企業のプライバシーガバナンスに関する
実践例の整理

（「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」の要件・重要項目別）

2023 年 4 月

総務省

経済産業省

目次

1. はじめに

本書は、「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」において、能動的に取り組むことの重要性が示されているプライバシーガバナンスに関して、実務において参照できる具体的な情報を充実してほしいという事業者からのニーズを踏まえ、プライバシーガバナンスの体制の構築、各ステークホルダーとのコミュニケーション等の実践例を整理したものである。

具体的には、「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」総務省、経済産業省、2023 年 4 月）の第 3 章及び第 4 章の「経営者が取り組むべき 3 要件」「プライバシーガバナンスの重要項目」について、要件・重要項目ごとに、プライバシーガバナンスに関する調査結果（取組状況例）[1]、2023 年度に実施した企業ヒアリング、その他公表情報から、実践例を整理しつつ、整理された実践例の理解を補助するために、見出しごとに、ガイドブックの記載内容から「ポイント」として、端的な記載を付している。

プライバシーガバナンスは、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、円滑な事業運営なども考慮して、企業自らが適切な形を検討することが重要である。「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」本文を参照いただき、本書で紹介する実践例に形式的に準拠するのではなく、あくまで参考とし、自社の業態・規模等に応じて、自ら適切な形を考えプライバシーガバナンスを実装いただきたい。また、本書に掲載する実践例は、網羅的に記載されているわけではないことにも留意いただきたい。

プライバシー問題は、商品やサービスによって異なり得る。また、プライバシー問題は、技術の進化や、個人個人の感じ方及び社会受容性の変化（これらは、コンテキストの違いや時間の経過等によって生じ得る）によっても変わり得る。「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」は、今後も、技術革新や社会動向を適切に踏まえて、更新を行っていくものである。なお、本書は、2023 年 4 月に公表された「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」に対応するものであり、今後「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」が改訂され、内容が更新されていく可能性があることにも留意いただきたい。

[1]「プライバシーガバナンスに関する調査結果（取組状況例）」（2022 年 3 月）（https://www.meti.go.jp/policy/it_policy/privacy/privacy_governance_research_syosai_torikumirei2022.pdf）

2. 経営者が取り組むべき三要件

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。

2.1. プライバシーガバナンスに係る姿勢の明文化

【ポイント】[2]

経営者が、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。

・姿勢の明文化

- ✓ 経営者がプライバシーを経営上の重要事項として認識している。
- ✓ プライバシー保護の軸となる基本的な考え方を提示する。
- ✓ 能動的にプライバシーリスク管理に対応する。
- ✓ プライバシーリスクに対し、受動的・事後的ではなく、能動的・事前的に対応する。(プライバシー・バイ・デザイン)
- ✓ プライバシーに関する取組を実施することのアカウンタビリティを確保する。
- ✓ 姿勢は、継続的に検証し見直す。

・明文化の形

- ✓ 姿勢を具体的な形で示す（文書化する)。
- ✓ 宣言、行動原則などを策定する。

・社内浸透・公表

- ✓ 経営者が姿勢をトップダウンで浸透させる。
- ✓ 組織全体に認識を根づかせる。
- ✓ 組織外へ姿勢を公開する。
- ✓ ステークホルダーからの信頼を高める根拠となる。

【実践例】

（例1） 中期戦略でデータ利活用による新しい価値提供が位置づき、データ利活用が本格化する前に、プライバシーへの適切な配慮を「社内の共通認識」とするとともにその実行性を担保する「社内運用の仕組み」が必要との問題意識の下、デ

[2] 【ポイント】は、整理された実践例の理解を補助するために、見出しごとに、「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」の記載内容を端的に記載したものである。各実践例の趣旨を正しく理解する上で、あるいは実践例を各社に最適化・応用する上でも、当該ガイドブックの内容について、「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」本体を参照いただきたい。

ータの有効活用とプライバシーへの配慮をバランスよく実現することを基本理念に、イノベーション創出に向けた行動原則の検討を開始。自社のビジョンの実現に向けて、リスクを正しく認識し、データ利活用のあり方を経営幹部が議論。外部の有識者からなる会合にて、法制度の理念や目的、社会一般の感覚に照らして適切であるかを確認し、基本的な考え方を整理して行動原則を作成した。トップメッセージとして発信し社内の啓発・運用を図ったのち、社外へも公表。行動原則については、年 2 回の副社長を委員長とする委員会で継続的に見直しの必要性を検証。【姿勢の明文化】

（例2） 外部有識者と経営陣による委員会を設置し、プライバシー保護を含めた自社のデータ活用の方向性について議論。従業員一人ひとりがパーソナルデータと向き合う際の理念として、パーソナルデータに係る指針を策定。【姿勢の明文化】

（例3） 主な事業領域がパーソナルデータを利活用するものであるため、設立当初から CEO がデータ利活用による価値創出を企業の目的に据え、プライバシーへの配慮が重要であることを強く認識。社外有識者会合の設置や国内外の最新動向にかかる社内勉強会開催を主導。それらの知見を踏まえて、CEO、COO が先陣を切って全体軸を決定し、プライバシーに係る宣言文を策定・公表。【姿勢の明文化】

（例4） パーソナルデータの利活用によりどのような価値を社会へ提供することを目指すかを明記。【明文化の形】

（例5） パーソナルデータの利活用にあたっては、法令遵守はもちろんプライバシーの保護は企業の責務と捉える姿勢を明記。【明文化の形】

（例6） 個人情報保護法に定める個人情報に限定せず、プライバシーに配慮して取扱うべき情報を対象として行動原則を定めていることを明記。【明文化の形】

（例7） 透明性の確保、消費者とのコミュニケーション、消費者の選択機会の提供、自社のビジネスパートナーの信頼性確認、適切なセキュリティ対策、体制整備などを明記。【明文化の形】

