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について

本資料は、経産省作成資料を説明用に改変したものです。

タイトルと背景

○○ガバナンス？

- ガバナンスとは、もともと「統治」という意味の英語 “governance” です。
- 様々な文脈で使われて（濫用されて）多義的な言葉となっている。
- 「ITガバナンス」「情報セキュリティガバナンス」などのように使うときは、企業その他の組織において、IT戦略や情報セキュリティが正しく確保される仕組みが作られて機能していることをいいます。
- **○○が正しく確保される仕組みが作られて機能していること**

○○ガバナンス？

経済産業省
Ministry of Economy, Trade and Industry

文字サイズ

サイト内検索

ホーム | 経済産業省について | お知らせ | 政策について | 統計 | 申請・お

政策について ▸ 政策一覧 ▸ 安全・安心 ▸ 情報セキュリティ政策 ▸ 情報セキュリティガバナンス確立促進事業 ▸ 情報セキュリティガバナンス

印刷

情報セキュリティガバナンスの概念

情報セキュリティガバナンスの概念・定義

情報セキュリティガバナンスとは、「企業における情報セキュリティガバナンスのあり方に関する研究会報告書」において、「コーポレート・ガバナンスと、それを支えるメカニズムである内部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用すること」と定義されました。

平成20年6月公開の「産業構造審議会情報セキュリティ基本問題委員会 中間とりまとめ（PDF形式：323ＫＢ）」の中で、「企業経営の主目標は、株主、顧客、取引先、従業員、社会等の利害関係者に対して責任を果たすこと、つまり、「企業価値の向上」及び「社会的責任の遂行」にあり、これを支える重要な取組の一つにリスク管理が位置づけられる。様々なリスクの内、情報資産に係るリスクの管理を狙いとして、情報セキュリティに関わる意識、取組及びそれらに基づく業務活動を組織内に徹底させるための仕組み*を構築・運用することを情報セキュリティガバナンスと位置づける。（*経営者が方針を決定し、組織内の状況をモニタリングする仕組み及び利害関係者に対する開示と利害関係者による評価の仕組みを指す）」と、その概念の一層の明確化を図りました。

プライバシーガバナンスの必要性

- 「情報セキュリティガバナンス」は、経産省の2008年のガイドライン※の公表後、間もなく「やらないとダメ」に。

- 手堅く役立つものをガイドラインにするので、それほど新しいものが出るわけではない。　　e.g.　IPAの十大脅威は2006年から

- プライバシーガバナンスもそうなるのではないか。

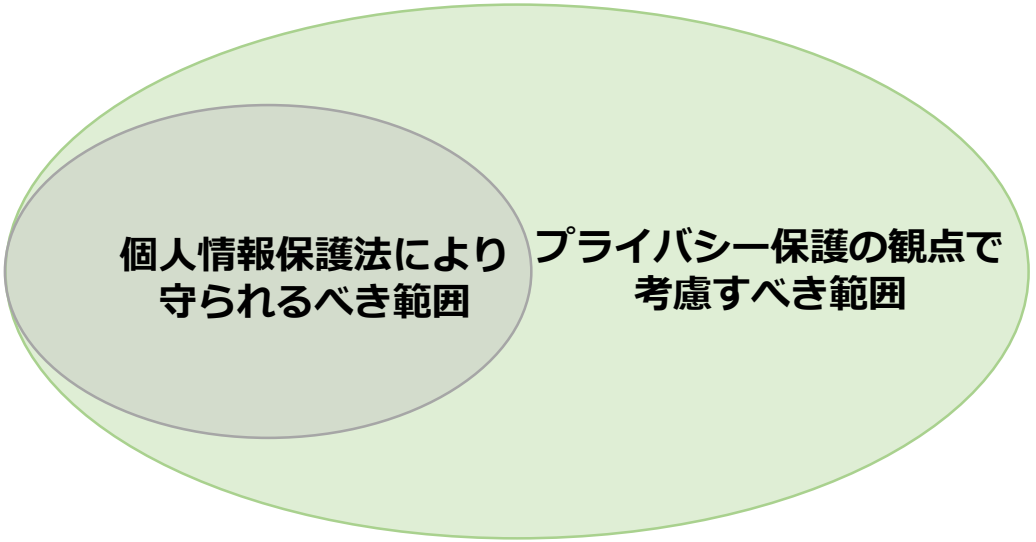
※　　産業構造審議会情報セキュリティ基本問題委員会中間とりまとめ～企業における戦略的な情報セキュリティガバナンスの確立に向けて～

