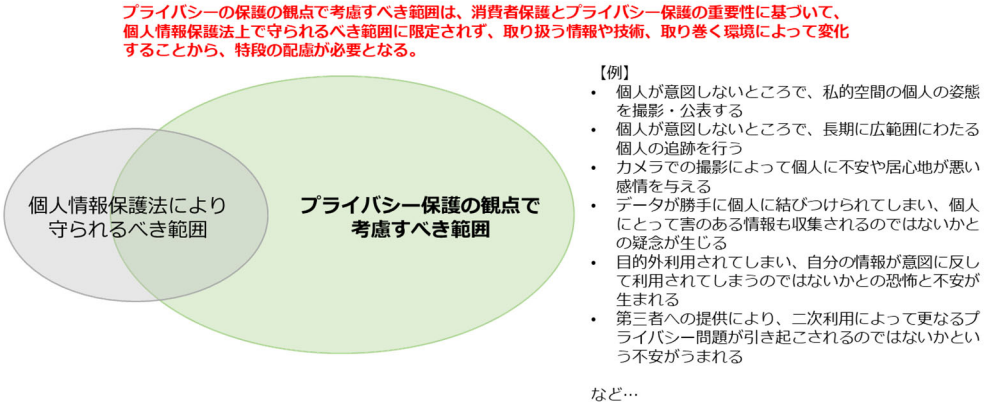
の基本的な権利を損なうことのないよう、プライバシー問題の発生を抑止・是正していくために、社内の体制の構築を含め、適切な対応を行うことは、このような社会的要請とも合致するものである。

現在、国内におけるプライバシー問題への対応は、個人情報保護法が主な規範として位置づけられている。このため、これまでは企業がビジネスを行う上でプライバシー問題を考える際には、コンプライアンス＝法令等遵守の観点から、「個人情報保護法を遵守しているか否か」が問われ、多くの場合、その点を中心に検討することで事業が行われてきた。また、スピードの速い技術革新、新たなプライバシー問題の発生や人々のプライバシー意識の高まりという状況変化の中で、必ずしも個人情報保護法の遵守の範囲にとどまらない形で、企業に対して社会受容性の観点から疑問が投げかけられたり、場合によっては企業がプライバシー問題に関する批判を避けきれず、炎上する事例が散見されるようになってきた。個人や社会に対するプライバシー問題の発生を抑止できなければ、差止請求や損害賠償請求のリスクが生じたり、社会からの信頼が揺らぐ事態にもなりかねない[17]。企業には、単なる外形的な法令等の遵守ではなく、その事業におけるパーソナルデータの利活用の様態に即して、個人の権利利益や社会的価値への影響を考慮した能動的な取組や説明が、強く求められるようになってきている。

の情報開示に努めることが、ESG 要素を含むサステナビリティに関する取組を促す観点からも重要である旨が言及されている。ESG 投資においても、人権は、社会（Social）の主要な要素の 1 つと位置づけられ、機関投資家と企業間の対話や、企業による非財務情報の開示においても、人権尊重を求める動きが広がっている。ESG 情報開示枠組みの 1 つであるグローバル・レポーティング・イニシアティブ（GRI）スタンダードには、企業が選択可能な形で「顧客プライバシー」に係る開示項目も設けられている。また、ESG 評価機関の掲げる ESG の主要問題の中に、プライバシー・データセキュリティが含まれている場合がある（例 MSCI ESG Ratings model）。今後、プライバシー問題への対応においても、統合報告書等による情報開示やマーケットとの対話を通じて投資家や社会からの評価を得ることが、企業にとって益々重要になると考えられる。

[17] 「犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用について」（個人情報保護委員会、2023 年）「第 4 章 肖像権・プライバシーに関する留意点」では、肖像権・プライバシー侵害を争点とする裁判例を紹介しつつ、「2 不法行為の成否と個人情報保護法の関係」の節において、顔識別機能付きカメラシステムを利用した撮影行為と不法行為及び個人情報保護法の関係について、「不法行為法と個人情報保護法はその目的や性格に異なる部分があることから、不法行為が成立する場合、同時に個人情報保護法違反となる場合もあり得るが、不法行為が成立したからといって必ずしも個人情報保護法違反となるわけではない」としつつ、個人情報保護法が、個人情報の性質や取扱方法を考慮する等、個人の権利利益に配慮していること、また肖像権・プライバシー侵害にかかる裁判例の動向を踏まえ、「（民法の）不法行為の成否を評価するに当たり考慮される要素は、個人情報保護法上も不適正利用の禁止規定（法第 19 条）や適正取得規定（法第 20 条第 1 項）の解釈などにおいて、考慮すべきであると考えられる」と示している。

図表 3　プライバシー保護の観点で考慮すべき範囲（イメージ）



しかしながら、昨今の批判を招いた事案等から企業が抱えている課題を考えると、国内においては、法令等の遵守が中心に位置づけられ、「遵守」という言葉のとおり、ある意味で受動的に、法令を守るための個別の対応そのものが主眼となってしまいがちである。個別の対応の背景にある本質的な目的、すなわち、企業において、プライバシー問題の発生をどう抑止するかという点に対する意識は希薄であるというのが現状である。こうした中で、プライバシー問題への対応自体が「コンプライアンスコスト」として捉えられ、法令等の遵守ができる範囲において可能な限り対応を「合理化」しようとするケースも見られる。これが高じた中で炎上が生じると[18]「法令は守っていたのに何故？」という事態に陥る。その結果、その企業自身に損失が生じることに加え、企業は保守的になりパーソナルデータの利活用に躊躇する、という悪循環が生まれかねない。

こういった現状に対して、顧客や消費者の信頼を得ながらパーソナルデータを利活用した新たなビジネスを拡大させている企業も、国内外に少なくない。これらの企業においては、プライバシーに関する取組を企業にとって単なる「コンプライアンス」と受け止めず、重要な経営戦略の一環として捉え、プライバシー問題に適切に対応することで、社会的に信頼を得て、企業価値向上へつなげている[19]。特に、企業の商品やサービスに関わるプライバシーリスクを減らし、プライバシーに親和的とすることは、消費者を含む社会からの信頼獲得につながることから、全ての企業がプライバシーに関する取組をコストとし

18 前述のとおり、炎上は必ずしも法令遵守の範囲にとどまらず、社会受容性の観点からも生じ得る。

19 例えば、2021 年 4 月に Apple が 4 つのプライバシー保護原則やアプリトラッキングの透明性向上に関する方針について公表した等の取組が見られる。

てではなく、むしろ製品・サービス等の品質や企業価値を高めることとして捉え直すことが求められている。

変化のスピードが速い時代においては、企業が法令を遵守するだけでは十分ではなく、リスク管理や社会から信頼を得るための取組が求められる。このため、企業は法令等遵守という狭義のコンプライを当然の前提としながらも、消費者やステークホルダーとのコミュニケーションを積極的にとり、能動的にプライバシー問題へ対応することが必要である。すなわち、消費者、その他ステークホルダーとの対話に基づいて、自らが果たすべき行為（行動規範）を定め、誠実に遵守（コンプライ）しつつ、社会に対して積極的にそれを開示して説明（エクスプレイン）し、消費者やステークホルダーとの対話を通じて、信頼を獲得していく、コンプライ・アンド・エクスプレイン型への組織的な転換が求められているといえよう。そして、一度設定した行動規範をただ遵守するのではなく、ゴールと常に変化する環境を踏まえ、最適な解決策を見直し続け

ることが、企業には求められている[20][21][22]。これらを踏まえて、企業のプライバシーガバナンスとは、プライバシー問題の適切なリスク管理と信頼の確保による企業価値の向上に向けて、経営者が積極的にプライバシー問題への取組にコ

---

[20] 政府は、これまでもパーソナルデータの利活用を推進するため、企業がプライバシー問題への対応を進める上でサポートとなる取組を行ってきた。特に IoT 推進コンソーシアムの下に設置され、経済産業省、総務省と共同で運営しているデータ流通促進ワーキンググループでは、3 年間にわたり、個別企業からのお悩み相談という形で、個別のビジネスにおいて課題となるプライバシー問題への取組について有識者から助言を行うとともに、蓄積された情報を「新たなデータ流通取引に関する検討事例集」という形で公表し、企業にとって有益な情報の提供に努めてきた（Ver1.0 を 2017 年に公表、Ver2.0 を 2018 年に改訂）。Ver2.0 策定後もワーキンググループでは検討を継続し、第 1 分冊として公表し、毎年度事例の追加を行っている。

また、2017 年以降、利活用の期待の高いカメラ画像について、その特徴を踏まえつつ利活用の促進を図るため、事業者が、生活者のプライバシーを保護し、適切なコミュニケーションをとるに当たって配慮すべき事項を整理した「カメラ画像利活用ガイドブック」を公表・改訂してきた（Ver1.0 を 2017 年に公表、Ver2.0 を 2018 年に改訂、Ver3.0 を 2022 年に改訂）。また、「カメラ画像利活用ガイドブック 事前告知・通知に関する参考事例集」（2019 年）及び民間事業者によるカメラ画像を利活用した公共目的の取組における配慮事項～感染症対策のユースケースの検討について～」（2021 年）も公表した。これらの取組に共通するのは、個人情報保護法の遵守は当然の前提としつつ、遵守に必要な助言にとどまらない、企業がより高いレベルでプライバシー問題への対応を行うという観点からの助言・情報提供をしてきたことである。一方で、これまでの取組は個別の事業に対して個別具体的な取組を示すことにとどまっていた。このため、コンプライ・アンド・エクスプレイン型への企業の組織転換に向けたサポートとなる、より普遍的な取組を検討すべく、「企業のプライバシーガバナンスモデル検討会」をデータ流通促進ワーキンググループの下に設置し、議論を進めることにした。

[21]「GOVERNANCE INNOVATION： Society5.0 の実現に向けた法とアーキテクチャのリ・デザイン」（経済産業省、2020 年）においても、企業によるコンプライ・アンド・エクスプレインの必要性について記載されている。
https://www.meti.go.jp/press/2020/07/20200713001/20200713001-1.pdf
「GOVERNANCE INNOVATION Ver.2: アジャイル・ガバナンスのデザインと実装に向けて」（経済産業省、2021 年）では、サイバー空間とフィジカル空間が高度に融合する多様で複雑なシステムの上に成り立つ Socitey5.0 におけるガバナンスモデルについては、ゴールと常に変化する環境を踏まえ、最適な解決策を見直し続ける必要があることが記載されている。
https://www.meti.go.jp/press/2021/07/20210730005/20210730005-1.pdf
「アジャイル・ガバナンスの概要と現状」（経済産業省、2022 年）は、上記 2 編のガバナンス・イノベーションの報告書の内容を一体的に理解するための解説として作成された。
https://www.meti.go.jp/press/2022/08/20220808001/20220808001.html

[22] 企業が AI を利活用したイノベーションを促進する際には、AI 原則を尊重し、AI が有するリスクの大きさに応じた規制を設けるリスクベースアプローチを採用することが求められるが、AI による影響力の範囲を検討する際には、プライバシーの保護は重要な観点となる。
「我が国の AI ガバナンスの在り方 ver. 1.1 AI 原則の実践の在り方に関する検討会 報告書」（経済産業省、2021 年）
https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20210709_1.pdf
「AI 原則実践のためのガバナンス・ガイドライン ver. 1.0」（経済産業省、2021 年）
https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20210709_6.pdf

ミットし、組織全体でプライバシー問題に取り組むための体制を構築し、それを機能させることが、基本的な考え方となる[23]。

一般に、企業のガバナンスは、経営者が経営戦略やリスク管理の観点から「方向づけ」を行い、定められた方向性の実現を目的として、企業活動が進められ、経営者はこの活動の状況を「モニタリング」し、目的に対して結果が得られているかを判断する「評価」を行い、この「方向づけ」「モニタリング」「評価」を基本のサイクルとして機能させることで、統制が行われると整理される[24]。

プライバシーガバナンスにおいても、経営者は、企業がパーソナルデータの利活用によりどのような価値を提供していくかを踏まえ、法令遵守を当然の前提としながらも、組織のプライバシー保護の軸となる基本的な考え方やプライバシー問題が個人や社会に生じるリスク（プライバシーリスク）管理に能動的に対応していく姿勢を自ら明文化して「方向づけ」を行い、その方向性の実現のためにプライバシーリスク管理の活動等を「モニタリング」し、その結果を明文化した内容に基づいて「評価」し、評価結果等を踏まえてまた「方向づけ」を行っていくというサイクルを機能させることが有効である。なお、リスク管理（リスクマネジメント）は、サービス・システムの企画、開発、運用といった事業プロセスにおけるリスクに対し、これを特定し、分析評価し、対応するという流れで行われることが一般的である。

さらに、プライバシーガバナンスにおいては、繰り返しになるが、スピードの速い技術革新や社会的要請等の外部環境の変化や、（個人個人の感じ方の相違や、社会受容性がコンテキストや時間の経過によって変わり得る等）プライバシーの概念が固定的に考えられないことを踏まえて、また、消費者やその他ステークホルダーとのコミュニケーションの中で、自らの取組を説明し信頼を獲得するとともに、プライバシーに関する懸念やフィードバックを踏まえて、取組を継続的に改善し続けることが必要である[25]。

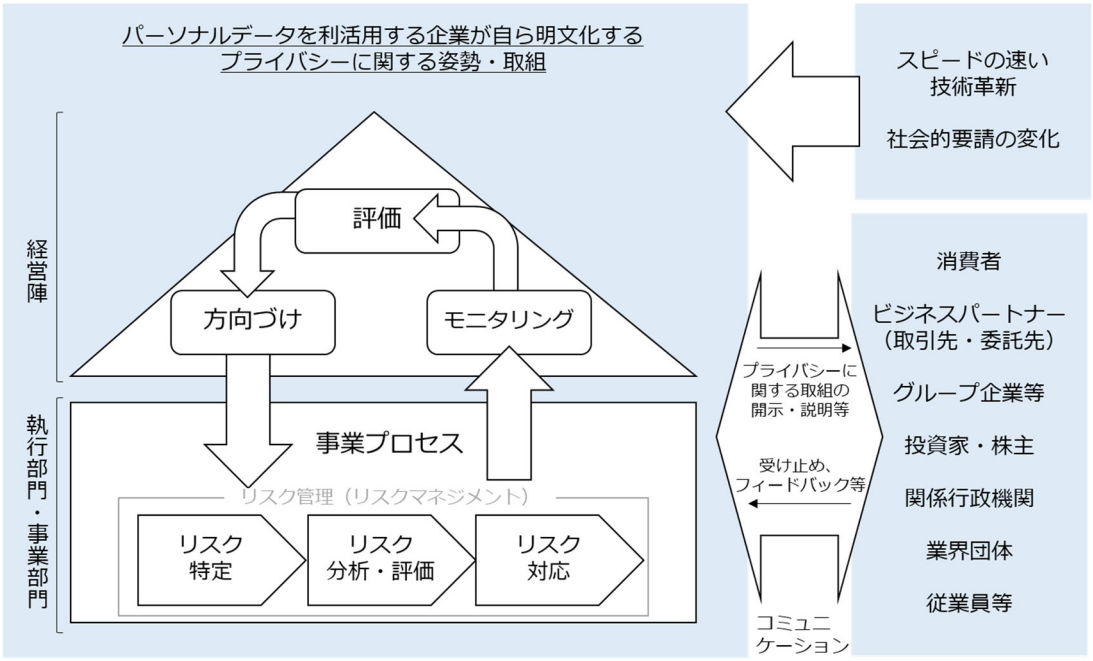
---

[23] 一般社団法人日本経済団体連合会でも、2019 年 10 月に「個人データ適正利用経営宣言」を公表し、経営者が、個人データの保護やサイバーセキュリティ対策が、事業リスクの低減のみならず、個人の安心・安全を獲得することで中長期的な企業価値の創造に寄与することを認識すべきとしている。

[24] 企業のガバナンスに必要とされる内容を整理したフレームワークは複数あるが、本ガイドブックの対象である、データやデジタル技術を活用しビジネスモデルを変革する DX を推進し、競争力向上を志向するような企業が参照できる一般的なモデルとして、IT ガバナンス（ISO/IEC38500）がある。

[25] 企業のガバナンスのあり方はそれぞれ異なると考えられる。図表 4 は一般的なフレームワークによる整理だが、本ガイドブックでは、基本的に企業のガバナンスにおいてこのようなサイクルが機能することを前提に、プライバシーガバナンスの構築に向けて、企業のガバナンス機