（例8） 体制整備に関して、プライバシー・バイ・デザインの思想に基づいたシステム開発、社内の教育の徹底、責任者や専門組織の設置、プライバシー影響評価を実施する仕組みの整備などを明記。【明文化の形】

（例9） 制定した行動原則について社内で Web 研修を実施。社内業務 PC へのポップアップ、ポスター掲示、ノベルティに印字して配布等を行いう事で社内啓発。【社内浸透・公表】

（例10） 行動原則・宣言文等を、Web サイトで公表。【社内浸透・公表】

2.2. プライバシー保護責任者の指名

【ポイント】

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。

・指名

- ✓ 経営者は、プライバシー保護責任者の責任と必要な権限を明らかにする。
- ✓ 経営者は、責任と権限を考慮し、プライバシー保護責任者を指名する。
- ✓ 経営者は、プライバシー保護責任者に対し、責任範囲を明確にするとともに、必要な権限を与える。
- ✓ 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指名する。

・モニタリング・評価・方向づけ

- ✓ 経営者は、プライバシー保護責任者からリスク管理の活動等について報告を受ける。
- ✓ 経営者は、モニタリングし、報告内容を評価し、それを踏まえて方向づけを行う。

【実践例】

（例1） 社内にコーポレートガバナンスの体制や、リスク管理体制がすでに構築されている大企業では、CXO（CIO（Chief Information Officer：最高情報責任者）、CDO（Chief Data Officer：最高データ責任者）、CPO（Chief Privacy Officer）、CISO（Chief Information Security Officer）等）や執行役員が、プライバシー保護やパーソナルデータの取扱いに責任を負う場合がある。【指名】

（例2） パーソナルデータの利活用を事業の主軸としている中小企業では、取締役がプライバシー保護について責任を負う場合もある。【指名】

（例3） スタートアップでは、役員や CXO（CTO（Chief Technology Officer：最高技術責任者）等）がプライバシー保護の責任を負う場合がある。個人情報保護管理者を兼ねることもある。【指名】

（例4） 事業部門が非常に大きい場合などは、事業部門側にプライバシー保護責任者を置くことで、その事業内容と消費者の反応に寄り添った形で、プライバシーリスクの把握や適切な対応を目指す場合がある。【指名】

（例5） 全社にまたがり（プライバシーに限らず）事業に関連して発生するリスク全般を管理する体制を構築している場合などは、そこで管理されるリスクの 1 つとして、プライバシーリスクを取り扱う形をとることがある。リスク管理部門側にプライバシー保護責任者を置き、全社的に整合したプライバシー保護の対応を行う場合がある。【指名】

2.3. プライバシーへの取組に対するリソースの投入

【ポイント】

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。

・リソース投入

- ✓ ヒト・モノ・カネ等の経営資源（リソース）の投入。
- ✓ 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する。
  - ➢ 十分な人員を配置する。
  - ➢ 人材育成を行う。
  - ➢ 新たな人材を確保する。
- ✓ 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。

・継続性

- ✓ プライバシーに関する取組に対して、経営資源を継続的に投入する。

・リソース投入結果の評価と説明

- ✓ リソースを投入した結果をモニタリングの上、リソースの追加投入要否等について適切に評価し、評価結果を踏まえた次の方向づけを行う。また、それらの取組全体について対外的に説明する。

【実践例】

（例1）	プライバシー保護組織を社内の PIA の事務局として機能させる場合、自社で対応する PIA の案件数などを考慮して、十分な人員を確保。【リソース投入】[3]
（例2）	多数の個人向けのサービスを提供する企業においては、プライバシーポリシーの表示や同意管理に関するシステムを一元化し、可能な限り自動化し、ヒューマンエラーを防ぐよう、システムを強化。【リソース投入】【継続性】

[3] 「個人情報保護に関する民間の自主的取組の在り方に関する調査　調査報告書」（2022 年 3 月）（https://www.ppc.go.jp/files/pdf/personal_pia_datamapping_report_2021.pdf）によれば、PIA の実施（開始から完了まで）に 1～2 ヶ月を要している事業者が多く、データガバナンス部門での対応が必要な PIA は月に 15 件～20 件程度という事業者が多いが、中には年間 300 件を超える事業者もあるとされている。

3. 体制の構築

適切な部門にプライバシーリスク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等を検討し、体制を構築する。

3.1. プライバシー保護責任者の役割

【ポイント】

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ができる体制を構築して、方針の実施を徹底する。

・方針の確立

- ✓ 経営者が姿勢を明文化した内容に基づき、方針を確立する。
- ✓ 方針に、緊急時対応、消費者救済、原因解析と改善の観点も含む。

・体制の構築・リスクマネジメントの実践

- ✓ 経営者が姿勢を明文化した内容を踏まえて、方針を確立し、プライバシーリスクマネジメントが実施できる体制を構築し、実践する。

・実践結果を報告

- ✓ 結果を経営者に報告する。

【実践例】

（例1） CIO 及び CISO を兼務する CPO が、コーポレート部門（プライバシーに関連する規制制度を把握)、法務部門（PIA の運用)、情報セキュリティ部門（情報管理、データ活用部門（ダッシュボード運用やポリシー検討）の取組を所管。【体制の構築】