背　景

- 「プライバシー問題」で炎上すると様々な問題が生じる（代表者謝罪、役員交代、事業廃止等）
- その一方で**何が炎上するのか分からない**。個人情報保護法だけ確認してもダメ。　⇒　e.g.　リクナビ事件
- 株主や債権者等に対して、「プライバシー問題」で役員が「**内部統制**」に関する義務違反で責任を負うことがありうるのではないか。
- 情報セキュリティの不備で漏えいしたらまずいことになったが、同じことがプライバシーについてもあるのではないか。
- そろそろプライバシー保護で差別化が図れるのではないか。

（参考）プライバシー保護の観点で考慮すべき範囲

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



【例】

- カメラによって個人に不安や居心地が悪い感情を与える
- データが勝手に個人に結びつけられてしまい、個人にとって害のある情報も収集されるのではないかとの疑念
- 目的外利用されてしまい、自分の情報が意図に反して利用されてしまうのではないかとの恐怖と不安が生まれる
- 第三者への提供により、二次利用によって更なるプライバシー問題が引き起こされるのではないかという不安がうまれる

など…

※ このガイドブックは、「プライバシー問題」の用語を違法性の問題として考えていない。受容性が低く炎上するリスクがあるようなものを広く「プライバシー問題」としている。

前提として－内部統制

2.ガイドブックの前提

1. 本ガイドブックの位置づけ

2. ガイドブックの前提
- 2.1　Society5.0の時代における企業の役割
- 2.2　プライバシーの考え方
- 2.3　企業のプライバシーガバナンスの重要性

3. 経営者が取り組むべき三要件
- 3.1　プライバシーガバナンスに係る姿勢の明文化
- 3.2　プライバシー保護責任者の指名
- 3.3　プライバシーへの取組に対するリソースの投入

4. プライバシーガバナンスの重要項目
- 4.1　体制の構築
  - 4.1.1　プライバシー保護責任者の役割
  - 4.1.2　プライバシー保護組織の役割
  - 4.1.3　事業部門の役割
  - 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
- 4.2　運用ルールの策定と周知
- 4.3　企業内のプライバシーに係る文化の醸成
- 4.4 消費者とのコミュニケーション
  - 4.4.1　組織の取組の公表、広報
  - 4.4.2　消費者との継続的なコミュニケーション
  - 4.4.3　問題発生時の消費者とのコミュニケーション
- 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
  - 4.5.1　ステークホルダーやビジネスパートナーへの対応
  - 4.5.2　プライバシー問題の情報収集
  - 4.5.3　その他の取組

5.（参考）プライバシーリスク対応の考え方
- 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
- 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）
- 5.3　プライバシーリスク評価（PIA）

6.（参考）プライバシー・バイ・デザイン

7. おわりに

参考文献
検討体制

2.ガイドブックの前提

- Society5.0において、イノベーションを絶えず生じさせることは、我が国の今後の経済成長を維持するために重要。同時に、イノベーションによって生じる**新たなリスクをコントロールし、社会的価値（財産・生命の安全、プライバシー、民主主義など）を実現**することが求められている。

- パーソナルデータの利活用の進展は、個々人の嗜好やニーズを踏まえた適確なアプローチを可能にし、ひいては社会課題解決にもつながることが期待される。他方で、**IoTやAIなどの技術進展に伴って、プライバシー問題も多様化**している。
  - データ解析の結果、機械的に不当な差別的扱いを受ける可能性
  - 個人の政治的選択に対して介入される可能性　など

