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ver1.2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では、独立したDPO（Data Protection Officer）の設置や、DPIA（Data Privacy Impact Assessment）の実施**など、企業に求められる体制・取組も位置づけられている。また、ニュースでの「プライバシー」言及回数が過去最高になるなど、**社会におけるプライバシーに対する関心が高まっている。**
- 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、プライバシー問題を能動的に対応することで、**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。
- 例えば、個人情報の特定やマッピング、利用者の同意の管理、データ要求の履行などを手掛ける**「プライバシーテック」と呼ばれる企業への出資は拡大**している。また、**プライバシーを巡って、巨大テックの対立や規制強化**、これによる**企業の業績や事業展開への影響**といった状況も生じている。

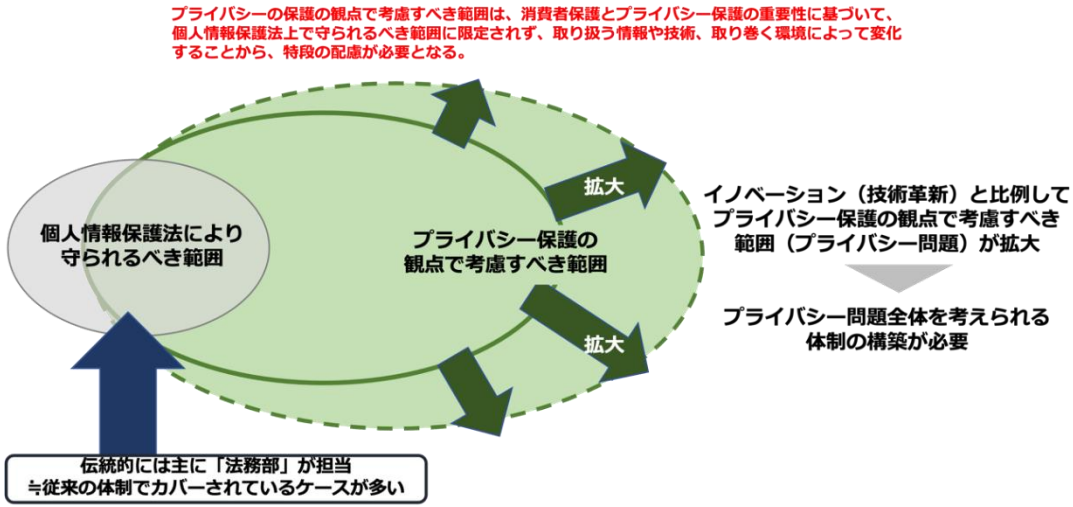
＜国内動向
：グローバルで活躍する国内企業の動き、個人情報保護法制度改正等への対応＞

- 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**となってきている。
- **個人情報保護法制度改正**を受けて、プライバシー保護を強化しつつ適切な利活用を進める動き。また、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され、**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。

