個人データの取扱いに関する責任者・責任部署の
設置・運用における取組の観点集
―データガバナンス体制構築に向けて―

２０２５年３月

株式会社　野村総合研究所

目次

本資料は、個人情報保護委員会事務局からの委託事業（令和６年度「実効性のある社内管理体制に関する調査」の成果物として作成されたものである。

個人情報等を含むデータの利活用を促進するためのデータガバナンス

近年、AI、IoT、クラウドサービス、５G 等のデジタル技術の飛躍的な進展により、多種多様かつ膨大なデータの収集・分析等が容易かつ高度化しており、このようなデータの中には個人情報を含む個人に関する情報[1]（以下「個人情報等」という。）が含まれることも多い。このようなデータが高度に利活用されることにより、サービスの向上や、地域の活性化、新産業・新サービスの創出、国際競争力の強化や我が国発のイノベーション創出が図られることが一層期待されている。

一方、大量の個人情報等を含むデータが集積され不適正に利用された場合には、個人の権利利益に対する大きな侵害につながるリスクも高まっている。そして、自分の個人情報等が悪用されるのではないか、知らない間に第三者に提供されているのではないかなどの個人の不安感も引き続き高まっている。このような中で、データがもたらす価値を最大限引き出すには、プライバシーやセキュリティ等への適切な対処を行うことにより、個人からの信頼を維持・構築することが重要である。

特に、デジタル社会においては、ビジネスモデルや技術の革新等も著しい中で、各主体は、個人情報等の取扱いに関して共通する必要最小限のルールであ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。）を遵守するとともに、政策、事務及び事業並びにシステム構築等の目的、個人が得ることが期待される便益やプライバシーに関するリスクを明確にし、それらをわかりやすく、丁寧に説明すること等を通じて透明性と信頼性を確保していくことが特に重要である。

このような取組を実現していくためには、「個人情報の保護に関する基本方針」（平成 16 年 4 月 2 日閣議決定　令和 4 年 4 月 1 日一部変更）において指摘されるように、解決しようとする課題とその課題を解決するために取り扱う個人情報等のデータとの関係を明確化しリスクを把握する観点から、データの内容や性質、量や範囲の必要十分性、データの流れ、データの取扱いに関わる者の範囲、データの利用目的、安全管理レベル等の事前評価のため、PIA[2]（個人情報保護評価又はプライバシー影響評価）の手法を用いることや、CPO（最高プライバシー責任者）や DPO（データ保護責任者）等の個人データの取扱いに関する責任者を設置・運用すること等によるデータガバナンスの体制（以下「データガバナンス体制」という。）を構築することが重要である。

しかしながら、このようなデータガバナンス体制を構築し実効性を担保する取組は、一部先進的企業において行われているものの、十分な広がりを見せていない実態があると指摘されている。実効性のあるデータガバナンス体制を整備し、適切にデータを取り扱うことは、消費者や取引先の企業等の顧客（以下「顧客等」という。）から求められており、顧客等からの信頼に基づく適正なデータ利活用を中長期的に推進していくための土台として、その実現のために必要とされる取組について検討していく必要がある。

---

[1] 「個人に関する情報」は、個人情報保護法で規定されているものに限定されるわけではなく、情報通信技術の高度化などの環境の変化を受けて、個人情報保護法の外縁部分にあるものも含めた、より幅広い、個人に関するあらゆるデータに対する配慮が求められるようになっている。

[2] PIA：個人情報等の収集を伴う事業の開始や変更の際に、プライバシー等の個人の権利利益の侵害リスクを低減・回避するために、事前に影響を評価するリスク管理手法である（出所：個人情報保護委員会「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）」https://www.ppc.go.jp/files/pdf/pia_overview.pdf）

本資料の構成について

本調査は、このような実態を踏まえて、データガバナンス体制を構築し、継続的に改善を図っている先進的な事業者の取組事例を踏まえて、データガバナンスに関する外部専門家の助言を得て、責任者及び責任部署の設置・運用について留意すべき点や取組の観点の例等の具体的な実践例をとりまとめ、参考資料として公表するものである[3]。

なお、本資料を参照される際には、各主体における個人情報等を含むデジタルデータの利用実態や体制等はそれぞれ異なっていることについて考慮した上で活用いただきたい。また、データガバナンスの取組は、情報通信技術の発展、提供サービスの変化、社会・経済動向の変化等に伴う個人の権利利益への影響や消費者・顧客とのコミュニケーションも踏まえつつ、継続的に取り組むものであることにご留意いただきたい。

本資料の構成としては、

第一に、実際の先進的な取組事例等も踏まえ、実効性あるデータガバナンスを実現するために「体制構築の重要性」を指摘した上で、具体的な体制構築のために必要となる「責任者・責任部署」の位置づけ・役割についてとりまとめた。

第二に、「責任者・責任部署」を実際に設置しこれを運用する際の留意点について、設置する際の留意点及び運用する際の留意点に分けてとりまとめた。（各項目の中において、各事業者に共通すると考えられるものをまずは「留意事項」として記載し、ヒアリング対象事業者が社内事情に応じて取り組んできたものを「取組の観点（例）」[4]として分けて記載している。また、データガバナンス体制の整備に今後取り組み始める事業者（中小規模事業者等）に向けて、「取組の観点（例）」のうち特に参照することが望まれる事項には、取組内容の末尾に（＊）を付している。）

第三に、付属資料として、今回のヒアリング対象事業者の中から小売業、製造業、サービス業、金融業等における「個人データの取扱いに関する責任者・責任部署の設置・運用の実践例」を記載している。

[3] 本資料作成に当たって、個人データの適切な取扱いのために責任者や責任部署設置等の体制の整備や運用に取り組んできた事業者 10 社へヒアリングを実施した。

[4] 「取組の観点（例）」は、ヒアリング対象事業者が社内事情に応じて取り組んできた観点であり、責任者や責任部署の設置や運用等をこれからしようとする事業者等において、自社に合わせたアプローチを考える際のヒントとなりうる事例をピックアップしているものであり、網羅的に全て実施していくべきものとは位置づけていないという前提で参照いただきたい。

１．実効性のあるデータガバナンス体制構築に向けた、個人データの取扱いに関する責任者及び責任部署の概要

（１）実効性のあるデータガバナンス体制構築の重要性

AI、IoT、クラウドサービス、５G 等のデジタル技術の飛躍的な進展とデジタル社会の進展により、個人情報等を含むデジタルデータの利活用が著しく拡大している。個人情報等を利活用した新たな事業・サービスは、消費者に様々な利便性を提供する一方で、その利活用の手法が複雑化、多様化していることに伴い、事業者が個人情報等を適正に取り扱っているかについて、消費者の不安感が高まっている。事業者において、デジタルデータの取得、管理又は提供といったライフサイクルに渡って適切に制御し、データの取扱いに関する透明性を確保する実効性のあるデータガバナンス体制を構築することにより、個人からの信頼と納得を確保する重要性が高まっている。これは、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 の実現に向けた取組を推進していくためにも重要である。

個人情報保護法に規定する義務は、あらゆる分野を対象とする法の性格上、必要最小限度の規律であることから、事業者においては、個人情報等を取り扱うに際し、個人の権利利益の保護の重要性を十分に認識し、形式的な法令遵守を超えて、実効性のあるデータガバナンスを実現することにより、自らの事業が個人の権利利益にどのように影響を与えるかを的確に理解し、個人情報等を適正に利活用することが求められている。

実効性のあるデータガバナンスを実現するためには、まずは企業の経営者・役職員が、データガバナンスの実現が、法令遵守を実現するのみならず、自社のデジタルデータを取り扱う事業に対する個人からの信頼と納得を確保し、自社におけるデジタルデータ利活用の推進に資する等その重要性と必要性を十分に理解し、積極的な取組を行っていくことが求められる。

このような取組を実効性のあるものとするためには、データガバナンス体制の構築と運用が必要不可欠である。データガバナンス体制とは、具体的には、これらの取組について必要とされる権限を持って推進する責任者やそれを支える責任部署から構成され、これを設置し適切に運用することが重要である。この際、データガバナンスを推進する責任者や責任部署の取組に対して経営層のしかるべき関与があることを示し、責任者や責任部署の取組のために必要な権限を付与することが欠かせない。

その上で、個人データの保護と利活用に関する社内ポリシーや社内ルール等を定め、日々の業務におけるサービスの企画立案、顧客への説明からデータの取扱い等の全プロセスにおいて、責任者や責任部署がこれを適切に運用できるよう、関連する事業部門やコーポレート部門等と意思疎通することが必要である。このほか、社内における取組が適切なものであるかという点について、監査や外部有識者による助言等何らかの客観的評価が行われることも大切である。

なお、個人情報保護法第 23 条において、個人データの安全管理措置を講じることが求められており、その手法として、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）において、基本方針の策定、個人データの取扱いに係る規律の整備等の措置を講ずることが挙げられる。

【参考】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）抜粋

10-1　基本方針の策定

個人情報取扱事業者は、個人データの適正な取扱いの確保について組織として取り組むために、基本方針を策定することが重要である。

具体的に定める項目の例としては、「事業者の名称」、「関係法令・ガイドライン等の遵守」、「安全管理措置に関する事項」、「質問及び苦情処理の窓口」等が考えられる。

10-2　個人データの取扱いに係る規律の整備

取得、利用、保存、提供、削除・廃棄等の段階ごとに、取扱方法、責任者・担当者及びその任務等について定める個人データの取扱規定を策定することが考えられる。なお、具体的に定める事項については、以降に記述する組織的安全管理措置、人的安全管理措置及び物理的安全管理措置並びに情報システムを使用して個人データを取り扱う場合は技術的安全管理措置の内容を織り込むことが重要である。