（例2） プライバシーに配慮したデータ利活用の責任を CDO が担う。事業部門は法務部門に相談をしつつ事業を推進するが、各事業部門にサービスごとに置かれるデータ保護とプライバシーの両面に対応する責任者を置き、全体に影響を与える事案は、各部門の責任者からなる会議体で検討を行い、CDO へ付議する。CDO は、データ保護について独立した立場から適正性に関して助言・監視・評価をする DPO からの助言も踏まえて、経営会議等へ付議する。【体制の構築】【実践結果を報告】

（例3） CPO を議長とする会議体で、プライバシーに係る重要事項・方針・具体的施策を決定。CPO の下にプライバシーガバナンスを推進する部署を組織し、ルール策定や事業部門の支援を実施。各事業部門にプライバシー対応の責任者を置き、その責任者を招集した定期的な会合を開催し、プライバシーに係る対応内容や全社的な課題について情報を集める。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付け、対応を行う。【方針の確立】【体制の構築】

（例4） セキュリティを統括する執行役員が、自身が所管するリスク所管部署においてプライバシー保護方針や基準の立案や、プライバシーに係る評価を行う。【体制の構築】

（例5） パーソナルデータの取扱いを統括する CIO が中核組織を所管し、プライバシー保護に関する知見を集約し、社員からの相談対応、助言等の実施、関連規則、マニュアルなどの整備、教育等を行う。パーソナルデータを取り扱うにあたっては、プライバシーリスクの事前評価を事業部が実施することとしており、高リスクの場合には、中核組織が確認・承認を行う。【方針の確立】【体制の構築】

（例6） （中小企業の例）取締役がプライバシー保護の責任者となり、その下のリスク管理部門に兼務でプライバシー保護にかかる中核組織を設置。事業の企画・推進に当たり、目的評価、取引先企業との契約、成果物納品のそれぞれのタイミングで、プライバシーリスクをリスク管理部門が確認する体制を構築。リスクが高い場合には、プライバシーの専門家を含む有識者会議に付議する。【体制の構築】

3.2. プライバシー保護組織の役割

【ポイント】

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。

・構成

- ✓ 自社のリソースに合わせて実行性のある組織を構築する。
- ✓ どのような部門に紐づけて構築するかは、企業規模、ガバナンス体制、取り扱う情報、組織の立地などによっても変わる。

・組織の役割

- ✓ 自社のプライバシーリスクを漏れなく見つける。
- ✓ 事業部と連携の上、プライバシーリスクマネジメントを実施し、対応策を検討する。
- ✓ 関連する社内の部門（法務、システム、情報セキュリティ、コンプライアンス、広報、CS、経営企画、人権・ESG・サステナビリティ部門等）とも、必要に応じ連携する。
- ✓ プライバシー問題発生時にプライバシー保護責任者への報告・対応をする。
- ✓ 常に関連する情報（社内の対応事案も含む。）の収集・蓄積・共有をする。
- ✓ 有識者（学識者・コンサルタント、弁護士、消費者団体等）との関係構築・相談を実施する。

・人材

- ✓ 複数部署の間に立った調整能力を有する。
- ✓ プライバシーに関する取組に係る専門知識を有する。

【実践例】

（例1） CPO の下で、法務部門の中から 6 名が PIA 事務局として、運用事務やプライバシーに係る行動原則の運用状況の確認や見直しの要否の検証を行う。コーポレート部門（プライバシーに関連する規制制度を把握）、法務部門（PIA の運用）、情報セキュリティ部門（情報管理、データ活用部門（ダッシュボード運用やポリシー検討）が連携する。

事業部門が自ら実施する施策をルールに基づいて自主点検し、PIA の評価対象となると、法務部門が施策を評価する。プライバシーへの影響が大きい場合には、社内の関係各部門が参加する本会議にて評価を行う。PIA の評価結果等は一覧化し、社内へ共有する。【構成】【組織の役割】

（例2） CPO の下に、プライバシーガバナンスを推進する部署を組成し、法的検討、社内教育・文化醸成、事業部支援、ルール策定、ガバナンス実装を推進。主要な事業部門にはプライバシー保護対応の責任者を任命し、重要事項についての情報共有や、プライバシー保護に影響する重要事案の報告等を受ける。【構

成】【組織の役割】

（例3） セキュリティを統括する執行役員の元にリスク所轄部署を設置、プライバシー保護方針や基準立案や、プライバシーに係る評価を行う。全ての対外的にリリースされるサービスにおいてプライバシー観点での検討が漏れなく実施されるよう、複数の審査ポイントを設け、法務、プライバシー、セキュリティの専門部署によるレビューを実施。評価が難しい案件は、リスク所轄部署が専門部署を集めて会議を開催し、複眼的視点で評価を実施。【構成】【組織の役割】

（例4） 法務部門の中にプライバシーに係る問題へ対応するチームを作り、事業部門からの担当者からの相談に対応。【構成】【組織の役割】

（例5） CIO の下に中核組織を設置し、プライバシー保護に関する知見を集約し、社員からの相談対応、助言等の実施、関連規則、マニュアルなどの整備、教育等を行う。パーソナルデータを取り扱うにあたっては、プライバシーリスクの事前評価を事業部が実施することとしており、高リスクの場合には、中核組織が確認・承認を行う。【構成】【組織の役割】

（例6） AI による社会価値創出に取り組み、法制度・倫理・社会受容性などをケアする専門組織を、CDO の下に設置。【構成】【組織の役割】

（例7） 法務・知財・IT の 3 部門の連携組織として運用し、個人情報やパーソナルデータの利活用について、事業部門から相談を受け付け、法令遵守、プライバシーへの配慮の上で事業推進されるよう支援。国内外の規制動向等の情報収集・社内共有、普及啓発等に取り組む。【構成】【組織の役割】