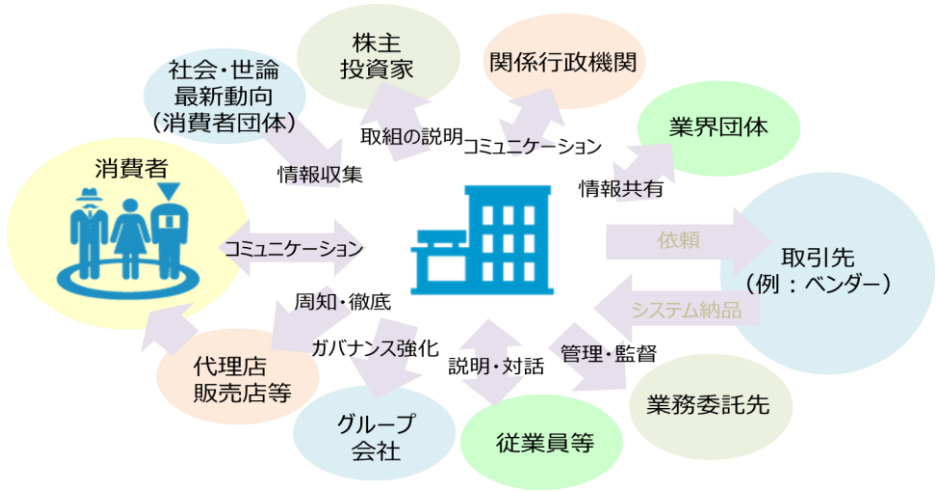
DX時代における企業のプライバシーガバナンスガイドブックver1.2の背景

- 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の必要性



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ver1.2の概要

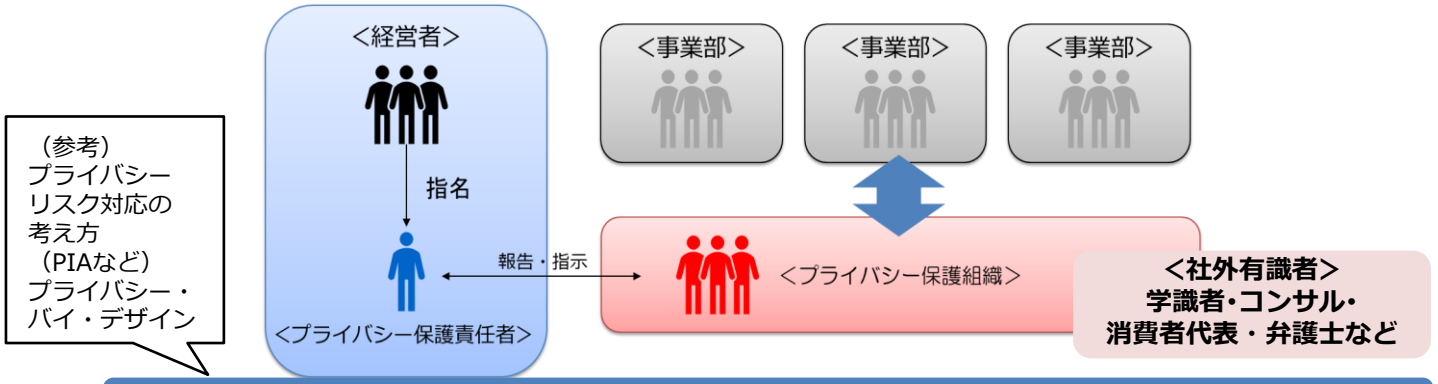
【対象読者】パーソナルデータを利活用した製品・サービスを提供し、消費者のプライバシーへの配慮を迫られることが想定される企業や、そのような企業と取引をしているベンダー企業等であって、
①**企業の経営陣**または**経営者へ提案できるポジションにいる管理職**等
②データの利活用や保護に係る事柄を総合的に管理する部門の責任者・担当者　など