※当該ガイドラインの全体は、個人情報保護委員会ホームページを参照

（２）責任者・責任部署の位置づけ・役割

実効性のあるデータガバナンス体制構築の第一歩として、社内でこの取組について権限を持って推進する責任者や責任部署を設置することが挙げられる。

個人情報保護委員会事務局「個人データの取扱いに関する責任者・責任部署に関する事例集」（2023 年 11 月）によると、責任者等の責任・役割とその設置による効果について、以下のように整理されている。

１　業務内容（個人データの取扱いに関する責任者等の責任（役割））

個人データの取扱いに関する責任者等の責任（役割）については、各事業者によって大きく異なるが、各事例によれば、以下のような責任を持つことがある。

① 事業部門からの相談への対応や事業部門への助言
② データ保護・プライバシー保護の観点からの事業の評価（PIA 等）
③ データ保護・プライバシー・利活用に関わる施策・基準・規定等の策定・導入
④ データの取扱状況の棚卸し及びリスク評価
⑤ 外部の専門家（弁護士等）や経営層との相談・意見交換
⑥ 社内教育

２　設置による効果

個人データの取扱いに関する責任者等の設置による効果としては、以下のようなものが挙げられる。

① データ保護・プライバシー保護の取組の推進
② 社内の相談窓口の明確化
③ 社内全体のデータ保護・プライバシー保護に関する意識の向上
④ 全社的な個人情報の取扱いのルール等の見直し
⑤ 事業部門とは異なった視点による助言や経営層への報告

出典：「個人データの取扱いに関する責任者・責任部署の設置に関する事例集」
2023 年 11 月　個人情報保護委員会事務局
https://www.ppc.go.jp/files/pdf/dpo_setchi_zirei.pdf

責任者を設置することにより、事業者内で統一した方針のもとで事業を実施することができるとともに、社内の知見等が責任者の下に集約されることが期待される。

また、個人データの適正な取扱いを担保するためには、データ利活用部門、法務部門、情報セキュリティ部門等の専門性が求められる。このため、責任部署の設置に当たっては、個人データの保護や利活用に知見を有する者に加え、法務部門、システム部門、情報セキュリティ部門等の実務経験のある者等を配置することが有効である。また、責任者がその職務を果たせるよう、責任部署は、責任者の指示のもとで自律的に活動することが求められる。

なお、データガバナンス体制の構築においては、経営層の理解を得て必要なリソースを確保したうえで、個人データの取扱いに関する社内ルール等を策定し、それらが遵守される仕組みを整備・運用していくことが重要である。社内ルールや仕組み等を定着させるためには、個人情報・プライバシー保護の重要性や必要性に対する事業部門等の理解を得るための教育や普及啓発も欠かせない。

データガバナンス体制の構築にはじめて取り組む事業者においては、必要な知見を有する者が社内にいない等のリソース確保で悩むことが想定される。このような場合、例えば個人情報・プライバシー保護に詳しい外部機関（法律事務所・コンサルティング会社等）等を業務委託等で活用しつつ、自社内の責任者の育成もあわせて行う等の工夫を講じることも有効である。

なお、個人情報保護法第 23 条において、個人データの安全管理措置を講じることが求められており、その手法として、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）において、組織的安全管理措置等の措置を講ずることが挙げられる。

【参考】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）抜粋

10-3　組織的安全管理措置

個人情報取扱事業者は、組織的安全管理措置として、次に掲げる事項を講じなければならない。

(1) 組織体制の整備
　安全管理措置を講ずるための組織体制を整備しなければならない
　(組織体制として整備する項目の例)
　・個人データの取扱いに関する責任者の設置及び責任の明確化　等
(2) 個人データの取扱いに係る規律に従った運用
(3) 個人データの取扱状況を確認する手段の整備
(4) 漏えい等事案に対応する体制の整備
(5) 取扱状況の把握及び安全管理措置の見直し

【取組の観点（例）】

- 責任者
  - ✓ 個人データの取扱いに関する全社的な責任者を任命し、必要な権限とリソースを付与する
  - ✓ 責任者には役員クラスを当て、経営会議に直接報告することができる等、発言力や影響力を持たせる
  - ✓ 責任部署から定期・不定期に報告を受けて、大所高所から意思決定をして指示を下す

- ✓ 新規事業や特定の事業を所掌しない中立的な立場にある
- ✓ 個人情報・プライバシー保護の他に、コンプライアンスや情報セキュリティあるいはデータ利活用の責任者を兼務する

● 責任部署

事業規模の大小に関わらず、取り扱う個人データの量が多い場合、個人データの取扱いが複雑な場合等は、責任者単独で全ての業務を担うことが困難である。このため、責任者を支える責任部署を設置して円滑に業務を推進している事業者がある。

責任部署を設置している事業者の事例を以下に挙げる（責任部署の組成に関する詳細は２．１（３）を参照）。

- ✓ 個人データの取扱いを一元的に管理する責任部署を、責任者のもとに設置している。責任部署は、定期・不定期に責任者に報告し、責任者の指示を受けて業務を行う
- ✓ 責任部署は、法務や情報セキュリティ等のコーポレート部門に設置される場合が一般的である。監査部門のような第三者的な立場から個人データの取扱いを監督する位置づけで設置される場合もみられる
- ✓ 組織形態は、専門組織として設置する場合、既存の部署の中にサブ組織として設置する場合、複数の部署から担当者を任命してバーチャル組織（複数の部署からの兼務者により構成される組織）として設置する場合等、企業の実情に応じて様々である
- ✓ 責任部署の役割は、ポリシー等のルール策定と運用、個人データの管理、個人データの取扱いに伴うリスク管理（PIA 等）、インシデント対応（漏えい等報告・本人通知）、請求権対応、スタッフの教育・研修、点検・監査、渉外活動等多岐にわたる
- ✓ 責任部署は、任務の遂行にあたり、事業部門からの相談対応、情報セキュリティ部門や広報部門との調整等、様々な部署との連携が求められる

２．個人データの取扱いに関する責任者及び責任部署の設置・運用における留意点

２．１　設置

データガバナンス体制の推進役となる責任者・責任部署が設置される契機は、「会社全体の DX 推進にあたり、個人情報・プライバシー保護も必要であることを社内外に示す必要性が生じたため」、「個人情報・プライバシー関係のインシデント発生をきっかけに、プライバシー・情報セキュリティ・データガバナンスを強化する必要性に迫られたため」、「GDPR の施行や個人情報保護法の施行・改正、個人情報・プライバシー保護や情報セキュリティ対策への要請の高まりに応えるため」等様々である。

しかし、いずれのケースにおいても、経営層の関与（個人情報・プライバシー保護を経営上の重要課題と認識して社内外に発信すること、データガバナンス体制の構築に向けた支援（例：責任者・責任部署への必要なリソース配分等）がなければ、実効性のあるデータガバナンス体制の構築はなしえない。また、どのような契機であれ、経営層の関与とそれに伴う責任者の設置・責任部署の組成は、自社の個人データの取扱状況や関係部署の状況等を考慮したうえで、実効性のあるものとするための仕掛けや工夫を講じながら進めている。

（参考）付属資料：実践例１～３

（１）経営層の関与

データガバナンス体制の実効性を担保するには、経営層の関与が重要である。経営層が個人情報・プライバシー保護のためのガバナンスに取り組む姿勢を鮮明に示すことで、責任者や責任部署の旗振りの下で、組織全体に号令をかけることが可能となる。

【取組の観点（例）】

- トップダウンで推進
  - ✓ 経営層が、トップダウンで責任者・責任部署の設置を推進し、データガバナンス体制の構築に積極的に取り組む（＊）
  - ✓ 経営上のトップリスクや最重要課題、製品・サービスの品質確保に関する重要な観点として、データ利活用に関するリスク（個人情報・プライバシーに関するリスクを含む）を、経営計画や社内規定等に明記する（＊）
  - ✓ 社内規程において、データ利活用に関するリスクに係る責任は、社長等の経営層が負うと明記する（＊）
  - ✓ 代表取締役を含む幹部が集まる場を複数回設け、ワークショップ形式でアイデア出しや議論を行い、個人データに係る全社的な指針の内容を検討する。同指針に基づいて、個人情報・プライバシー保護に係るデータガバナンス体制の構築をトップダウンで進める（＊）
  - ✓ 経営層の個人情報・プライバシー保護の重要性に関する理解が不十分な場合には、個人情報・プライバシー保護を進める担当者から、①顧客の信頼ひいては事業継続に関わる影響があること、②事業部門にとってはむしろ製品・サービスの品質向上に寄与することを、継続的に伝える（社内の意識醸成等に関する詳細は２．２（５）を参照）。（＊）

（2）責任者の任命と権限の付与

具体的には、トップダウンで推進する、影響力のある役員クラスを責任者に任命する、実効性の担保に必要な権限を責任者に付与することが重要である。

なお、実務として、経営層の命を受けて管理職クラスの者が中心となってデータガバナンス体制の構築を推進することも考えられる。その場合、実効性の担保に必要な権限をその者に付与すること、経営層に相談できる体制を構築すること等、個人情報・プライバシー保護に係る業務を経営層の委任の下で円滑に実施できる環境を整備することが重要である。

【取組の観点（例）】

- 影響力のある役員クラス（※）を責任者に任命
  - ✓ 個人情報・プライバシー保護に関して中立的な判断ができる、かつ、社内での発言力や影響力を十分に担保できるよう、特定の事業を所掌しない役員を責任者として任命する（＊）
  - ✓ 事業部門・コーポレート部門双方での実務経験がある、コーポレート部門の担当役員を責任者として任命する（＊）
  - ✓ 個人情報・プライバシー保護に関して、データ利活用と保護の両立に責任を負う事業部門（第1線）の責任者、主に法務視点での確認等に責任を負うコーポレート部門（第2線）の責任者、第1・2線の活動内容を確認したうえで助言等を行う責任を負う監督・助言部門（第3線）の責任者と、複数名の責任者を任命する[5]
  - ✓ 活動の後ろ盾となる責任者を確実に任命できるよう、法務・コンプライアンス担当等の特定の役職に就いている役員クラスが責任者となる旨の選定基準を定める（＊）
  - ✓ 役員クラスの任命が難しい場合は、管理職クラスに兼務させる等、何らかの形で個人情報・プライバシー保護の責任者を任命する（＊）

