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
ver1.0

2020 年 8 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

目次

1. 本ガイドブックの位置づけ 1
2. ガイドブックの前提 3
   2.1. Society5.0 と企業の役割 3
   2.2. プライバシーの考え方 5
   2.3. 企業のプライバシーガバナンスの重要性 8
3. 経営者が取り組むべき三要件 13
   3.1. プライバシーガバナンスに係る姿勢の明文化 15
   3.2. プライバシー保護責任者の指名 16
   3.3. プライバシーへの取組に対するリソースの投入 17
4. プライバシーガバナンスの重要項目 18
   4.1. 体制の構築 18
      4.1.1. プライバシー保護責任者の役割 19
      4.1.2. プライバシー保護組織の役割 19
      4.1.3. 事業部門の役割 22
      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 22
   4.2. 運用ルールの策定と周知 23
   4.3. 企業内のプライバシーに係る文化の醸成 23
   4.4. 消費者とのコミュニケーション 24
      4.4.1. 組織の取組の公表、広報 24
      4.4.2. 消費者との継続的なコミュニケーション 25
      4.4.3. 問題発生時の消費者とのコミュニケーション 27
   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 28
      4.5.1. ステークホルダーへの対応 28
      4.5.2. プライバシー問題の情報収集 31
      4.5.3. その他の取組 31
5. （参考）プライバシーリスク対応の考え方 32
   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 32
   5.2. プライバシーリスクの特定（プライバシー問題の洗い出し） 33
   5.3. プライバシー影響評価（PIA） 37
6. （参考）プライバシー・バイ・デザイン 40
7. おわりに 43

参考文献 44

検討体制 46

1. 本ガイドブックの位置づけ

サイバー空間とフィジカル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、サービス・製品の高度化を通じて、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とともに、プライバシー保護への要請が高まっている。この要請に対し、企業は、消費者のプライバシーを可能な限り守ること、その姿勢を貫くことにより、消費者からの信頼の獲得につなげることが、企業のビジネスにおける優位性をもたらしうる。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的に迫られることが想定される企業や、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）
- 消費者へ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

[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。

・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、関心をお持ちの方は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た適用が認められるものであり、個々の企業の状況に応じて柔軟に利用されたい。

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。

[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、企業規模に関わらず、生じうるものである。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。

2. ガイドブックの前提

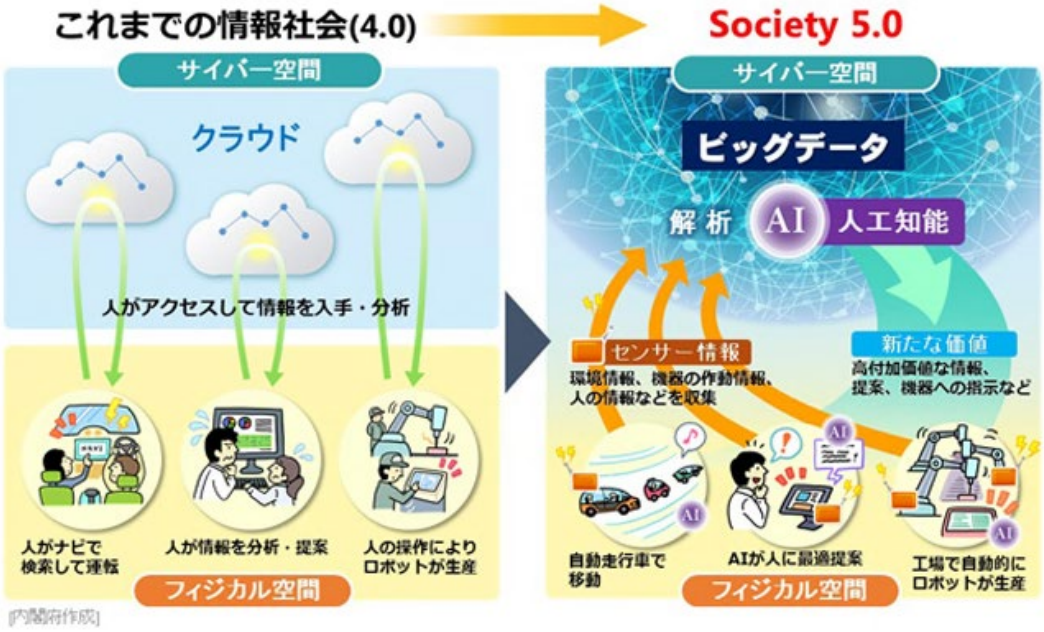
2.1. Society5.0 と企業の役割

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繋げる IoT（Internet of Things）によって現実世界（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仮想空間（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る。また、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[4]。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）[5]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・ガバナンス改革の検討も進められている。

[4] 内閣府 Society5.0（ https://www8.cao.go.jp/cstp/society5_0/index.html ）

[5] 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、国境を超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[6]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、ソフトウェアを起点とする社会の構造変革が進展する中で我が国が今後の経済成長を維持するためには、Society5.0 を実現するためにフィジカル空間とサイバー空間をシームレスに結ぶ、創造的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る新たなリスクもある。そのリスクに新たなプライバシーに係る問題が含まれ

[6] 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ガバナンスが必要である。この観点から、イノベーション促進の中心的存在である企業は、積極的に社会的価値と経済価値の両方を創造する取組を推進するとともに、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、企業において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、こうした課題に積極的に取り組み、その解決を図ることは消費者を含む社会からみると、その企業の商品やサービス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うる。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繋がりうることから、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。

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と、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える可能性があり、その結果として対象やその特徴を間違えたり、特にサイバー空間の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が助長されたり、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）：計測の活用の目的を消費者に伝えることが難しい
AI を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[7]

ところで、プライバシーは従来、「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ものが[8]、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の必要性の理解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」などに発展していった。IoT や AI などの技術進展によって、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、あるいは個人の政

[7] 「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。

[8] 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。

治的選択に対して介入される可能性が生じている[9]、というような現時点であまり顕在化していないプライバシーに関わる新しい問題まで含まれるようになりつつある。

他方で、国内における商店街や商業施設等への防犯カメラの設置などのケースを見ると、当初は設置そのものへの懸念が取り上げられ大きな社会的議論を巻き起こしていたが、今では一定の配慮の下で設置されることに対する社会の受容性は高まりつつある。その一方、防犯カメラによる画像の当初の防犯目的の範囲を超える利用や、識別機能を有する監視カメラの登場などにより、撮影された画像データに関する懸念は高まりつつあり、欧州や米国で厳格な規制[10]が始まりつつある。

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価値に対する悪影響まで、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、個人的な感じ方の相違、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、プライバシーという概念を固定して考えられない点に、対応の難しさがあるといえる。その時代において、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から、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[11]。プライバシーに関する問題が個人や社会に顕在化するリスク（以下「プライバシーリスク」という。）に、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となる。

企業がプライバシー保護の取組を推進する上で、プライバシーリスクとは企業のリスクである前に個人にとってのリスクであること、そしてそれが社会全

---

9 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。

10 欧州では、2019 年 7 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」案を公表した。これには 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案であり、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。一方、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、その位置づけはまさに揺れ動いている。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。直近では、顔認識ソフトウェアの提供中止を表明する企業も現れてきている。