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

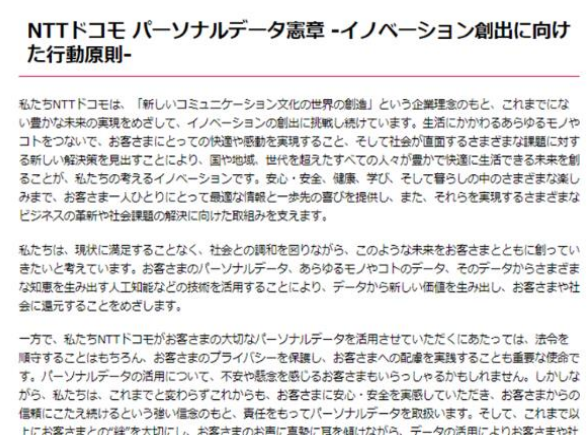
プライバシーガバナンスに係る取組の例（ver1.0掲載事例）

○プライバシーガバナンスに係る姿勢の明文化

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。

事例：NTTドコモ パーソナルデータ憲章の公表

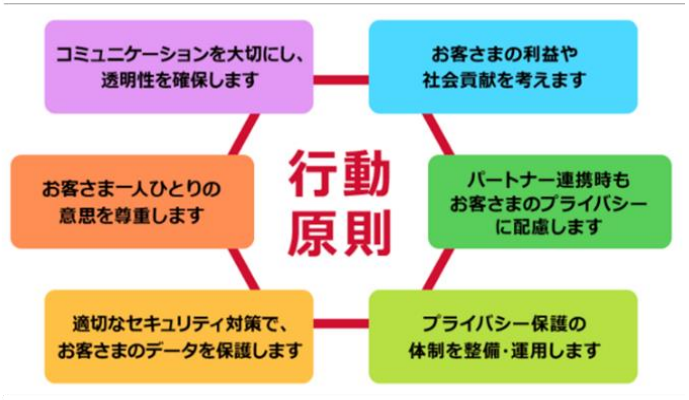
株式会社NTTドコモでは、「パーソナルデータ憲章―イノベーション創出に向けた行動原則―」を作成し、公表している。このパーソナルデータ憲章は、NTTドコモが「新しいコミュニケーション文化の世界の創造」という企業理念の下、これまでにない豊かな未来の実現をめざして、イノベーション創造に挑戦し続けていること、社会との調和を図りながら、未来をお客様と共に創っていきたいと考えていること、パーソナルデータの活用に当たり法令順守はもちろん、お客様のプライバシーを保護し、配慮を実践することも重要な使命であることなどを宣言し、行動原則として6つの原則を提示している。


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、それら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みを支えます。

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っていき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はもちろん、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。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との「絆」を大切にし、お客さまのお声に真摯に耳を傾けながら、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

○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）

事例：NTTドコモ パーソナルデータダッシュボードの提供

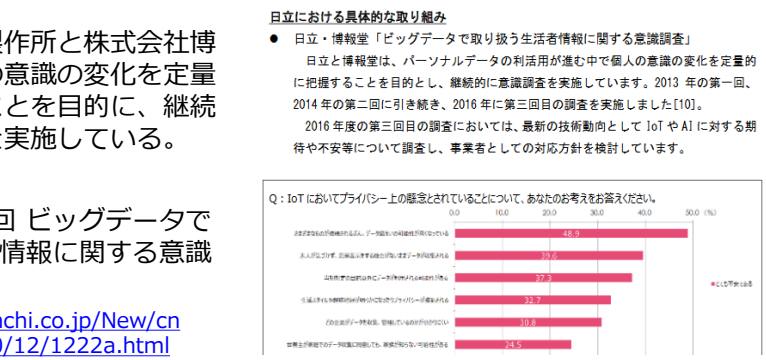
株式会社NTTドコモは、お客様自身のデータの提供先と種類の確認・変更、データ取扱いに係る同意事項の確認などの機能を提供している。

（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5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/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