図表 4　プライバシーガバナンスのフレームワーク（イメージ）

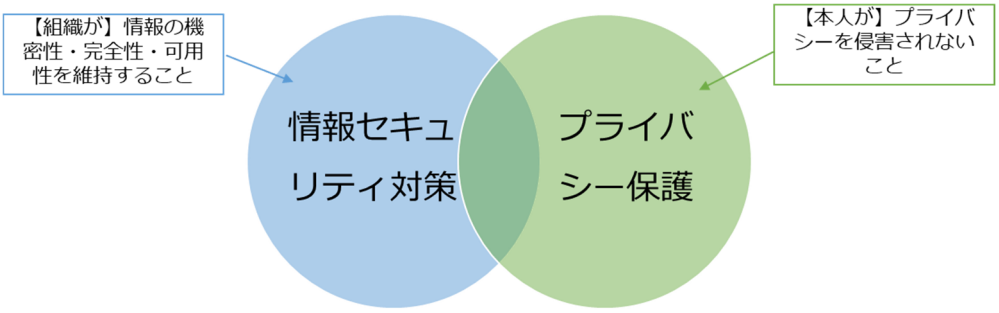


能やリスク管理プロセスの中に、プライバシーの観点から実装が望まれる具体的な内容を整理した。

コラム 情報セキュリティ対策とプライバシー保護

情報セキュリティ対策と、プライバシー保護は、DX 時代においては双方ともに欠かせない取組であるが、両者は概念として異なるものである。情報セキュリティ対策は、企業にとって自己の資産である情報の機密性・完全性・可用性の維持を目的とする。それに対し、プライバシー保護は、本人のプライバシーをはじめとする基本的な権利を損なうことのないよう、企業が、適切な対応を行うことを目的とする。そのためには、パーソナルデータに対する情報セキュリティ対策はもちろんのこと、より広範に（消費者本人や、場合によっては社会的に）、想定されるプライバシーリスクを特定し、分析・評価する必要があり、特に、適切な実施にあたっては消費者とのコミュニケーションが欠かせないものとなる。

消費者のプライバシー保護には、消費者のパーソナルデータに対する情報セキュリティ対策がなされていることは重要である。ただし、時には、企業の資産である情報の機密性を担保するために、企業の従業員本人の過度な監視が生じるといったように、情報セキュリティ対策とプライバシー保護との間にコンフリクトが生じる場合もある。



3. 経営者が取り組むべき三要件

Society5.0 の実現において、企業は、データの利活用によるイノベーション創出の中心的存在として期待されている。データの利活用が前提となる社会において、企業が一貫した姿勢で消費者のプライバシーを守っていくことは、個々の製品・サービス等の品質を高めることにつながり、企業のビジネスにおける優位性をもたらすとともに、消費者やステークホルダーからの信頼を獲得することとなり、企業価値の向上につながる。即ち、プライバシー保護とデータ利活用を単に二項対立として捉えるのではなく、プライバシーに配慮しながらデータ利活用のメリットを最大化していくという視点で捉えることが求められる。経営者は、プライバシーに関する取組を経営戦略の一環として捉え、競争力の要素として検討することが重要である。

もちろん、企業が、プライバシーリスクに配慮できない、あるいは、個人や社会に対するプライバシー問題の発生を抑止できない、という場合には、当該企業が差止請求や損害賠償請求（民法 709 条）を受ける、または当該企業に対する社会からの信頼が揺らぐ、といった事態になり得る。企業の売上や利益への悪影響にもつながるだけでなく、場合によっては企業の存続・事業の継続に懸念が生じることもあり得る。このような点からも、経営者としてはプライバシーに関する取組を行う必要がある。

株式会社の経営者は、善良な管理者としての注意義務（善管注意義務）を負う。かかる善管注意義務には、会社の規模に応じたリスク管理体制の構築も含まれる。したがって、かかる体制の不備により、損失が発生した場合には、関連部署の担当役員だけでなく、その他の役員も損害賠償責任を問われることとなり得る[26]。DX を推進する企業にとって、パーソナルデータを適切に管理し利活用することは業務執行において重要であり、適切な内部統制の構築ができずに、漏えいや炎上の結果として企業に損害が発生した場合には、その損害の責任を経営者個人が問われ得ることになる点に注意が必要である[27][28]。

---

[26] 会社法 423 条（対会社責任）、429 条（第三者責任）、民法 709 条（一般不法行為）による。

[27] あらゆる炎上について取締役が個人として責任を負うわけではないが、会社が保有するパーソナルデータやその利用形態に応じた適切なリスク管理体制として「炎上対策」が求められる場合には、それを欠いた結果として生じる炎上について、内部統制構築義務違反を理由として個人として責任を負うことがある。

[28] このため、企業の中には、受託業務のセキュリティ・可用性・処理のインテグリティ・機密保持・プライバシーに関わる内部統制の保証報告書（いわゆる SOC2 レポート）を取得することで信頼確保を図るクラウドサービスプロバイダー等のアウトソーシング事業者が増えつつある。

以上の観点から、企業の経営者には、プライバシーに関する取組を競争力の要素として、重要な経営戦略上の課題として捉えるとともに、コーポレートガバナンスとそれを支える内部統制の仕組みを企業内に構築・運用することが求められる。

プライバシーガバナンス実現のために、経営者がまずすべきことは、以下の３点である。

要件１：プライバシーガバナンスに係る姿勢の明文化 要件２：プライバシー保護責任者の指名 要件３：プライバシーへの取組に対するリソース投入

3.1. プライバシーガバナンスに係る姿勢の明文化

企業がそれぞれの企業理念の下、データを利活用しイノベーションによる価値創出を目指していく中で、組織として一貫した姿勢で、消費者のプライバシーを守っていくことが、製品・サービス等の品質を向上させ、消費者や社会からの信頼を獲得することにつながる。そして、企業価値を高めることとなる。

経営者はこれからの経営上の重要事項の１つとして、このことを認識し、企業がデータを利活用することによりどのような価値を提供していくかを踏まえ、組織の一貫した対応を可能とするプライバシー保護の軸となる基本的な考え方や、プライバシーリスク管理に能動的に対応していく姿勢を、明文化し、組織内外に知らしめることが必要である。

明文化した姿勢をトップダウンで浸透させることで、組織全体に認識を根付かせることができる。また、組織内に限らず、組織外の消費者やステークホルダー（株主、取引先等）などに対しても公表することで、企業が信頼を高める根拠となる。経営者には、明文化した内容に基づいてプライバシーに関する取組を実施することへのアカウンタビリティ[29]を確保することが求められる[30]。

---

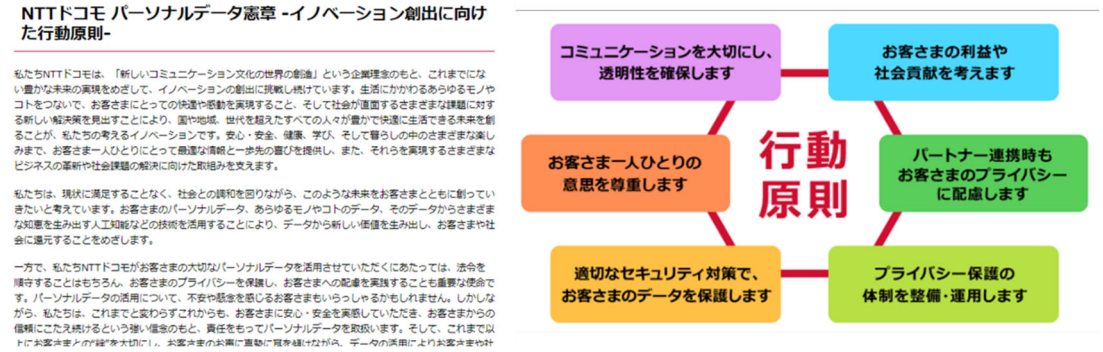
[29] Accountability は、単に説明を果たすという責任にとどまらず、最終的な、包括的な責任を果たすことができる状態を指す。

[30] 姿勢を明文化するに当たって、基本的なプライバシー保護の考え方として参照できるグローバルスタンダードの１つに、プライバシー・バイ・デザイン（PbD）というコンセプトがある。これは、ビジネスや組織の中でプライバシー問題が発生する都度、対症療法的にプライバシーリスクへの対応を考えるのではなく、プライバシー保護をビジネス構築の最初の設計段階であらかじめ考慮すべきであるという考え方である。プライバシーガバナンスに係る姿勢として、このような PbD の考え方や PbD7 原則（本ガイドブック「7.（参考）プライバシー・バ

明文化の具体的な形としては、宣言の形をとったプライバシーステートメントや、組織全体での行動原則などを策定するケースもある[31]。

事例：NTT ドコモ パーソナルデータ憲章の公表

株式会社 NTT ドコモでは、「パーソナルデータ憲章―イノベーション創出に向けた行動原則―」を作成し、公表している。このパーソナルデータ憲章は、株式会社 NTT ドコモが「新しいコミュニケーション文化の世界の創造」という企業理念の下、これまでにない豊かな未来の実現をめざして、イノベーション創造に挑戦し続けていること、社会との調和を図りながら、未来をお客様と共に創っていきたいと考えていること、パーソナルデータの活用に当たり法令順守はもちろん、お客様のプライバシーを保護し、配慮を実践することも重要な使命であることなどを宣言し、行動原則として 6 つの原則を提示している。



（出典）https://www.nttdocomo.co.jp/info/notice/pages/190827_00.html

テクノロジーの発展や社会的な要請などを踏まえ、行動原則や対応方針の内容及びその運用は、社会の信頼に応え続けられるよう、継続的に検証し、適宜見直しを行うことが必要である。

3.2. プライバシー保護責任者の指名

プライバシーガバナンスの実現には、経営者による関与と、プライバシーガバナンスに係る姿勢について明文化した内容（3.1 に記載）の具体的な実践が不可欠である。そのために、経営者は、企業のプライバシーに関する取組の、組織全体の責任者を担当幹部（以下「プライバシー保護責任者」という。）と

イ・デザイン」参照）の 1 つである「ゼロサムではなくポジティブサム」などは、企業が担う役割や姿勢の明文化と親和性が高く、整合的であることから、経営者にとって参考となる。

[31] なお、既に多くの企業が「プライバシーポリシー」を表題とする文書を掲げているが、この「プライバシーポリシー」は、「個人情報の保護に関する法律についてのガイドライン（通則編）」3-6 に示される「個人情報保護を推進する上での考え方や方針」や、JISQ15001:2017「個人情報保護マネジメントシステム－要求事項」で求められる内部向け個人情報保護方針及び外部向け個人情報保護方針に該当する場合が多い。大事なことは、形式を問わず、経営者自身の意思が滲み出てくるようなメッセージを明文化することである。

して指名し、経営者が姿勢を明文化した内容を踏まえて、その実践を行うための責任を遂行させることが必要である。経営者は、明文化した内容が実践されていることをモニタリングするために、プライバシー保護責任者に対し、サービス・システム企画、開発、運用といった事業プロセスにおけるリスク管理の活動等について報告を求め、その内容を、明文化した内容に照らして評価し、それを踏まえて方向づけを行うことで、組織の内部統制を効果的に機能させる（P.17 参照）。その際には、プライバシー保護責任者の責任範囲を明確にし、プライバシー問題の発生を抑止するために必要な対応を遂行するための権限も与える必要がある。経営者は、自社の有するプライバシーリスクや組織構造の特性を踏まえ、円滑な業務運営等も考慮して、適切な立場の者をプライバシー保護責任者として指名することが望ましい。[32][33][34]

[32]プライバシー保護責任者は組織内において個人データ処理の目的及び手段の決定に関与する権限のある役職（役員クラス）が担うことで効果的に機能する場合もあり得る。

[33] 「個人情報保護法　いわゆる 3 年ごと見直し　制度改正大綱」の第 3 章第 3 節の 2.（3）には、「個人データの取扱いに関する責任者の設置については、体制整備の一環として、個人情報の取扱いに関して、部署横断的・専門的な立場から各部署・従業員の指導・監督等を行うことは有効である。」と記載されている。

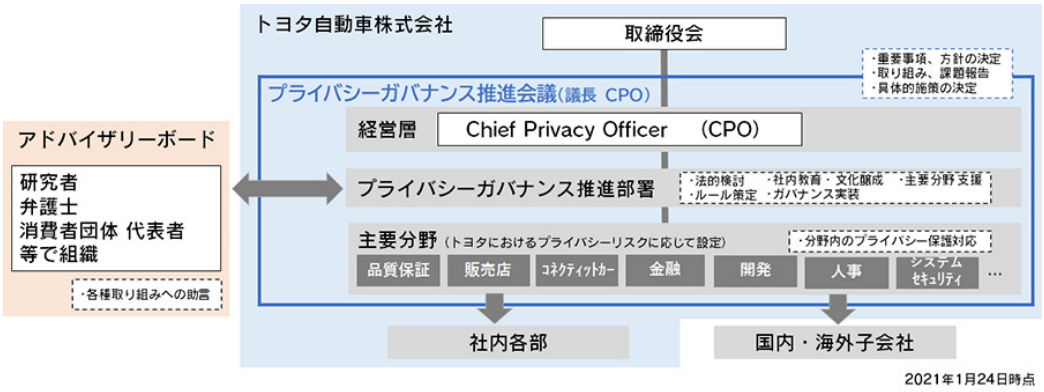
[34] 一般データ保護規則（GDPR）では、一定の条件において、利益相反規定において強い独立性が担保されている、データ保護オフィサー（DPO: Data Protection Officer）を設置する義務規定があるが、DPO は組織内において個人データの取扱いの目的及び方法を決めることにつながる地位（役員等）には就けないとされている。

なお、英国においては、英国一般データ保護規則（UK GDPR）に定められる DPO の設置規定があるが、特に小規模な組織において DPO の任命に苦労することを踏まえ、DPO の設置規定を見直し、組織内のデータ保護リスクに責任を持つ上級責任者（Senior responsible individual）を上級管理職（senior management）の一員として置くこととする法案「Data Protection and Digital Information Bill」の審議が進んでいる。

事例：トヨタ自動車　Chief Privacy Officer（CPO）の指名

トヨタ自動車株式会社では、お客様に寄り添ったプライバシー保護を実現するため、全社横断的なガバナンス体制を構築し、Chief Privacy Officer（CPO）を指名した。CPO の下、プライバシーリスクに応じて主要な業務分野（品質保証・販売店・コネクティッドカー・金融・開発・人事・システムセキュリティ等）を特定し、分野ごとにプライバシー保護対応の責任者を指名した。

また、CPO を議長とするプライバシーガバナンス推進会議を設置して定期的に会議を開催し、各分野におけるプライバシー保護対応の内容や、プライバシーに関する全社共通の課題、消費者とのコミュニケーション等の重要事項について、共有し検討を行う。加えて、プライバシー保護に影響する重要事案が発生した際には、各事業部門から報告を受けたプライバシーガバナンス推進部署が速やかに事象を把握し、具体的な対応策を検討の上、CPO 及び経営層に報告し対策を講じるよう、取り組んでいる。プライバシーガバナンス推進会議に対しては、外部有識者による専門委員会である「アドバイザリーボード」が助言を行う。



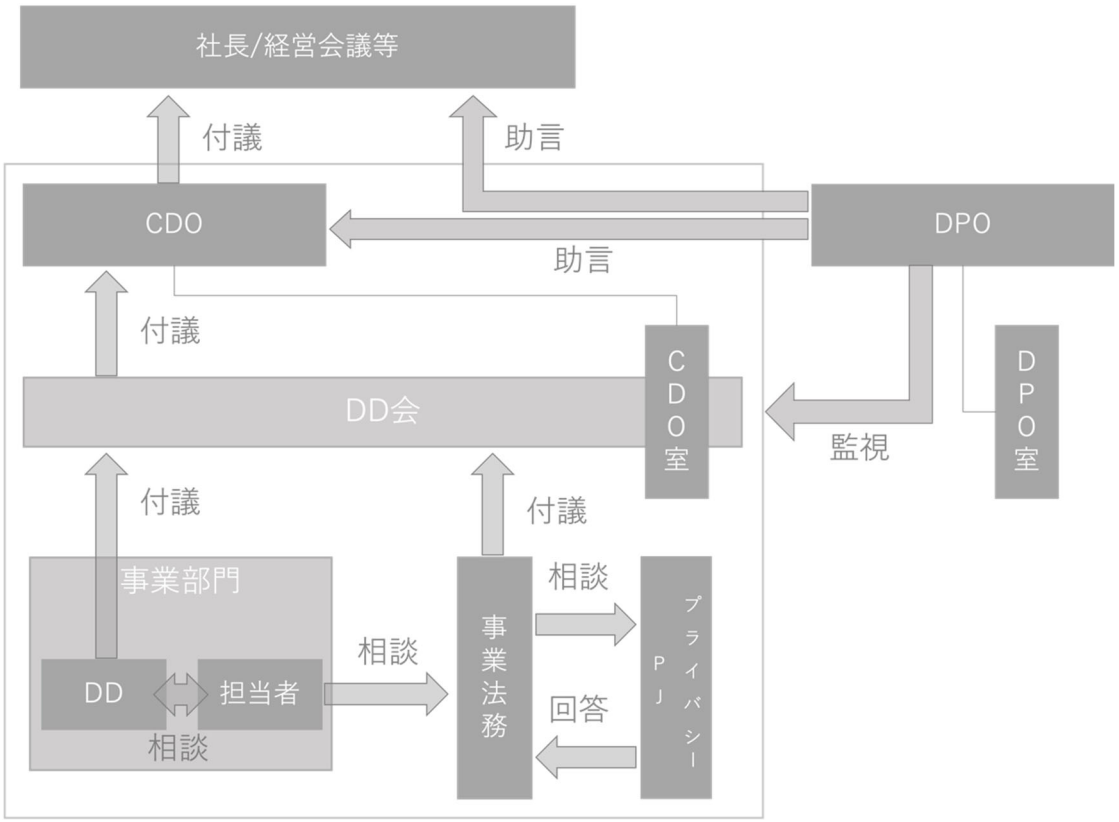
（出典）https://global.toyota/jp/sustainability/privacy/initiatives/