（※）役員クラス以外の実務に長けた社員等を責任者に任命する場合には、必要な権限を責任者に付与すること、経営層に報告・相談できる体制を構築すること、個人データの取扱いにおいて個人情報・プライバシー保護に係る業務を適切に実施できる環境を整備すること等が重要である。例えば、法令違反や顧客等のプライバシー侵害が生じるおそれがあるような事業の企画等を認知した場合に、リスク低減に向けた措置を講じることを求めたり、必要に応じて事業実施を止めたりする実効性のある権限行使ができることが重要である。

- 実効性の担保に必要な権限を責任者に付与
  - ✓ 個人情報・プライバシー保護に対する考え方や対応方針等を示す全社的な

[5] スリーラインディフェンス：企業の価値保全や目的達成への貢献を目指し、企業組織のリスク管理や内部統制の役割を3つの「防御線（ライン）」に分け、それぞれの役割と責任を明確化するフレームワーク。
第1線：事業部門に属する部門が該当。適切な業務遂行を担う
第2線：コンプライアンス部門、情報セキュリティ部門など、コーポレート部門に属する部門が該当。第1線の支援やモニタリングを担う
第3線：内部監査部門など、内部統制部門に属する部門が該当。第1・2線の活動内容を独立した立場から監視する役割を担う

指針を策定する権限を付与する（＊）
- ✓ 個人情報・プライバシーが関係する製品・サービスのリリースに関して、高リスクの案件や一定の条件を満たした案件は、責任部署によるリスク評価等と責任者の承認が必須と社内規程等で定める（＊）
- ✓ 何か困ったことがある場合に報告・相談できるよう、責任者に対して社長等の経営層に直接報告できる権限を付与する、あるいは責任者と社長等の経営層との関係性を醸成する。これによって、経営層がその報告に迅速に対応できる（＊）

（３）責任部署の組成

責任部署を設置することで、円滑に業務を推進している事業者は多い。責任部署を組成する方法には、事業者の業種や規模、事業者における個人データの取扱い方、個人データの適切な取扱いに対する顧客の期待、事業環境等様々な要因が影響する。これらの要因は、事業者ごとに異なるものであるため、各事業者がそれぞれ最適な方法を検討する必要がある。

検討に際して、専門組織を新たに設置するのか、それとも複数の部署からなるバーチャル組織を設置するのか、第三者的な立場から助言・監督する部署を設置するかといった組織形態の観点、どのような職能を有するスタッフで構成するのかといった人材の観点を精査すること等も挙げられる。

【取組の観点（例）】

- 専門組織を新たに設置
  - ✓ 個人情報・プライバシー保護を所管する責任部署を新設する（＊）
  - ✓ 情報セキュリティの視点も踏まえて、個人情報・プライバシー保護と情報セキュリティ双方を所管する責任部署を新設する（＊）
  - ✓ 会社全体の DX 推進やデータ利活用推進のために新設された部署の中に、個人情報・プライバシー保護を担うチームを新設する（＊）
  - ✓ 全社的な情報管理を所管する部署の中に、個人情報・プライバシー保護を担うチームを新設する（＊）

- 様々な職能を有する人材を登用
  - ✓ 責任部署のスタッフには、専任者に加えて、関係部署と円滑に連携できるよう、事業部門・データ利活用部門・システム開発部門・政策渉外部門・情報セキュリティ部門等との兼務者も複数名入れる（＊）
  - ✓ 製品・サービスにリスク低減策を実装できているか確認できるよう、データサイエンティストやエンジニア等も責任部署のスタッフに入れる

- バーチャル組織を組成
  - ✓ 個人データに係る全社的な指針を制定する際に、データ利活用を推進する部署と法令対応を担当する部署が、バーチャル組織を組成し、共同で所管する。その後、互いに対等の立場と考え、個人情報・プライバシー保護に関する活動を一体となって推進する（＊）
  - ✓ 様々な視点からの意見等を収集できるよう、法務部門・情報セキュリティ

部門・データ利活用部門・顧客対応部門・広報部門・経営企画部門等からなるPIA用の会議体を組成し、個別案件への対応方針等を週1回程度議論する

- ✓ 法務部門・情報セキュリティ部門・顧客対応部門・データ利活用部門・IT部門等からなる会議体を組成し、個人情報・プライバシー保護に係るルールや個別案件への対応方針等を、月に1回程度開催する会議体の中で議論しながら検討・整理していく（＊）

- 第三者的な立場から個人データの取扱いを助言・監督する位置づけで設置
  - ✓ 事業部門（第1線）や法務、情報セキュリティ、データ利活用等を担うコーポレート部門部門（第2線）それぞれの個人データの取扱いを助言・監視する役割を担う第三者的立場の部署（第3線）として設置する
  - ✓ 自社内でリソースが不足する場合、外部専門家を組織の職員として登用したり、業務を委託したりする。その際、いずれ外部専門家に頼らずとも自社で担えるよう、責任者候補としてスタッフを配置・養成する（＊）

（4）責任者・責任部署の知識・技能

責任者及び責任部署のスタッフには、個人情報保護法等の法制度に加えて、情報システムやデータベースに関する技術、自社の事業及び製品・サービスや組織運営に係る知識等、広範な知識・技能が必要である。また、個人の権利利益を保護する取組の意義等を事業部門等に理解してもらいつつ、実務における事業部門等との確認や調整を行って適切に業務を遂行していく対人能力、プロセス設計能力、業務調整能力といった技能もあわせて求められる。さらに、倫理観や個人情報・プライバシー保護に対する信念といった姿勢・価値観を備えていることが大切である。

なお、当初から、取組の観点（例）で挙げた知見・技能を有する人材を確保することは困難なケースも多い。そのような場合には、個人情報保護委員会や外部機関が公表しているコンテンツを活用して人材育成等を行うことが重要である。

また、このような責任者・責任部署の業務につく人材は、高度な知識・技能を求められており、技術動向やサービス動向や社会的動向等も踏まえつつ知識・技能をアップデートしていく必要性もあることから、デジタルガバナンス体制を支えるこのような人材の内部育成又は外部からの支援の確保を計画的に行うとともに、このような人材のキャリアパスやその働きに報いる仕組みを投資として位置づけることも重要である。

【取組の観点（例）】

- 知識
  - ✓ 個人情報保護法及び事業分野に係る法制度
  - ✓ 情報システムやデータベースに関する技術（情報システムやデータベースの構造、データの収集・処理・削除等の技術的な仕組み）
  - ✓ 自社の事業及び製品・サービス（ビジネスモデルやサービス内容、利用するデータの種類やその取扱い）
  - ✓ 組織運営（組織内での意思決定プロセス、組織の運営規則や手続）
  - ✓ 倫理的・社会的な課題、個人情報・プライバシー保護が個人や社会に与える影響

次に掲げる事項は、データガバナンス体制を構築している事業者において、責任者や責任部署のスタッフに求める技能として挙げられた事項を参考に整理したものである。

【取組の観点（例）】

- 対人能力
  - ✓ 関係部門との信頼関係を構築し、協力体制を築く
  - ✓ 専門分野の知識を活かしつつ、他の関連分野と連携して業務を推進する
  - ✓ 個人情報・プライバシー保護と事業活動（マーケティング、データ利活用等）のバランスを取りながら、合意形成する
  - ✓ 必ずしも専門知識を持たない人でも理解しやすいよう、専門用語を避け、平易で分かりやすい言葉を用いて、他部門に説明してコミュニケーションを円滑に行う

- プロセス設計能力
  - ✓ 事業領域や組織文化に即して、個人情報保護法やデータ保護規制への対応を実務に落とし込み、手順化する
  - ✓ （海外展開している場合は）グローバルスタンダードや国内外の規制、文化の違いを理解し、当該観点を実務に落とし込んで手順化する
  - ✓ 法規制の及ばない領域（倫理的・社会的な課題等）を理解し、当該観点を実務に落とし込んで手順化する

- 業務遂行能力
  - ✓ 組織全体のビジョンや目標に基づき、個人情報・プライバシー保護の方針や計画を策定する
  - ✓ 策定した計画や手順化したプロセスに基づき、確実に遂行する
  - ✓ 自らの判断を実行に移し、製品・サービスに定着させるまでやり遂げる

- 姿勢・価値観
  - ✓ 誠実さや高い職業倫理観
  - ✓ 個人情報・プライバシー保護の意義に対する深い理解とそれを貫く意思・信念
  - ✓ 個人としての個人情報・プライバシーに関する一般的な感覚（個人情報・プライバシーに関する権利への意識、企業の行動に対して不快に感じるポイント等）
  - ✓ 個人情報・プライバシー保護に関する専門性を恒常的に高める意欲
  - ✓ 個人情報・プライバシー保護の領域に限らず、常にアンテナを高く張りながら、自社の事業をよく理解して、課題解決に取り組む姿勢

２．２　運用

体制の運用にあたっては、責任者と責任部署を設置した場合には日常からの両者間の円滑なコミュニケーションが図られていることが重要である。責任者・責任部署においては、事業部門がデータを利活用する際に日頃から相談がしやすいような仕組み作りや、関連する情報セキュリティ部門等といった他のコーポレート部門との連携を図ることが重要である。また、責任者・責任部署の業務実施に必要な体制、予算、情報システムといったリソース（ヒト・モノ・カネ・情報等）の確保が重要である。さらに、実効性ある体制実現には、全役職員が個人情報・プライバシー保護の重要性等を理解していくための日頃からの社内意識醸成や教育が不可欠である。また、個人情報・プライバシー保護の自社の取組を社外に発信等していくことも有効である。