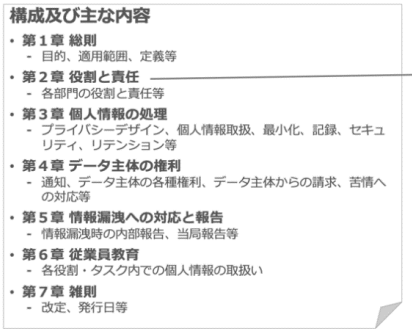
プライバシーガバナンスに係る取組の例（ver1.1掲載事例）

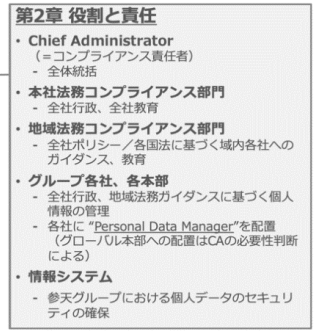
○体制の構築

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。

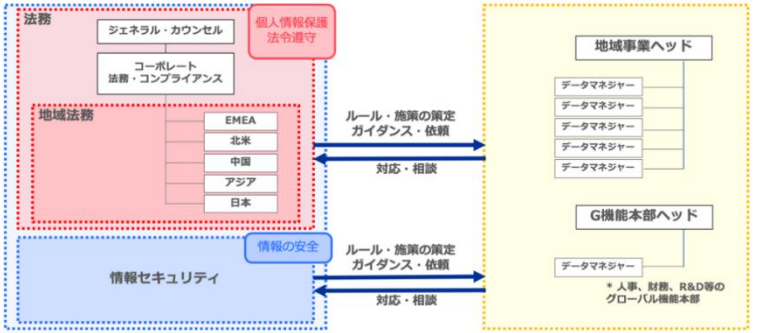
事例：参天製薬　グローバルでプライバシーガバナンスを構築

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。





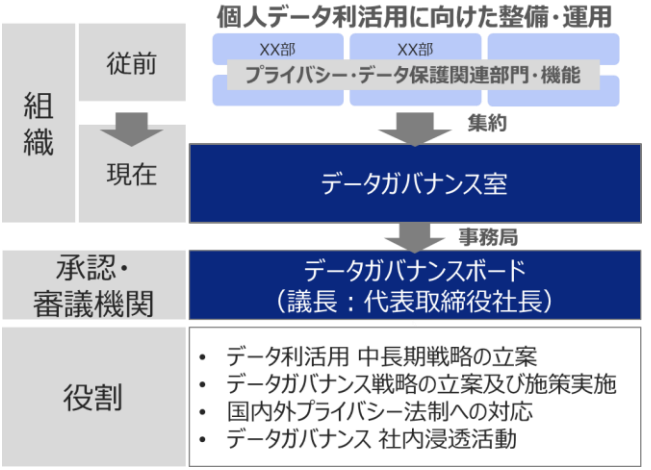
Global Data Privacy Policy（出典）（社内資料）



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）

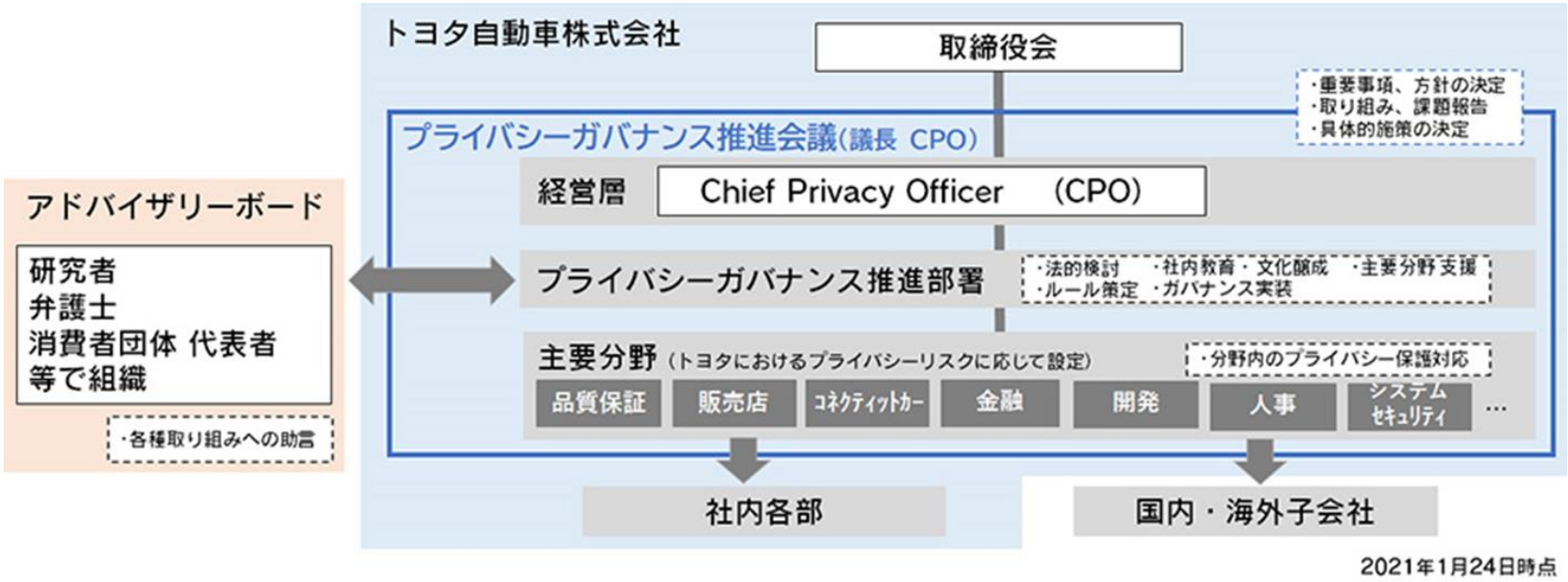
プライバシーガバナンスに係る取組の例（ver1.2追加事例）

○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、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

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