事例：ヤフー　最高データ責任者（CDO）、データ保護責任者（DPO）の指名

ヤフー株式会社では、法令を遵守しプライバシーに配慮したデータの利活用を推進するために、CDO（Chief Data Officer/最高データ責任者）を指名した。CDO の下、サービス単位でデータ利活用とプライバシー保護の両面に対応する DD（Data Director/データ責任者）を指名した。さらに、データ保護の取組について、利用者や社会の視点で、独立した立場から適正性に関する助言・監視・評価を行う、DPO（Data Protection Officer/データ保護責任者）を指名した。

事業部の事案に係るプライバシー保護の対応については、事業部門の担当者が法務部門に相談し、法務担当者から必要に応じて法務部門内のプライバシー対応チームに相談して、同チームが検討して回答する。DPO は、判断の過程とその内容が適切かを検討する。

全社的に影響を与える事案については、各サービスの DD の会議体である DD 会で検討した内容を、CDO へ付議する。DPO は、CDO が適切に決裁をするために必要な助言を行う。



（出典）（社内資料）

3.3. プライバシーへの取組に対するリソースの投入

経営者は、姿勢を明文化した内容の実践のため、必要十分なヒト・モノ・カネ等の経営資源（リソース）を投入することが求められる。自社のパーソナルデータの利活用に係るプライバシーリスクに能動的に対応するための体制を構

築し、そこに十分な人員を配置することや、人材育成、新たな人材の確保を実施することが必要である。

プライバシーに関する取組は、事後的に追加するものではなく、事前に検討され、戦略、事業、システムへ組み込まれるべきものである[35]。また、プライバシーリスクは、経営状況や外部環境に必ずしも依存せず、常時発生する可能性がある。そのため、プライバシーに関する取組に対して、リソースが継続的に投入され、取組自体の継続性が高められることが期待される。

なお、経営者は、リソースを投入した結果について、モニタリングの上、リソースの追加投入要否等について適切に評価し、評価結果等を踏まえた次の方向づけを行っていく（そしてそのプロセスを繰り返していく）ことが必要である。また、それらの取組全体について対外的に説明をしていくことが望ましい。

[35] PbD の考え方や PbD7 原則（本ガイドブック「7.（参考）プライバシー・バイ・デザイン」参照）にある「事前的／予防的」「初期設定としてのプライバシー」などは参考となる。

4. プライバシーガバナンスの重要項目

4.1. 体制の構築

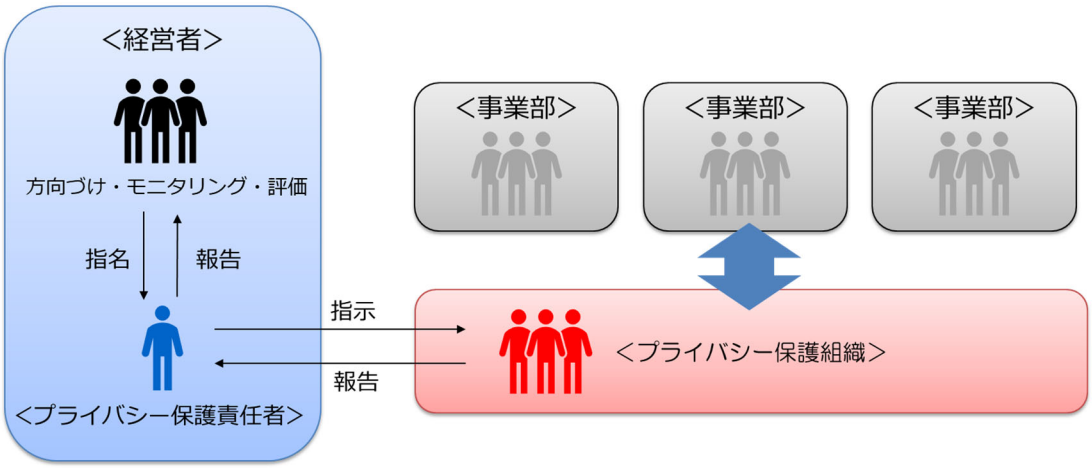
パーソナルデータを利活用する企業が、プライバシーガバナンスを機能させるためには、組織内の各部門の情報を集約し、各事業におけるプライバシーリスクを漏れなく見つけ、プライバシーリスク管理（リスクマネジメント）を行い、対応策を多角的に検討することが必要となる。リスクの特定、分析・評価、対応、継続的なレビュー・見直しといったリスクマネジメントの機能を、社内の体制の中に実装していく必要がある[36][37]。

経営者は、上記を実現するため、プライバシー保護責任者を中心として、中核となる組織（以下、「プライバシー保護組織」という。）を企業内に設けることが望ましいと考えられる。

図表 5　プライバシー保護の体制の構築

[36] プライバシーリスクを特定し、特定されたプライバシーリスクに対して、起こり得る結果や、起こりやすさ等を分析し、経営者が明文化したプライバシーガバナンスに係る姿勢等に照らして対応の優先度等を評価し、どのように管理・対応するかを決定する。対応結果についてもレビューを行い改善していくことが望ましい。

[37] リスクマネジメント手法の参考として、日本の個人情報保護法の遵守を基礎とした JIS Q 15001（個人情報保護マネジメントシステム）があり、国際的には ISO/IEC27001 及び ISO/IEC27002 を拡張し情報セキュリティマネジメントシステムに加えて個人識別可能情報（PII）の処理により影響を受ける可能性のあるプライバシーを保護するための要求事項とガイドラインが ISO/IEC27701 として発行されており、体系化されたものも存在する。これらのマネジメントシステムの規格を参照することもできる。ISO/IEC27001 及び ISO/IEC27002 は JIS Q 27001 及び JIS Q 27002 として JIS 規格が発行されている。ISO/IEC27701 も今後 JIS 規格が発行される見込みである。



急速な技術革新や消費者のプライバシー意識の高まりによって、日々、プライバシー保護の観点で考慮すべき範囲は拡大している。そのため、プライバシーリスクに対して、技術革新、社会的要請、消費者の意識などに対して多角的な検討・機敏な対応を担保できるような、プライバシー保護組織の構築が必要である。加えて、消費者等のパーソナルデータをグローバルに取り扱う場合には、プライバシー保護に対応するために諸外国の法令の適用に関して十分な配慮をすることやグローバルな体制構築が求められる[38][39]。

現時点では、プライバシー保護組織が設けられている企業は必ずしも多いとは言えないが、プライバシー保護組織を設けることで、新規事業部門を含む社内の関係部局とのネットワークを構築して密なコミュニケーションの醸成、社外有識者などからの関連情報や知見の収集・蓄積と社内共有、多角的なプライバシーリスクに係る対応策の検討等を実質的に推進していくことができる。

経営者は、自社の有するプライバシーリスクや、自社の組織構造・組織風土の特性（既存の各部門のキャラクターや役割、関係性等も含む）、リソース等を踏まえ、円滑な業務運営等も考慮して、適切な部門に、プライバシーリスク

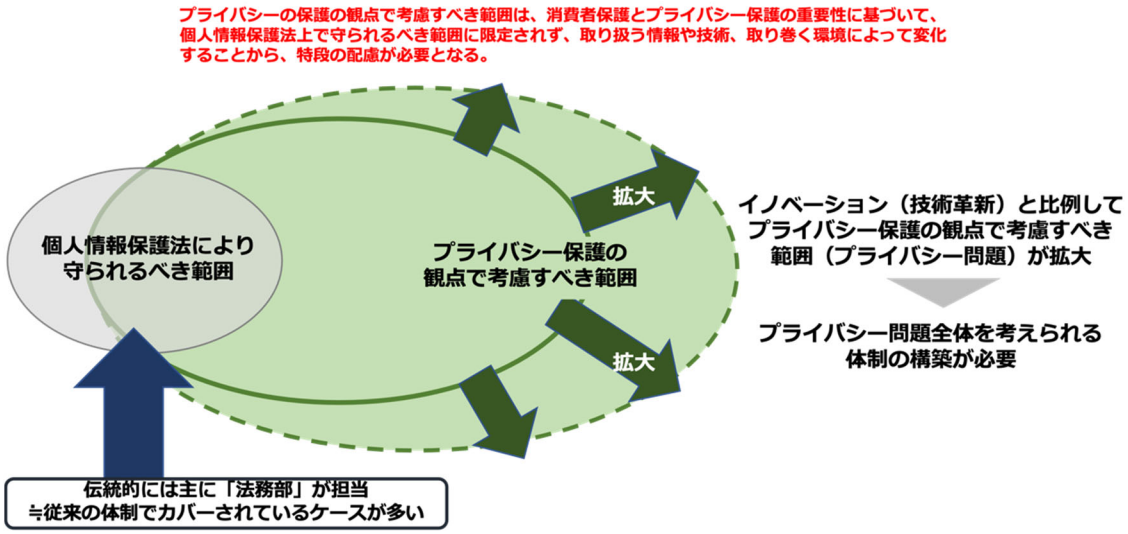
---

38 令和２年改正個人情報保護法では、本人の同意に基づいて外国にある第三者に個人データを提供する場合には、本人に対して提供する情報を充実させること（当該外国の名称、適切かつ合理的な方法により得られた当該外国における個人情報の保護に関する制度に関する情報、当該第三者が講ずる個人情報の保護のための措置に関する情報）、本人の同意がなくても外国にある第三者が基準適合体制を整備していることを根拠として個人データを提供する場合には、移転先の第三者に対して定期的な確認や支障時の対応を行うなど、一定の措置を講ずることを求めている。また、外国にある第三者への個人データ提供の有無にかかわらず、個人情報取扱事業者は、保有個人データに関する事項について、本人の知り得る状態に置かなければならず、安全管理のために講じた措置として本人の知り得る状態に置く内容の事例として、個人データを保管している外国の個人情報の保護に関する制度を把握した上での安全管理措置の実施を挙げている。

39 諸外国の法令等に係る情報収集方法については、「6.（参考）諸外国の法令等に係る情報収集方法」を参照のこと。

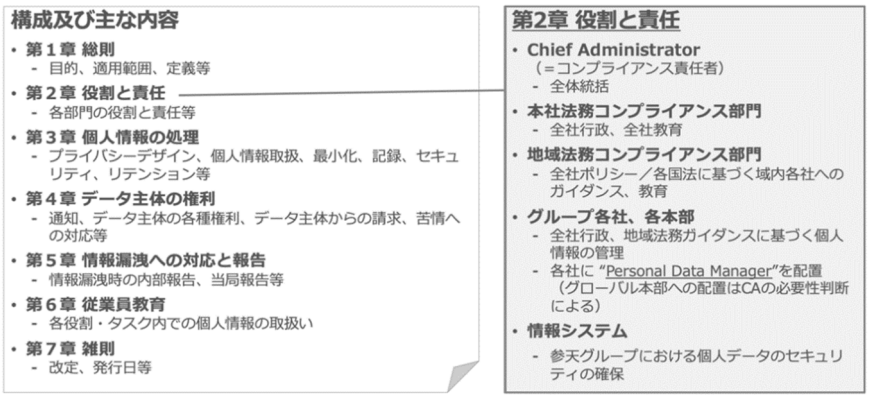
マネジメントの機能や、プライバシーに関する取組の中核となる役割を持たせることを検討する等し、体制を構築していくことが望ましい。

図表 6　拡大するプライバシー問題へ対応するための体制構築の必要性

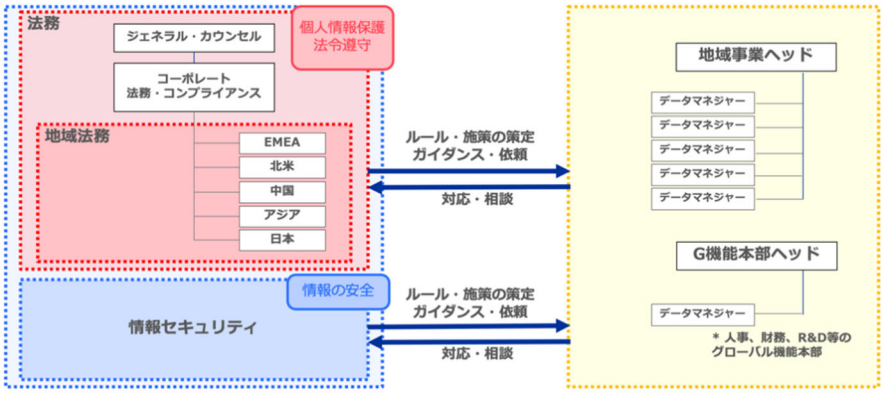


事例：参天製薬　グローバルでプライバシーガバナンスを構築

参天製薬株式会社では、パーソナルデータの取扱いについて、グローバルで体制構築を実施している。2020 年 4 月、参天製薬のプライバシーに関する基本事項を定めたグローバルポリシーを制定した。グローバル本社の下、地域・機能へ Data Manager を通じてガイダンスと働きかけを行っている。



Global Data Privacy Policy（出典）（社内資料）

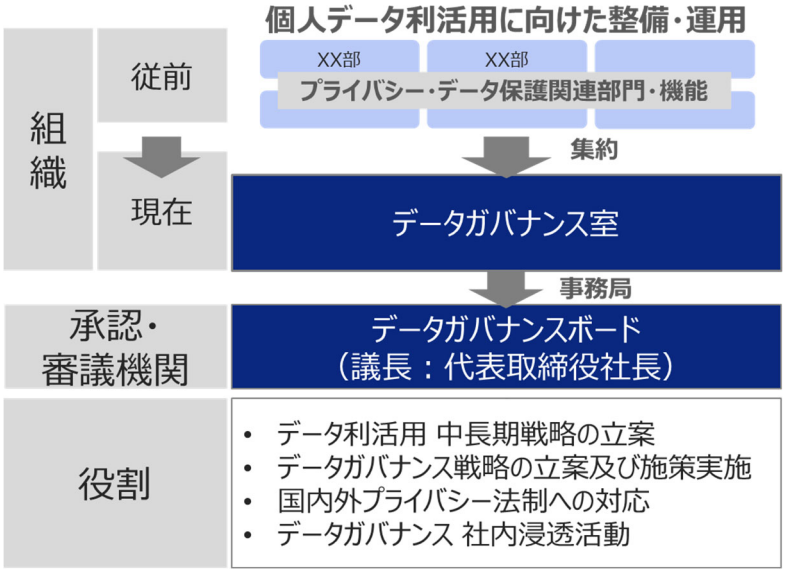


個人情報保護体制構築（出典）（社内資料）

事例：KDDI　データガバナンス室の設置

KDDI 株式会社は、個人データ利活用に向けた整備・運用について、各組織ごとに有していた機能を一元化・統合する形で 2020 年度新組織としてデータガバナンス室を設立した。

データガバナンス室は、管掌役員を社長とする組織として配置され、データ利活用・ガバナンス戦略立案等を所掌する。また、データガバナンスに係る意思決定機関として社長を議長とするデータガバナンスボードを組織している。



（出典）（社内資料）

4.1.1.　プライバシー保護責任者の役割

プライバシー保護責任者は、経営者が姿勢を明文化した内容等を踏まえて、経営者から与えられた権限に基づき実践のための方針を確立し、事業プロセスにおけるプライバシーリスクマネジメント（プライバシーリスクを特定・把握、評価し、対応策を検討）ができる体制を構築して、方針の実施を徹底する。方針には、実際にプライバシー問題が顕在化してしまった場合の緊急時対応や消費者救済、原因解析と改善の観点も含める必要がある。

プライバシー保護責任者は経営者に対して報告を行い、経営者は、その内容が、プライバシーガバナンスに係る姿勢を明文化した内容に照らして評価する。

4.1.2.　プライバシー保護組織の役割

プライバシー保護責任者の下に、実質的なプライバシーに関する取組の機能を担う中核組織として、プライバシー保護組織を設置することが望ましい。プライバシー保護組織の設計は、プライバシーガバナンスの重要性（2.3 参照）を踏まえて行われる必要があるが、具体的な設置形態は、企業によって異なることが想定される。例えば、専門的な知見を有する専任者を確保することが困