（例8） グループ企業がグローバルに展開しているため、グローバルポリシーを制定し、グローバル本社から各地域組織の事業部門へ、ガイダンスや働きかけを行う、グローバルな体制を構築。【構成】【組織の役割】

（例9） 事業部門とは独立した形で、CISO の下に情報セキュリティに係る組織を設け、セキュリティガバナンスの一環で、個人情報やプライバシーについても取り扱う体制を構築。【構成】【組織の役割】

（例10） （中小企業の例）経営層と事業部門の間にリスク管理部門を置き、プライバシー保護に係る中核組織を兼務で構成。事業部門におけるリスク管理の内容に係る報告や相談に対応。パーソナルデータの利活用に当たっては、目的、データ利用用途、手段（セキュリティ）について確認。リスク評価を実施。【構成】【組織の役割】

（例11） （中小企業の例）外部有識者を招いて隔週で社内勉強会を開催し、プライバシー保護組織のメンバーの専門知識を充実させている。【人材】

（例12） （中小企業の例）経営者の下に恒常的なタスクフォースとして事業部門、管理部門、技術部門からの兼務の 8 名で中核組織を構成。個人情報保護のコンプライアンス対応、個人情報の保護体制に係る第三者認証制度に係る運用、プライバシーへの対応を実施。【構成】【組織の役割】

3.3. 事業部門の役割

【ポイント】

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。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を推進する。

・プライバシーリスクマネジメント

- ✓ プライバシー問題を引き起こさないか確認する。
- ✓ 当事者としての自覚を持つ。
  - ➢ 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する。
- ✓ 主体的な行動をする。
  - ➢ 消費者の受容性などにも配慮する。
  - ➢ 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。

・プライバシー保護組織との連携

- ✓ 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を推進する。
- ✓ 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する。

【実践例】

（例1） 事業部門側にサービス毎にプライバシーに係る責任者を設置。プライバシー統括部署との定例会議にて、具体的な案件・論点共有や全社の取組を共有・議論。新規商品開発に当たっては、要件定義前、開発テスト前企画後、リリース前に、プライバシーリスクに係るリスク管理部門側の評価に対応する。【プライバシーリスクマネジメント】【プライバシー保護組織との連携】

（例2） パーソナルデータを利活用する際には、事業部門でプライバシーリスクに係る自主点検を行い、PIA の対象となった場合には、PIA の事務局である法務部門や必要に応じて社内各部門の多角的な評価を受ける。この評価結果をもって事業部門がサービス開始に向けた社内審議を進める。【プライバシーリスクマネジメント】【プライバシー保護組織との連携】

（例3） 各事業部門は、新しく個人情報の取扱いを行う場合、リスク評価の事務局やリスク主管部署（法務・セキュリティ部門等）とリスクを共有したり、洗出しを行い、リスク評価と低減策に対しての回答を得る。その回答をもって経営会議への付議や、決裁文書の起案を進める。【プライバシーリスクマネジメント】【プライバシー保護組織との連携】

（例4） （中小企業の例）事業部での事業推進にあたっては、目的評価、取引先との契約、成果物納品のタイミングで、データ利活用の内容について資料化を行い、リスク管理部門に付議。評価結果を踏まえて、事業推進を行う。【プライバシ

ーリスクマネジメント】【プライバシー保護組織との連携】

（例5） 事業部門内に、サービス単位で、データ保護とプライバシーの両面に対応する責任者を指名。法務部門内に設置されたプライバシー対応チームに相談しつつ事業を推進するが、全体に影響を与える事案が生じた場合には、各事業部の責任者が集まる会議体に付議して検討し、必要に応じ CDO へ付議する。【プライバシー保護組織との連携】

（例6） プライバシーリスクがあると判断される事業部門には、部門ごとにプライバシー保護対応の責任者を指名。CPO の下に開催される定期的な会合にて、事業部門における対応内容を報告し、全社的な課題の共有を図る。【プライバシー保護組織との連携】

3.4. 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

【ポイント】

独立した立場からの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モニタリング・評価する。

・内部監査部門

- ✓ 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。

・アドバイザリーボード、諮問委員会

- ✓ 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・諮問委員会等を設置し、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る。
  - ➢ 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。
- ✓ 有識者の専門的かつ客観的な意見を、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。

・その他

- ✓ 独立した立場から適切なプライバシーリスクマネジメントをモニタリング・評価

【実践例】

（例1） 従来、情報セキュリティに係るルールの遵守状況について内部監査を実施しており、パーソナルデータに関するルール整備後には、パーソナルデータに係るルールの遵守状況に対しても内部監査を実施。【内部監査部門】

（例2） 事業部門側に個人情報・プライバシー保護に係る責任者を置き、プライバシーリスクマネジメントの実施状況を年次単位で自己評価し、リスク管理部門側に報告を上げ、リスク管理部門側が確認を行う。この流れに対して、別途、内部監査部門が適切かを確認している。【内部監査部門】

（例3） プライバシーに係る行動原則の制定や、制定後の見直しの必要性、プライバシーに関する企業の取組、PIA の実施報告等を、外部有識者からなる会議体（学識経験者、弁護士、消費者保護に係る非営利団体等）を年に 2 回程度、定期的に継続開催し、第三者的立場からの評価・検討を実施。【アドバイザリーボード、諮問委員会など】

（例4） プライバシーに関する取組について第三者の視点で確認するため、弁護士・研究者・消費者団体代表等様々な分野の有識者からなる有識者会議を設置し、運用。有識者会議は、CEO に対する助言機関として、客観的かつ厳格な評価をもらい、予見可能性を高める。【アドバイザリーボード、諮問委員会など】