（１）責任者と責任部署とのコミュニケーション

責任者と責任部署との関係は、事業者によって様々であるが、いずれにおいても、両者間の円滑なコミュニケーションが重要である。具体的には、定例会議を設定する、チャットツール等を活用する等の取組が挙げられる。

なお、責任部署を新たに設置せず、複数部署の兼務者から構成されるバーチャル組織を組成する場合であっても、責任者との円滑なコミュニケーションが求められる点は同様である。

【取組の観点（例）】

- 定期的な会議の設定
  - ✓ 法令の最新動向等の情報共有や個人情報・プライバシー保護に係る意思決定等を遅滞なく確実に行えるよう、定期的な会議（隔週・月１回等）を設定する（＊）
  - ✓ 子会社等にも責任部署がある場合、法令の最新動向等の情報共有や子会社等で対応に悩んでいることに関する相談対応等を遅滞なく確実に行えるよう、親会社と子会社等の間での定期的な会議（月１回等）を設定する

- チャットツール等で連絡が取りあえる体制を整備
  会議以外の場でも、日常的にコミュニケーションがとれるよう、チャットツールやメール・電話等でも連絡がとれる体制を整備する（＊）

（２）事業部門との連携（事業部門からの相談への対応・助言等）

責任者・責任部署は、事業部門における新製品・サービスの企画・構想段階からリリース後も継続的に、個人情報・プライバシー保護の観点で、データの利活用におけるリスク評価やPIA、データマッピング等を実施している。

これらは、個人情報・プライバシー保護に欠かせない取組であると同時に、製品・サービスの品質を高めることに寄与し、ひいては事業部門の活動を推進するものである。そのため、これらの取組の意義を社内で十分に理解してもらうことが大切である（社内の意識醸成等に関する詳細は２．２（５）を参照）。

また、これらのリスク評価等の取組を円滑に進めるために、責任者・責任部署は、事業部門から正確かつ十分に情報収集し、リスクを適切に管理して、ビジネス推進に資す

る専門的かつ実践的な助言をすることが求められる。

このため、責任部署と事業部門との間をスムーズに連携するための仕組みとして、橋渡し役を設置したり、事業部門に窓口担当者を配置したりする等の仕組みづくりが行われている。また事業部門が責任部署に相談しやすくするための工夫や、多数の案件を効率的にチェックするためにツールを活用する等の取組が挙げられる。

【取組の観点（例）】

- 事業部門とスムーズに連携するための仕組みづくり
  - ✓ 橋渡し役の設置：責任部署と事業部門との間に、データ保護のためのサポート組織を設置し、事業部門と責任部署の橋渡し役となって、情報共有や調整を行う。サポート組織は、事業部門からの相談を受け付け、責任部署への情報連携や初期対応等を担う
  - ✓ 事業部門に窓口担当者を配置：各事業部門に専任の窓口担当者（カウンターパート）を配置し、責任部署との連絡を一元化する。窓口担当者は、事業部門内でのデータ保護に関する相談の集約や事業部門特有の案件等の初期対応を行い、必要に応じて責任部署への情報連携や初期対応等を行う
  - ✓ 事業部門に責任者・責任組織を設置：各事業部門にデータ保護の責任者や責任組織を設置し、データの適切な取扱いを監督する。データ保護の責任者は、①本社の責任組織から派遣②事業部門の製品・サービス責任者が兼任のいずれかの手段により設置する。②の場合、本社の責任組織が最終チェックを実施後、製品・サービスをリリースする
  - ✓ 合同のプロジェクトチームを組成：法令改正や新規製品・サービスの開発時等、リスクの大きさや影響度に応じて、責任部署が主導して事業部門と連携したプロジェクトチームを編成し、課題への対応方針を決定する（＊）
  - ✓ 責任部署と事業部門の定期的な意見交換：責任部署と事業部門で定期的な意見交換の場を設定し、制度改正や技術革新といった外部環境変化等に関する情報共有を通じて、責任部署が現場に即した助言・ルール整備等を行う（＊）

- 事業部門が責任部署へ相談しやすくするための工夫
  - ✓ 相談窓口（責任部署が運用）の連絡先を社内イントラやチャットツール等の固定メッセージ等複数の場所に掲載し、相談窓口へのアクセス経路を明確にする（＊）
  - ✓ 「どのタイミングで」「どの部署に」「どのような情報を提供すればよいか」といった相談の流れをフローチャートや簡易ガイドとして作成し、社内イントラやチャットツール等に掲載する（＊）
  - ✓ 簡易な相談フォームを作成し、相談内容（概要、データの種類、利用目的等）を入力するだけで責任部署に送信できる仕組みを導入する（＊）
  - ✓ 事業部門の担当者が案件の概要（取り扱うデータ項目、利用目的等）を登録することで、個人情報・プライバシー保護に関わるリスクが自動で判定できるフォームを作成する
  - ✓ チャットツール等での簡易相談を受け付ける専用チャンネルを設置する（＊）
  - ✓ 全社ミーティングや社内サイトでのインタビュー記事等で、定期的に相談窓口の利用方法や個人情報・プライバシー保護の重要性を周知する

- ✓ 責任部署から事業部門に対して、「どんな些細なことでも相談してください」といったメッセージを定期的に発信する（＊）

- ツール活用等による業務の効率化・最適化（評価方法の明確化含む）
  - ✓ 事業部門からの相談内容や案件のリスク評価等の進捗状況を一元管理できるシステムを導入し、案件の優先順位や対応状況を可視化する。システムには、相談内容の記録、進捗管理、リスク評価・対応履歴の保存・検索機能等を備える
  - ✓ 相談フォーム（相談内容の概要、データの種類、利用目的等）のテンプレート化やコミュニケーションを行うプラットフォームの統合により、情報共有や調整を迅速に行える環境を整備する。例えば、チャットツール等に案件管理システムを連携させ、リアルタイムでの情報共有を可能にする（＊）
  - ✓ データの種類や利用目的に応じて、リスク評価基準を数値化し、システムで自動判定できる仕組みを導入する。高リスクの案件や一定の条件を満たした案件のみ人間が確認を行い、詳細なリスク評価・対応方針の決定を行う
  - ✓ PIA の実施件数を積み重ねる中で、リスクの度合いは小さいが PIA の付議基準に係る案件が出てきた場合等には、PIA の付議基準の見直しを行う（＊）
  - ✓ 製品・サービスのリリース等に際して、新たな申請・届出のプロセスを設置するのではなく、既存業務のプロセス内に個人情報・プライバシー保護に関するチェックの観点を追加することで、事業部門が通常の業務をこなしつつも、自然と遵法性やプライバシーの保護を確保できるよう工夫し、事業部門の負担軽減に努める（＊）
  - ✓ 評価基準の明確化：責任部署の担当者の誰もが同じ基準でリスクを判断できるよう、評価基準を作成する。その際、国内外の法令の執行リスク、自社のリスク評価の経験から蓄積・抽出したリスクを取り入れる。なお、顧客ごとにプライバシーの捉え方は様々であることを十分に配慮し、通底する考え方として、「顧客に胸をはって説明できるか」や「顧客の立場に立って気持ち悪いと感じる等、不快に感じさせることはないか」等の観点を拠り所とする

（３）他コーポレート部門との連携

データガバナンス体制には、情報セキュリティ部門やリスクマネジメント部門等、他のコーポレート部門と役割分担を明確にするとともに、密接に連携して事に当たることが求められる。このため、平時、有事どちらにおいても、関係部門が円滑に連携できる体制を構築することが重要である。

具体的には、役割分担の明確化及び連携のための仕組みづくり、個人データの漏えい等のインシデントを未然に防止する体制整備、インシデントを迅速に検知・対応する体制整備の取組が挙げられる。

なお、国内外の法制度や技術、ビジネス等の環境変化が大きい状況に対応するためには、異なる専門性を有するコーポレート部門同士で、密に連携することが大切である。

【取組の観点（例）】

- 役割分担の明確化及び連携のための仕組みづくり
  - ✓ 責任者・責任部署、各部門の役割や責任範囲を明文化した内部規程を作成し、全社で共有することで、役割分担を明確にする（＊）
  - ✓ 案件の内容やリスクレベルに応じて、適切な会議を設定する。例えば、通常の案件は定例会議で共有し、リスクの高い案件は特別会議を開催して迅速に対応する（＊）
  - ✓ 個人情報・プライバシー保護に関するワンストップの相談窓口を設置する。責任部署で回答が難しい案件等は、必要に応じて他部門（法務部門、情報システム部門、リスク管理部門等）に連携し、迅速に対応する（＊）

- インシデントを未然に防止する体制の整備
  - ✓ お客様センターに寄せられる声や問合せ内容を定期的に分析し、データ保護やセキュリティに関する改善点を抽出する。問合せ内容や抽出した改善点等をもとに、各種プロセスの見直しや顧客からの不安の声が多い領域に対する FAQ の整備等を行う（＊）
  - ✓ 委託先の関与する業務を定期的に監督する。新たに委託先を選定する際には、情報管理体制、過去の実績、法令遵守状況等の観点で審査を行う。委託先に対して、自社と同等程度の情報管理水準を求める。この際、委託先への要求は、企業規模にかかわらず、同一の基準を求め、一定の水準を満たさない企業は委託先として選定しない（＊）

- インシデントを迅速に検知・対応する体制の整備（※１、※２）
  - ✓ 社内に設置された CSIRT（Computer Security Incident Response Team）がシステムやネットワークの監視を 24 時間体制で行い、異常が検知された場合は即座に対応を開始し、個人データの取扱いに関する責任者・責任部署に連携する
  - ✓ 影響度の大小を問わず、情報管理に関する全てのミスやトラブルを簡易なフォームにて報告する仕組みを整備し、全ての情報が集約されるようにする。影響度が大きい案件は、個別に対応できる体制を構築する（＊）
  - ✓ インシデント発生時の対応フローを内部規定やマニュアルで明文化し、対応を主導する部門等、各部門の役割を明確にする。（役割の例：初期対応は CSIRT が担当し、法務部が顧客対応をサポートする/全てのインシデント対応をリスクマネジメント部が主導する）（＊）
  - ✓ 模擬的なデータ漏えいシナリオ等を用意し、定期的な社内訓練を実施することで、インシデント発生時の対応手順を社員に体験させる。また、訓練を通じて、内部規程で定められたプロセスが適切に機能しているかを確認し、必要に応じてプロセスの改善を図る（＊）
  - ✓ 対応の遅延や情報伝達の漏れ等を防ぐため、チャットツール等を活用し、関係者全員が一箇所でやりとりできるようにする。また、インシデント発生時には対応事項の担当者を明確に任命する（＊）