11 プライバシー問題については「5.2.プライバシーリスクの特定（プライバシー問題の洗い出し）」を参照のこと。

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、企業活動に常時組み込むことが重要となる。

本書においては、上記のような、個人へのプライバシー侵害から社会的価値に対する悪影響まで、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と位置づけ、企業が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、個人がプライバシーリスクを感じることとなる。そして、人々のプライバシーリスクへの不安や変化と相まって、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を阻害される。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とはいえない。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対応に当たっては、企業は、サイバー空間を介していても、取り扱うのは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、真剣に考えを尽くすことが必要である。企業の社会的責任の観点からも、消費者あるいは個人の基本的な権利を損なうことのないよう [12]、プライバシー問題の発生を抑止していくための適切な対応が求められる。

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。）が主な規範として位置づけられている。このため、これまで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。一方で、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

[12] 「Guidance on social responsibility」（ISO 26000：2010）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、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』の策定も進むなど、その導入を企業に求める動きも加速している。

て社会的受容性の観点から疑問が投げかけられたり、企業がプライバシー問題に関する批判を避けきれず、いわゆる「炎上」する事例が散見されるようになってきた。単なる外形的な法令等遵守ではなく、その事業におけるパーソナルデータの活用様態に即して、個人の権利利益や社会的価値への影響を考慮したより積極的な取組や説明が、企業には強く求められている。

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、法令等遵守が中心に位置づけられる中で、「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、個別の対応の背景にある本質的な目的、すなわち、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の希薄さが挙げられる。こうした中、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。これが高じると「法令は守っていたのに炎上する」という事態が生じることとなり、その企業自身に損失が生じることに加え、炎上を経験した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。

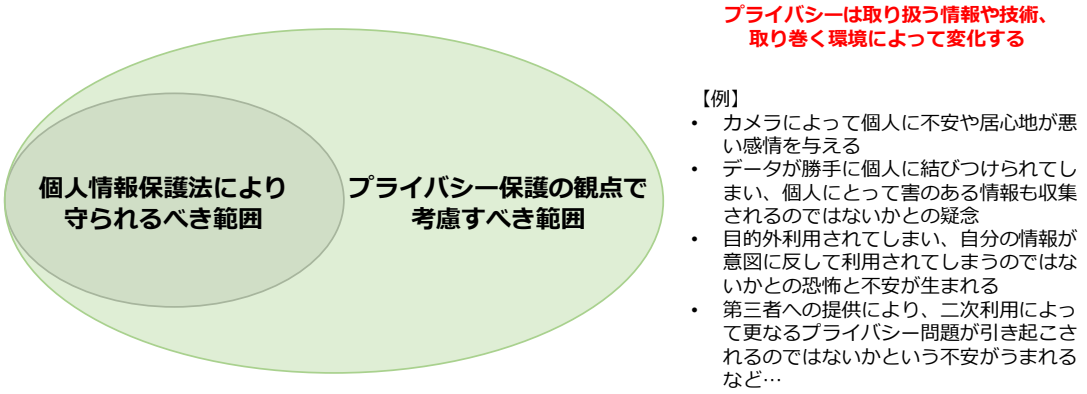
これに対して、国内外を問わず、顧客や消費者の信頼を得ながらパーソナルデータを利活用した新たなビジネスを拡大させている企業も少なくない。これらの企業においては、プライバシー保護を企業にとって単なる「コンプライアンス」と受け止めず、重要な経営戦略の一環として捉え、自社ビジネスに関連して起こり得るプライバシーリスクを適切に評価して対応する仕組み・体制を構築するよう、経営者が積極的に取組を推進するとともに、ステークホルダーや社会に対して発信し、プライバシーリスク対応を超えた社会的信頼の獲得が追求されている。特に、企業の商品やサービスに関わるプライバシーリスクを減らし、プライバシーに親和的とすることは消費者を含む社会からの信頼獲得につながることから、プライバシー対策をコストとしてではなく、むしろ商品やサービスの品質を高めることとして捉えなおすべきである。

変化のスピードが速い時代において、法令等遵守だけでは、リスク管理や、社会から信頼を得るにあたり、十分な対応とはいえない。このため、企業は法令等遵守（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。さらに、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、ステークホルダーとの対話を通じて、信頼を確保していく、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[13][14]。

すなわち、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、経営者が積極的にプライバシー問題への取組にコミットし、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[15]。

図表 3　プライバシー保護の観点で考慮すべき範囲



---

[13] 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）。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）。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」も公表した（2019 年公表）。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。

[14]「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 年公表）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。

[15] 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。

コラム -新型コロナウイルス感染症対策とパーソナルデータの活用-

新型コロナウイルス感染症への対策に当たっては、各国において、パーソナルデータの活用のニーズが急速に高まった。

各国における取組の例として、例えば感染者の位置情報を衛生当局が把握し、隔離の実効性を確保する手段を取るケースや、Bluetooth の機能を利用した接触把握型のアプリにより感染者との接触可能性について通知する取組などがあげられる。また、感染症対策の取組がどの程度実行されているかを可視化し、行動変容を促す観点から混雑状況に関するデータの利用なども行われている。

これらの取組においては、公的機関が自らデータを収集するための仕組みを作る例もあるが、迅速な対応が必要となる中で、すでに多くのパーソナルデータを保有している民間事業者が自らの判断のもとで、社会的責任を果たす観点からパーソナルデータの分析結果を公表したり、政府が事業者に対してデータの提供の協力を求めたりすることとなった。

日本においても、政府からプラットフォーム事業者や移動通信事業者等に対するデータ提供要請が行われた。

データ提供を要請された企業は、コロナ対策という公益のためのデータ提供とユーザのデータ・プライバシーを守ることによるユーザとの信頼関係のバランスという課題の中で、企業の判断としてユーザのプライバシーを保護しながらどこまでのデータ提供を行うことができるか、迅速かつ適切な判断を迫られた。

要請に対応した企業においては、自社が多くのパーソナルデータを扱いそれを利用してビジネスを行うことから、平時より、パーソナルデータの扱いの重要性について、経営陣及び事業部門が強く認識しており、自社内での検討の体制が固まっていた。このため、要請への対応について迅速な検討と判断を行うことが可能となった。

データ提供の要請に応えた企業の中には、提供先である政府に対して、政府が、提供データの利用目的を確約し、その利用成果を適切な時期に公表すること、適正な利用が担保されない場合などに企業側がデータの提供を中止できることについて、協定で前もって合意した上で、提供したケースもあった[16]。これは企業がプライバシーガバナンスを機能させ、ユーザのプライバシーリスク低減に責任をもって対応した例と言えるだろう。

一方、ステークホルダーの安全や企業の社会的信頼を守る目的で、従業員や取引先等にライフログ[17]を奨励するなど、企業が自主的にコロナ対策の準備を進める取組

[16] 例えば、要請に対してデータ提供を行ったヤフー株式会社は、同社のプライバシー有識者会議のアドバイスを基に、厚生労働省と、新型コロナ感染症のクラスター対策に資する情報提供に係る協定を結び、提供を行っている。

[17]ライフログとは、利用者のネット内外の活動記録（行動履歴）が、パソコンや携帯端末等を通じて取得・蓄積された情報をいう。（総務省「ライフログ活用サービスＷＧからの報告～ヒアリングを踏まえた今後の検討の視点～」より）