難な場合には、兼務の従業員のみでプライバシー保護組織を構成するなど、自社のリソースに合わせて実効性のある組織を構築することが大切である。

プライバシー保護責任者は、プライバシー保護組織の存在を企業内へ周知徹底する必要がある。

プライバシー保護組織の第一の役割は、企業内の各部門から新規事業やサービス内容に関する様々な情報を集約するなどし、プライバシー問題が消費者や社会に発現するリスクを漏れなく見つけることである[40]。そのため、事業部門などから寄せられるプライバシーに関連した相談を幅広く受けるだけでなく、事業部門に対して能動的に問題意識の共有を働き掛けるなど、日ごろから常に接点を持つことが望ましい[41]。新規事業や新規技術開発部門が悩みを抱え込まずに、自由に相談できる体制や環境が形成されることが大切である。

また、技術革新のスピードは速く、プライバシー問題は個人個人の感じ方の相違や、社会受容性がコンテキストや時間の経過で移り変わることから、常に関連する情報（市場動向、技術、制度など）を収集する必要がある。プライバシー問題に詳しい有識者（学識者、コンサルタント、弁護士、消費者団体など）との関係性を構築し必要に応じて相談することも必要である。

さらに、見つかったプライバシー問題に対して、事業部門と連携して、対象となる事業の目的を可能な限り実現しつつプライバシーリスクマネジメントを行い、場合によっては単なるリスク回避に限らず、よりポジティブな改善案の提案も含め、多角的に対応策を検討することが求められる[42]。この際には、ビジネススキームの観点はもちろんのこと、法制度やコンプライアンス上の観点、システムや情報セキュリティ上の観点での確認も必要である。加えて、サービスの利用者や消費者の受容性などの観点なども踏まえて、検討を行う必要がある。

検討に当たっては、必要に応じて、新規事業や新規技術を開発する部門とともに、関係する法務、システム関連、情報セキュリティ、コンプライアンス、広報、CS（カスタマーサービス）、経営企画、人権・ESG・サステナビリテ

[40] プライバシー問題については「5.2.プライバシー問題の洗い出し」を参照のこと。

[41] 企業によっては、新規事業・ビジネス開発に係る案件などについて、リスク特定、分析・評価の実施をルール化し、そのプロセスの中に、プライバシー保護組織の機能をもつ部署を組込んでいる場合もある。

[42] PbD の考え方や PbD7 原則（本ガイドブック「7.（参考）プライバシー・バイ・デザイン」参照）にある「ゼロサムではなくポジティブサム」などは、参考となる。

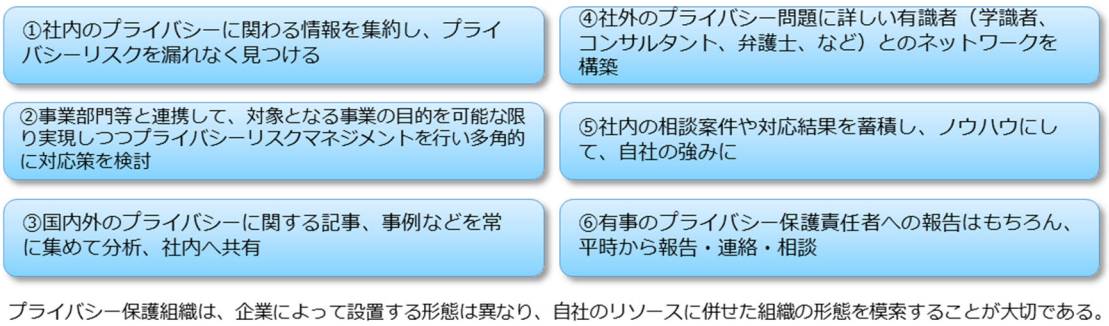
ィ部門[43]などとの連携を図ることが重要である。それぞれの部署の担当メンバーを決めておくなど、柔軟かつ迅速に必要なメンバーを招集できる体制を担保しておくことが望ましい[44]。

さらに、実際の事業において、プライバシー問題が発生してしまった場合の初動対応やその後の被害救済等の事後対応、原因解析と改善対応についても、事業部門と連携し、情報を集約・検討しプライバシー保護責任者へ報告し、指示を仰ぐ必要がある。

また、プライバシー問題に係る検討をした際の情報を履歴として蓄積し、必要に応じて活用できるようにしておく必要がある。定期的に社内のプライバシーに関する相談や案件の情報を取りまとめ、プライバシー保護責任者への報告や社内全体への共有を実施していくことなども重要である。

こうしたプライバシー保護組織が機能するためには、多角的な観点からなされる検討内容を取りまとめ、複数部署の間に立って調整できる人材も不可欠である。そのため、そのような人材を適切に配置することに加え、プライバシーに関する取組は高い専門性が必要な領域であることを念頭に置き、中長期的な視野に立ち、計画的に人材を育成していく必要がある。

図表 7　プライバシー保護組織の役割



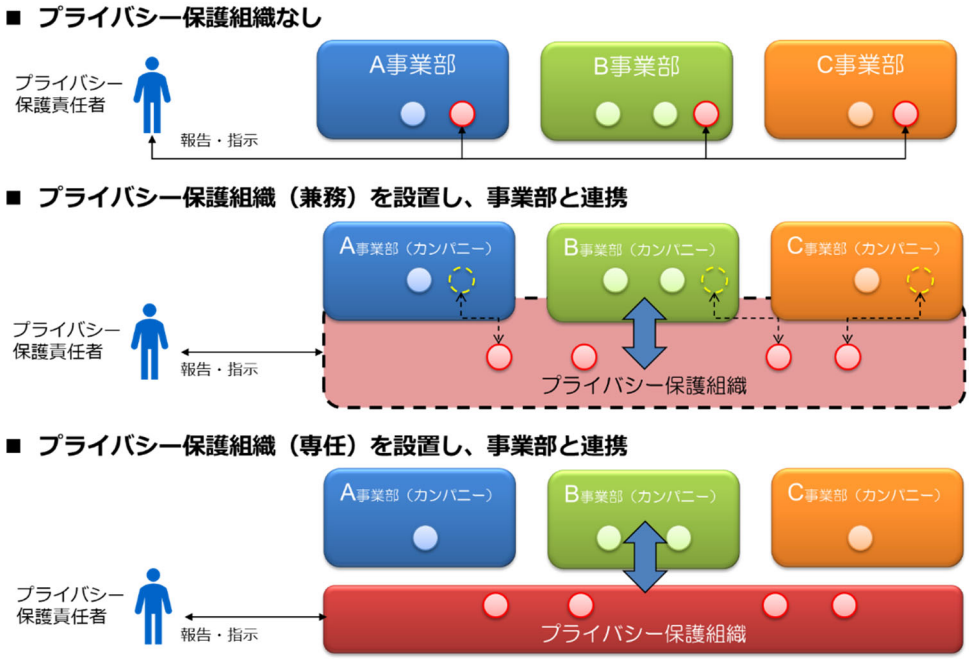
---

[43] プライバシー問題を発生抑止していくために、社内体制の構築を含め適切な対応を行うことが、企業の社会的責任や「ビジネスと人権」等の社会的要請とも合致するものであることは、「2.3 企業のプライバシーガバナンスの重要性」本文や脚注 15、脚注 16 を参照。

[44] 従来、企業がビジネスを行う上で、プライバシー問題を考える際には、個人情報保護法を遵守しているかどうかを中心に検討した上で事業が行われていることが主流であった。そのため個人情報保護法により守られるべき範囲については、法務部が主幹部署として担当し対応をしている場合も多い。一方で、プライバシー保護の観点で考慮すべき範囲は、日々、技術革新や消費者のプライバシー意識の高まりによって、その領域が変化・拡大しており、プライバシー問題に対して多角的な検討を担保できるようなプライバシー保護組織の構築が必要である。企業の事業内容や取り扱うデータなどによってプライバシー保護組織の適切な構成は異なるが、技術者のリソースを厚めにしたり、情報セキュリティのメンバーが中心になるケースなどもある。

実際にプライバシー保護組織を、どのような部門に紐付けて構築するかについては、企業規模やガバナンス体制、取り扱う情報の中身、組織の立地など様々な要素によって変わってくると考えられる（下図に例示）。重要なことは、どのような体制であれ、企業が引き起こし得る、プライバシーリスクや実際の問題を素早く把握し、プライバシー保護責任者へ報告し、指示を仰ぐことができるような体制にするということである。

図表 8　プライバシー保護組織の企業内での位置づけの例



4.1.3.　事業部門の役割

事業部門は自部門で扱う製品・サービス並びにデータなどがプライバシー問題を引き起こさないか当事者として確認する必要がある。事業部門の自覚と主体的な行動が非常に重要である。自部門だけで考えず、プライバシー保護組織と日頃から相談や連携をして、プライバシーリスクマネジメント（プライバシーリスクの特定、分析・評価、対策など）を推進することが必要である。また、消費者との接点がある場合には、消費者との信頼関係を構築する上で重要なポジションであることを十分に認識し、消費者の受容性などにも配慮する必要がある。

また、サービス提供や事業を担う部門として、CS 部門などと連携し、平時から消費者の意見を広く受け取れる体制を構築することが重要である。例えば、製品・サービス等のレビュー（例えばアプリストア上のレビュー）や SNS 上での消費者による情報発信などにも目を配り、いち早く消費者の反応などを

把握することも必要である。また、問題発生時には、プライバシー保護組織と迅速に連携して対応を進められるよう、日頃から情報を共有しておくことが大切である。

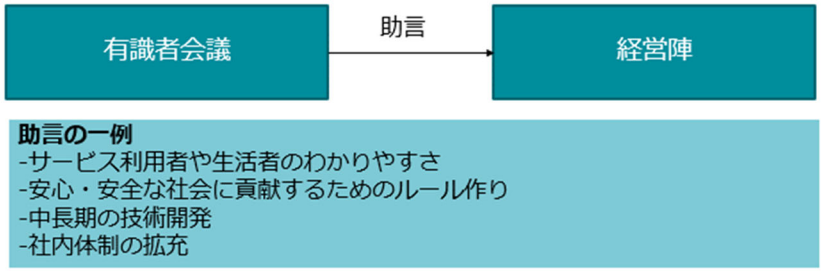
4.1.4. 内部監査部門やアドバイザリーボードなどの第三者的組織の役割

プライバシーリスクマネジメントが適切に行われていることを、独立した立場からモニタリング・評価することができれば、社内の取組を徹底でき、企業の取組について社外からの信頼を更に高める根拠にもなる。例えば、業務執行部門及びリスク管理部門等から独立した内部監査を実施する体制を構築することが考えられる。また、第三者的な立場である外部有識者からなるプライバシー保護に関するアドバイザリーボード、諮問委員会などを設置し、専門的な知見から、モニタリング・評価を受けるケースも検討すべきである。有識者としては、プライバシー問題に詳しい学識者、コンサルタント、弁護士、消費者団体などが想定される。

アドバイザリーボード等を設置することで、サービスリリース前に客観的な忌憚ない意見をもらうことや、問題発生時の適切な対応について事前に意見をもらうなどが想定できる。有識者の専門的かつ客観的な意見は、経営者や社員へフィードバックする体制・仕組みを構築することで、組織全体としてプライバシー問題・プライバシーリスクへの意識を高めていくこともできる。

事例：セーフィー　外部有識者会議の設置

セーフィー株式会社では、膨大なデータを預かる映像プラットフォームの健全性を保つ取組として、外部有識者会議を設置し、年に数回開催している。外部有識者会議は、法学者や弁護士、社外取締役、ビジネスパートナー等により構成される。「セーフィー データ憲章」の策定に係る議論や、変化する社会情勢の中でプラットフォーマーとしての責務を果たすために必要な取組についての継続的な議論を行っている。有識者からの助言を踏まえ、技術開発やルール等の継続的な改善や、データ活用の際のプライバシー配慮に係るユーザ企業に対する啓発活動などにも取り組んでいる（カメラ設置事業者向けの Web ページでの情報発信など）。

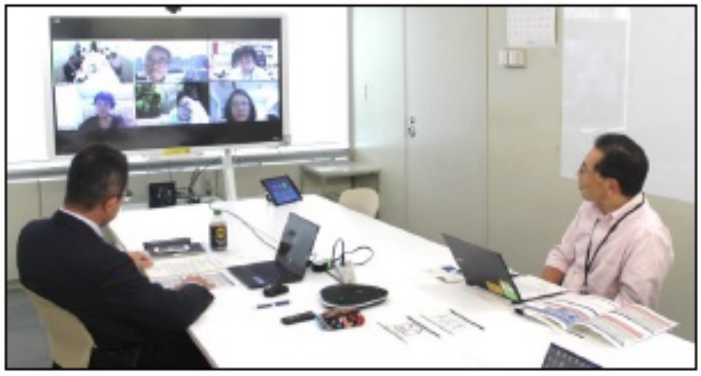


（出典）（社内資料）

事例：NEC　デジタルトラスト諮問会議の設置

日本電気株式会社は、外部有識者から多様な意見を取り入れ、経営判断や施策立案へ活かすために「デジタルトラスト諮問会議」を設置し、年 2 回開催している。諮問会議メンバーは、法学者、法律家、消費者団体代表、サステナビリティや人権などの分野の NPO 関係者等を含む 5 名で構成され、専門的な知見だけでなく、生活者の立場からも意見を取り入れている。

デジタルトラスト諮問会議では、プライバシーに関する国内外の動向を踏まえ、規制や社会受容性等の今後の動向、取組を強化すべき内容等について議論している。



(出典) https://jpn.nec.com/csr/ja/society/ai.html

4.2. 運用ルールの策定と周知

4.1 で記載した体制が実質的に機能するためには、製品・サービスや技術が開発・提供される前に、プライバシーリスクが、プライバシー保護責任者やプライバシー保護組織によって把握され、適切な検討がなされる必要がある。そのような運用が徹底されるためのルールを、プライバシー保護責任者の責任の下、組織内で策定しておくことが重要である。

例えば、プライバシー保護のための対策や、「どのタイミング」で「誰が」プライバシーリスクを特定、分析・評価するかなどの観点から、ルール化することが望ましい[45]。ただし、画一的な対応を招かぬよう、原理・原則の理解や定着を心掛けるとともに、継続的に内容の見直し・修正を行うなどのメンテナンスも必要である。

プライバシー保護責任者やプライバシー保護組織は、ルールを組織全体に周知徹底する必要がある。

[45] 「どのタイミング」で「誰が」プライバシーリスクを特定、分析・評価するかなどの観点については、「5.4. プライバシーリスク評価（PIA）」に例を記載。

4.3. 企業内のプライバシーに係る文化の醸成

プライバシーガバナンスに係る体制や運用を実質的に機能させていくためには、経営者が姿勢を明文化した内容について、組織全体へ浸透させ、プライバシーリスクに適切な対応ができるような企業文化[46]を、組織全体で醸成していくことが不可欠である。単なるコンプライアンスという意識ではなく、企業に所属する従業員一人一人が、一個人や一消費者としての立場から、プライバシーに関する問題について当事者意識をもっていることが重要である。このような従業員が、企業によるパーソナルデータ利活用に対する消費者の意識や不安、求めている情報や取組等についての理解を深め、社会と向き合った丁寧な対応を能動的にしていく状態が最も望ましい姿である。そのような企業文化を根付かせるためにはビジネスプロセスの様々なタイミングにおいて、継続的な取組を行うことが必要である。また、プライバシーに係る基礎的な知識の習得を促すだけでなく、自社がパーソナルデータの利活用によりどのような価値を提供していくかを踏まえて明文化したプライバシーガバナンスに係る姿勢等について、その大切さを経営者やプライバシー保護責任者が常に発信し続けることも~~が~~必要である。こうした取組は社内における専門人材の人材育成の基盤となるものである。

プライバシーは、日々変化するため、最新の事象や事業内容に合わせた教育が必要である。以下は、企業文化の醸成に係る取組の例である。

- 新入社員配属時、部署移動時のタイミングでの教育サポート
- 社員必携の冊子などの中で、プライバシー問題に対する姿勢に言及
- 定期的な e-learning や研修教育
- 人事部開催のセミナーとの連携
- プライバシー問題に対する方針と連動したハンドブック等の配布
- プライバシー保護責任者の活動を社内広報する等の啓発活動
- 定期的な配置転換（ジョブローテーション）の対象組織として、プライバシー保護組織を入れる
- パーソナルデータを取り扱う部署に対し、教育を集中的に実施

[46] 企業文化とは、従業員が共有する価値観や行動様式の集合体を指す。

4.4. 消費者とのコミュニケーション

プライバシーガバナンスには、消費者との継続的なコミュニケーションが必要である。また、企業は消費者のパーソナルデータ利活用に対する意識や不安、求めている情報や取組等について理解し、社会の受け止めの変化などを常に把握するとともに、企業がイノベーション創出やプライバシーリスクマネジメントに、いかに能動的に取り組んでいるのか、実際の問題が生じてしまった場合の対応をどのように行うのかという点について、消費者に対して積極的に、分かりやすく、丁寧に説明を行うことも重要である。消費者に対するアカウンタビリティを果たすよう務めることが、消費者との信頼関係を構築していく上で不可欠である。

