

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ver1.1の背景

<国際動向（EU・米国の動き）：プライバシーの企業価値への影響の高まり>

- EUではGDPRにより基本的人権の観点から、米国ではFTC法（第5条）により消費者保護の観点から、多額の罰金や制裁金の執行がなされ、**経営者がプライバシー問題を経営上の問題として取り扱うことが認識**されている。
- **GDPRにおいては、独立したDPO（Data Protection Officer）の設置**など、企業に求められる体制も位置づけられている。
- そのような環境下で、プライバシーを経営戦略の一環として捉え、プライバシー問題に適切に対応することで、**社会的に信頼を得て、企業価値向上につなげている企業も**現れている。

<国内動向

：グローバルで活躍する国内企業の動き、個人情報保護法制度改正大綱への対応>

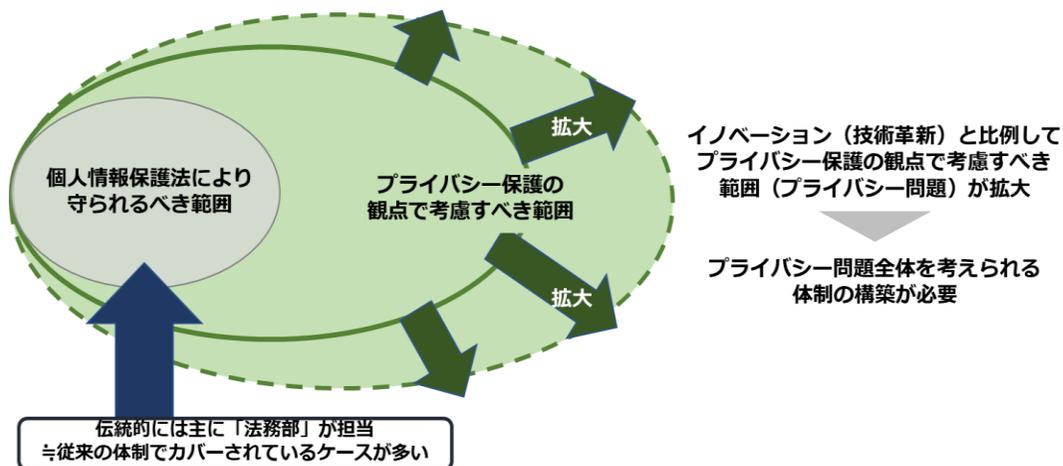
- 国際的なデータ流通により経済成長を目指すDFFTを実現する観点からも、セキュリティやプライバシーの確保を通じた、人々や企業間の信頼が必要とされている。**海外で求められるレベルへの目配せが国内企業にも必要**となってきた。
- **個人情報保護法制度改正大綱**でも、特にデジタル技術を活用した分野においては、**民間主導の取組**の更なる推進が必要としている。その一環で、**個人データの取扱いに関する責任者の設置やPIAの実施などの自主的取組が推奨**されている。

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ver1.1の背景

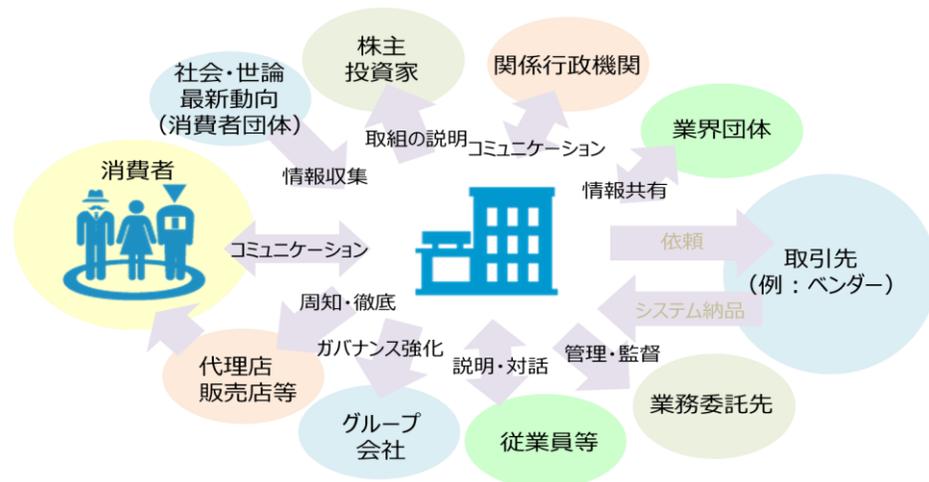
- 昨今ビジネスモデルの変革や技術革新が著しく、イノベーションの中心的役割を担うDX企業は、イノベーションから生じる様々なリスクの低減を、自ら図っていかなければならない。
- プライバシーに関する問題について、個人情報保護法を遵守しているか否か（コンプライアンス）の点を中心に検討されることが多かった。しかし法令を遵守していても、本人への差別、不利益、不安を与えるとの点から、批判を避けきれず炎上し、企業の存続に関わるような問題として顕在化するケースも見られる。
- 企業は、プライバシーに関する問題について能動的に対応し、消費者やステークホルダーに対して、積極的に説明責任を果たし、社会からの信頼を獲得することが必要である。経営者は、プライバシー問題の向き合い方について、経営戦略として捉えることで、企業価値向上につながるといえる。