も進んでおり、近々こうした形態でのパーソナルデータ活用も顕在化する可能性がある。その際、ユーザや消費者との関係だけでなく、従業員や取引先のプライバシーについても十分な配慮が必要であることは、論を待たない。

今後は経済活動を行いながら適切な感染症拡大防止対策を実施する必要があることから、引き続き企業は有効な利用の在り方とプライバシーを踏まえた適切なパーソナルデータの取扱いを両立していくことが求められるであろう。

こうした事例は、今後の社会においては、パーソナルデータを保有し活用している企業が、公益性の観点からの大きな役割を担う可能性と、それに対応するためにもあらかじめプライバシーに関する社内のガバナンスを確立しておくことが効果的であることを示唆している。

3. 経営者が取り組むべき三要件

Society5.0 の実現に向けて、企業は、データ利活用によるイノベーションの担い手として期待されている。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、個々のサービスや製品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得ることとなり、企業価値の向上につながる。このため、デジタル社会において、経営者は、プライバシーに関わる取り組みを経営戦略として捉え、プライバシーを競争力の要素として検討することが重要となる。

もちろん、企業が、プライバシーリスクに配慮できなかったり、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ず、社会からの信頼が揺らぐ事態になれば、企業の売上げ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という面からも、取組の必要がある。

そもそも、株式会社の経営者は、善良な管理者といての注意義務（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、関連部署の担当の役員だけでなく、その他の役員も損害賠償責任を問われることとなりうる [18]。デジタル・トランスフォーメーションを推進する企業にとっては、パーソナルデータの管理と適切な利用は重要な業務執行であり、適切な内部統制の構築ができないことにより、漏えいや炎上の結果として企業に損害が発生する場合には、その損害の責任を経営者個人が問われうることになる点に注意が必要である [19][20]。

---

[18] 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。

[19] 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。

[20] 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。

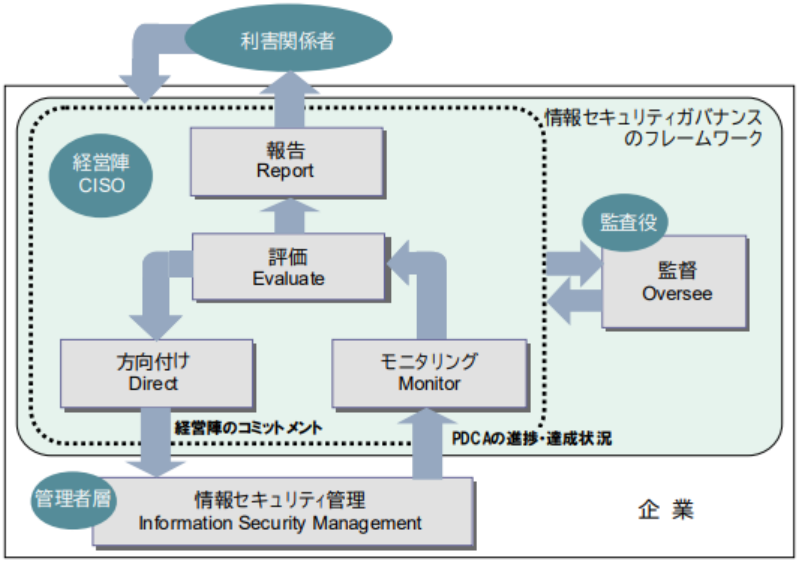
以上の観点から、企業の経営者には、プライバシー問題を競争力の要素として、重要な経営戦略上の課題として捉えるとともに、コーポレートガバナンスとそれを支える内部統制の仕組みを企業内に構築・運用することが求められる。

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

図表 4 （参考）情報セキュリティガバナンスのフレームワーク

参考までに、情報セキュリティガバナンスのフレームワークを以下に示す。情報セキュリティガバナンスフレームワークは、経営戦略やリスク管理の観点から行う「方向づけ（Direct）」、ガバナンス活動の状況を指標に基づき可視化する「モニタリング（Monitor）」や結果を判断する「評価（Evaluate）」、これらのプロセスが機能していることを確認する「監督（Oversee）」、結果を利害関係者等に提示する「報告（Report）」の 5 つの活動から構成されるものとされている。プライバシーガバナンスにおいても同様の枠組みの下で整理するが有効であると考えられる。



（出典）「情報セキュリティガバナンス導入ガイダンス」（平成 21 年 6 月、経済産業省）
「図 1-2 情報セキュリティガバナンスのフレームワーク」
https://www.meti.go.jp/policy/netsecurity/downloadfiles/securty_gov_guidelines.pdf

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、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、商品やサービスの品質を向上させ、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。

このことを経営者はこれからの経営上の重要事項の 1 つと認識し、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。

また、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に能動的に対応していく姿勢をトップダウンで浸透させることで、組織全体にプライバシー問題への認識を根付かせることができる。また、組織内部に限らず、消費者やステークホルダー（株主、取引先等）など組織外に対しても公表することで、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問題への取組を実施することへのアカウンタビリティ [21]を確保することが求められる [22]。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 [23]。

---

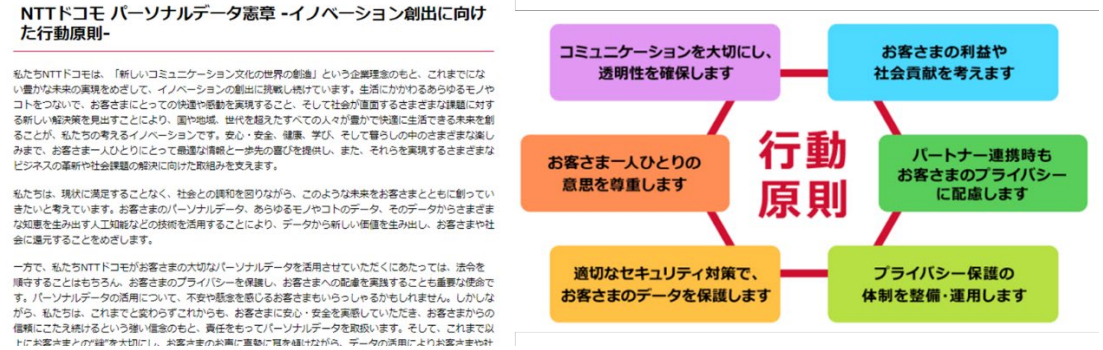
[21] Accountability は、説明責任にとどまらず、最終的な、包括的な責任を果たすことができる状態を指す。

[22] 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、対処療法的にプライバシーリスク対応を考えるのではなく、あらかじめプライバシー保護をビジネス構築の最初の段階で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「6.（参考）プライバシー・バイ・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。

[23] 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。

図表 5　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、組織全体のプライバシー問題への対応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、プライバシー保護責任者から報告を求め、評価をすることで、組織の内部統制をより効果的に機能させる。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[24][25]。

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、必要十分な経営資源（ヒト・モノ・カネ）を投入することが求められる。プライバシー問題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。

プライバシーに係る取組は、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[26]。また、プライバシー問題は、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、プライバシーへの取組に関する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。