トヨタ自動車株式会社では、お客様に寄り添ったプライバシー保護を実現するため、全社横断的なガバナンス体制を構築し、Chief Privacy Officer（CPO） を指名した。CPOの下、プライバシーリスクに応じて主要な業務分野（品質保証・販売店・コネクティッドカー・金融・開発・人事・システムセキュリティ等）を特定し 、分野ごとにプライバシー保護対応の責任者を指名した。
また、CPOを議長とするプライバシーガバナンス推進会議を設置して定期的に会議を開催し、各分野におけるプライバシー保護対応の内容や、プライバシーに関する全社共通の課題、消費者とのコミュニケーション等の重要事項について、共有し検討を行う。加えて、プライバシー保護に影響する重要事案が発生した際には、各事業部門から報告を受けたプライバシーガバナンス推進部署が速やかに事象を把握し、具体的な対応策を検討の上、CPO及び経営層に報告し対策を講じるよう、取り組んでおります。 プライバシーガバナンス推進会議に対しては、外部有識者による専門委員会である「アドバイザリーボード」が助言を行う。



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

プライバシーガバナンスに係る取組の例（ver1.2追加事例）

○プライバシー保護責任者の指名

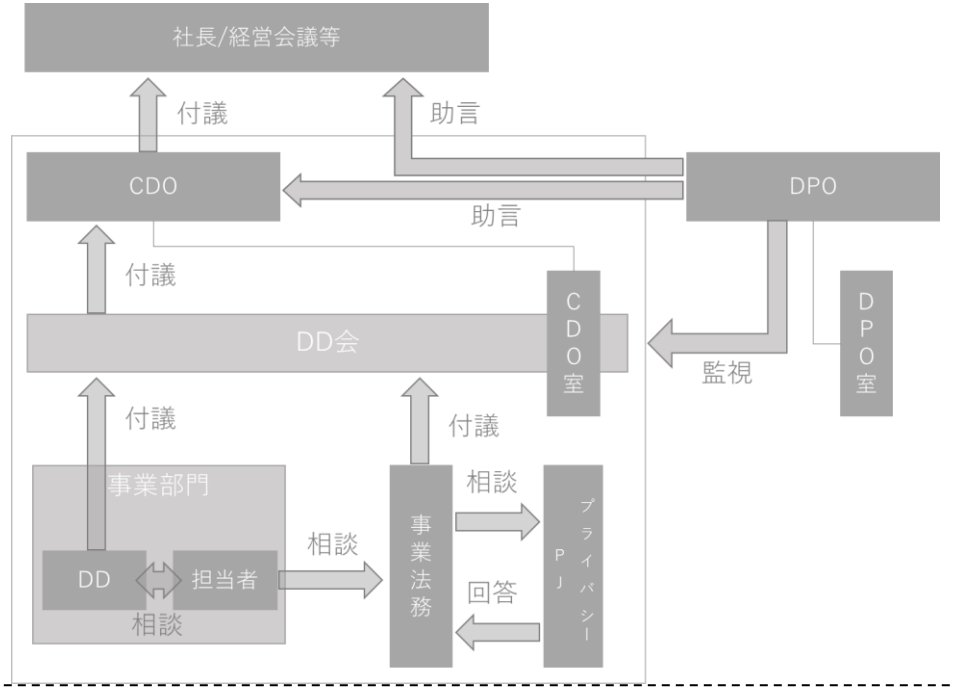
組織全体のプライバシー問題への対応の責任者を指名し、経営者が姿勢を明文化した内容を踏まえて、その実践を行うための責任を遂行させることが必要である。経営者は、プライバシー保護責任者から報告を求め、評価をすることで、組織の内部統制をより効果的に機能させる。その際には、プライバシー保護責任者の責任範囲を明確にし、プライバシー問題の発生を抑止するために必要な対応を遂行するための権限も与える必要がある