プライバシー保護の観点で考慮すべき範囲と体制構築

プライバシーは取り扱う情報や技術、取り巻く環境によって変化する



ステークホルダーとのコミュニケーション



企業が社会からの信頼の獲得するためのプライバシーガバナンスの構築に向けて、
まずは取り組むべきことをガイドブックとして取りまとめた

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ver1.1の概要

【対象読者】 パーソナルデータを活用した製品・サービスを提供し、消費者のプライバシーへの配慮を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であって、

- ① **企業の経営陣**または**経営者へ提案できるポジションにいる管理職等**
- ② 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

経営者が取り組むべき3要件

要件1：プライバシーガバナンスに係る姿勢の明文化

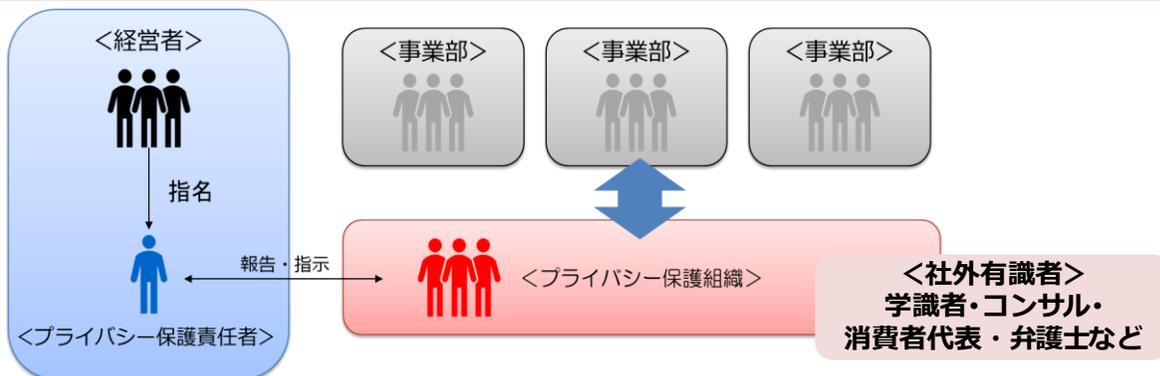
経営戦略上の重要課題として、プライバシーに係る基本的考え方や姿勢を明文化し、組織内外へ知らしめる。経営者には、明文化した内容に基づいた実施についてアカウンタビリティを確保することが求められる。

要件2：プライバシー保護責任者の指名

組織全体のプライバシー問題への対応の責任者を指名し、権限と責任の両方を与える。

要件3：プライバシーへの取組に対するリソースの投入

必要十分な経営資源（ヒト・モノ・カネ）を漸次投入し、体制の構築、人材の配置・育成・確保等を行う。



プライバシーガバナンスの重要項目

1. **体制の構築** (内部統制、プライバシー保護組織の設置、社外有識者との連携)
2. **運用ルールの策定と周知** (運用を徹底するためのルールを策定、組織内への周知)
3. **企業内のプライバシーに係る文化の醸成** (個々の従業員がプライバシー意識を持つよう企業文化を醸成)
4. **消費者とのコミュニケーション** (組織の取組について普及・広報、消費者と継続的にコミュニケーション)
5. **その他のステークホルダーとのコミュニケーション**
(ビジネスパートナー、グループ企業等、投資家・株主、行政機関、業界団体、従業員等とのコミュニケーション)