---

[24] なお、ここでいうプライバシー保護責任者は、一般データ保護規則（GDPR）でいうところの、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）とは必ずしも同じものとは限らない。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）に就けないとされているが、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うる。企業に特有の組織構造に応じて、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。

[25] 「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。

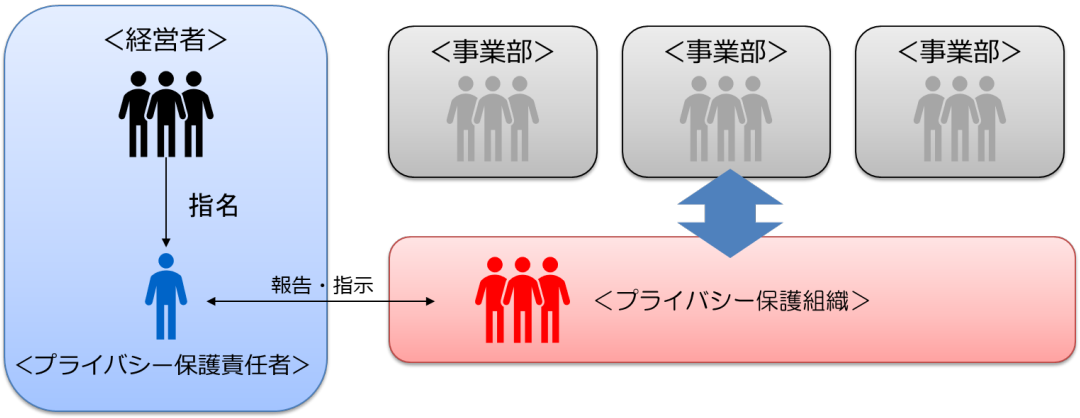
[26] PbD の考え方や PbD7 原則（本ガイドブック「6.（参考）プライバシー・バイ・デザイン」参照）にある「事前的／予防的」「初期設定としてのプライバシー」などは参考となる。

4. プライバシーガバナンスの重要項目

4.1. 体制の構築

プライバシーガバナンスを機能させるには、各部門の情報を集約し、事業におけるプライバシー問題を見つけるとともに、対象となる事業の目的の実現とプライバシーリスクマネジメント [27]を可能な限り両立させるために、対応策を多角的に検討することが必要となる。上記を実現するため、指名されたプライバシー保護責任者を中心として、中核となる組織を企業内に設けることが望ましいと考えられる（本ガイドブックでは「プライバシー保護組織」と呼ぶ）。

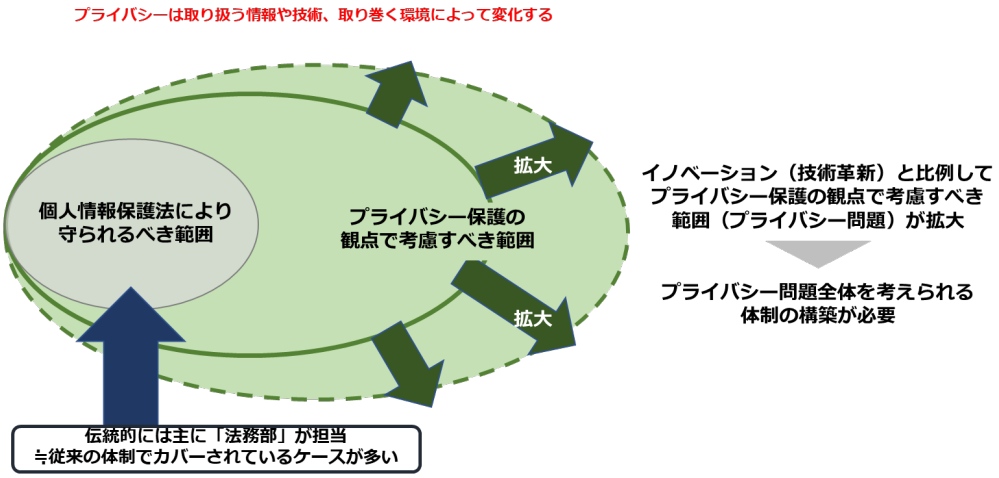
図表 6　プライバシー保護の体制の構築



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ごく少数であるが、プライバシー保護組織を設けることで、社内の新規事業部門との密なコミュニケーションを醸成したり、関連情報を社外有識者などから収集したり、多角的に対応策を検討するなどを、実質的に行っていくことができる。

[27] 組織が直面するプライバシーリスクについて最適な対応を行うため、経営者が示したプライバシーガバナンスに係る姿勢を具体化した目的を設定し、これを達成するために、組織の意思を決定し、パフォーマンスを改善することで、組織における価値を創出し保護するための活動をいう。

図表 7　拡大するプライバシー問題へ対応するための体制構築が必要



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、プライバシーリスクを把握、評価し、対応策を検討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と合致しているかを確認・徹底する。

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保護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は、企業によって設置する形態は異なり、例えば、専門的な知見を有する専任者を確保が困難な場合には、兼務の従業員のみで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することを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[28]。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[29]。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、プライバシー問題は個人的な感じ方の相違や、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。また、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、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マネジメントを超えた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[30]。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、システム上・情報セキュリティ上の観点での確認も必要である。またサービスの利用者や消費者の社会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）、政策企画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[31]。

---

[28] プライバシー問題については「5.2.プライバシーリスクの特定（プライバシー問題の洗い出し）」を参照のこと。

[29] 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、リスク評価の実施をルール化し、評価プロセスの中に、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。

[30] PbD の考え方や PbD7 原則（本ガイドブック「6.（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。

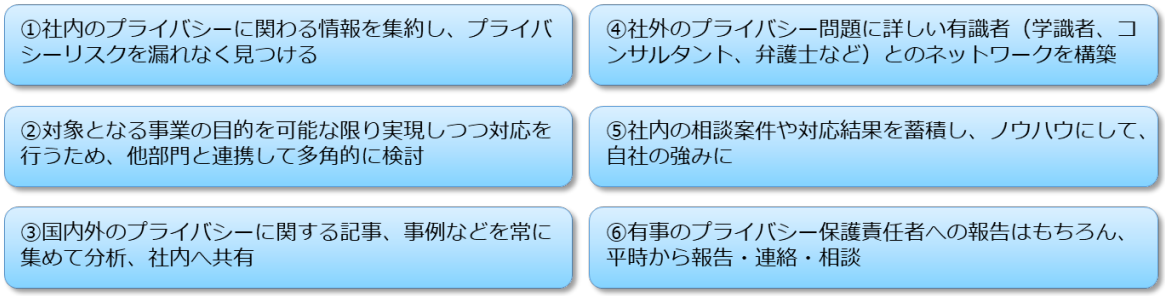
[31] 従来、企業がビジネスを行う上で、プライバシー問題を考える際には、コンプライアンス＝法令等遵守の観点から個人情報保護法を遵守しているかどうかを中心に検討した上で事業が行われていることが主流であった。そのため個人情報保護法により守られるべき範囲については、法務部が主幹部署として担当し対応をしている場合も多い。一方で、プライバシー保護の観点で考慮すべき範囲は、日々、技術革新や消費者のプライバシー意識の高まりによってその領域が変化・拡大しており、プライバシー問題に対して多角的な検討を担保できるようなプライバシー保護組織の構築が必要である。企業の事業内容や取り扱うデータなどによってプライバシー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。