（例5） プライバシーに係る体制構築を社内で進める際に、外部アドバイザーの支援を得て推進。【アドバイザリーボード、諮問委員会など】

（例6） 米国公認会計士協会の SOC 2 （Service Organization Control Type2）レポートや、クラウド事業者がパブリッククラウド上で管理する個人情報に焦点をあてた ISO 規格の認証を取得。【その他】

（例7） （中小企業の例）法学者、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有識者会合を設置し、経営陣に対して助言を行う会議体を継続的に開催。データ利活用に係る行動原則の策定に対する助言や、消費者へのわかりやすい説明、ルール・社内体制の整備などについて助言を受けて進めている。【アドバイザリーボード、諮問委員会など】

（例8） （中小企業の例）プライバシーに係る有識者会合を組成し、法律、ビジネス、技術、消費者等の観点から公正かつ中立的な視点での評価・意見を収集。年間4回程度の頻度で、パーソナルデータの取扱いに当たっての課題を相談。【アドバイザリーボード、諮問委員会など】

（例9） （中小企業の例）業界団体での活動を通して、プライバシー領域に詳しい有識者（弁護士）とネットワークを構築し、有識者からよいプラクティスの紹介等、アドバイスを受けて体制構築を推進。継続的に自社サービスのプライバシー保護について相談できる関係性を維持。【アドバイザリーボード、諮問委員会など】

4. 運用ルールの策定と周知

【ポイント】

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、適切な検討がされるように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、組織内で策定する。

・運用ルールの策定

- ✓ プライバシーリスクマネジメントの運用が徹底されるためのルール
  - ➢ 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。
- ✓ プライバシー保護責任者の責任の下、組織内でルールを策定する。
- ✓ ルール化する内容
  - ➢ プライバシー保護のための対策
  - ➢ 「どのタイミング」で「誰が」プライバシーリスクを特定、分析・評価するか等

・継続的な見直し

- ✓ 継続的に内容の見直し・修正を行うなどのメンテナンスを行う。

・運用ルールの周知

- ✓ ルールを組織全体に周知徹底する。

【実践例】

（例1） 要件定義前、開発テスト前、リリース前に、審査組織が確認を行う体制を整備。評価が難しい場合には、リスク担当執行役員を議長とし、専門部署を集めた委員会を開催し、多様な専門性を踏まえた評価を実施。懸念が表明された場合は場合によっては内容の見直しや実施を取りやめる。【運用ルールの策定】

（例2） パーソナルデータを取り扱う事案については、開発前に、全部門が自主点検を行い、付議基準に当てはまり PIA の評価対象となると、PIA 事務局が施策の概要をヒアリングし、簡易なものについてはその場で評価を与える。影響が大きい場合には、コーポレート部門、法務部門、情報セキュリティ部門、データ活用部門、CS 推進部門、広報部門などが参加する PIA 本会議にて質問や評価を行う。【運用ルールの策定】

（例3） 運用ルールに関して、法律の改正などで見直す必要がある際には、外部有識者会合にて見直しの内容について助言をいただきつつ進める。【運用ルールの見直し】

（例4） 各事業部が、新しく個人情報の取扱いを行う場合、リスク評価の事務局やリスク主管部署（コンプライアンス部門等）とリスクの共有や、リスクの洗い出しを行い、リスク評価と低減策の回答を得る。その回答をもって経営会議への付議や決裁文書起案を進めることで、プライバシーリスクに係る決裁者の適正な

判断を実現。パーソナルデータ管理細則を定め、OECD8 原則、その他各種プライバシーに関する法令等から利活用の原則を策定。パーソナルデータ管理細則の準拠状況を確認するためのチェックシートを作成し、事業部門は、リスク主管部署（コンプライアンス部）の指示に従って、準拠状況を報告する。

（例5） （中小企業の例）事業部での事業推進や案件引合の際に、目的評価、取引先との契約、成果物納品の 3 回のタイミングでデータ利活用の内容について資料化を行い、リスク管理部門に付議。結果を踏まえて事業推進を行う。リスク評価時にはチェックシートを用いているが、リスク評価の実施結果を保護方針やチェックシートにフィードバックし、適宜アップデートを行っている。【運用ルールの策定】【継続的な見直し】

（例6） グローバルに展開する各国の拠点でプライバシー保護に係る適切な対応ができるよう、グローバルデータプライバシーポリシーを制定し、データ主体保護や委託先管理等に関するグローバル共通/最低基準を設定し、各種書類雛形の提供。グローバルデータプライバシーポリシーの下、必要に応じ、各国の現地法制への対応を含む、ローカライゼーションを行う。【運用ルールの策定】

（例7） GDPR に準拠して、プライバシーリスクが高い案件については、適宜 DPIA を実施。【運用ルールの策定】

（例8） （中小企業の例）個人情報保護マネジメントシステムの第三者認証の要求事項により、年 1 回教育を実施する必要があり、基本的にはその実施月をターゲットに、その前に関連法令の最新状況を精査し、必要に応じルールや規約等の見直しを行っている。直ちに見直すべき内容は上記に限らず、柔軟に見直しを実施。【運用ルールの見直し】

（例9） 全従業員に対し、業務遂行時に参照すべきプライバシーに関するマニュアルの提供とオンラインでのトレーニングを実施。【運用ルールの周知】

5. 企業内のプライバシーに係る文化の醸成

【ポイント】

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を組織全体で醸成する。

・プライバシーに係る文化

- ✓ 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。
- ✓ 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。