企業価値の向上・
ビジネス上の優位性

社会からの信頼獲得

消費者・
その他の
ステーク
ホルダー

(参考) プライバシーガバナンスに係る取組の例



(参考) プライバシーガバナンスに係る取組の例

○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。

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を策定するケースもある。

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を確保することが求められる。

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、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よ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。

NTTドコモ 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-

私たちNTTドコモは、「新しいコミュニケーション文化の世界の創造」という企業理念のもと、これまでにない豊かな未来の実現をめざして、イノベーションの創出に挑戦し続けています。生活にかかわるあらゆるモノやコトをつないで、お客さまにとっての快適や感動を実現すること、そして社会が直面するさまざまな課題に対する新しい解決策を見出すことにより、国や地域、世代を超えたすべての人々が豊かで快適に生活できる未来を創ることが、私たちの考えるイノベーションです。安心・安全、健康、学び、そして暮らしの中のさまざまな楽しみまで、お客さま一人ひとりにとって最適な情報と一歩先の喜びを提供し、また、それを実現するさまざまなビジネスの革新や社会課題の解決に向けた取組を支えます。

私たちは、現状に満足することなく、社会との調和を図りながら、このような未来をお客さまとともに創りたいと考えています。お客さまのパーソナルデータ、あらゆるモノやコトのデータ、そのデータからさまざまな知恵を生み出す人工知能などの技術を活用することにより、データから新しい価値を生み出し、お客さまや社会に還元することをめざします。

一方で、私たちNTTドコモがお客さまの大切なパーソナルデータを活用させていただくにあたっては、法令を順守することももちろん、お客さまのプライバシーを保護し、お客さまへの配慮を実践することも重要な使命です。パーソナルデータの活用について、不安や懸念を感じるお客さまもいらっしゃるかもしれませんが、しかしながら、私たちは、これまでと変わらずこれからも、お客さまに安心・安全を実感していただき、お客さまからの信頼にこたえ続けるという強い信念のもと、責任をもってパーソナルデータを取扱います。そして、これまで以上にお客さまの「疑」を大切にし、お客様のお声に「疑」を懸念しながら、データの活用によりお客さまや社



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

(参考) プライバシーガバナンスに係る取組の例

○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。

事例：参天製薬 グローバルでプライバシーガバナンスを構築

参天製薬株式会社では、パーソナルデータの取扱いについて、グローバルで体制構築を実施している。2020年4月、参天製薬のプライバシーに関する基本事項を定めたグローバルポリシーを制定した。

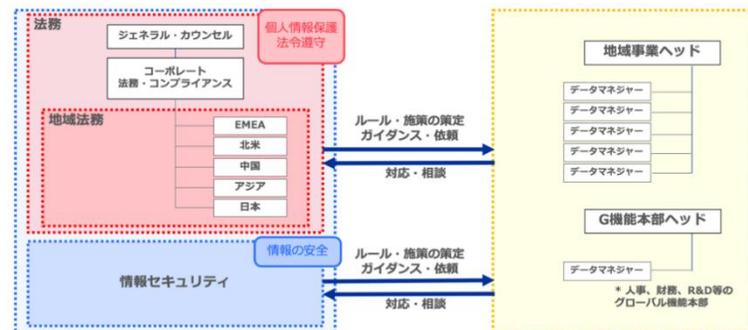
グローバル本社の下、地域・機能へData Managerを通じてガイダンスと働きかけを行っている。

構成及び主な内容

- 第1章 総則
 - 目的、適用範囲、定義等
- 第2章 役割と責任
 - 各部門の役割と責任等
- 第3章 個人情報の処理
 - プライバシーデザイン、個人情報取扱、最小化、記録、セキュリティ、リテンション等
- 第4章 データ主体の権利
 - 通知、データ主体の各種権利、データ主体からの請求、苦情への対応等
- 第5章 情報漏洩への対応と報告
 - 情報漏洩時の内部報告、当局報告等
- 第6章 従業員教育
 - 各役割・タスク内での個人情報の取扱い
- 第7章 雑則
 - 改定、発行日等

第2章 役割と責任

- Chief Administrator (=コンプライアンス責任者)
 - 全体統括
- 本社法務コンプライアンス部門
 - 全社行政、全社教育
- 地域法務コンプライアンス部門
 - 全社ポリシー/各国法に基づく域内各社へのガイダンス、教育
- グループ各社、各本部
 - 全社行政、地域法務ガイダンスに基づく個人情報の管理
 - 各社に“Personal Data Manager”を配置(グローバル本部への配置はCAの必要性判断による)
- 情報システム
 - 参天グループにおける個人データのセキュリティの確保