4.4.1. 組織の取組の公表、広報

企業のプライバシー保護の考え方や、プライバシーリスクをどのように特定し、分析・評価し、コントロールしているか等を取りまとめ、社外に公表することも重要である。

例えば、透明性レポート（transparency report）[47]のように、消費者が特に懸念する項目等を、積極的に分かりやすく公表していく方法は有効である。データの高度な利活用が進むほど、新しいプライバシーリスクが発生することから、消費者の懸念を解消できるよう、取組の情報を定期的に取りまとめて発信することで、消費者も安心してサービスを利用することができる。

また、パーソナルデータを利活用した新規プロジェクトの実施方針・内容などを、実施前に社会へ公表するケースも増えてきた。消費者からのコメントを受け付け、検討し、反映してから実際に試行し、その結果を踏まえて見直しをし、事業開始するという取組も、消費者や社会との信頼関係を構築していくコミュニケーションのあり方として一般化しつつある。

4.4.2. 消費者との継続的なコミュニケーション

定期的なレポートだけではなく、新たな機能追加や利用規約等の改訂のタイミング等では、どのようにサービスやプライバシーリスクに係る対応を改善したのか、消費者に向けて、迅速に、分かりやすく Web サイト等で知らせることで、消費者も迅速に情報を得ることができ、サービスへの信頼につながる。なお、情報更新時には、更新された内容を利用者へプッシュ通知で知らせた

[47] 透明性レポートとは、消費者へのデータ取扱いの透明性を担保するために、企業が定期的に公表するレポート。

り、プライバシー設定についてあまり関心を払っていない利用者に対しては確認や見直しを働きかける案内を通知するなども大切である。企業から消費者へ、継続的に、積極的なアプローチをすることは、企業の信頼確保の観点からも重要である。

消費者が自らのデータの利活用について自らの意思を反映できるよう、問合せ窓口の提示や、データの取扱いに係るコントロールパネルの提供なども継続的なコミュニケーションの在り方のひとつと言える。

事例：NTT ドコモ パーソナルデータダッシュボードの提供

株式会社 NTT ドコモは、お客様自身のデータの提供先と種類の確認・変更、データ取扱いに係る同意事項の確認などの機能を提供している。

（出典）https://datadashboard.front.smt.docomo.ne.jp/

また、プライバシーは変化し得るものという特徴を踏まえ、消費者意識について消費者との各種接点から、把握ができるよう努める必要がある。

特に、データ解析を主な事業とする企業などが、日ごろから対面で消費者と接する事業会社との協業する場合などは、データ解析を主な事業とする企業自らもプライバシー保護の知見を高める必要があり、継続的にプライバシー問題に関わる意識調査等を行い、社会受容性などについて把握することも一つの方法である。また、調査を実施しただけで満足することなく、その結果を自社の取組へ反映させていくことが重要である。

事例：日立製作所・博報堂 生活者情報に関する意識調査の実施

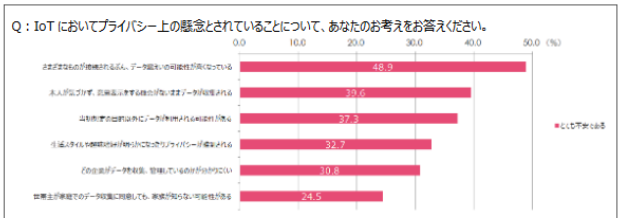
株式会社日立製作所と株式会社博報堂は、個人の意識の変化を定量的に把握することを目的に、継続的に意識調査を実施している。

日立における具体的な取り組み

- 日立・博報堂「ビッグデータで取り扱う生活者情報に関する意識調査」

  日立と博報堂は、パーソナルデータの利活用が進む中で個人の意識の変化を定量的に把握することを目的とし、継続的に意識調査を実施しています。2013 年の第一回、2014 年の第二回に引き続き、2016 年に第三回目の調査を実施しました[10]。

  2016 年度の第三回目の調査においては、最新の技術動向として IoT や AI に対する期待や不安等について調査し、事業者としての対応方針を検討しています。



（出典）
https://www.hitachi.co.jp/products/it/bigdata/bigdata_ai/personaldata_privacy/index.html
（参考）「第五回 ビッグデータで取り扱う生活者情報に関する意識調査」（日立製作所、2020 年）
https://www.hitachi.co.jp/New/cnews/month/2020/12/1222a.html

4.4.3. 問題発生時の消費者とのコミュニケーション

実際にプライバシー問題が生じてしまった場合には、迅速に問題発生を特定し、内容を把握した上で、対応することが重要である。そのために、4.1 に記載のとおり、関係する部門も含め、組織全体として問題発生時の体制や対応の流れを、製品・サービス等のリリース前に検討し、構築しておくことが必要である。

漏えい等の実害を受けた消費者に対しては、実際に発生した問題について、発生している事象の内容、原因、問題の対応のために企業が実施している措置などを、謝罪とともに分かりやすく伝える必要がある。特に、二次被害が発生するおそれのある消費者に対しては、二次被害の回避軽減のための措置（暗証番号の変更等）を迅速に実施してもらう必要があるため、可能な場合には必ず個別の通知を行うこととし、個別の通知ができない場合には、プレスリリースを出すなど、あらゆる手段をつくす必要がある。なお、問題の性質によっては、情報提供を行うことにより被害を拡大する場合があるので、セキュリティの専門家と相談の上、情報提供を行うべきである。

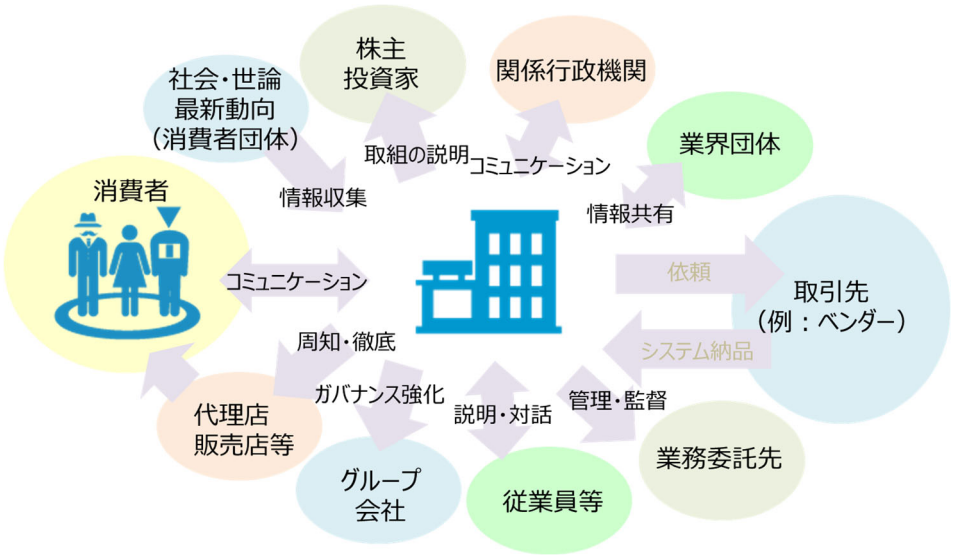
4.5. その他のステークホルダーとのコミュニケーション

プライバシーガバナンスでは、ステークホルダーと継続的にコミュニケーションをし、企業がイノベーション創出や、プライバシーリスクマネジメントにいかに能動的に取り組んでいるのかを、企業のステークホルダーに対して積極的に説明し、信頼を獲得していくことが重要である。

4.5.1. ステークホルダーへの対応

プライバシーに関する取組は消費者だけではなく、各ステークホルダーとの関係構築が欠かせない。

図表 9　ステークホルダーとのコミュニケーション



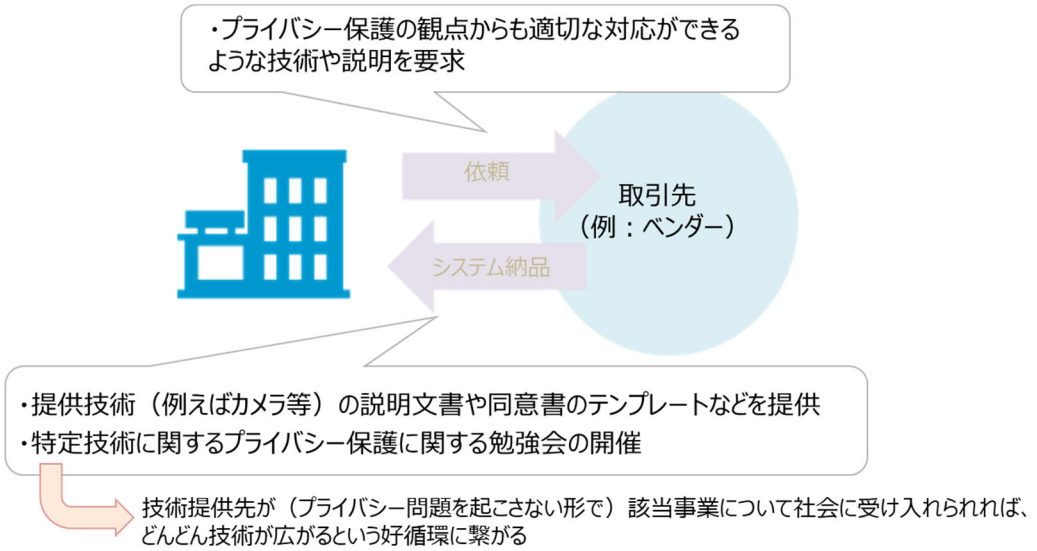
（１） ビジネスパートナー（取引先・業務委託先）

企業が事業を推進する際には、ビジネスパートナーなど、複数の企業と協働で実施する場合もあり、ビジネスパートナーも含めてプライバシーリスクに適切な対応ができなければ、自社を含む関係企業及び当該事業全体の信頼を失うことになる。

技術革新のスピードが速い領域では、新たなプライバシーリスクが発生しやすいことから、消費者のプライバシーに対する懸念が変化することを前提に、ベンダー等のシステム関係の取引先と密にコミュニケーションを図ることが特に重要となる。消費者のプライバシーリスクに対する懸念を絶えず見直し、システム面で事前に対応ができないかを検討し、対応を行うことが望ましい。

発注側の企業は、プライバシー保護の観点からも適切な対応ができるような技術や説明を取引先（ベンダー等）に要求し、取引先は説明を尽くすとともに、発注側の企業がプライバシー問題に配慮したシステム運用ができるよう、提供技術の説明文書や、技術を利用する際のプライバシーに関わるガイドライン、同意書のテンプレート等を提供したり、発注側の企業の理解を深めるための勉強会の開催を行うなども、有効な対応として考えられる。発注側の企業の製品・サービス等がプライバシー問題を起こさない形で社会に受容されることで、取引先側の技術もさらに広がっていくという好循環につながる。

図表 10　取引先とのコミュニケーションの例



また、業務を他社に委託する場合、その業務による問題が生じたときには委託元にも責任が発生する。このため、プライバシー保護の観点からも適切な対応ができる委託先を選ぶべきである。委託元は、対応に関わる体制・技術などの説明を委託先に要求すべきであり、委託先は、委託元のプライバシーへの取組を高めるように委託元に協力すべきである。プライバシー問題が起きたときは、委託元がその顧客や消費者に対して真摯に対応するべきである。

（２） グループ企業等

グループ内の子会社などが主体となって推進する事業であっても、プライバシー問題が発生すればグループ全体のブランドや信頼が失墜し得るため、グループ全体での、プライバシーリスクへの対応についても、意識する必要がある

だろう。グループ全体のプライバシー保護組織のあり方や、持株会社がどのような役割と責任を負うべきかについても、検討が必要となる。

また、海外に拠点がある場合には、現状、プライバシーに係る取組は各国で異なるため、国ごとに対応が必要であることに注意が必要である[48]。

（３） 投資家・株主

投資家も、企業業績への影響や社会的責任という観点から、リスク管理体制の強化について、コストでなく先行投資として評価を高める傾向がみられる[49]。株主や投資家に対しても、企業は、プライバシーリスクへの対応について明確な説明を行うよう、ますます求められるようになるだろう。透明性レポートの作成・公表、統合報告書、サステナビリティレポートへの記載なども、透明性の高い説明の一方法となると考えられる。企業の規模やリソース等に応じて適切な方法を選択することが重要である。

（４） 関係行政機関

個人情報保護委員会等、パーソナルデータの利活用やプライバシー問題に取り組む行政機関の相談窓口を日頃から確認し、プライバシーリスクが高いと思われる事業を開始する際には、事前に相談を行うことが重要である[50]。また、業界によっては、個別の業法や所管省庁が制定するガイドラインを遵守し、所管省庁とのコミュニケーションをとりながら、業界の特殊性を踏まえた、適切な運用が求められる場合もある。

（５） 業界団体

業界によっては、業界の健全な発展を図り、消費者への理解を醸成していくため、業界団体や認定個人情報保護団体などを組成し、調査・研究、広報・PR活動、意見発表、関係省庁との連絡・意見具申などを実施している場合がある。同業他社が同じ技術分野でプライバシー問題が生じてしまうと、自社の同様の製品・サービス等についても消費者の信頼を失ってしまう可能性がある。

---

[48] 諸外国の法令等に係る情報収集方法については、「6.（参考）諸外国の法令等に係る情報収集方法」を参照のこと。

[49] ダボス会議の「ステークホルダー資本主義」や米国のビジネスラウンドテーブルの BRT 宣言などから、ステークホルダー全体の利益を考える機運が高まっている。

[50] 個人情報保護委員会が設置している PPC ビジネスサポートデスクでは、事業者における個人情報の保護及び適正かつ効果的な活用についての啓発の一環として、新技術を用いた新たなビジネスモデル等における個人情報保護法上の留意事項等について、相談を受け付けている。

そこで、業界団体などを通じ、プライバシー問題・プライバシーリスクにかかる情報共有に積極的に参加し、積極的に情報提供及び情報入手を行うことが必要である。また、入手した情報を有効活用できるような環境整備が必要である。[51]

（６） 従業員等

企業は従業員のプライバシーに関する情報を取り扱うことが多いことから、従業員に対してもプライバシーへの配慮が必要となる。他方で、セキュリティやその他の事業運営上の要請から、従業員のプライバシーを制限する必要が生じる場面がある。また、従業員に関する情報を管理する以上その漏えいのリスクも存在する。したがって、従業員も、コミュニケーションをとるべき主体として捉え、従業員との対話や従業員代表を通じた説明・周知などの取組が重要である[52]。また、このとき、その企業の従業員だけでなく、求職者、退職者、取引先の従業員等に対しても、配慮が必要となる。

4.5.2. プライバシー問題の情報収集

プライバシーは日々変化するため、前述の消費者の意識調査等の取組だけではなく、国内外の法制度の動向や業界団体との情報交換、社会や世論などの最新動向を継続的に入手することが重要である。

特に、個人情報保護委員会の Web サイトでは、個人情報保護法、関連するガイドライン及び Q&A など、関連する情報の発信が行われている。また、経済産業省の個人情報保護関係のサイトでは、過去に経済産業省が実施した、パーソナルデータなどに係る検討結果などが情報発信されている[53]。

また、アドバイザリーボードに招聘する有識者や、プライバシー問題に詳しい弁護士などからの情報収集も有益である。

---

[51] 例えば、一般社団法人電子情報技術産業協会（JEITA）では、2023 年 3 月に「スマートホーム IoT データプライバシーガイドライン」を策定し、スマートホームにおける生活データであるスマートホーム IoT データの取り扱いに関する基本的な指針を示すとともに、同データについて、個人情報保護やプライバシーに配慮しながら収集・活用するために、各関係者が考慮すべき最低限のあるべき姿を示している。

[52] 2019 年には、求職者（新卒）の採用に関してデータ分析・利用への不適切な事例が生じたが、従業員の監視についても同様の構造が生じ得るものであり、分析を提供した側だけでなく、それを利用した企業には同等以上の責任が生じていることに留意すべきである。

[53] 経済産業省 Web サイト「プライバシーガバナンス」ページ
https://www.meti.go.jp/policy/it_policy/privacy/privacy.html

4.5.3. その他の取組

プライバシーリスクの把握や対応策の検討について、個社での対応・検討が困難であったり、業界での対応や、業界横断での対応が必要な場合には、業界団体、政府、官民で運営されているコンソーシアムなどを中核として、有識者を集め、その適切な対応や配慮すべき事項について検討し、結果を公表していくなどの取組も行われている[54]。

[54] 例えば、「カメラ画像利活用ガイドブック」（経済産業省・総務省・IoT 推進コンソーシアム）の検討・公表など。

5. （参考）プライバシーリスク対応の考え方

プライバシー問題に対応する際には、リスクの特定を行い、リスクに応じて柔軟に対応策をとるリスクベースのアプローチで考える必要がある。プライバシーリスクマネジメント（リスク特定、分析・評価、対応）等を進める際に、参考となる考え方や情報などを示す。体系的に記載をしているわけではなく、あくまで参考情報であり、各企業が自らプライバシーリスクマネジメントを行う際に、参照いただきたい。