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における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、これらのメンバー及び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が不可欠である。このため、そのような人材を適切に配置することに加え、プライバシー保護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。

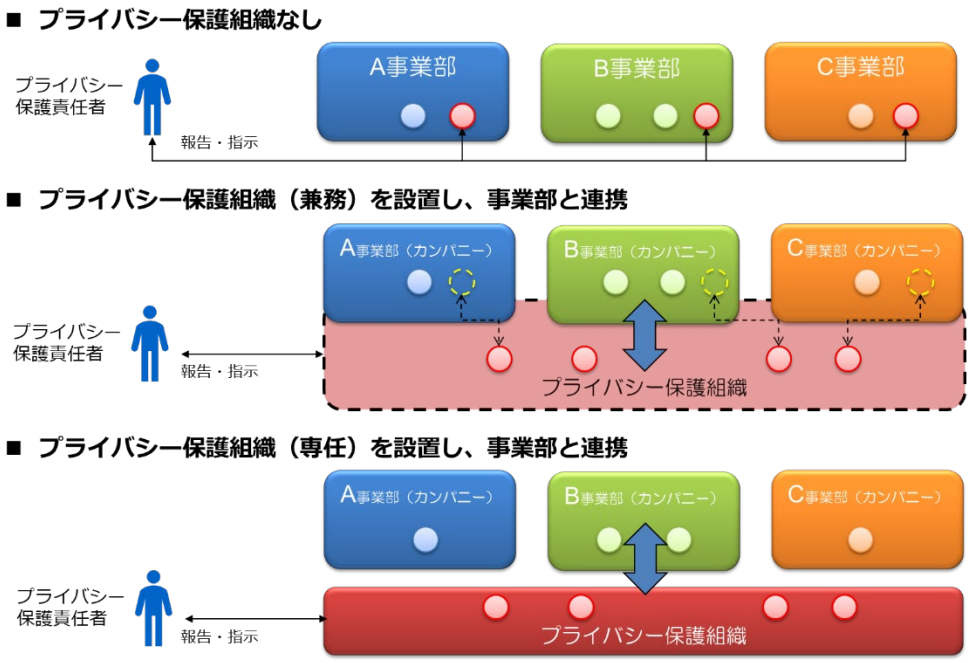
図表 8　プライバシー保護組織の役割



プライバシー保護組織は、企業によって設置する形態は異なり、自社のリソースに併せた組織の形態を模索することが大切である。

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だろう（下図に例示）。重要なことは、どのような体制であれ、企業が引き起こしうる、消費者の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 9　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をする必要がある。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の洗い出しや特定、その対策などを検討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考慮する必要がある。

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

プライバシー問題に係るリスク管理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、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、第三者的な立場の外部の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、評価・モニタリング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、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への意識を高めていくこともできる。

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、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[32]。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共に、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。

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を適切に対応できるような企業文化を組織全体で醸成していくことが不可欠である。企業に所属する従業員一人一人が、一個人や一消費として当たり前のようにプライバシーに関する問題意識をもっていることが重要である。こ

[32] 「どのタイミング」で「誰が」プライバシーリスクを評価するかなどの観点については、「5.3. プライバシーリスク評価（PIA）」に例を記載。

のような従業員が、消費者や社会と向き合った丁寧な対応を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継続的な取組が必要だが、経営者やプライバシー保護責任者がプライバシーを意識して常に大切であると発信し続ける必要がある。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。

- 定期的な e-learning や研修教育
- 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
- 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
- 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
- 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
- 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

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、消費者や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、分かりやすく説明を行うことも重要である。このような取組を積極的に行うことで、消費者との信頼関係を構築していくことが不可欠である。

4.4.1. 組織の取組の公表、広報

企業のプライバシー問題への考え方や、リスクをどのように把握し、評価し、コントロールしているかを取りまとめ、社外に公表する。

例えば、透明性レポート（transparency report）[33]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。消費者が懸念

[33] 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。

点を解消できるよう、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。

図表 10　事例：LINE TRANSPARENCY REPORT の公表

LINE 株式会社の「TRANSPARENCY REPORT」では、消費者から預かるデータをどのように取り扱っていたかを定期的に報告し、プラットフォーム運営に当たっての考え方を公表している。

（出典）https://linecorp.com/ja/security/transparency/top

また、直近では、プライバシー問題に係る企業の方針や、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・反映してから実際に施行し、事業開始していくという取組も、消費者・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在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、新たな消費者へ向けた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が改善したのか、迅速に、分かりやすく Web サイト等でお知らせすることで、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、利用者へプッシュ通知でお知らせをしたり、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、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が大切である。

図表 11　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うるものという特徴を踏まえ、消費者の意識について、各種消費者との接点から、把握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は、日頃対面で消費者と接する事業会社との協業に当たって、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。その際には、調査実施自体で満足することなく、意識調査等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。

図表 12　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

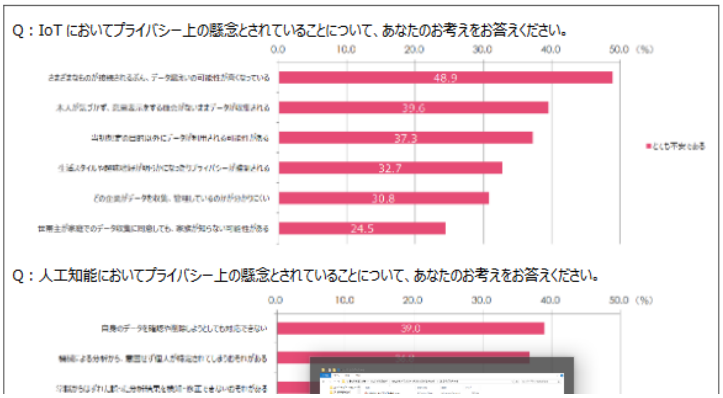
株式会社日立製作所と株式会社博報堂は、個人の意識の変化を定量的に把握することを目的に、継続的に意識調査を実施している。

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）「第四回 ビッグデータで取り扱う生活者情報に関する意識調査」を実施
https://www.hitachi.co.jp/New/cnews/month/2019/06/0606.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、迅速に問題発生を発見し、内容を把握のうえ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、サービス・製品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、分かる範囲で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、謝罪と共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うえ情報提供を行うべきである。

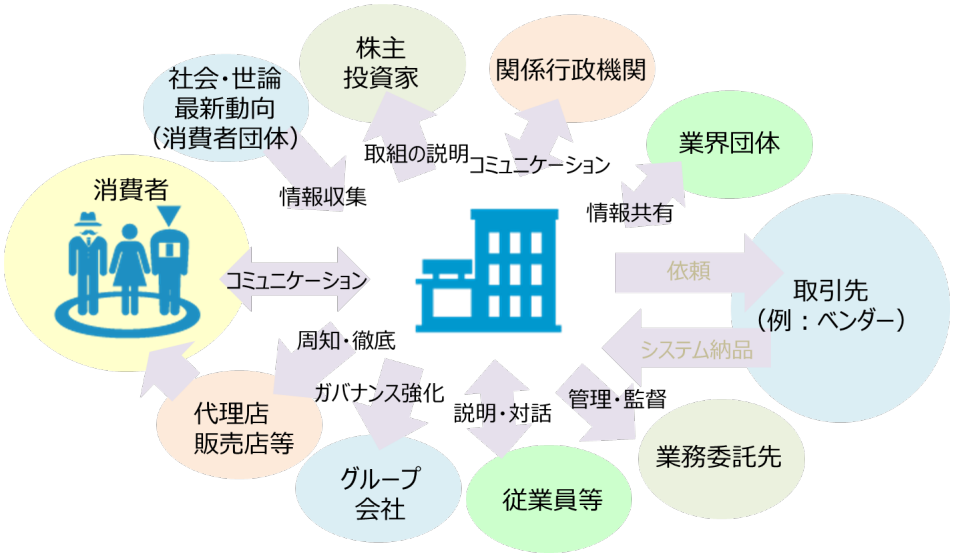
4.5. その他のステークホルダーとのコミュニケーション

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、ステークホルダーに対して積極的に説明し、信頼を確保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