（※１）個人データの取扱いには、外部からのハッキングや、自社・委託先における社内ルール違反・事務ミス等様々な形で個人データを含む情報が

漏えい等するインシデントが発生するリスクを伴う。インシデントが発生した場合、本人の権利利益を侵害するおそれがあり（例えば、クレジットカード番号であれば財産的な被害、氏名や住所、連絡先であれば何らかのプライバシーの侵害等の二次被害が生じる可能性）、法令に定める要件に該当する場合は、本人に対する通知や漏えい等報告を行う必要がある。このため、事業者は、その保有する個人データの取扱状況等を踏まえながら体制を構築する必要がある。なお、個人データの取扱いを委託している場合、委託先において漏えい等があった際に委託元である自社へ速やかな通知等がされる体制を双方で構築する必要がある。

（※２）個人データの漏えい等の対策を、責任者や責任部署とは別に、情報セキュリティ部署が担っている場合が想定される。この場合、責任者・責任部署と情報セキュリティ部署との間で情報共有等の連携を速やかに行い、各部署の担当業務に従った顧客等への対応が行われる体制構築もある。

（４）リソースの確保（ヒト・モノ・カネ・情報等）

責任者や責任部署が、国内外の法制度や技術、ビジネス等の環境変化も踏まえつつ役割を遂行するためには、十分な体制の構築のみならず、活動に必要な予算や効率的な業務遂行に有効となる情報システムといった、リソース（ヒト・モノ・カネ・情報等）の確保が重要となる。

また、十分な知見を有する人材が社内にいないが個人データの取扱いにおいて客観的・専門的な助言等が必要な場合には、外部リソース（弁護士、コンサルタント等）の活用などが挙げられる。

【取組の観点（例）】

- 経営層の理解
  - ✓ リソースの確保に向けて、経営陣に個人情報・プライバシー保護の重要性・必要性の理解を促し、経営上の重要課題と位置づける（＊）

- 社内リソースの確保
  - ✓ 責任者や責任部署のスタッフに求められる知識、技能、態度・価値観を有する、または素養のある人材を社内で探し、兼務または異動を含む適切な配置を行う
  - ✓ 必要な知識、技能、態度・価値観を有する、または素養のある人材を採用する（＊）
  - ✓ 事業部門や子会社等に配置した窓口担当者（カウンターパート）に対して、個人情報・プライバシー保護に関する教育を行い、同質の職能を有する仲間を増やす
  - ✓ 技術等の最新動向について、社内の専門家と意見交換し、情報収集する（＊）
- 外部リソースの活用
  - ✓ 国内外の法制度や最新技術等に関する情報収集のために、業界団体や法律事務所等が開催するセミナーや勉強会に参加し、他社の担当者とデータガ

バナンス体制に関する意見交換等を行う（＊）
- ✓ 外部の法律事務所やコンサルティング会社等に相談し、法令解釈や、個人情報・プライバシー保護上のリスク、データガバナンス体制構築等に関する専門的な知見や第三者観点での意見を得る（＊）
- ✓ 限られたリソースで効果的に業務を行い、またスタッフの負担を軽減・省力化するために、既成の情報システムやツールを活用する

（５）個人情報・プライバシー保護に係る社内意識の醸成、教育

実効性のあるデータガバナンス体制を実現するためには、全役職員が、個人情報・プライバシー保護の重要性や必要性を理解して、日々の業務に取り組むことが求められる。

特に、事業部門においては、個人データを取扱う製品・サービスを企画する場合や、個人データの漏えい等が発生した場合において、社内ルール等に基づき、責任者・責任部署に対して速やかに相談・報告を行うことが重要である。これらの取組を機能させるためには、その意義や、個人情報・プライバシー保護の重要性や必要性を事業部門が正しく理解することが欠かせない。

既にデータガバナンス体制を構築してきた事業者においては、個人情報・プライバシー保護と事業の推進は、決して二律背反の関係ではなく、顧客等からの信頼を得るためにも重要な取組である等のメッセージを社内に分かりやすく発信し、事業部門の理解促進に努めている。

（参考）付属資料：実践例４～６

【取組の観点（例）】

- 全従業者の意識醸成に向けた施策
  - ✓ 個人情報・プライバシー保護に対する関心を高め、日常の業務や行動に結びつけて考えてもらえるよう、マンガや動画を用いて、社内規程やルール等を平易に解説する（＊）
  - ✓ 個人情報・プライバシー保護の強化月間を設定し、外部有識者による講演会の開催、事業所内でのパネル展示、社内外のインシデント事例の紹介等により、集中的な意識啓発を行う
  - ✓ 個人情報・プライバシー保護の優れた取組事例の表彰制度を設け、他部門の優れた取組を全社に共有するとともに、自組織における個人情報・プライバシー保護の取組を考えるきっかけとする（＊）
  - ✓ 責任者・責任部署の設置意義や業務内容等を社内に広く知ってもらうため、社内サイト等でインタビュー記事を掲載する（＊）
  - ✓ PIA を実施したことにより安全に製品・サービスをリリースできたことを、事業部門の生の声等を用いて社内サイト等で紹介する（＊）

- 社内教育の実施：全従業者向け
  - ✓ 法令や規則等の知識の伝達にとどまらず、業務で迷いや悩みが生じた際の判断の拠り所となる考え方を従業員に共有する。例えば、「フェアネス」や「ブランドの保全」といった、会社として大切にしている価値観・考え方を伝え、それらが製品・サービス設計やビジネスを進める上での前提条件であることを明確にする（＊）

- ✓ 個人情報・プライバシー保護の考え方等について、責任部署のスタッフから研修を行う
  （研修内容の例：自社が重視する個人情報・プライバシー保護の考え方・指針、対応のポイント、相談方法、社内の具体的なデータ利活用事例と気を付けるべき点、社内外のインシデント・炎上事例）（＊）
- ✓ 個人情報・プライバシー保護に関する理解度を確認するためのｅラーニングを年１回行う（＊）
- ✓ よくある質問（FAQ）や、過去に発生した不適切なデータ利用の事例をまとめた資料を作成し、社内イントラやチャットツール等に掲載し、事業部門が自己解決できるようにする

- 社内教育の実施：責任部署またはバーチャル組織のスタッフ向け
  - ✓ 個人情報保護法及び事業分野に係る法制度の解釈、諸外国の法制度の動向等についてスタッフ内で共有し、法制度への理解を促進する（＊）
  - ✓ 過去の相談対応や、PIA・データマッピング等を通じて得られた、個人情報・プライバシー保護にあたっての考え方やポイント、自社の事業への理解等についてメンバー内で共有し、知識・技能の向上をはかる（＊）
  - ✓ 情報システムやデータベースの構造やセキュリティ等に関する研修を実施する（＊）
  - ✓ OJT を通じて知識・技能等の向上を図れるよう、ベテランが若手をサポートする体制を整備する
  - ✓ 責任者や責任部署のスタッフが海外のカンファレンスや各種セミナー等に参加することを推奨し、そこで得た情報を、責任部署内で共有させる（＊）

- 社内教育の実施：経営層向け
  - ✓ 短時間（20 分程度）で、個人情報・プライバシー保護の重要性を会社のミッション、ビジョン、バリューと紐づけて端的に説明する（＊）

- 社内教育の実施：責任者向け
  - ✓ 国内外の法令の最新動向や、データ利活用や DX をより一層進めるうえでの課題や危機感、懸念等を共有する（＊）
  - ✓ 特に、責任者が新たに着任した際にはスタッフから、自社のデータガバナンス体制に関する取組の経緯・現状や、社会的な影響の大きかった過去のインシデント事例の説明と併せて、データ利活用の推進にあたっての個人情報・プライバシー保護の重要性や必要性を説明する（＊）

（６）信頼獲得等に向けた対外活動

個人データを利活用する事業は、顧客等の信頼のうえに成り立つものである。個人情報・プライバシー保護の取組を、社外に対してわかりやすく説明することは、その信頼の獲得に有効である。対外活動を行う際には、顧客等の理解度やおかれた状況等も想定したうえで、目的に沿った内容・説明方法等を検討することが考えられる。

【取組の観点（例）】

- 会社の公式 HP 等で取組内容を公表
  - ✓ 会社のホームページ上に個人情報・プライバシー保護に関する姿勢等を説明する専用ページを作成する（＊）
  - ✓ 顧客が不安に思いやすい事項を想定したうえで、不安を解消するためのコンテンツ（個人データに係る基本方針・考え方、データガバナンス体制、PIA の概要や実施件数、個人データの取扱い方法の説明等）をイラストも交えて分かりやすく説明する（＊）
  - ✓ 個人データの取扱い方を一般的に想定しづらい特定の製品・サービスについて、取得するデータの種類・取得のタイミング・利用目的・第三者提供の有無等を、個別に分かりやすく説明する（＊）
  - ✓ プライバシーや情報セキュリティに係る取組を報告書等の形で取りまとめ、公表する（＊）

- セミナーやイベントで自社の取組を発表
  - ✓ 個人情報・プライバシー保護に関するセミナーやイベントにおいて自社の取組を発表する（＊）
  - ✓ セミナーやイベントへの参加を通じて、有識者や他社担当者との人脈を構築し、自社の取組をよりよくするための一助とする（＊）