・企業文化を根付かせる継続的な取組

- ✓ 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。
- ✓ 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。
- ✓ プライバシーに係る基礎的な知識習得を促すだけでなく、明文化した姿勢等について、大切さを経営者やプライバシー保護責任者が常に発信。
- ✓ 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。

【実践例】

（例1） 全社員に対して、プライバシー保護、個人情報保護に関する e-learning 等を実施。【企業文化を根付かせる継続的な取組】

（例2） （中小企業の例）人材を採用する際に、プライバシーを第一に考える社の方針に共感できる人材を選考。【企業文化を根付かせる継続的な取組】

（例3） 人事部で開催される従業員の行動規範に係るセミナーや研修に、個人情報・プライバシーに関する内容を含めてもらい、従業員全体の意識向上を図る。【企業文化を根付かせる継続的な取組】

（例4） プライバシー保護の中核となる組織が、個人情報保護法、関連するガイドライン等、海外のプライバシー保護に係る規制等の調査・分析を行い、社内への情報提供。セミナー開催、コラムなどでも社内へ発信。【プライバシーに係る文化】【企業文化を根付かせる継続的な取組】

（例5） グローバル企業における多様性を尊重する企業文化の中で、プライバシーの尊重についても理解が醸成されている。【プライバシーに係る文化】

（例6） （中小企業の例）ファミリートレーニング（職場全体で行われる全員参加型の研修）にてプライバシーについて討論する時間を設け、従業員全員の意識醸成。【企業文化を根付かせる継続的な取組】

（例7） プライバシーに関する基本的な考え方やあるべき姿、行動原理をハンドブック

としてまとめ、全社員に配布。【企業文化を根付かせる継続的な取組】

（例8） （中小企業の例）プライバシーに係る社の宣言文を、社内全員で議論しながら策定し、社員全員のプライバシーに対する共通認識を醸成。【企業文化を根付かせる継続的な取組】

（例9） プライバシーに係る行動原則を策定した際に、Web 研修だけでなく、業務用 PC へのポップアップや、社内ポスター掲示、ノベルティに印字しての配布等を実施。【企業文化を根付かせる継続的な取組】

（例10） （中小企業の例）B2B 企業の経営者自らが実施する、顧客企業や提携先に対してプライバシー保護の重要性を伝えるセミナーに従業員を同席させることで、社としてのプライバシー保護へのコミットメントを従業員にも意識づける。【企業文化を根付かせる継続的な取組】

（例11）プライバシーについての考え方を全部門入社後数か月～1 年かけて教育し、関係する従業員の意識を統一する。【企業文化を根付かせる継続的な取組】

6. 消費者とのコミュニケーション

パーソナルデータの利活用に関する消費者の意識や不安、求めている情報等を理解し、企業のプライバシーに関する取組を積極的に分かりやすく丁寧に説明する。

6.1. 組織の取組の公表、広報

【ポイント】

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を取りまとめ、社外に公表する。

・公表・広報する内容

- ✓ 企業のプライバシー保護の考え方
- ✓ 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
  - ➢ 透明性レポート（transparency report）
    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

・公表・広報するタイミング

- ✓ 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、実施前に公表するケース
  - ➢ 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

【実践例】

（例1） 企業のパーソナルデータの利活用やプライバシーに係る考え方をまとめた行動原則などを公表。注力する事業領域により、その領域（例えば、AI活用）の本人の権利利益（プライバシーも含む。）に係る基本的な方針や理念を策定し、公表する場合もある。【公表・広報する内容】

（例2） プライバシー性の高いセンシティブなデータの保護に対する考え方や、企業としてリスクをどう評価しコントロールしているかを整理してホワイトペーパとして公表。消費者の同意を得た上で慎重に利活用するとの考え方を明記。CRO の元、センシティブ情報の専門チームを組成し、事前・事後のリスク評価や助言指導を行っていること、リスク評価の際に重視している観点（利用目的や利用方法が適切か、取扱う主体が明確か)、情報セキュリティ上の安全管理措置等を整理して公表。併せて、センシティブデータを利活用するメリット（事例）について、イラストも交えて、消費者へわかりやすく解説。【公表・広報する内容】

（例3） 消費者が特に懸念を持つ事項（消費者からの情報の削除申請への対応、違反投稿への対応、捜査機関からの消費者の情報の開示・削除申請への対応等）につ

いて、考え方や対応件数の推移などを定期的に Web サイトを通じて公表。【公表・広報する内容】【公表・広報するタイミング】

（例4） プライバシーセンターを Web サイトで公開。パーソナルデータに係る指針の内容、第三者視点の取り入れ、プライバシー保護における責任所在の明確化、リスク評価プロセスの導入、パーソナルデータの取扱い（活用、外部連携、活用処理）の説明、プライバシーに配慮したガバナンス体制等を、イラストや具体例を用いてわかりやすく説明。【公表・広報する内容】【公表・広報するタイミング】

（例5） 公共空間に AI カメラを設置し、見守り・異常行動検知や人流分析等の取組を行う際に、運用開始前に運用指針を定め、Web サイトから公表。運用を開始前に、データの取扱いやプライバシーへの対応について、地域住民に対する説明会を開催して、質問や懸念に対応。【公表・広報するタイミング】

6.2. 消費者との継続的なコミュニケーション

【ポイント】

企業の信頼確保の観点から、企業から消費者へ、継続的に、積極的なアプローチをする。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、消費者に向けて、対応・改善した内容を迅速に、分かりやすく Web サイト等で知らせる。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。