プライバシー問題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 13　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）

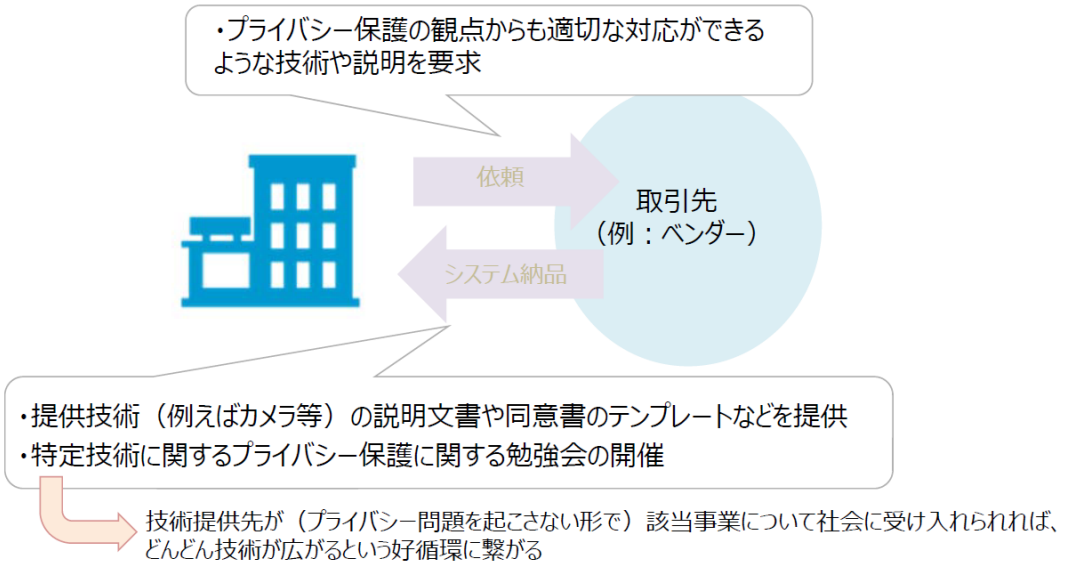
企業が事業を推進する際には、ビジネスパートナーなど、複数の企業と協働で実施する場合もあり、ビジネスパートナーも含めてプライバシー問題に適切に対応できていなければ、自社を含む関係企業及び当該事業全体の信頼を失うことになる。

特に、技術革新に比例して、新たなプライバシーリスクが発生していることから、ベンダー等のシステム関係の取引先と密なコミュニケーションを図ることが特に重要となる。スピードの速い技術革新と、変化する消費者のプライバシー問題に対する懸念を前提に、密接にコミュニケーションをとり、消費者のプライ

バシー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。発注側の企業のサービス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 14　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り、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、同時に委託元のプライバシーへの取組を高めるように委託先が協力すべきである。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うるため、グル

ープ全体での、プライバシー問題への対応についても、意識する必要があるだろう。

また、海外に拠点がある場合には、現状、プライバシーへの取組は各国で別個の取組を行っており、国ごとに対応が必要であることに注意が必要である。

（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もコストから先行投資として評価を高める傾向がみられる [34]。株主や投資家に対しても、企業のプライバシー問題への対応について、明確な説明を行うことがますます求められるだろう。トランスペアレンシーレポートの作成・公表なども、透明性の高い説明の一助となると考えられる。

（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 [35]。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、事業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を起こしてしまうと、自社の同様のサービスについても消費者の信頼を失ってしまう可能性がある。そこで、業界団体などを通じ、プライバシー問題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。

---

[34] 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。

[35] 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、相談を行っている。

[36] 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うるものであり、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。

（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、従業員へのプライバシー配慮が必要となる。他方で、セキュリティ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[36]。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。

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。

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、業界での対応や、業界横断での対応が必要で、個社での対応・検討では困難な場合には、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[37]。

---

[36] 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うるものであり、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。

[37] 「カメラ画像利活用ガイドブック ver2.0」（経済産業省・総務省・IoT 推進コンソーシアム、2018 年）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

以下、プライバシーリスクを管理する際の具体論について、参考となる考え方などを示す。なお、ここで記載している考え方は、国際標準や国際機関・各国の取組を踏まえたものであるが、企業内で活用するに当たっては、その背景や長所・短所をよく踏まえた上で、個別に適用していくことが望ましい。

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

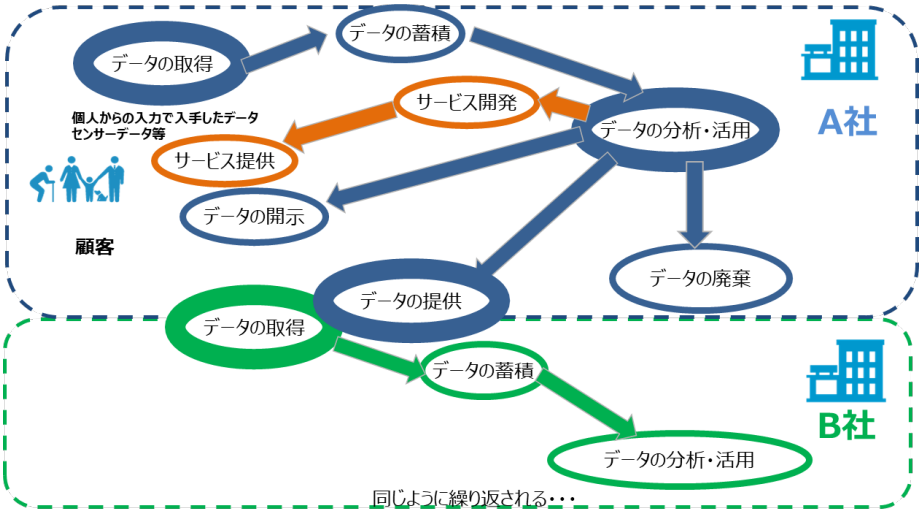
新規事業を行う際に、プライバシーに関するリスクの洗い出しを行う。そのためには、まず、対象事業がどのようなパーソナルデータのライフサイクルとなるのかを整理する必要がある。