（7）活動の振り返り、改善

責任者及び責任部署が、期待されている役割をどの程度達成しているのかを定期的に評価し、活動の改善を行うことは、データガバナンス体制の実効性を高める上で重要である。具体的には責任者及び責任部署が達成すべき目標の明確化や、社内外を問わず第三者的立場からの評価の実施等が考えられる。

【取組の観点（例）】

- 社内における活動の評価、見直し・改善
  - ✓ 組織全体の方向性に沿って、責任者及び責任部署が達成すべき個人情報・プライバシー保護の実効性に係る目標を明確化する。その際、組織全体が目指す方向性を従業員が理解することを重視し、定量/定性的な目標を設定する。（目標の例：顧客と会社間の信頼関係を構築する）（＊）
  - ✓ 四半期ごとや年次単位で目標の進捗状況を確認・評価する。評価結果は、責任部署や関係部署が集まる会議体で共有し、改善策や今後の方針を議論する。年度末には、評価結果や次に実現したいことを踏まえ、次年度の経営計画・業務計画等に反映する（＊）

- 外部を活用した活動の評価、見直し・改善
  - ✓ 外部の専門家や有識者（弁護士、学術分野の研究者、他社の個人データの取扱いに関する責任者等）を招き、アドバイザリーボードや、有識者会議の開催、個別相談を定期的に実施する。会議等では、実効性のあるデータガバナンス体制構築に向けた取組や、製品・サービス等に関するリスク低減策について意見を収集する

- ✓ 業界団体や勉強会、セミナーやカンファレンス等に参加し、定期的に他社との意見交換や情報共有を行う。得られた知見は、社内で共有するための報告書フォーマット等を用いて、社内関係者に展開する（＊）
- ✓ お客様センターに寄せられた意見の分析、顧客へのアンケート実施、対面イベントでの顧客からの意見収集等を通じて、個人情報・プライバシー保護に係る活動に対するコメントを集め、活動内容の見直し・改善を行う（＊）

付属資料：個人データの取扱いに関する責任者・責任部署の設置・運用の実践例

本資料作成に当たって、個人データの適切な取扱いのために責任者や責任部署設置の体制の整備や運用に取り組んできた事業者 10 社へのヒアリングを実施した。

そのヒアリング結果等を踏まえ、本付属資料において、下記のような掲載事例を示している。実際の検討を行う際のご参考としていただきたい。

【設置・運用の実践例】

・実践例１　A 社（小売業）

：責任部署を複数部署から構成される委員会が担って推進

・実践例２　 B 社（製造業）

： プライバシーを情報品質の一つに掲げ、多様なバックグラウンドを有するスタッフで構成される責任部署が中心となって推進

・実践例３　 C 社（サービス業）

：責任部署、全プロダクトに設置された責任者、その間をとりもつ部署が相互に連携して推進

【社内意識醸成・教育の実践例】

・実践例４　D 社（金融業）

：事業部門が適切にデータを利活用するためのハンドブックの作成

・実践例５　E 社（製造業）

：全従業員を対象とする個人情報・プライバシー保護の重点強化期間の設定

・実践例６　F 社（サービス業）

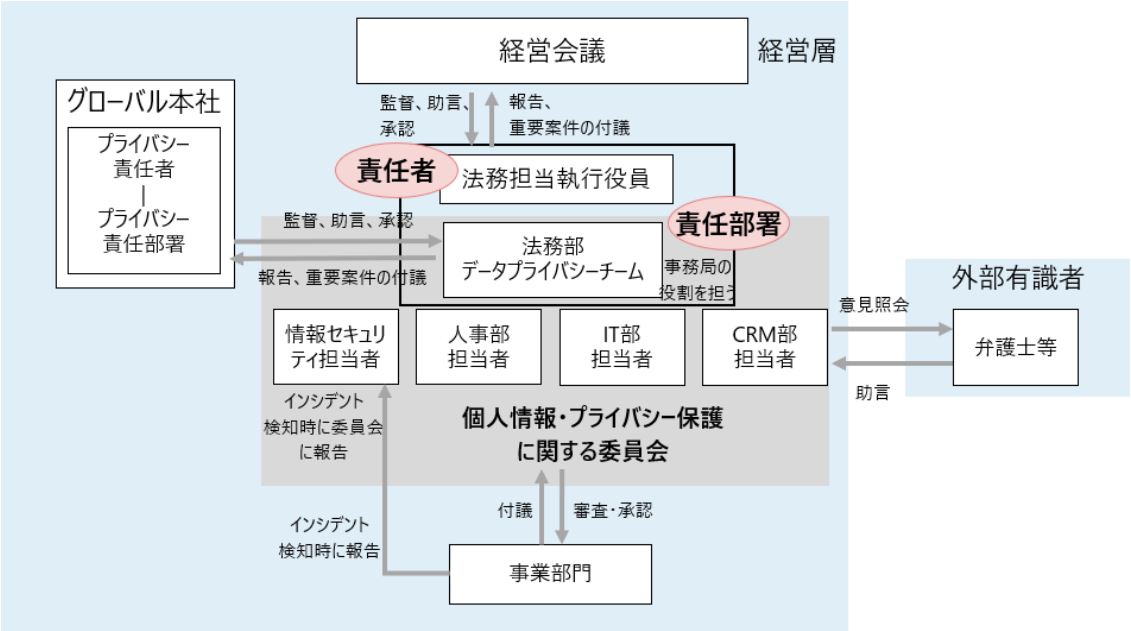
：各種セミナーやカンファレンス等で得た最新情報の共有や、勉強会の開催

※上記の実践例は、令和 7 年 3 月 31 日時点のもの

実践例１　A 社（小売業）

：責任部署を複数部署から構成される委員会が担って推進

体制図



１　個人データの取扱いに関するガバナンス体制

（１） 個人データの取扱いに関する責任者

責任者は、法務担当執行役員である。実務面では、法務部データプライバシーチーム（DP チーム）のマネージャーが、個人データ保護に係る業務を主導しており、責任者は、DP チームを中心とする委員会（後述）が策定した方針や規程類等の承認を行う。

DP チームのマネージャーは、個人情報・プライバシー保護に係る実務経験が豊富で、他社でプライバシーオフィサーを務めた経歴を持つ。同マネージャーは、データガバナンスの業務を兼務している。

（２） 個人データの取扱いに関する責任部署等

責任部署は、DP チームを中心に、人事部、IT 部、顧客管理部等の個人情報に関わる主要な部署のスタッフで構成する委員会が担う。従前は、個人データの取扱いに関する対応を、法務部が法務業務の一環として行っていたが、それでは、個人情報・プライバシー保護を実効的に担保するには限界があるという危機感から、見直された。

責任部署である委員会は、複数の部署からのスタッフによって、多様な観点から、個人データを取扱うシステム・サービスの企画や改善を行う案件のリスク評価や対応

策の検討等を行う場として機能している。また、案件の実施可否を判断し、適宜、経営会議等へ付議しており、個人情報・プライバシー保護における意思決定プロセスの中核を成している。

２ 個人データの取扱いに関する責任者・責任部署の任務・役割

（１） 責任者・責任部署の任務

責任部署である委員会は、月１回の定例会議を軸に、必要に応じて個別の案件やテーマに特化した会議を開催し、個人情報・プライバシー保護に関する案件の方針を取りまとめて、原則、責任者の承認を得る。なお案件の性質やリスクに応じて、承認プロセスを柔軟に運用している。例えば、委員会で合意が得られない場合など、責任者以外の経営陣の承認が必要な案件については、責任者やDPチームのマネージャーが経営会議等に付議する。また、委員会で協議後に、テーマに応じてIT部や顧客管理部が承認することもある。

委員会ではDPチームが旗振り役となり、参加者や必要資料の判断を含む委員会の運営、案件の性質を踏まえた承認プロセスの設定等を行い、以下に示す取組を主導する。また、これらの取組について、全社的な指針である「ブランドの保全」に照らして、活動の振り返りや改善を適宜行っている。

① グローバル本社のルールや指針等を基盤とした個人情報・プライバシー保護の規程類や基準の作成
- EU域内にあるグローバル本社が日本を含む各地域の拠点に展開したルール等をもとに、日本拠点の規定類や基準を策定する。グローバル本社のルール等をそのまま反映するのではなく、日本の法令等を踏まえた調整が必要な場合には、グローバル本社と相談しつつ内容の調整を行う

② 事業部からの相談対応と個別案件のリスク評価（適切な承認プロセスの運用、PIAの実施を含む）

③ 一定の条件を満たす案件に関するグローバル本社への付議
- グローバル本社の方針に基づき、グローバルで開始されたプロジェクトを日本で実行する場合など、一定の条件を満たす案件は、グローバル本社への付議が義務付けられている

④ 役職員への周知啓発・教育活動

また、委員会の構成や活動は、グローバル本社のプライバシー責任部署が定めたルールや指針等に基づいており、同責任部署とも密接に連携している。具体的には、グローバル本社で定めたルールや指針等を日本国内の運用に適用する際、日本特有の事情を考慮した調整等が必要な場合には、グローバル本社のプライバシー責任部署に付