・コミュニケーション内容

- ✓ 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。
- ✓ 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。

・コミュニケーションの方法・タイミング

- ✓ 新たな機能追加や利用規約等の改定のタイミング等
- ✓ 利用者へプッシュ通知
- ✓ 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
- ✓ 問合せ窓口の掲示、データの取扱いに係るコントロールパネルの提供
- ✓ 消費者意識について消費者との各種接点（消費者へダイレクト、直接の消費者との接点がなければアンケート調査等を利用など）から、把握ができるよう努める。

・コミュニケーション結果の反映

- ✓ 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。

【実践例】

（例1） ダッシュボードにて、データの提供先、種類の確認・変更、同意事項の確認などの機能を提供。プライバシーポリシーの改定等があった場合には、迅速にその内容を通知する。【コミュニケーション内容】【コミュニケーションの方法・タイミング】

（例2） 利用者のプライバシーに係るポータルサイトを開設し、ユーザ自身が容易に、自らのパーソナルデータの利用状況を確認し、変更が可能なよう、各サービスの利用規約や第三者提供等への同意状況を可視化し、自らいつでも確認・変更が可能なコントロール機能を提供。【コミュニケーション内容】【コミュニケーションの方法・タイミング】

（例3） 購買データを利活用するサービスにおいてダッシュボードを提供。自身の購買データを連携している先のサービスを確認し、データ連携や解除を自在にコン

トロールできる機能を提供。【コミュニケーション内容】【コミュニケーションの方法・タイミング】

（例4） 年に 1 回～2 回、利用者に自社のパーソナルデータに係る取組の認知度と受容性の観点で調査を実施（定量的なアンケート形式とインタビュー形式の組合せ）。調査結果を踏まえて、ユーザ向けに提供しているコンテンツの改善を図っている。【コミュニケーション内容】【コミュニケーションの方法・タイミング】【コミュニケーション結果の反映】

（例5） リスクに直面する消費者がプライバシーに関し、何を期待しているのか等について把握をするため、継続的に消費者の意識調査を実施。【コミュニケーション内容】

6.3. 問題発生時の消費者とのコミュニケーション

【ポイント】

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、構築する。問題発生時には、迅速に問題を特定し、内容を把握した上で、対応する。

・事前の準備

- ✓ 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。

・事後の対応

- ✓ 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。
- ✓ 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。
- ✓ 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。

【実践例】

（例1） 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、CPO 及び経営層に報告をし、分析・対策を実施することを、事前にルールとして定めている。【事前の準備】

（例2） 同業他社で事故が起きた場合には、自社ではプライバシーリスクに対して適切な対応をしていること（社内でガイドライン等を整備し、従業員教育を徹底していること等）について提携先や顧客に、迅速に説明を実施するようにしている。【事後の対応】

7. その他のステークホルダーとのコミュニケーション

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する。

7.1. ステークホルダーへの対応

（1）ビジネスパートナー（取引先・業務委託先）

【ポイント】

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、特に技術革新のスピードが速い領域では、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。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、対応を行う。

・ビジネスパートナーも含めたプライバシーリスクへの適切な対応

- ✓ 発注側企業と取引先（ベンダー企業）の関係：発注企業はベンダー企業に、プライバシーに関する取組に必要な情報を要求し、ベンダー企業は説明を尽くす。
- ✓ 委託元と委託先の関係：委託元はプライバシーに係る対応について委託先に説明を求め、委託先は協力する。

【実践例】

（例1） ベンダー企業側から取引先企業に、説明文書や同意文書等のテンプレートを提供するなど、取引先企業の円滑な事業推進のための支援を行う。【ベンダー企業】

（例2） ベンダー企業の経営者自らが顧客企業に対して、プライバシーに関する社内セミナーを実施。【ベンダー企業】

（例3） コンテンツ管理を行う顧客企業向けに、消費者に対して適切な法令に基づき適宜通知する責任が顧客企業にあることを前提に、プライバシーやデータ保護についてホワイトペーパを整備して解説。質問の多い内容や啓発が特に必要な内容はWebサイトでQA形式でも発信。【ベンダー企業】

（例4） 同業他社で事故が起きた場合に自社は十分な対応（教育等のガイドラインを整備）を行っていることを提携先や顧客企業に迅速に説明。【ベンダー企業】

（例5） 顧客企業に向けての提案都度、営業担当が、プライバシーに関する協議を顧客企業と行う。【ベンダー企業】

（例6） 委託先選定時に、情報セキュリティ管理体制（組織的安全管理措置、技術的安全管理措置等）について質問票を用意し確認。【委託元企業】

（例7） 委託先選定のグローバル一律基準を策定。パーソナルデータの取扱いの委託契約に盛り込む最低要件を決め、契約書ひな形を各グローバル拠点へ配布し、委託先管理の水準を保っている。【委託元企業】

（2）グループ企業等

【ポイント】

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意識し、検討する。

・グループ企業におけるガバナンス

　✓　持株会社の役割と責任

・グローバル企業におけるガバナンス

　✓　国ごとの対応

【参考事例】

（例1）　持株会社がデータガバナンスの方針や守るべきルールを定め、子会社側の遵守状況を監督。【グループ企業におけるガバナンス】

（例2）　データビジネスを中心に扱う子会社側で先行してプライバシーガバナンスを構築し、グループ全体のプライバシーに関する取組を進める際に、子会社の取組を参考にして推進。【グループ企業におけるガバナンス】

（例3）　グローバルプライバシーポリシーを制定し、グローバル共通／最低基準を設定。【グローバル企業におけるガバナンス】

（3）投資家・株主

【ポイント】

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。株主や投資家に対しても、プライバシーリスクへの対応について、明確な説明を行うことがますます求められる。