特に整理すべきポイントは以下の通りである。

- ✓ 対象事業の関係者（消費者、パートナー、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
- ✓ 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。また、どの部分を外部事業者に委託するか、データの取得を２社以上で行う共同利用なのか等、データのライフサイクルの確認に合わせて、関係する取引事業者との関係性についても、早い段階で整理が必要である。（この段階で対象事業のスキームを決めておかないと、プライバシー問題だけではなく、法的な観点からも実施すべき責務が変わる点に注意が必要である。）

図表 15　パーソナルデータのライフサイクルの例



対象事業の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、パーソナルデータの取扱いやその目的を丁寧に説明する必要がある。

5.2. プライバシーリスクの特定（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で、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、そのプライバシー問題への対応方法を検討する。

ここでのポイントは以下の通り。

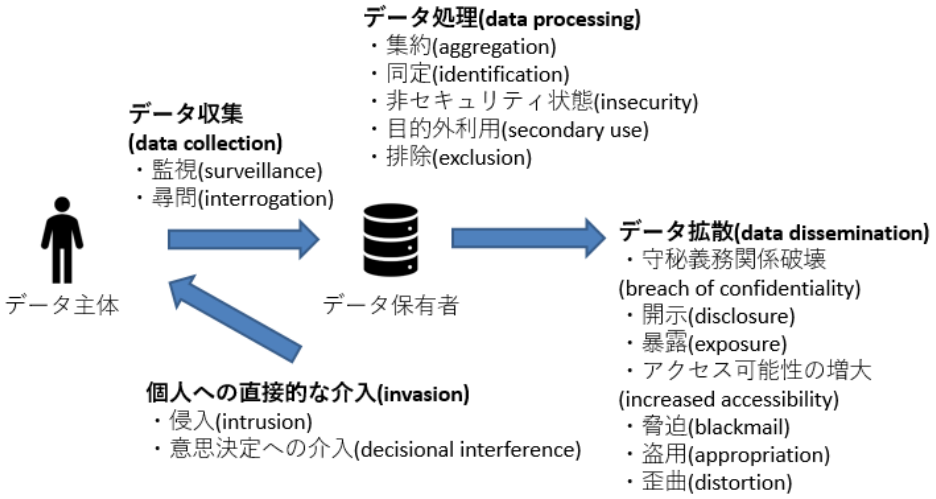
- ✓ プライバシー問題はリスクベースアプローチ [38] で考えること
- ✓ 事業の特性に応じて、プライバシー問題の体系的な整理を行うこと
- ✓ 組織の目的、能力、プライバシー問題に適したプライバシーリスク特定のためのツールや技術を用いること [39]

[38] プライバシー問題に係るリスクの特定を行い、リスクに応じて柔軟に対応策を取る考え方である。特定されたリスク、関連するシステム及びプロセスについてプライバシー影響評価を実施すること、プライバシーリスクマネジメントを実践することなどが含まれる。

[39] 「ISO/IEC29134:2017」は PIA の実施プロセス及び PIA 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る。

以下は一例であるが、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うる可能性があ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決定する中で、以下を活用してプライバシー問題を洗い出し、対応を検討する方法も一つである。

図表 16　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、2005 年）より Figure1 を翻訳

図表 17　プライバシー問題の例

データ収集	監視	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
	尋問	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[40]	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
	同定	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
	非セキュリティ	パーソナルデータを不適切に保護し、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
	排除	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
データ拡散	守秘義務関係破壊	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個人へ裏切りの感情を与えてないか
	開示	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	生活の諸側面の他者への暴露により、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。
	アクセス可能性の増大	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。
	脅迫	パーソナルデータの暴露、他者への開示などを条件に、脅迫者と非脅迫者に強力な権力関係を作り出し、支配され、コントロールされる事態になっていないか。
	盗用	他者のアイデンティティやパーソナリティを誰かの目的のために用い、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コントロールを失わせ、自由と自己開発へ介入することになっていないか。
	歪曲	個人が他者に知覚され判断される仕方を操作し、虚偽であり、誤解させることで、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。自分自身についての情報をコントロールする能力と、社会にとって自分がどのようにみられるかを限定的にしないすることになっていないか。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評判や性格を捻じ曲げることになっていないか。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	侵入	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
	意思決定への介入	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、2005 年）を参照して事務局作成

[40] 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「同定」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。）

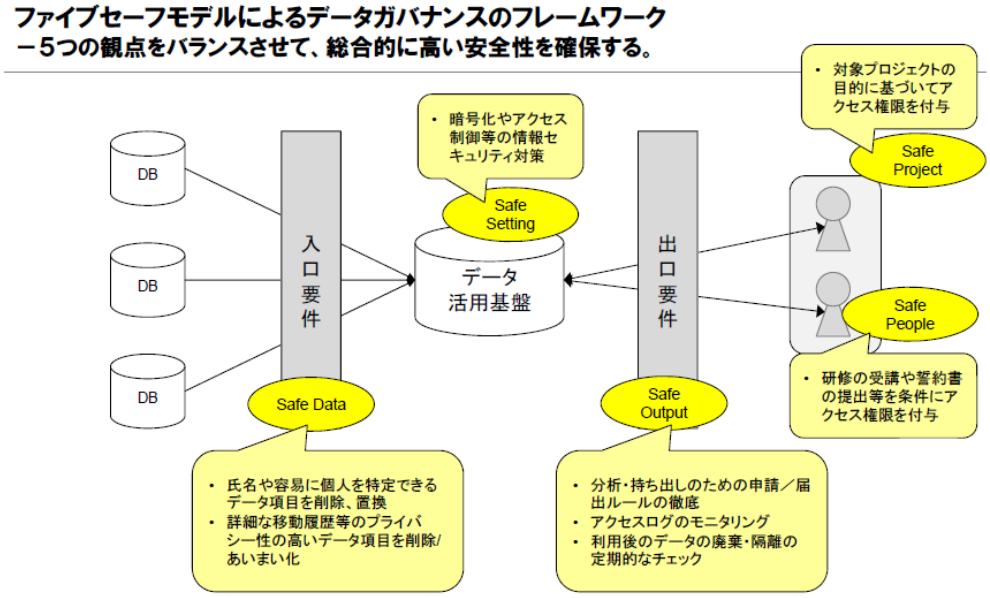
また、プライバシー問題に適したプライバシーリスク特定のためのツールとして参照できるフレームワークとして、「ファイブセーフモデル」がある。これは、データの有用性を確保しつつデータを安全に取り扱う方法として、イギリスの統計局（ONS）において、機密情報を利用した研究を規律するために 2003 年から運用されてきた。「ファイブセーフモデル」においては、EU をはじめとする諸外国で、統計の個票データ利活用のみならず、データ利活用時の安全対策ルールとして広く実績もあり、プライバシー問題及びその対策方法を考える上で参考となりうる。

図表 18　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 19　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