事例：ヤフー　最高データ責任者（CDO）、データ保護責任者（DPO）の指名

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

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

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



（出典）（社内資料）

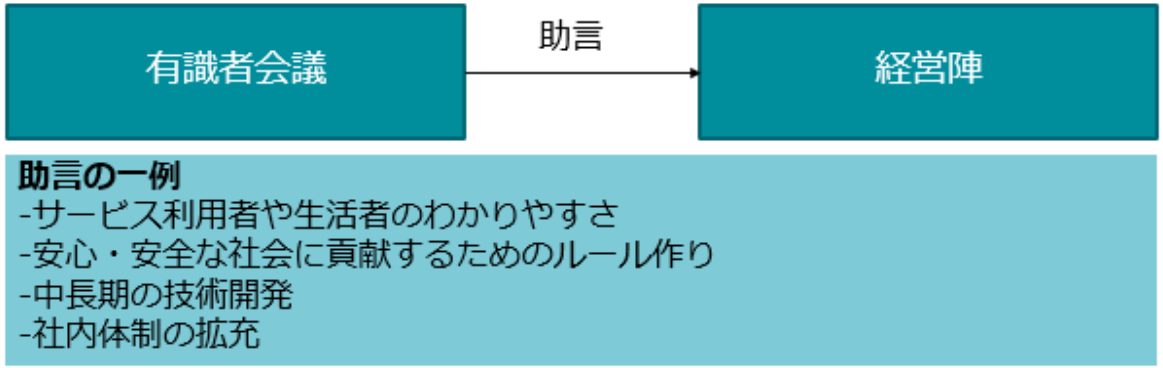
プライバシーガバナンスに係る取組の例（ver1.2追加事例）

○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。

事例：セーフィー　有識者会議の設置

セーフィー株式会社では、膨大なデータを預かる映像プラットフォームの健全性を保つ取組として、外部有識者会議を設置し、年に数回開催している。外部有識者会議は、法学者や法律家、社外取締役等により構成される。データ憲章の策定・公表に向けた議論や、変化する社会情勢の中でプラットフォーマーとしての責務を果たすために必要な取組についての継続的な議論を行っている。有識者からの助言を踏まえ、技術開発やルール等の継続的な改善や、データ活用の際のプライバシー配慮に係るユーザー企業に対する啓発活動などにも取り組んでいる。



（出典）（社内資料）

事例：NEC　デジタルトラスト諮問会議の設置

日本電気株式会社は、外部有識者から多様な意見を取り入れ、経営判断や施策立案へ活かすために「デジタルトラスト諮問会議」を設置し、年2回開催している。諮問会議メンバーは、法学者、法律家、消費者団体代表、サステナビリティや人権などの分野のNPO関係者等を含む5名で構成され、専門的な知見だけでなく、生活者の立場からも意見を取り入れている。
デジタルトラスト諮問会議では、プライバシーに関する国内外の動向を踏まえ、規制や社会受容性等の今後の動向、取組を強化すべき内容等について議論している。