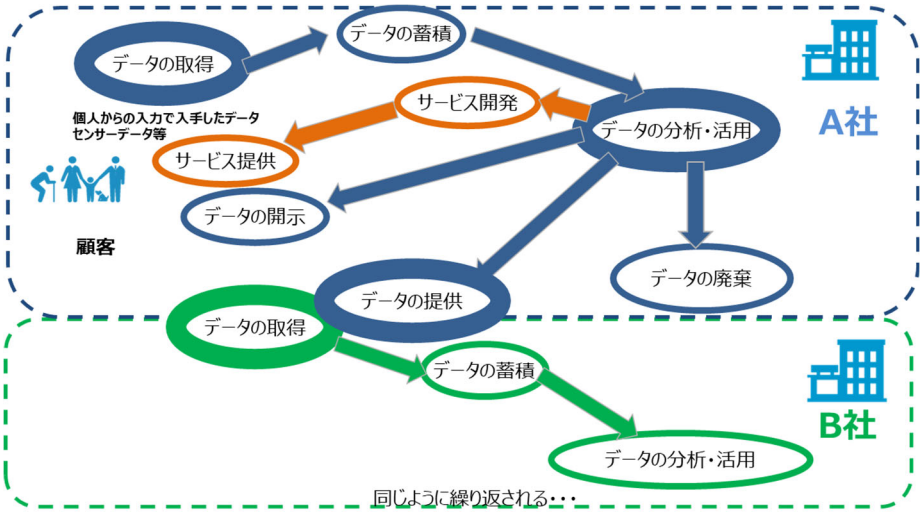
5.1. 関係者と取り扱うパーソナルデータの特定とライフサイクルの整理

プライバシーリスクの特定のために、対象事業におけるパーソナルデータのライフサイクルを整理する必要がある。特に整理すべきポイントは以下のとおりである。

- ✓ 対象事業の関係者（消費者、ビジネスパートナー（取引先・業務委託先等））を特定する
- ✓ 対象事業で取り扱うパーソナルデータを特定する（特定するパーソナルデータは、直接取得するデータだけではなく、第三者からの購入やプロファイリングによって推測されるデータも含むこと）

以下の図は、データの取得からデータの再提供や廃棄に至るまでのライフサイクルを、例として示したものである。どの部分を外部事業者に委託するか、データを共同利用する外部事業者がいるか等、データのライフサイクルの確認に合わせて、関係する事業者（ビジネスパートナー）との関係性も整理が必要である。（早い段階で関係する事業者との間でスキームを決めておかないと、法令遵守の観点においても、それぞれの事業者が実施すべき義務が明確にできない点に注意が必要である。）

図表 11　パーソナルデータのライフサイクルの例



パーソナルデータのライフサイクルの可視化を行う中で、消費者が認識しやすい部分と、認識しづらい部分も見えてくる。特に、カメラやセンサーなどの IoT 機器により取得されたパーソナルデータや、プロファイリング等で推測されたデータの利活用などについては、プライバシー問題が起こりやすいため、プライバシーリスクを特定、分析・評価し、対応するとともに、パーソナルデータの取扱いやその目的を、消費者へ丁寧に説明する必要がある。

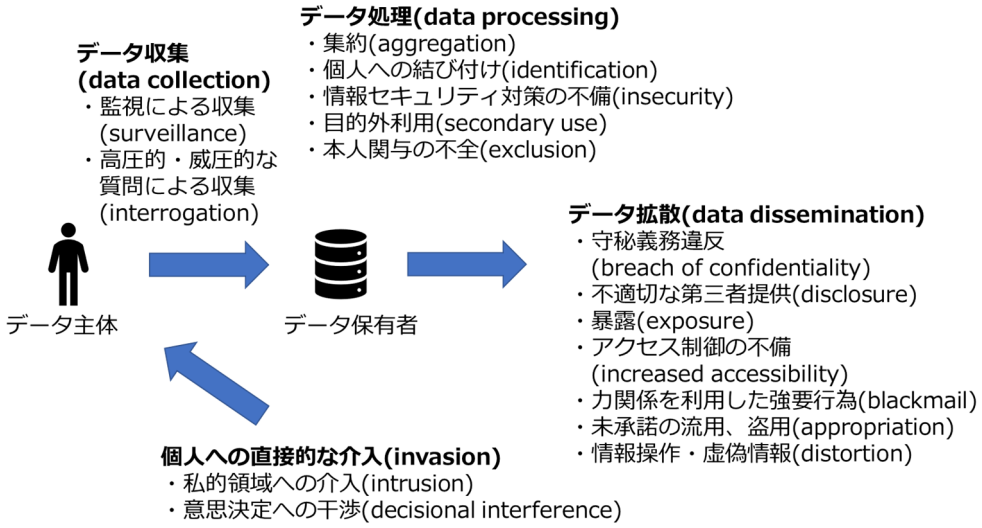
また、ISO/IEC 29100: 2011 Privacy Framework（JIS X 9250:2017 プライバシー保護の枠組みと原則）の第 4 章のプライバシーフレームワークの基本要素の中には、PII（Personally identifiable information）処理における登場者（actor）の役割、登場者間の PII やりとりのシナリオ、PII の認識（どのような場合を PII とみなすべきか）の記載もあり、参考にできる。

5.2. プライバシー問題の洗い出し

パーソナルデータのライフサイクルの中、どのようなところにプライバシー問題が発生するかについて洗い出した上で、そのプライバシー問題への対応方法を検討する。

以下はあくまでも一例であるが、パーソナルデータのライフサイクルの各段階の中で、どのようなプライバシー問題が発生し得るかを示したものである。対象事業のシステム要件や運用を検討する際に、このような情報を参考にしつつ、対象事業の特性を考慮し、経営者がプライバシーガバナンスの姿勢等について明文化した内容に照らして、自らプライバシー問題を洗い出すことが重要である。

図表 12　プライバシー問題を作り出す諸活動の類型



（出典）「A Taxonomy of Privacy」（DANIEL J. SOLOVE、2006 年）より Figure1 を参照して事務局作成

図表 13　プライバシー問題の例

データ収集	監視による収集	継続的なモニタリングにより、個人に対して不安や居心地が悪い感情を与えてないか
	高圧的・威圧的な質問による収集	個人に圧力をかけて情報を詮索してないか、深く探るような質問で個人が強制を感じ、不安になってないか
データ処理[55]	集約	ある個人の情報の断片を集め、それにより、個人が想像しなかった新しい事実が明らかになることにより、個人の期待を裏切ってないか
	個人への結び付け	あらゆるデータを個人に結び付けることで、個人にとって害のある情報も結び付けられてしまい、個人に不安、不満を与えてないか
	情報セキュリティ対策の不備	パーソナルデータの適切な保護ができないことによって、個人に対して不利益を被るようなことが起こってないか
	目的外利用	個人の同意なしに当初の目的とは違うデータ利用を実施し、個人を裏切るような行為になってないか
	本人関与の不全	個人のデータの開示・訂正の権利を与えない等、重要な意思決定に対して個人のコントロールが効かないようになっていないか

[55] AI を前提とした社会においては、個人の行動などに関するデータから、政治的立場、経済状況、趣味・嗜好等が高精度で推定できることがあり、本人の望まない形での流通や利用により、個人の自由、尊厳、平等の侵害といった問題が発生する可能性があるが、「集約」や「個人への結び付け」といったプライバシー問題において、それらの問題が観念されるだろう。（「人間中心の AI 社会原則」（総合イノベーション戦略推進会議、2019 年）にも「プライバシー確保の原則」が定められている他、「プロファイリングに関する最終提言」（パーソナルデータ＋α研究会、2022 年）においても、パーソナルデータとアルゴリズムを用いて、特定個人の趣味嗜好、能力、信用力、知性、振舞いなどを分析又は予測すること（プロファイリング）に対して、その効用とプライバシー権、平等原則、民主主義との関係における問題のリスクを踏まえ、適切に対応するための留意点がまとめられている。）

データ拡散	守秘義務違反	特定の関係における信頼関係により取得した個人のデータを他社に開示するなどで、（暴露されたデータの性質にかかわらず）その関係性を破壊していないか。個人へ裏切りの感情を与えてないか
	不適切な第三者提供	個人のデータを第三者へ開示されることで、二次利用先で更なるプライバシー問題が生じていないか
	暴露	生活の諸側面を他者へ暴露することにより、深刻な恥辱を経験し、個人の社会参加能力を妨害することになっていないか。
	アクセス制御の不備	パーソナルデータへの他者のアクセス可能性を増大させ「開示」のリスクを高めていないか。
	力関係を利用した強要行為	パーソナルデータの暴露、他者への開示などを条件にとるなど、強力な権力関係が作り出され、個人が支配され、コントロールされる事態になっていないか。
	未承諾の流用、盗用	他者のアイデンティティやパーソナリティ（例として、名前、肖像等が挙げられるが、これらに限らない）を許可なく誰かの目的のために用いることで、個人が自分自身を社会に対してどのように掲示するのかについてのコントロールを失わせ、自分自身を物語る著作性における個人の自由へ介入することになっていないか。
	情報操作・虚偽情報	個人が他者に知覚され判断される見方を操作し、虚偽や、誤解を招くような情報を示すことで、個人の恥辱やスティグマ、評判上の危害に帰結することはないか。自己アイデンティティと公共的生活に従事する能力に不可欠な、個人の評判や性格を捻じ曲げることになっていないか。それにより、社会的関係の恣意的かつ不相応な歪曲が行われる恐れはないか。
個人への直接的な介入	私的領域への介入	必要以上の個人へのアプローチ（メールや電話等）により、個人の日常の習慣が妨げられ、居心地が悪く不安な感情を引き起こされてないか。
	意思決定への干渉	個人の生活において重要な意思決定に対して AI を用いている場合等において、決定方法が不透明で、個人に萎縮効果が働いてないか。

（出典）「A Taxonomy of Privacy」（DANIEL J. SOLOVE、2006 年）を参照して事務局作成

5.3. プライバシーリスクの特定

自社のパーソナルデータのライフサイクルおいて、プライバシー問題が個人や社会に生じるリスク（プライバシーリスク）を特定する際には、フレームワーク等を参考にすることもできる。

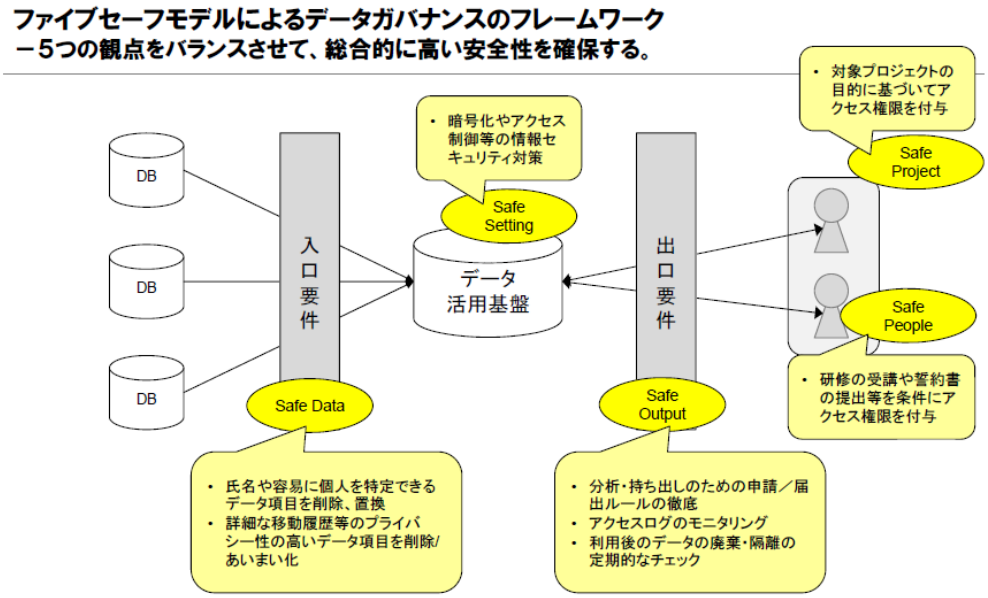
例えば、「ファイブセーフモデル」は、データの有用性を確保しつつデータを安全に取り扱う方法として、イギリスの統計局（ONS）において、機密情報を利用した研究を規律するために 2003 年から運用されてきた。「ファイブセーフモデル」においては、EU をはじめとする諸外国で、統計の個票データ利活用のみならず、データ利活用時の安全対策ルールとして広く実績もあり、プライバシー問題及びその対策方法を考える上で参考となり得る。

図表 14　参考：ファイブセーフモデルの概要

項目	説明
安全なプロジェクト（Safe Project）	データ利用の目的・取扱いが法的、社会的規範の見地から適切か？
安全な利用者（Safe People）	研究者は、個票データを適切な方法で使うことについて信頼できるか？
安全なデータ（Safe Data）	データ自体に機密開示のリスクはないか？
安全な設備環境（Safe Setting）	設備環境は、承認されていない利用を制限しているか？
安全な分析結果（Safe Output）	分析結果は、機密開示のリスクはないか？

（出典）Tanvi Desai, et al. “Five Safes: designing data access for research” (University of the West of England), 2016

図表 15　参考：ファイブセーフモデルによる
データガバナンスのフレームワーク



5.4. プライバシー影響評価（PIA）

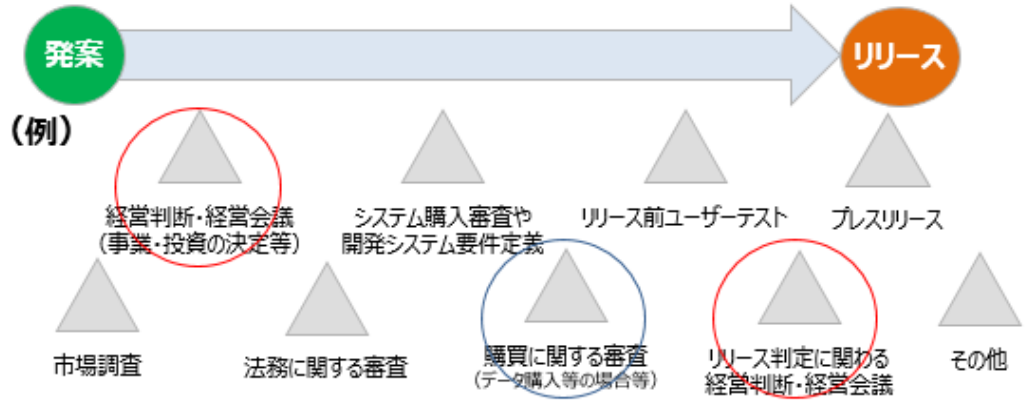
プライバシー影響評価（PIA: Privacy Impact Assessment）とは、個人情報及びプライバシーに係るリスクの特定、分析・評価を通じて、その対応検討を行う手法である。

プライバシーリスクを特定、分析・評価・対応するに当たっては、どのタイミングで誰がプライバシーリスクを特定、分析・評価するかが重要である。例えば、サービスをリリースする直前にプライバシーリスクが高いことが判明し

ても、対策を練る時間がない。逆に早すぎるタイミングであっては、プライバシーリスクのイメージが湧かないということも考えられる。

下図は、事業部門が製品やサービスをリリースするまでのステップを例示したものである。対象事業のプライバシーリスクが大きいと想定される事業においては、事業検討初期のタイミングとリリース判断のタイミングで、経営者を含めてプライバシーリスクを特定、分析・評価するなどの方法が考えられる。システム要件定義を検討する前からプライバシーリスクを特定、分析・評価して対策を講じ、リリース判断のタイミングでそのリスクがきちんと低減されているのかを確認する、残存リスクがあればリリース後の対応を事前に考えておく等の対応をすることも考えられる。また、外部サービスを導入する場合や、自社でパーソナルデータを取得せず、外部からデータを購入する場合などにおいては、契約の法務審査や購入審査のタイミングで、法務部やプライバシー保護組織と、プライバシーリスクを特定、分析・評価することも有用だと考えられる。

図表 16　例：製品やサービスをリリースするまでのステップ



どのタイミングで、誰がプライバシーリスクを特定、分析・評価するかは、事業規模や事業内容、取り扱うパーソナルデータの内容等によって異なるが、例えば、パターンごとに類型化してルールを定めるなどが重要である[56][57]。