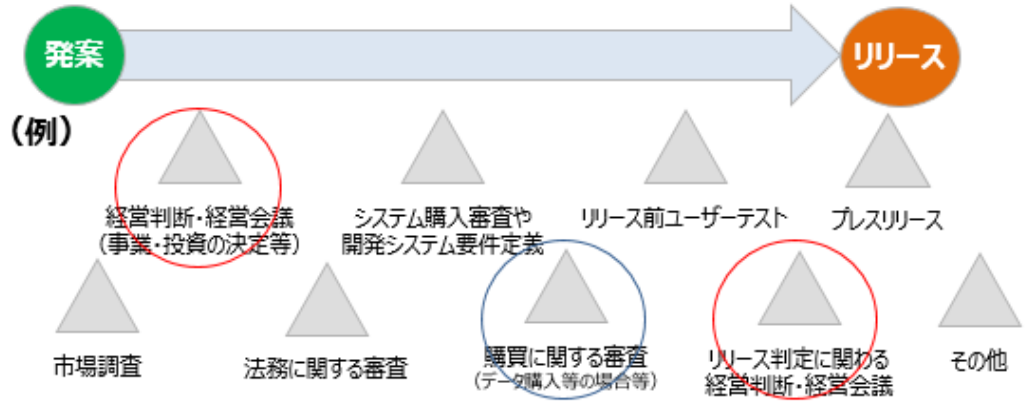
5.3. プライバシー影響評価（PIA）

プライバシー影響評価（PIA）とは、個人情報及びプライバシーに係るリスク分析、評価、対応検討を行う手法である。

企業は組織内に、プライバシーリスクを評価する仕組みを構築する必要がある。事業を検討するに当たって、どのタイミングで誰がプライバシーリスクを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あろう。

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、経営者とプライバシーリスクを評価するなどの方法があり得るだろう。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、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ことで、プライバシーリスクを対応することができる。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評価することも有用だろう。

図表 20　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評価をする仕組みを組み込むのかは、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大きく

変わってくるが、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[41][42]。

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、評価用のチェックリストを作成すること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。

なお、ISO/IEC 29134:2017 では PIA の実施プロセス及び PIA 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る。実施プロセスは、大きく「PIA の必要性の決定」「PIA の実行」「PIA のフォローアップ」の 3 項目にわかれ、「目標」「インプット」「期待されるアウトプット」「アクション」「実施のガイダンス」が具体的に説明されている[43][44]。

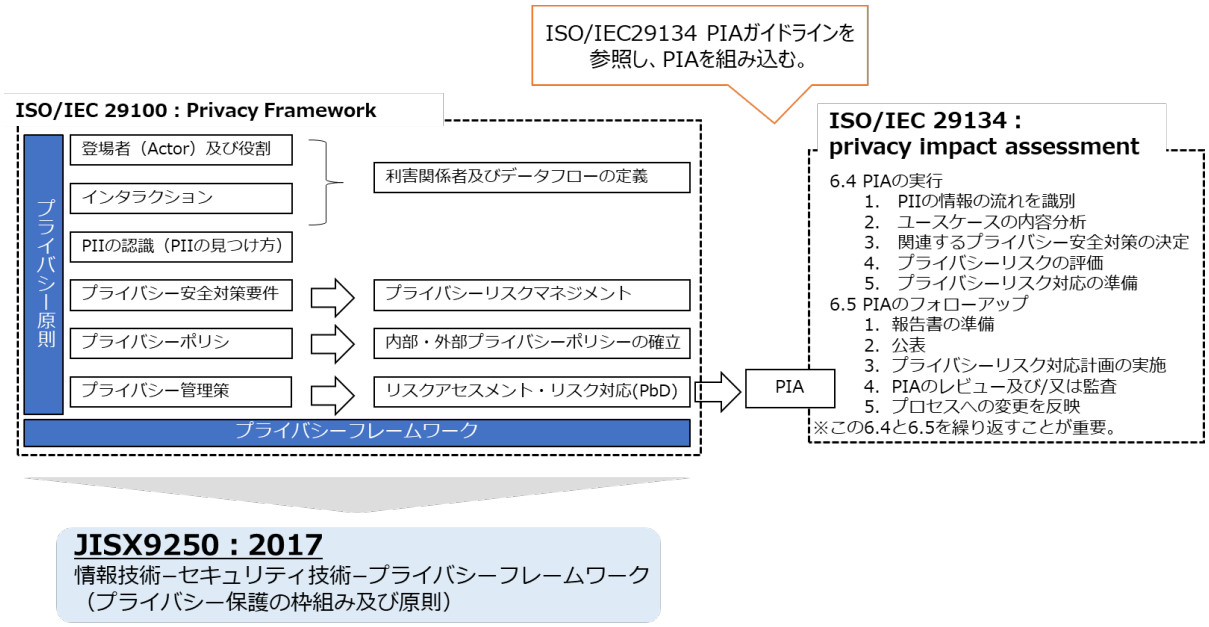
[41]企業内に既に構築されている、セキュリティなどの他のリスクを評価する体制や運用フローをうまく活用したり、パーソナルデータを多く利活用する部署から優先的にルールを整備するなどの工夫により、効率的な運用につながる場合もある。

[42] 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。

[43] 今後、ISO/IEC 29134:2017 についても、JIS 規格が発行される見込みである。

[44] 「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。

図表 21　参考：プライバシーフレームワーク（ISO/IEC29100）と
プライバシーインパクトアセスメント（ISO/IEC29134）



JISX9250 : 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）

6. （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、対処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 22　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、全ての機能に対して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繋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に関する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。

7. おわりに

今後、予想される Society5.0 を含めて、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。

そのデータのなかでも、パーソナルデータはビジネスの源泉となる一方で、プライバシー保護という課題を企業に課す。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、プライバシーに関わる問題は多様化・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り、何らかの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。このため、企業が何らかの活動においてプライバシーに関わ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えて、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るが、必ずしもコストとはいえない。むしろ商品やサービスの品質向上のひとつであり、他社に対する重要な差別化要素となっている。

このため、企業は組織としてのプライバシー対応、つまり企業ガバナンスとしてプライバシー問題に取り組むことが求められており、本ガイドブックは、企業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、今後の企業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。プライバシー問題は企業だけで解決できることは多くなく、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について提示した。

今まさに進む企業の DX 化において、本ガイドブックが企業におけるプライバシー活動の一助となり、その結果として企業の商品やサービスの価値、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・加筆が期待されるものである。

参考文献

- 「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」（ISO 26000：2010）
- 「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/
- 「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://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
- 「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://www.meti.go.jp/press/2017/03/20180330005/20180330005.html
  - 総務省プレスリリース　：
    http://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://www.meti.go.jp/press/2017/03/20180330005/20180330005.html
  - 総務省プレスリリース　：
    http://www.soumu.go.jp/menu_news/s-news/01kiban18_01000040.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://www.meti.go.jp/press/2020/07/20200713001/20200713001.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
- 「情報セキュリティガバナンス導入ガイダンス」（経済産業省、2009 年）
  https://www.meti.go.jp/policy/netsecurity/downloadfiles/securty_gov_guidelines.pdf
- 「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）
- 「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、2005 年、University of Pennsylvania Law Review, Vol. 154, No. 3, p. 477, January 2006、GWU Law School Public Law Research Paper No. 129）
  https://papers.ssrn.com/sol3/papers.cfm?abstract_id=667622
- 「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）
  https://www.soumu.go.jp/main_content/000196322.pdf
- 「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

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、令和元年度～令和２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 23　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	NTT セキュアプラットフォーム研究所
	林　達也	株式会社イエラエセキュリティ ／ココン株式会社
	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	弁護士法人英知法律事務所
	若目田　光生	一般社団法人日本経済団体連合会　デジタルエコノミー推進委員会企画部会　データ戦略ワーキング／株式会社日本総合研究所