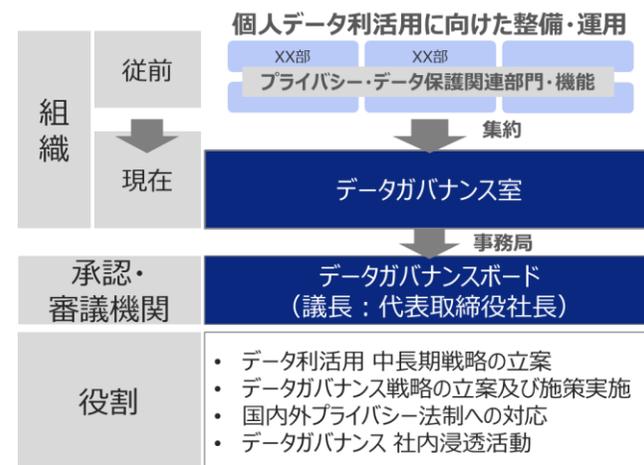
Global Data Privacy Policy (出典) (社内資料)

個人情報保護体制構築 (出典) (社内資料)

事例：KDDI データガバナンス室の設置

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

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



(出典) (社内資料)

(参考) プライバシーガバナンスに係る取組の例

○消費者とのコミュニケーション (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。
- 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。

- 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。
- 特にデータ分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。

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/>



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。

(参考) 「第五回 ビッグデータで取り扱う生活者情報に関する意識調査」

<https://www.hitachi.co.jp/New/cnews/month/2020/12/1222a.html>

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。

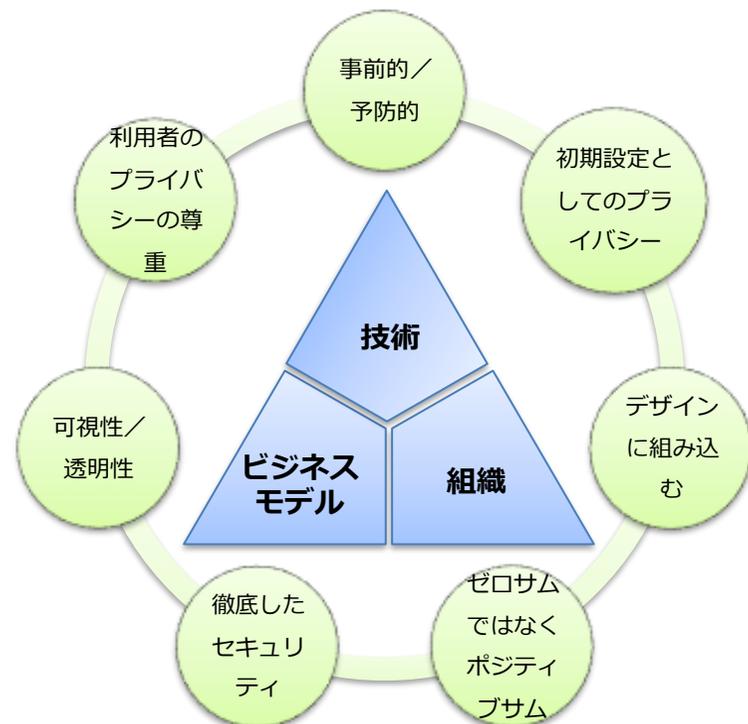


(出典) https://www.hitachi.co.jp/products/it/bigdata/bigdata_ai/personaldata_privacy/index.html

(参考) プライバシー・バイ・デザイン、プライバシー影響評価 (PIA)

- 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**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**という考え方である。
- **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。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。今後、**JIS規格も発行される見込み**である。
- **個人情報保護法改正大綱**でも「民間の自主的な取組を促進するため、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」と記載がある。

プライバシー・バイ・デザイン 7つの原則



プライバシー影響評価 (PIA)

PIAの必要性の決定

- しきい値分析
- PIA準備のための命令
- PIAの実施要領及び範囲の判断

PIAの実行

- PIAの事前準備
- 利害関係者のエンゲージメント
- プライバシーリスクアセスメント
- プライバシーリスク対応

PIAのフォローアップ

- 報告書の準備
- 公表
- プライバシーリスク対応計画の実施
- PIAのレビュー及び/又は監査
- プロセスへ変更を反映