議し、承認を得ている。これにより、グローバル本社の基準との適合性を確保しつつ、日本特有の事情に対応できる体制を実現している。

（2） 責任部署と責任者との連携

責任者は、責任部署を担う委員会に参加し、委員会内で関係部署と協議して、個別案件の方針の承認を行う。こうして、意思決定の効率化が図られている。

また、グローバル対応として、グローバル本社のプライバシー責任部署と月に1回定例会議を行い、国内マーケットの課題や方針を議論する。

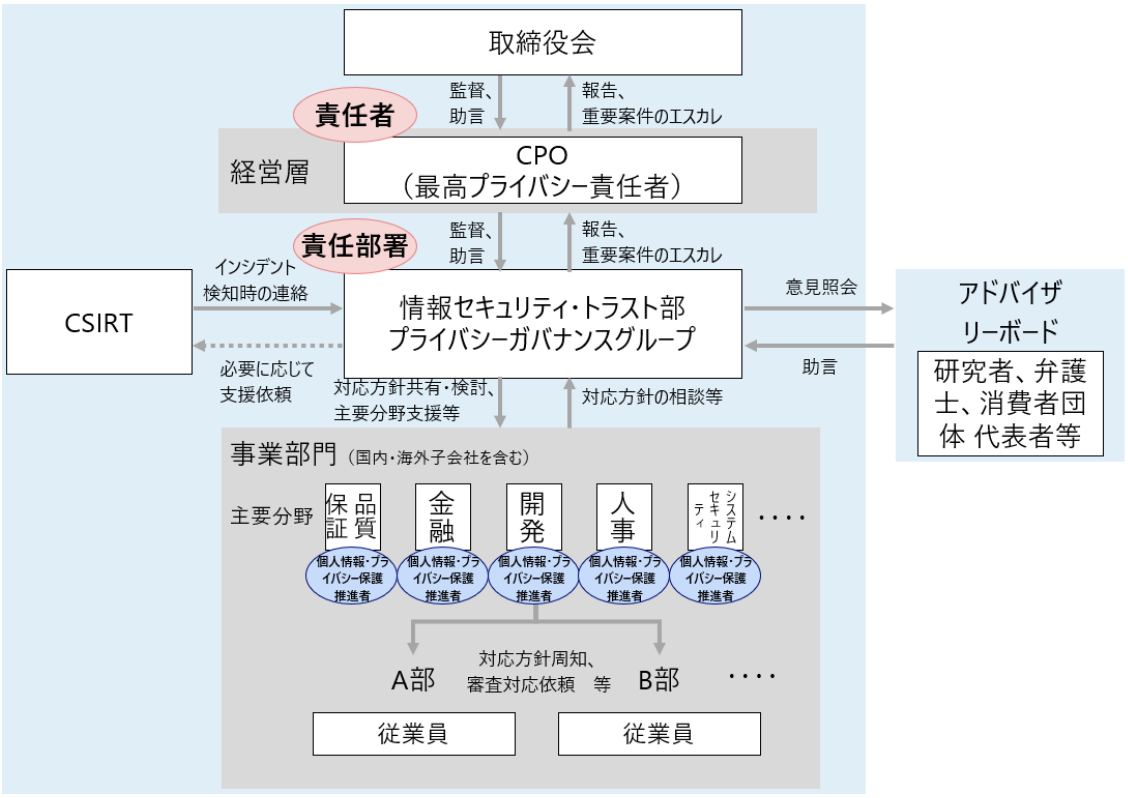
（3） インシデント対応における連携

インシデント発生時は、第一に、日本の情報セキュリティ部へ連絡する仕組みを構築している。同部が報告内容を精査し、個人情報やプライバシーに関わる可能性がある場合には、委員会のメンバーを巻き込んで詳細な調査を実施する。その結果を踏まえ、必要に応じて経営陣へのエスカレーションや個人情報保護委員会への報告の要否を判断する。

実践例２　B 社（製造業）

：プライバシーの尊重を製品・サービスの品質の一つの要素に掲げ、多様なバックグラウンドを有するスタッフで構成される責任部署が中心となって推進

体制図



１　個人データの取扱いに関するガバナンス体制

（１） 個人データの取扱いに関する責任者

責任者は、CPO（最高プライバシー責任者）である。CPO は、独立性を確保するため、新規事業や執行事業を持たない役員を任命しており、代表取締役副会長が兼務している。CPO は、渉外・広報部の責任者を長年務めた後、代表取締役副会長に就任した経歴を持つ。

（２） 個人データの取扱いに関する責任部署等

責任部署は、情報セキュリティ・トラスト部のプライバシーガバナンスグループ（PG グループ）が担う。また、主要な業務分野ごとに「個人情報・プライバシー保護推進者」を設置している。

ア．情報セキュリティ・トラスト部　プライバシーガバナンスグループ（PG グループ）

B 社では、製造業で重視される製品の品質と同様に、情報セキュリティ、プライバシー、データ保護の 3 要素を「情報の品質」として定義し、これらを重要視して一体的に推進する全社的な取組を新たに開始した。情報セキュリティ・トラスト部は、その取組の推進役を担う部署である。情報品質を重視する文化を社内に根付かせるため、「情報品質保証規則」を策定し、情報セキュリティ・トラスト部が全社的な推進権限を持つことを明確化した。

PG グループは、個人データ保護の推進役として主体的に対応するが、一定規模以上のインシデントや新規性の高い案件等、重要案件については責任者に判断を仰ぐ。

PG グループのスタッフは約 20 名で、法務、技術、営業、人事、情報セキュリティ、渉外等、多様なバックグラウンドを持つスタッフが所属する。

また、情報品質活動の一環として、社内外の事例共有等を通じて法令遵守意識の向上を図る専用の会議体を定期的に開催している。この会議体では、CPO と CISO（最高情報セキュリティ責任者）が合同で議長を務め、各事業本部の本部長クラスが参加している。

イ．主要な業務分野ごとの個人情報・プライバシー保護推進者

主要な業務分野（開発、人事、システムセキュリティ等）ごとに個人情報・プライバシー保護推進者を配置している。同推進者は、PG グループが策定したリスク評価や対応方針に基づき、担当分野でのプライバシー保護対応を担うとともに、事業部と PG グループとの橋渡し役として機能する。

２ 個人データの取扱いに関する責任者・責任部署の任務・役割

（１） 個人データの取扱いに関する責任者・責任部署の任務

PG グループは、法務部から個人データの取扱いに係る法令対応業務を全面的に移管されており、情報セキュリティ、プライバシー、データ保護を統合的に推進する部署として、以下の任務・役割を有する。これらの取組は、研究者や弁護士等で構成される外部アドバイザリーボードの知見を活用し、活動方針の共有や自己評価の報告を通じて、振り返りや改善を適宜行っている。

① 個人情報・プライバシー保護の規定類や基準の策定・更新（事業部の知見やお客様センターに寄せられる声等を活用）

- 月 1 回程度、開発中の新技術における個人情報の取扱いについて、1 日かけて開発部門と集中的に議論を実施。必要に応じて、規定類や基準の見直し・反映等を行う
- 個人情報に関連する相談がお客様相談センターに来た場合、PG グループに情報連携される体制を整備

② 情報セキュリティ、プライバシー、データ保護を統合した審査体制の整備・運用
- 「情報の品質」に係る総合的な相談窓口を設置。社内イントラや各種資料等で、相談窓口へのアクセス経路を周知する

③ 法令解釈、各事業部からの相談対応、PIA（プライバシー影響評価）の審査
- 事業部門が案件の概要（取り扱うデータ項目、利用目的等）を登録すると、リスクが自動で数値化され、リスクが高い案件は別途でPIAを実施する仕組みを導入している

④ 国際的な規制や基準に対応するグローバルガバナンス体制の構築・運用

⑤ 情報品質向上を目的とした会議体運営や役職員への周知啓発・教育活動
- CPO及びCISOが共同で議長を務める「情報の品質」専用の会議体を設置し、責任部署の活動や個人データの取扱いに関する社内外の事例等について、事業部門に共有し、議論を行う
- 2か月間の「情報の品質」強化月間を設け、社外有識者による講演会や、「情報の品質」に係る社内外のインシデントやクイズを並べたパネル展示会等を開催し、役職員への周知啓発を図っている

⑥ 外部との信頼構築を目的とした対外的な渉外活動や情報発信
- プライバシーに関する自社の取組みや発生させたインシデントに対する認知度、ブランドイメージ等を調査する、プライバシー意識調査を独自に実施している

⑦ PIAデータと連携したデータマッピング効率化のプロセス整備・運用

（2） 責任部署と責任者との連携

責任者と定例会議を実施し、適宜メールやチャット等で報告を行う。一定規模以上のインシデントや新規性の高い案件等、重要案件については、案件の概要やアドバイザリーボードの助言を踏まえた対応案を報告し、責任者の判断を仰ぐ。

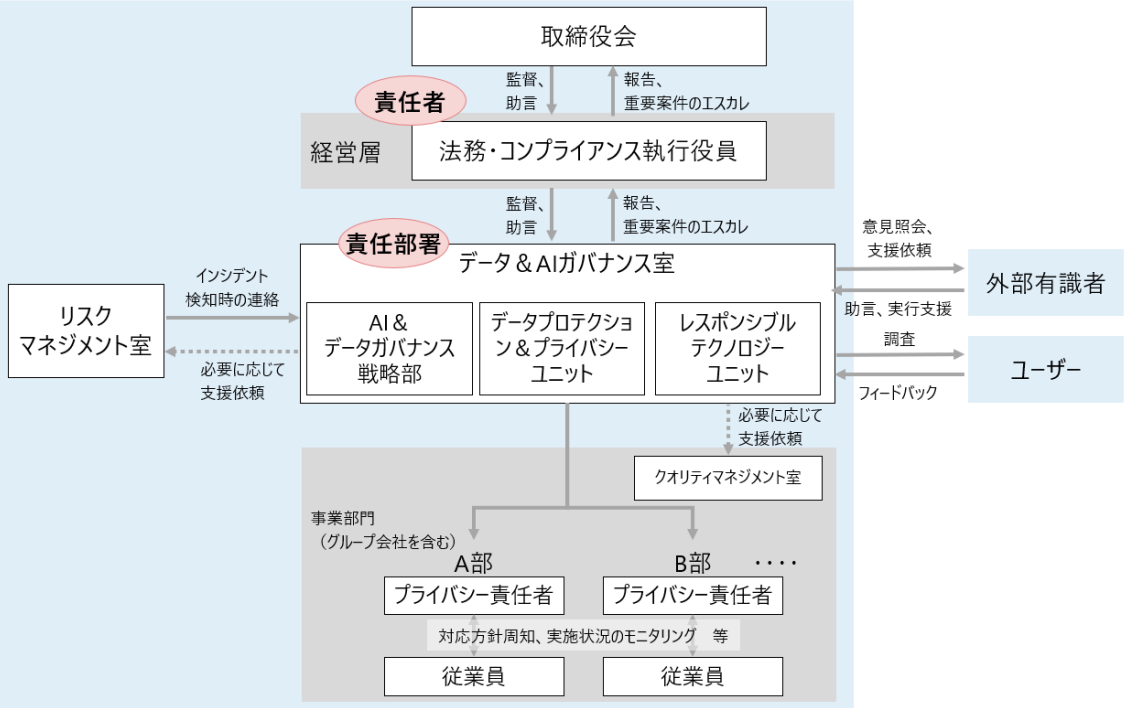
（3） インシデント対応における連携

インシデント対応に関して、CSIRTが中心となってインシデント検知を行い、外部ツールや外部委託も一部で活用している。報告すべき事項が事業部門内での誤った判断により報告されない事態を防ぐため、インシデントを検知した場合は、空振りを厭わず速やかにPGグループへ情報を共有するよう、各部の責任者に周知徹底している。子会社でのインシデント対応は原則として子会社が行うが、必要に応じて支援要請に応じる。