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

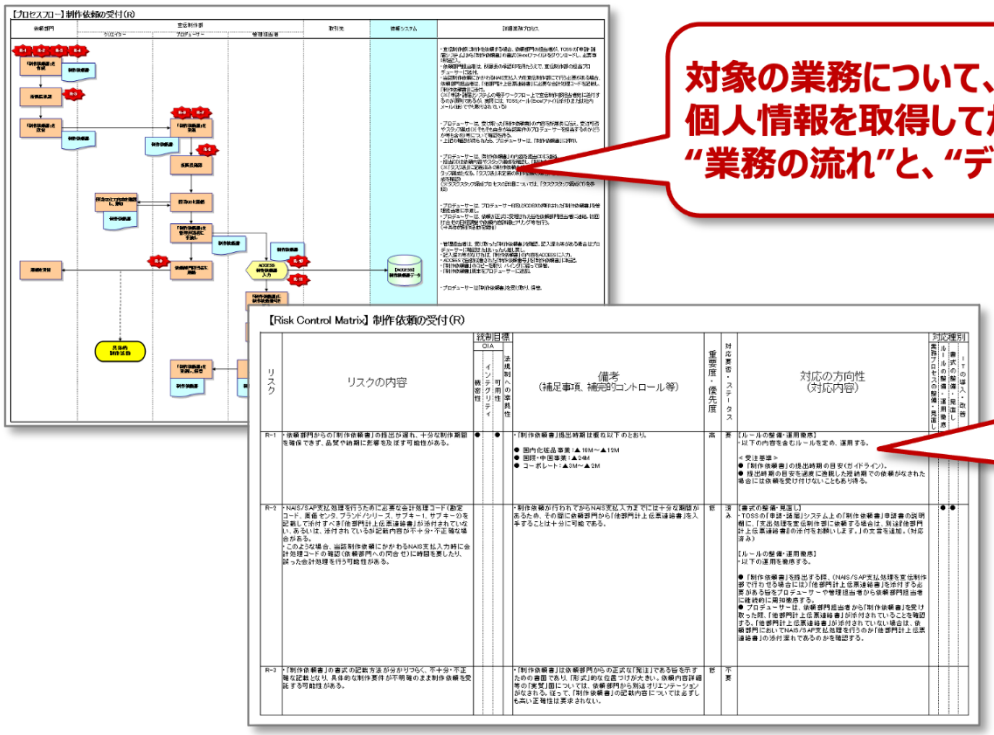
プライバシーガバナンスに係る取組の例（ver1.2追加事例）

○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。

事例：資生堂　プライバシー影響評価（PIA）の実践

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



対象の業務について、
個人情報を取得してから、利用・保管、消去するまでを、
“業務の流れ”と、“データの流れ・保管”を押さえて理解する。

機密性・インテグリティ・可用性が損なわれる恐れはないか、
プライバシー関連法規制に違反することはないか、
その他のリスクはないかを確認し、対策を検討する。

個人データの取扱い方を可視化し、リスクを特定する

（出典）（社内資料）

プライバシーガバナンスに係る取組の例（ver1.2追加事例）

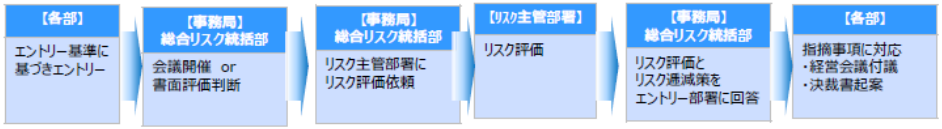
○プライバシー影響評価（PIA）

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。

事例：JCB　サービスコントロールミーティングの実践

株式会社ジェーシービーでは、商品・サービスの立案時に、リスク懸念事象を早期検知することによるリスクの抑制を目的として、プライバシーに限らずリスクを評価するプロセスとしてサービスコントロールミーティング（Service Control Meeting/SCM）を構築・運用している。
SCM事務局やリスク主管部署（法務・セキュリティ部門など）が、SCM起案部署（事業部門など）とリスクの共有や洗い出し、リスク評価を行うプロセスを実施している（年間約数百件程度）。経営会議に付議されたり、決裁書が起案される案件については、SCMにて可視化されたリスクや当該リスクに対する対応方針を文書として添付させることで、経営者や決裁者がリスクを踏まえて適正に判断できるようにしている。