また、一定期間運用して得られた知見を集約し、プライバシーリスクを把握するために必要な情報についてテンプレート化を行ったり、チェックリストを

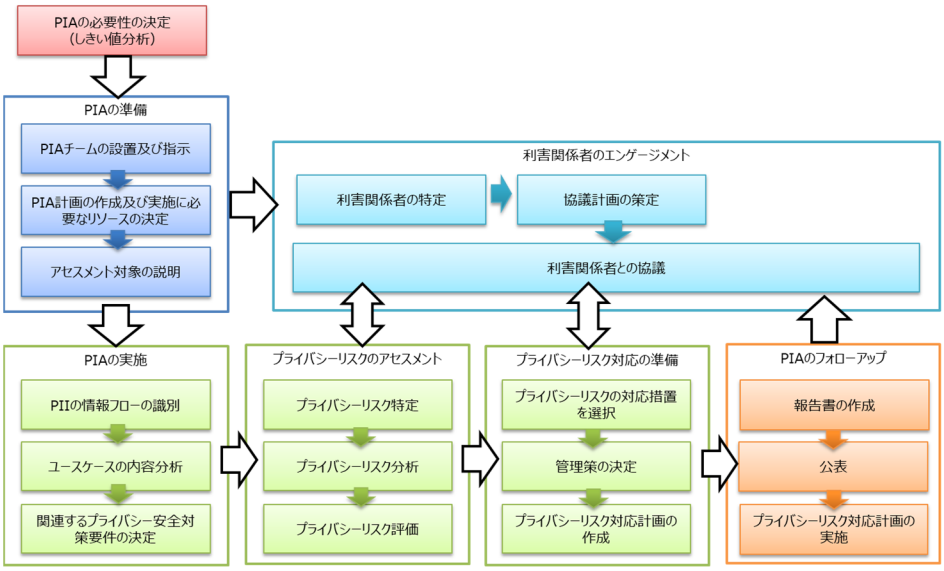
[56] 企業内に既に構築されている、セキュリティなどの他のリスクを特定、分析・評価する体制や運用フローをうまく活用したり、パーソナルデータを多く利活用する部署から優先的にルールを整備するなどの工夫により、効率的な運用につながる場合もある。

[57] ウォーターフォール型の開発でなく、アジャイル型での開発の場合には、プロダクトオーナーをはじめ現場の関係者がプライバシー問題への認識を常に持ち、対応を行うことが必要になる。また、リリース判断のタイミングでリスクが低減されていることを確認することを徹底することが重要である。

作成するなどの方法を採用してもよい。ただし、チェックリストやテンプレートが画一的な対応を招かぬよう、携わるメンバーへ原理・原則への理解を常に醸成することが必要である。また、継続的に見直し・修正を行うなどのメンテナンスも必要である。

ISO/IEC 29134:2017 Guidelines for privacy impact assessment（JIS X 9251：2021 プライバシー影響評価のためのガイドライン）では、PIA の実施プロセス及び PIA 報告書の構成等についての推奨事項が示されている[58]。

図表 17 参考：ISO/IEC 29134（JIS X 9251）の主な内容



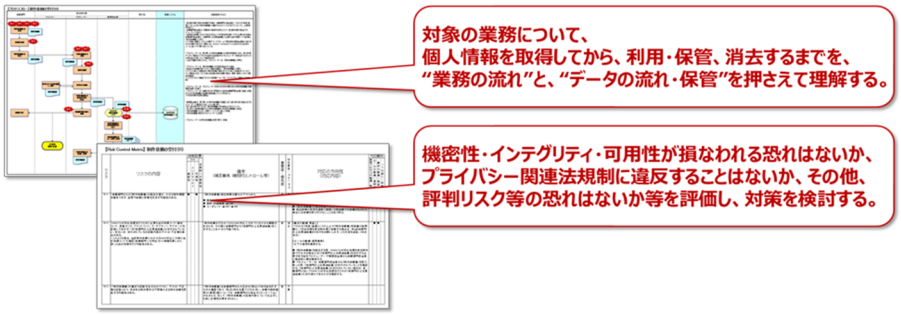
※ISO/IEC29134を参考に作成

[58] この規格で用いられている用語及び定義は、ISO/IEC29100 Privacy framework（JISX9250 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と原則））による。プライバシー安全対策要件（privacy safeguarding requirements）については、こちらの規格で説明されている。
なお、ISO/IEC29100（JISX9250）には、プライバシーフレームワークとして次の内容が示されている。1）PII（Personally identifiable information）処理における登場者（actor）と役割、2)登場者間の PII やりとりのシナリオ、3)PII の認識（どのような場合を PII とみなすべきか）、4)PII 処理において組織が考慮しなければならない一連の要求事項（privacy safeguarding requirements）に影響を及ぼす様々な要因（法令及び規則、契約、ビジネス、その他（privacy preferences 等））、5)PII 処理に関与する組織の経営陣が確立すべき内容、6)プライバシー管理策。また、国や国際機関によって策定されてきた既存の原則に由来するプライバシー原則が、11 項目に整理されている。ISO/IEC 29134（JIS X 9251）が示すプライバシー影響評価（PIA）は、リスクマネジメントに組み入れられることがよいとされており、ISO/IEC27701 においても、管理策実践のための規範の追加の手引きとして本規格が言及されている。

また、2021 年には、個人情報保護委員会から、事業者の自主的な取組を促進するために[59]「PIA の取組の促進について-PIA の意義と実施手順に沿った留意点-」が公表されている[60]。

事例：資生堂　プライバシー影響評価（PIA）の実践

株式会社資生堂では、個人情報保護に関する業務の一環として、プライバシー影響評価（Privacy Impact Assessment／PIA）に取り組んでいる。プライバシー影響評価の実施においては、内部統制評価で使用される①業務フロー、②業務詳細記述、③RCM（リスクコントロールマトリックス）の考え方を用いて個人データの取扱い方を可視化し、リスクの特定や軽減を促している。



個人データの取扱い方を可視化し、リスクの特定や軽減を促す

（出典）（社内資料）

59 「個人情報保護法　いわゆる 3 年ごと見直し　制度改正大綱」の第 3 章第 3 節 2.（2）には、「民間の自主的な取組を促進するために、委員会としても、PIA に関する事例集の作成や表彰制度の創設など、今後、その方策を検討していくこととする。」と記載されている。

60「PIA の取組の促進について―PIA の意義と実施手順に沿った留意点―（概要）」（個人情報保護委員会、2021 年）https://www.ppc.go.jp/files/pdf/pia_overview.pdf「PIA の取組の促進について―PIA の意義と実施手順に沿った留意点―」（個人情報保護委員会、2021 年）https://www.ppc.go.jp/files/pdf/pia_promotion.pdf

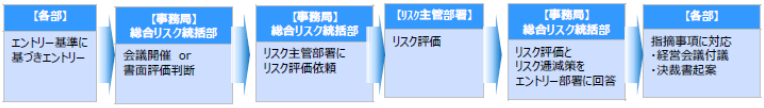
事例：JCB　サービスコントロールミーティングの実践

株式会社ジェーシービーでは、商品・サービスの立案時に、リスク懸念事象を早期検知することによるリスクの抑制を目的として、プライバシーに限らずリスクを評価するプロセスとしてサービスコントロールミーティング（Service Control Meeting/ SCM）を構築・運用している。

SCM 事務局やリスク主管部署（法務・セキュリティ部門など）が、SCM 起案部署（事業部門など）とリスクの共有や洗い出し、リスク評価を行うプロセスを実施している（年間約数百件程度）。経営会議に付議されたり、決裁書が起案される案件については、SCM にて可視化されたリスクや当該リスクに対する対応方針を文書として添付させることで、経営者や決裁者がリスクを踏まえて適正に判断できるようにしている。

SCM において、プライバシーに関するリスクも情報セキュリティリスクとして管理や評価の対象となる。パーソナルデータ利活用ビジネスを推進するにあたっては、お客様の適切なプライバシー保護を図るための社内ルールとして「パーソナルデータ管理細則」を定め、SCM 起案部署は管理細則への準拠状況を「パーソナルデータ利活用チェックリスト」で確認している。

【SCM フロー】



【SCMエントリー基準例】

エントリー基準	エントリー条件(除外条件)
新規商品・サービス・ビジネス開発	全件(除外条件無し)
商品・サービス終了	全件(除外条件無し)
新規カード立上げ	全件(除外条件無し)
提携カード解消	消費者不利益に該当しない場合を除く
DM・キャンペーン・施策	景品表示法などの法令評価が済んでいる場合を除く
情報システム・機器の導入および更改	インターネットなどの外部接続をしない場合・ハード単体の導入を除く
個人情報を取扱う業務委託	既存業務委託のうち、個人情報取扱の変更が無い場合を除く

【パーソナルデータ管理細則】

パーソナルデータ管理規則	条
第１章　総則	１．目的
	２．定義
第２章　パーソナルデータ利用時の原則	３．顧客心情の尊重
	４．顧客によるコントロール
	５．明確でわかりやすいポリシー
	６．プライバシーリスクの大きさに応じた対策
第3章　匿名加工情報の利用	７．匿名加工情報の利用
	８．匿名加工情報の作成等
	９．識別行為の禁止、
	10．匿名加工情報の提供
	11.社内手続

【パーソナルデータ利活用チェックリスト】

#	原則	基準
1	経緯（コンテキスト）の尊重	お客様に不安を抱かせない、予期できる範囲で利用すること
		お客様がパーソナルデータを提供した際の経緯（コンテキスト）に沿って、本人の期待と合致する形態で利活用を行うこと
2	個人によるコントロール	お客様に、自分のデータをコントロールする機会（どのように利用されるかについて関与する機会）を確保すること
		サービスに応じて、オプトイン・オプトアウトを適切に使い分けること
3	明確でわかりやすいポリシー	お客様に、何のデータをどのように使うかわかりやすく伝えること
4	プライバシー・リスクの大きさに応じた対策	データ種別ごとのプライバシー性、データ利用形態のリスク度合に応じて、プライバシーへの影響を事前に評価して対策すること

（出典）（社内資料）

6. （参考）諸外国の法令等に係る情報収集方法

技術革新のスピードは速く、プライバシー問題は個人個人の感じ方の相違や、社会受容性がコンテキストや時間の経過で移り変わることから、企業はプライバシー保護組織などを中核として、関連する情報（市場動向、技術、制度など）を継続的に収集する必要がある。

諸外国の法令等について自ら情報収集をする際には、個人情報保護委員会が調査を実施した国については、個人情報保護委員会の Web サイト[61]を参照することができる。また、当該国の法令データベースのほか、データ保護機関や、政府における法令所管省庁の Web サイトを参照することが有用である。さらに、裁判所の判例が重要な規範を構成している場合もあり、応用的な調査として、当該国の裁判所等の Web サイトで判例を参照することも考えられる。

例えば、英国では、英国の規制監督当局である情報コミッショナーオフィス（ICO：Information Commissioner's Office）の Web サイト[62]において、ICO の執行措置の情報のほか、事業者向けのデータ保護のガイド等が提供されている。法律については、英国国立公文書館の Web サイト[63]にて逐条解説と併せて提供されている。法案に関しては、議会が立法権を有し、上院・下院を可決した法案が国王の裁可により法律となる[64]が、英国議会の Web サイトの議会法案（Parliamentary Bills）のページ[65]に、当該法案のページが作成され、法案の概要、所管部門、法案、審議の進捗、ニュース、関連するドキュメント（法案についての逐条解説（Explanatory Notes）を含む）等について、情報提供されている。

---

61 個人情報保護委員会の Web サイト「外国における個人情報の保護に関する制度等の調査」 https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/#gaikoku

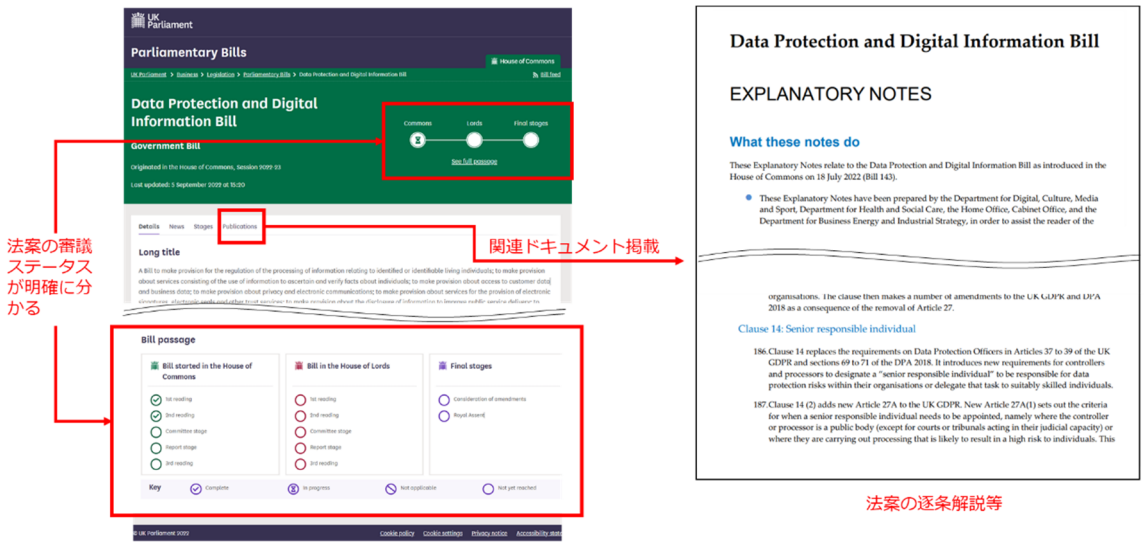
62 英国情報コミッショナーオフィス（ICO）Web サイト https://ico.org.uk/

63 英国国立公文書館 Web サイト https://www.legislation.gov.uk/

64 「イギリスの議会制度」（国立国会図書館、調査と情報―ISSUE BRIEF― ,2019.5） https://dl.ndl.go.jp/view/download/digidepo_11286064_po_1056.pdf?contentNo=1

65 英国議会（UK Parliament）Web サイト 議会法案（Parliamentary Bills）ページ https://bills.parliament.uk/

図表 18　英国議会の Web サイトでの法案に係る情報提供



（出典）UK Parliament Web サイト「Data Protection and Digital Information Bill」ページ
（ https://bills.parliament.uk/bills/3322 ）
（出典）「Data Protection and Digital Information Bill EXPLANATORY NOTES」
（ https://publications.parliament.uk/pa/bills/cbill/58-03/0143/en/220143en.pdf ）

米国は 50 の州で構成される連邦国家であり、米国連邦法については、下院の法改正顧問局（Office of the Law Revision Counsel）が公表している Web サイト（The United States Code）[66]で参照することができる。また，米国で消費者プライバシーを所管している連邦取引委員会（FTC：Federal Trade Commission）の Web サイト[67]でも関連する情報を得ることができる。法案に関しては、議会が立法権を有し、下院・上院で可決した法律案に大統領が署名すると法律となる[68]。米国連邦法に係る公式の Web サイト（CONGRESS.GOV）[69]にて、連邦法の法案や、審議の進捗等、情報提供がされている。なお、米国においては、カリフォルニア州消費者プライバシー法（CCPA）及びこれを改正したカリフォルニア州プライバシー権法（CPRA）等、州において個人情報保護を包括的に保護する法律が制定されるケースもあり、州のデータ保護の担当部局等の情報発信を確認する必要もある。

このように、諸外国の法令等については、当該国（州）のデータ保護機関や、政府の法令所管省庁、議会等から情報収集することができるが、そのほか

66 米国法改正顧問局 Web サイト（The United States Code） http://uscode.house.gov/
67 米国連邦取引委員会（FTC）Web サイト https://www.ftc.gov/
68 「アメリカ合衆国の議会制度」（国立国会図書館、調査と情報―ISSUE BRIEF ― ,2019.3）
https://dl.ndl.go.jp/view/download/digidepo_11247815_po_1045.pdf?contentNo=1
69 米国連邦法に係る公式の Web サイト（CONGRESS.GOV） https://www.congress.gov/

にも、民間事業者が有料で提供しているプライバシーに関連する法律や関連するニュースのデータベースを利用する方法がある。また、EU の GDPR（一般データ保護規則）のように、各国で対応が必要な規範については、法律事務所等において、各国の対応状況（可決された法律があるか、ドラフト（法案を含む）段階か、ドラフトもない状態か等）等を情報提供する、トラッカー（Tracker）と呼ばれる Web サイトが提供されることがある。トラッカーは無料で提供される場合も多いが、情報が最新のものであるか、サイト更新時期に注意しつつ利用する必要がある。

また、実際に、消費者等のパーソナルデータをグローバルに取り扱う場合には、プライバシー保護に対応するために諸外国の法令等に関して十分な配慮をすることが求められる。網羅的・全般的な情報収集が必要となる場合には、本章で示した方法等に加えて、資格や専門性を確認した上で、現地の法律事務所へ照会することも考えられる。

7. （参考）プライバシー・バイ・デザイン

基本的なプライバシー保護の考え方として参照できるグローバルスタンダードの 1 つに、プライバシー・バイ・デザイン（Privacy by Design（PbD））というコンセプトがある。これは、ビジネスや組織の中でプライバシー問題が発生する都度、対症療法的に対応を考えるのではなく、あらかじめプライバシーを保護する仕組みをビジネスモデルや技術、組織の構築の最初の段階で組み込むべきであるという考え方であり、以下の 5 つにまとめられている。

1. プライバシーに対して関心を持ち、その問題を解決しなければならないということを認識する
2. 公正な情報取扱い（Fair Information Practices（FIPs））の原則を適用する
3. 情報技術とシステムの開発時に情報ライフサイクル全体を通したプライバシー問題を早期に発見し軽減する
4. プライバシーに係る指導者や、有識者から情報提供が必要である
5. プライバシー保護技術（PETs）を取り入れ、統合していく