実践例３　Ｃ社（サービス業）

：責任部署、全プロダクトに設置された責任者、その間をとりもつ部署が相互に連携して推進

体制図



１　個人データの取扱いに関するガバナンス体制

（１） 個人データの取扱いに関する責任者

個人データの取扱いに関する責任者は、法務・コンプライアンス担当執行役員である。現法務・コンプライアンス担当執行役員は、HR 領域の事業企画、全社横断の新規事業開発を経験後、法務に異動。事業支援・経営支援の法務領域とデータプライバシーや AI ガバナンス領域双方の責任者を務めてきた経歴を持つ。

（２） 個人データの取扱いに関する責任部署等

データ利活用に関連するリスクはＣ社グループの中で、数少ないトップリスクに位置づけられており、手厚い体制がとられている。

「データ＆AI ガバナンス室」（DAG 室）が個人データの取扱いに関する責任部署（責任部署）である。さらに「クオリティマネジメント室（QM 室）」や全てのプロダクトに「プライバシー責任者」を設置して、データ保護・プライバシー保護を推進している。

ア データ＆AI ガバナンス室(DAG 室)

責任部署を担う DAG 室は、データ保護・プライバシー保護や AI のガバナンスを担い、ユーザーとの信頼関係を維持・強化することを目的とする。データプロテクション＆プライバシーユニット（DPP ユニット）とレスポンシブルテクノロジーユニット（RT ユニット)、及び AI＆データガバナンス戦略部の３つの組織から構成される。

DAG 室では、データ利活用・AI 活用に係る事前レビューからリリース後の継続的なモニタリングまで幅広く対応できるよう、多様なスキルを有する人員で構成される。近年は、AI 等の技術に対応するためにリソースの拡充を進めている。DPP ユニットのユニット長は法務担当を長年務めてきた経歴を、RT ユニットのユニット長は AI システムの基盤開発等に携わってきた経歴をそれぞれ有する。また、DAG 室のスタッフは、取り扱う案件について多様な観点から検討できるよう、弁護士資格を有する者、データサイエンティスト、エンジニア、マーケティングや渉外に知見のある者等、多様な経歴を持つ約 40 名で構成される（他部との兼務者を含む)。また、外部有識者（大学教授・弁護士・コンサルタント）から適宜助言を得るための体制を合わせ持つ。

イ クオリティマネジメント室（QM 室）

QM 室は法務部門、セキュリティ部門、DAG 室等のコーポレート部門の要請を、事業部門が円滑にプロダクトへ実装できるよう支援することを目的とする。同室のスタッフは、事業部門の実態も踏まえた支援を行えるよう、各事業部門に精通した者で構成されている。

ウ プロダクトごとのプライバシー責任者

事業部門においてデータ保護・プライバシー保護の実装に責任を負う者を明確にするために、プロダクトごとにプライバシー責任者を設置し、その責任者には、プロダクトの責任者を当てている。つまり、同責任者は、いわゆる事業 KPI 達成と同じく、プロダクトへのデータ保護・プライバシー保護の実装に対する責任を負う。

２ 個人データの取扱いに関する責任者・責任部署の任務・役割

（１） 責任者・責任部署の任務

DAG 室は、個人情報保護法の遵守に加え、プライバシー保護及びフェアネス（公正性）の担保を、プロダクトのライフサイクルを通じて確実にするための任務を負う。主な任務を次に示す。

① 遵守すべき規程類や基準の作成

② 全事業を対象としたチェック・リリース後の継続的なモニタリング

・ ①で定めた規程類や基準に則って確認する。事業の要件定義・開発・リリー

スといったフェーズ毎に、適法性、プライバシー等の観点からチェックを行う（標準プロセスレビュー）

- 判断に悩む案件に関しては、DAG 室・事業部門等で話し合いを重ね、「ユーザーや社会に対して、データ利活用を正々堂々と公表・説明できるか」を基準に最終的な判断をしている
- DAG 室が承認しない限り、このプロセスが終了せず、事業を次のフェーズに進めることができない
- 抜け漏れなく確認できるよう、新規事業を始める場合だけでなく、既存事業において取り扱っている個人情報のライフサイクルに何らかの変更があった場合等にも、チェックプロセスを経る仕組みになっている

③ プロダクトごとのプライバシー責任者との定期的なディスカッション

- 事業領域ごと（金融、HR 等）に会議体を分けて、DAG 室と各領域のプライバシー責任者が月 1 回程度意見交換を行う
- 議題は多岐にわたるが、プロダクトを取り巻く環境や課題等のヒアリング、DAG 室が新規で定めた規程類や基準の紹介・影響を受けるプロダクトの洗い出し等も当該会議で実施する

④ 役職員への周知啓発・教育活動

- 会社として何を大事にしてプロダクトを展開しているのかを 1 人 1 人の役職員が理解できるよう、全役職員向けの研修では、パーソナルデータや AI 活用の基本的な指針をきちんと伝える

⑤ プライバシーセンターでの情報発信

- ユーザーが抱える不安を解消して信頼関係を構築するため、プライバシーを守る体制、レビュープロセス、有識者とのディスカッション内容等を情報発信する

（2） 責任部署と責任者との連携

標準プロセスレビューのプライバシー観点でより議論を尽くすべき案件がある場合、個人データの取扱いに関する責任者である法務・コンプライアンス担当執行役員が座長となり、関連部署の担当者等が出席する会議体（商品委員会）を設置し、同会議において DAG 室から検討中のプライバシー保護施策の方向性・実装方法等を説明し、経営層も含めた議論・方針決定を行っている。

また、DAG 室のメンバーは、チャットやメールで法務・コンプライアンス担当執行役員に直接相談できる体制が整っているため、商品委員会の開催を待たずに相談することも可能である。

（3） インシデント対応における連携

インシデント対応は、情報セキュリティ部門のCSIRTチームが中心となってインシデント検知を行い、検知した場合はリスクマネジメント室にエスカレーションし、その後はリスクマネジメント室が中心となって対応を進めていくこととなっている。

DAG室の所管に関連するインシデントが検知された場合には、DAG室に情報共有がされ、DAG室で漏えい等へ該当するかの判断、個人情報保護委員会への報告等の対応をする。

実践例４　D 社（金融業）

：事業部門が適切にデータを利活用するためのハンドブックの作成

データ利活用の多様化に伴い、事業部門が個人情報の取扱いに関して適切に判断することが難しくなっている。そこで、責任部署が中心となって、データを利活用する際の原則や注意すべき点を取りまとめたハンドブックを作成し、事業部門の誤解や理解不足の解消を図っている。作成にあたっては、事業部門のデータ利活用ニーズや課題を丁寧にヒアリングした上で、法令や契約、ビジネスリスク回避の観点で原則として遵守すべきことに加えて、事業部門がやってはいけないことを例示した。加えて、問題のない利活用事例も示すことで、データ利活用を過度に牽制しないように工夫した。他社や社内の実例を交えることで、実践的でわかりやすい内容となっている。

ハンドブックの普及にあたっては説明会や個別研修を実施している。また、事業部門の理解をさらに深めるために、ハンドブックの内容の見直しや拡充、説明会や研修内容の改善を継続的に図っている。

実践例５　E 社（製造業）

：全従業員を対象とする個人情報・プライバシー保護の重点強化期間の設定

「情報セキュリティ、プライバシー、データ保護」の３要素を「情報の品質」と定義し、情報の適切な取り扱いを“製品・サービスの品質”の一つの要素として企業における重要課題と位置づけた。これらの品質向上に向けた専用の会議体を設置するとともに、独自の品質強化期間を設け、全社員を対象とした意識啓発活動を実施している。２か月間の品質強化期間中は、社員が個人情報・プライバシー保護の重要性を理解し意識を醸成することを目的として、各事業所でのパネル展示や社外有識者による講演会、クイズ形式の参加型イベント等を行うとともに、社内外の直近のインシデントを題材にした啓発動画を作成する等の社員が身近に感じてもらえるように工夫した多彩な取組を行っている。

実践例６　F 社（サービス業）

：各種セミナーやカンファレンス等で得た最新情報の共有や、勉強会の開催

責任部署のスタッフの知識・技能の向上や、関連法令や技術最新動向等を把握することを目的に、外部セミナーやカンファレンスへの参加を奨励している。また得られた知見を責任部署内で共有することで、不参加のスタッフも知見を獲得できる機会を設けている。

また責任部署内では、カジュアルな形式のプライバシー勉強会を週次で開催し、個人情報・プライバシー保護に係る知識の習得に加え、関連する顧客からの問い合わせ内容とその対応の共有等の実務に直結したテーマに関する議論を行っている。

これらの取組によって、スタッフのレベルを均一化するとともに、最新の動向を常に踏まえた助言・対応ができるように責任部署内の知見をアップデートし続けている。