SCMにおいて、プライバシーに関するリスクも情報セキュリティリスクとして管理や評価の対象となる。パーソナルデータ利活用ビジネスを推進するにあたっては、お客様の適切なプライバシー保護を図るための社内ルールとして「パーソナルデータ管理細則」を定め、SCM起案部署は管理細則への準拠状況を「パーソナルデータ利活用チェックリスト」で確認している。

【SCMフロー】



【SCMエントリー基準例】

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

【パーソナルデータ管理細則】

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

【パーソナルデータ利活用チェックリスト】

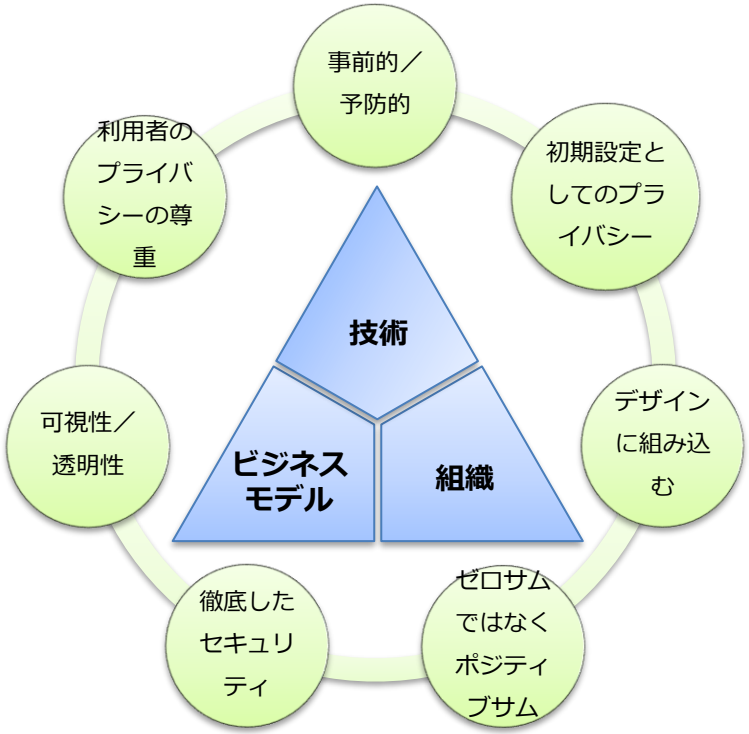
#	原則	基準
1	経緯（コンテキスト）の尊重	お客様に不安を抱かせない、予期できる範囲で利用すること
		お客様がパーソナルデータを提供した際の経緯（コンテキスト）に沿って、本人の期待と合致する形態で利活用を行うこと
2	個人によるコントロール	お客様に、自分のデータをコントロールする機会（どのように利用されるかについて関与する機会）を確保すること
		サービスに応じて、オプトイン・オプトアウトを適切に使い分けること
3	明確でわかりやすいポリシー	お客様に、何のデータをどのように使うかわかりやすく伝えること
4	プライバシー・リスクの大きさに応じた対策	データ種別ごとのプライバシー性、デー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

（出典）（社内資料）

（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。今般、2021年1月に**JIS規格が発行された（JIS X 9251:2021）**。ただし、PIAは全てのサービスに適用するものではなく、あくまで事業者の自主的な取組を促すものである。
- **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」と記載があり、2021年7月には個人情報保護委員会よりPIAの取組に関するレポートも公開されている。

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