また、併せて、7 つの原則が示されている。

図表 19　プライバシー・バイ・デザイン 7 つの原則の概要

原則	内容
事前的／予防的	事後的でなく事前的であり、救済策的でなく予防的であること。プライバシー侵害が発生する前に、それを予防することを目的とする。プライバシー・バイ・デザインのアプローチは、受け身ではなく先見的にプライバシー保護を考え、対応することが特徴である。
初期設定としてのプライバシー	プライバシー保護は、初期設定で有効化されていること。これは、プライバシー・バイ・デフォルトともいわれる。プライバシー保護の仕組みは、システムに最初から組み込まれる。そして、パーソナルデータは、個人が何もしなくてもプライバシーが保護される。個人は、個別に設定を変更するといった措置は不要である。
デザインに組み込む	プライバシー保護の仕組みが、事業やシステムのデザイン及び構造に組み込まれること。事後的に、付加機能として追加するものではない。プライバシー保護の仕組みは、事業やシステムにおいて不可欠な、中心的な機能である。
ゼロサムではなくポジティブサム	プライバシー保護の仕組みを設けることによって、利便性を損なうなどトレードオフの関係を作ってしまうゼロサムアプローチではなく、全ての正当な利益及び目標を収めるポジティブサムアプローチを目指すこと。企業にとって、プライバシーを尊重することで、様々な形のインセンティブ（例えば、顧客満足度の向上、より良い評判、商業的な利益など）が考えられる。
徹底したセキュリティ	データはライフサイクル全般にわたって保護されること。プライバシーに係る情報は生成される段階から廃棄される段階まで、常に強固な

	セキュリティによって守られなければならない。全てのデータは、データライフサイクル管理の下に安全に保持され、プロセス終了時には確実に破棄されること。
可視性／透明性	プライバシー保護の仕組みと運用は、可視化され透明性が確保されること。どのような事業または技術が関係しようとも、プライバシー保護の仕組みが機能することを、全ての関係者に保証する。この際、システムの構成及び機能は、利用者及び提供者に一様に、可視化され、検証できるようにする。
利用者のプライバシーの尊重	利用者のプライバシーを最大限に尊重し、個人を主体に考えること。事業の設計者及び管理者に対し、プライバシー保護を実現するための強力かつ標準的な手段と、適切な通知及び権限付与を簡単に実現できるオプション手段を提供し、利用者個人の利益を最大限に維持する。

（出典）「Privacy by Design 7 つの原則」を基に事務局作成

プライバシー・バイ・デザインは、プライバシー保護の仕組みを設けることにより、利便性を損なうなどのトレードオフの関係を作ってしまうゼロサムアプローチではなく、企業がプライバシーを尊重することで企業価値の向上につながる様々な形のインセンティブを得られるなど、全ての正当な利益及び目標の達成を実現するポジティブサムアプローチを目指すものである。

他方で、ビジネスや社会環境の変化は、当初想定していなかったプライバシー問題を発生させる可能性がある。この場合最初にプライバシー・バイ・デザインを実施しているから十分であるということには必ずしもならない。このためプライバシー・バイ・デザインによる仕組みの構築とそれを不断に見直し改善していくプロセスを併せて検討していくことになる。

8. おわりに

今後、Society5.0 の実現を含め、これからの企業活動において、データの利活用はイノベーション創出の源泉であり、ビジネスのコアとなることが予想されている。

利活用が期待されるデータの中でも、パーソナルデータはビジネスの源泉となる一方で、利用者への安心を訴求する上でプライバシー保護が欠かせない。デジタル・トランスフォーメーション（DX）の推進・実現と、信頼（トラスト）の確保は不可分であり、その一環としてプライバシー保護は重要である。もちろん、我が国においては、企業はプライバシー保護に真摯に取り組んできたが、その多くは個別事例に対する対応であった。今後、取り扱うデータが広がるとともに、プライバシーに関する問題は多様化・複雑化することが予想され、従前の対応方法では限界が生じることになると考えらえるため、より戦略的・組織的な対応が必要となっている。社会におけるプライバシーへの関心は高まっており、消費者を含む社会はプライバシーの観点から企業を評価・峻別し始めている。企業が何らかの活動においてプライバシーに関する問題を引き起こした場合、その活動だけでなく、企業全体に深刻な影響を与える事態も予想される。逆に、適切にプライバシー的課題に対処する企業は社会からの高い信頼を獲得し、それが企業のビジネスにおける優位性につながる。つまり、企業にとって、プライバシー対応は不可欠であり、必ずしもコストとはいえない。むしろ商品・サービス等の品質向上に資する取組の１つであり、他社に対する重要な差別化要素とすることがでる。

このため、企業は組織としてのプライバシー問題への対応、つまり企業のガバナンスとしてプライバシー保護に取り組むことが求められており、本ガイドブックは、経営者及び経営戦略・支援に当たる方々向けに、今後、企業に求められるプライバシーガバナンスとして、経営者が取り組むべき要件、そして組織体制を明らかにした。また、プライバシー問題は企業だけで解決できるものではなく、消費者を含む社会との関係、例えば、企業のプライバシー対応の公知や消費者とのコミュニケーションの重要性について提示した。

今まさに企業において DX が進められている中で、本ガイドブックが企業におけるプライバシーに関する取組の一助となり、その結果として企業の商品・サービス等の価値、そしてその企業自身の経済的かつ社会的な価値を高められることを狙うものである。

なお、プライバシー問題は対象となる商品やサービスに依存するだけでなく、技術の進歩や社会の関心においても変化していく。その意味においては、本ガイドブックも適宜、変更・加筆に取り組んでいく。

参考文献

- 「プライバシーガバナンスに関するアンケート結果（速報版）」（一般財団法人日本情報経済社会推進協会（JIPDEC）、2021 年）
  - JIPDEC プレスリリース：
    https://www.jipdec.or.jp/topics/news/20211018.html
- 「Society5.0」（内閣府、ホームページ）
  https://www8.cao.go.jp/cstp/society5_0/index.html
- 「OECD Principles on AI」（OECD、2019 年）
  https://www.oecd.org/going-digital/ai/principles/
- 「人間中心の AI 社会原則」（総合イノベーション戦略推進会議、2019 年）
  https://www8.cao.go.jp/cstp/aigensoku.pdf
- 「AI 利活用ガイドライン」（総務省、2019 年）
  https://www.soumu.go.jp/menu_news/s-news/01iicp01_02000081.html
- 「Guidance on social responsibility」（ISO26000：2010）
  https://www.iso.org/standard/42546.html
- 「社会的責任に関する手引」（JIS Z 26000：2012）
- 「ビジネスと人権に関する指導原則」（国連人権理事会、2011 年）
  https://www.unic.or.jp/texts_audiovisual/resolutions_reports/hr_council/ga_regular_session/3404/
- 「『ビジネスと人権』に関する行動計画（2020-2025）」（ビジネスと人権に関する行動計画に係る関係省庁連絡会議、2020 年）
  https://www.mofa.go.jp/mofaj/press/release/press4_008862.html
- 「『ビジネスと人権に関する調査研究』報告書」（法務省、2021 年）
  https://www.moj.go.jp/JINKEN/jinken05_00045.html
- 「責任あるサプライチェーン等における人権尊重のためのガイドライン」（経済産業省、2022 年）
  https://www.meti.go.jp/press/2022/09/20220913003/20220913003.html
- 「『責任ある機関投資家』の諸原則≪日本版スチュワードシップ・コード≫」（金融庁、2020 年改訂）
  https://www.fsa.go.jp/news/r1/singi/20200324/01.pdf
- 「コーポレートガバナンス・コード～会社の持続的な成長と中長期的な企業価値の向上のために～」（株式会社東京証券取引所、2021 年改訂）
  https://www.jpx.co.jp/equities/listing/cg/tvdivq0000008jdy-att/nlsgeu000005lnul.pdf

- 「MSCI ESG Ratings Methodology: Privacy & Data Security Key Issue」（MSCI ESG Research LLC、2022 年）
  https://www.msci.com/documents/1296102/34424357/MSCI+ESG+Ratings+Methodology+-+Privacy+%26+Data+Security+Key+Issue.pdf/562b0a5b-b0ec-8bab-23dc-1c14967a08dc?t=1666182600406
- 「Expanding testing for the Privacy Sandbox for the Web」（Google LLC、2022 年）
  https://blog.google/products/chrome/update-testing-privacy-sandbox-web/
- 「犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用について」（個人情報保護委員会、2023 年）
  https://www.ppc.go.jp/files/pdf/kaoshikibetsu_camera_system.pdf
- 「新しいデータ流通取引に関する検討事例集 ver.2.0」（経済産業省・総務省・IoT 推進コンソーシアム、2018 年）
  - 経済産業省プレスリリース：
    https://warp.da.ndl.go.jp/info:ndljp/pid/11623215/www.meti.go.jp/press/2018/08/20180810002/20180810002.html
  - 総務省プレスリリース：
    https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000045.html
- 「新たなデータ流通取引に関する検討事例集第 1 分冊」（経済産業省・総務省・IoT 推進コンソーシアム、2020-2022 年）
  https://www.meti.go.jp/policy/it_policy/privacy/privacy.html#data
- 「カメラ画像利活用ガイドブック ver.2.0」（経済産業省・総務省・IoT 推進コンソーシアム、2018 年）
  - 経済産業省プレスリリース：
    https://warp.da.ndl.go.jp/info:ndljp/pid/11067906/www.meti.go.jp/press/2017/03/20180330005/20180330005.html
  - 総務省プレスリリース：
    https://warp.da.ndl.go.jp/info:ndljp/pid/11486163/www.soumu.go.jp/menu_news/s-news/01kiban18_01000040.html
- 「カメラ画像利活用ガイドブック　事前告知・通知に関する参考事例集」（経済産業省・総務省・IoT 推進コンソーシアム、2019 年）
  - 経済産業省プレスリリース：
    https://warp.da.ndl.go.jp/info:ndljp/pid/12232105/www.meti.go.jp/press/2019/05/20190517001/20190517001.html
  - 総務省プレスリリース：

https://warp.da.ndl.go.jp/info:ndljp/pid/11389499/www.soumu.go.jp/menu_news/s-news/01kiban18_01000066.html

- 「民間事業者によるカメラ画像を利活用した公共目的の取組における配慮事項」（経済産業省・総務省・IoT 推進コンソーシアム、2021 年）
  - 経済産業省プレスリリース：https://warp.da.ndl.go.jp/info:ndljp/pid/12232105/www.meti.go.jp/press/2020/03/20210319007/20210319007.html
  - 総務省プレスリリース：https://warp.da.ndl.go.jp/info:ndljp/pid/12344921/www.soumu.go.jp/menu_news/s-news/01kiban18_01000113.html
- 「カメラ画像利活用ガイドブック ver3.0」（経済産業省・総務省・IoT 推進コンソーシアム、2022 年）
  - 経済産業省プレスリリース：https://warp.da.ndl.go.jp/collections/content/info:ndljp/pid/12323307/www.meti.go.jp/press/2021/03/20220330001/20220330001.html
  - 総務省プレスリリース：https://warp.da.ndl.go.jp/info:ndljp/pid/12213407/www.soumu.go.jp/menu_news/s-news/01kiban18_01000152.html
- 「GOVERNANCE INNOVATION：Society5.0 の実現に向けた法とアーキテクチャのリ・デザイン」（経済産業省、2020 年）
  https://warp.da.ndl.go.jp/collections/content/info:ndljp/pid/12323307/www.meti.go.jp/press/2020/07/20200713001/20200713001.html
- 「GOVERNANCE INNOVATION Ver.2：アジャイル・ガバナンスのデザインと実装に向けて」（経済産業省、2021 年）
  https://www.meti.go.jp/press/2021/07/20210730005/20210730005.html
- 「アジャイル・ガバナンスの概要と現状」（経済産業省、2022 年）
  https://www.meti.go.jp/press/2022/08/20220808001/20220808001.html
- 「我が国の AI ガバナンスの在り方 ver.1.1：AI 原則の実践の在り方に関する検討会報告書」（経済産業省、2021 年）
  https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/20210070901_report.html
- 「AI 原則実践のためのガバナンス・ガイドライン ver.1.0」（経済産業省、2021 年）
  https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/20210070902_report.html

- 「Society5.0 の実現に向けた個人データ保護と活用の在り方」（一般社団法人日本経済団体連合会、2019 年）
  https://www.keidanren.or.jp/policy/2019/083.html
- 「個人データ適正利用経営宣言」（一般社団法人日本経済団体連合会、2019 年）
  https://www.keidanren.or.jp/policy/2019/083_sengen.pdf
- 「Information technology － Governance of IT for the organization」（ISO/IEC 38500:2015）
- 「情報技術―IT ガバナンス」（JIS Q 38500:2015）
- 「個人情報保護法 いわゆる３年ごと見直し 制度改正大綱」（個人情報保護委員会、2019 年）
  https://www.ppc.go.jp/files/pdf/200110_seidokaiseitaiko.pdf
- 「個人情報保護マネジメントシステム―要求事項」（JIS Q 15001:2017）
- 「Information technology -- Security techniques -- Information security management systems -- Requirements」（ISO/IEC 27001:2013）
- 「情報技術―セキュリティ技術―情報セキュリティマネジメントシステム―要求事項」（JIS Q 27001:2014）
- 「Information technology -- Security techniques -- Code of practice for information security controls」（ISO/IEC 27002:2013）
- 「情報技術―セキュリティ技術―情報セキュリティ管理策の実践のための規範」（JIS Q 27002:2014）
- 「Security techniques -- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management -- Requirements and guidelines」（ISO/IEC 27701:2019）
- 「スマートホーム IoT データプライバシーガイドライン」（一般社団法人電子情報技術産業協会スマートホーム部会、2023 年）
  https://home.jeita.or.jp/smarthome/iot/index.html
- 「Information technology － Security techniques － Privacy framework」（ISO/IEC 29100：2011）
- 「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）」（JIS X 9250：2017）
- 「Information technology － Security techniques － Guidelines for privacy impact assessment」（ISO/IEC 29134：2017）
- 「情報技術―セキュリティ技術―プライバシー影響評価のためのガイドライン」（JIS X 9251:2021）

- 「PIA の取組の促進について―PIA の意義と実施手順に沿った留意点―（概要）」（個人情報保護委員会、2021 年）
  https://www.ppc.go.jp/files/pdf/pia_overview.pdf
- 「PIA の取組の促進について―PIA の意義と実施手順に沿った留意点―」（個人情報保護委員会、2021 年）
  https://www.ppc.go.jp/files/pdf/pia_promotion.pdf
- 「UNDERSTANDING PRIACY」（DANIEL J. SOLOVE、2008 年）
- 「プライバシーの新理論」（DANIEL J. SOLOVE、大谷卓史（訳）、2013 年）
- A Taxonomy of Privacy（DANIEL J. SOLOVE, University of Pennsylvania Law Review, Vol. 154, No. 3, p. 477, January 2006, GWU Law School Public Law Research Paper No. 129）*available at* SSRN: https://ssrn.com/abstract=667622
- 「プロファイリングに関する最終提言」（パーソナルデータ＋α研究会、2022 年）
  https://wp.shojihomu.co.jp/wp-content/uploads/2022/04/ef8280a7d908b3686f23842831dfa659.pdf
- 「Privacy by Design The 7 Foundational Principles」（Ann Cavoukian、Information & Privacy Commissioner Ontario, Canada、2011 年）
  https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf
- 「Privacy by Design　7 つの基本原則」（堀部政男（訳）、総務省パーソナルデータの利用・流通に関する研究会（第 1 回）参考資料 7-2、2012 年）
  https://www.soumu.go.jp/main_content/000196322.pdf

検討体制

本ドキュメントは、IoT 推進コンソーシアム「データ流通促進ワーキンググループ」（座長：森川博之 東京大学大学院教授）の元に、2019 年度～2022 年度にかけて「企業のプライバシーガバナンスモデル検討会」（座長：佐藤一郎 国立情報学研究所教授）を設置し、検討の結果を取りまとめたものである。

図表 20　企業のプライバシーガバナンスモデル検討会　委員構成

区分	氏名 （順不同、敬称略）	所属
座長	佐藤　一郎	国立情報学研究所
委員	板倉　陽一郎	ひかり総合法律事務所
	落合　正人	ＳＯＭＰＯリスクマネジメント株式会社
	クロサカ　タツヤ	株式会社企
	小林　慎太郎	株式会社野村総合研究所
	宍戸　常寿	東京大学大学院法学政治学研究科
	高橋　克巳	日本電信電話株式会社 NTT 社会情報研究所
	林　達也	LocationMind 株式会社 株式会社パロンゴ
	日置　巴美	三浦法律事務所
	平岩　久人	PwC あらた有限責任監査法人
	古谷　由紀子	公益社団法人日本消費生活アドバイザー・コンサルタント・相談員協会 ／サステナビリティ消費者会議
	村上　陽亮	株式会社 KDDI 総合研究所
	森　亮二	英知法律事務所
	若目田　光生	一般社団法人日本経済団体連合会 株式会社日本総合研究所