・透明性の高い説明方法

　✓　透明性レポート、統合報告書、サステナビリティレポート　等

【実践例】

（例1）　年 1 回取りまとめるサステナビリティレポートで、プライバシーに係る基本的考え方、推進体制（CPO の下で重要方針・具体的指針を決めていくこと、アドバイザリーボードの設置等）、社内規則の整備、教育の実施状況、その年の取組状況等を公表。【透明性の高い説明方法】

（例2）　年 1 回取りまとめるサステナビリティレポートで、個人情報保護方針と体制整備、個人情報の管理と普及啓発に係る報告とともに、パーソナルデータに対する対応として、行動原則にのっとった取組状況や消費者への自社の取組の発信

状況を報告。今後 PIA の実施状況なども掲載の予定。【透明性の高い説明方法】
（例3） （中小企業の例）プライバシーリスクやそれに配慮した事業推進について投資家・株主に説明し、理解の上で投資をいただくようにしている。【透明性の高い説明方法】
（例4） ESG 視点のマテリアリティとしてプライバシーを取り上げ、サステナビリティレポートに記載。【透明性の高い説明方法】

（4）関係行政機関

【ポイント】

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、必要に応じて事前に相談する。

・個人情報保護委員会等への事前相談
・所管省庁とのコミュニケーション

【実践例】

（例1） プライバシー保護に係る新しい事業を推進する上で、新規事業における規制の解釈・適用有無について相談できる省庁の窓口に相談。【所管省庁とのコミュニケーション】
（例2） 個人情報の取扱いに不明瞭な点があったため、個人情報保護委員会へ相談。法的な整理について助言を得て、知見を充実。【個人情報保護委員会等への事前相談】

（5）業界団体

【ポイント】

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。

・業界団体の活動への積極的な参加

（実践例）

（例1） IT やエレクトロニクス産業を中核とした業界団体において、個人データに係る専門委員会を設置し、個人情報保護法等の規制の在り方やプライバシー配慮の観点からのルール整備に向けて関係省庁への提言を実施。グローバル法制度についても積極的な働きかけを実施。【業界団体の活動への積極的な参加】
（例2） デジタルコンテンツサービス関連産業の業界団体において、コンテンツプロバイダの事業に関する情報収集、課題解決支援の一環で、プライバシー対応ワーキンググループを組成し、個人情報保護、プライバシーの法制制度状況等への

対応を推進。【業界団体の活動への積極的な参加】

（例3） 金融・クレジット業界団体の活動を通じて知り合った企業のコンプライアンス部門同士で、プライバシーに関する最新の情報交換を定期的に実施。【業界団体の活動への積極的な参加】

（6）従業員等

【ポイント】

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。

・従業員への配慮

- ✓ 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となる。

・求職者、退職者、取引先の従業員等への配慮

【実践例】

（例1） 従業員のプライバシー保護に関しても社内規定で整備し、企業としてコミットメント。例えば、従業員を対象とした実証実験を行う場合も、消費者のデータを取り扱う際と同様に、社内の PIA 評価の対象としている。【従業員への配慮】

7.2. プライバシー問題の情報収集

【ポイント】

プライバシーに関する議論は日々変化するため、消費者の意識調査等の取組や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。

・社会や世論などの最新動向を継続的に入手
- ✓ 消費者の意識
- ✓ 国内外の法制度の動向

・入手手段
- ✓ 業界団体との情報交換
- ✓ 関係省庁からの情報発信（個人情報保護委員会、経済産業省等）
- ✓ 有識者（アドバイザリーボードに招へいする人）
- ✓ 弁護士（プライバシー問題に詳しい人）

【実践例】

（例1） 外部有識者会合を開催する際に、プライバシーに関連する国内外の最新動向などの情報交換も実施。【社会や世論などの最新動向を継続的に入手】【入手方法】

（例2） プライバシーに詳しい外部有識者を招いて情報交換や社内向けの勉強会を開催。【入手方法】

（例3） 関係省庁からの情報発信や、業界団体への参画通じた情報収集により、関連法令の最新状況について把握。【社会や世論などの最新動向を継続的に入手】【入手方法】

（例4） プライバシーに係る体制構築を社内で進める際に、外部アドバイザーの支援を得て推進。【入手方法】

（例5） （中小企業の例）業界団体での活動でプライバシー領域に詳しい有識者（弁護士）とネットワークを構築し、有識者からよいプラクティスのインプット等、アドバイスを受けて体制構築を推進。継続的に自社サービスについて相談できる関係性を維持。【入手方法】

7.3. その他の取組

【ポイント】

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等の取組を行う。

・業界での対応を可能とする取組の組成

・業界横断での対応を可能とする取組の組成

【実践例】

（例1） 同業他社がプライバシーに係る問題を生じてしまうと、自らの事業の信頼も毀損するため、業界の健全化のために位置情報の利活用に係る業界団体を創設し、関連する法規制・ガイドラインの他関連する情報を共有【業界での対応を可能とする取組の組成】

（例2） プライバシーテックに係る業界団体をつくり、個人情報やプライバシー保護について関係省庁や有識者と議論を行った内容を、同じ分野の事業者が同じ問題に直面しないよう、情報共有【業界での対応を可能とする取組の組成】

（例3） 官民で運営されるコンソーシアムの中にワーキンググループを組成し、IoT や AI の利活用が進む中で、カメラ画像の利活用に当たりプライバシーの観点から配慮すべき事項を取りまとめ公表【業界横断での対応を可能とする取組の組成】