- 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なく、フィジカル空間の生身の人間と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。
- 企業は、プライバシー問題が顕在化するリスクは、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体に影響を及ぼす可能性があることを認識する必要がある。
- **企業がプライバシーに関して真摯に検討し取り組むことは、社会から信頼を獲得し、企業価値向上につながる**ことから、単なる「コンプライアンス」として受け止めず、経営戦略として捉え、競争力の要素として検討していくことが重要。

- 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の信頼を得るにあたり、十分な対応といえない。法令等遵守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よくコミュニケーションをとり、能動的にプライバシー問題に取り組み、説明し、信頼を獲得していく必要がある。
- **経営者が積極的にプライバシー問題にコミットし、組織全体としてプライバシー問題へ取り組むための体制を構築し、機能させることが、プライバシーガバナンスの基本的な考え方**となる。

内部統制とは何か

3つの内部統制の法的根拠

- 金融商品取引法 → 内部統制報告制度

- 会社法
  - 第362条4項等 → 業務の適正確保体制決定義務
  - 取締役の善管注意義務 → 判例の内部統制構築義務

内部統制とは何か

内部統制とは？

株主に対する受託責任を果たすための「仕組み」（が経営者によって作られ、それが機能していること）

「仕組み」の具体的な内容は以下のとおり

① 法令遵守体制
② 損失危険管理体制
③ 情報保存管理体制
④ 効率性確保体制
⑤ 企業集団内部統制
⑥ 監査役監査の実効性確保体制
⑦ 財務報告内部統制

判例における内部統制 – 大和銀行事件

大和銀行事件（大阪地裁H12.9.20）

【事案】

- 大和銀行ニューヨーク支店の従業員Aが同行に無断で簿外取引を継続した結果、同行に巨額の損失を与えたことつき、**取締役12名に対し、1人あたり830億円から75億円という巨額の損害賠償が命じられた株主代表訴訟事件である。**
- Aはトレーダーとして、米国財務省証券（以下「財務省証券」）を他の証券会社との間で売買し、その資金手当てのため、大和銀行が業務上保管していた顧客および大和銀行自身の財務省証券を順次売却した。
- Aの違法行為は、(a)トレーダーとしての財務省証券の簿外取引と(b)保管中の財務省証券の無断売却の二つに分けられる。

- 2つの事件

＜甲事件＞

内部統制システムの不備によって見過ごされた簿外取引自体により、11億ドルの損失を会社に与えたこと

＜乙事件＞

簿外取引と発覚後の隠ぺい行為を理由として米国当局から刑事訴追を受け、罰金の支払を命じられるとともに弁護士費用を支出して3億5000万ドルの損失を会社に与えたこと

- 取締役固有の違法行為・・・

  隠ぺい！　→　違法行為(c)

判例における内部統制

- はるか離れた米国のトレーダーを取締役が直接監督するのは無理。それでも裁判所は、不正行為を防止する「仕組み」（＝内部統制）ができていなかったことについて取締役に責任があるとして、巨額の損害賠償責任を認めた。
- このため「内部統制」がおそろしいものとして一躍有名に・・
- 内部統制とは、リスク管理のための体制が構築・運用されていること。
- 担当取締役でないこと、組織的・物理的に距離があること等により、直接の監督義務違反が否定される事案でも、内部統制構築義務違反により責任が認められる場合がある。
- 今のところ、プライバシー問題の「炎上」について取締役の責任が認められた事案はないが、時間の問題かも…

判例における内部統制 – 高木乳業事件①

ジャージー高木乳業事件（金沢地裁H15.10.6）
（名古屋高裁金沢支部H17.5.18）

【事案】

- 牛乳・乳飲料の製造販売会社が、違法な牛乳の再利用により食中毒事件を起こし、業務停止命令を受けて解散を余儀なくされたところ、解雇された従業員やその遺族から、同社代表取締役である被告が、将来賃金の逸失等について損害賠償請求を受けた事案である。

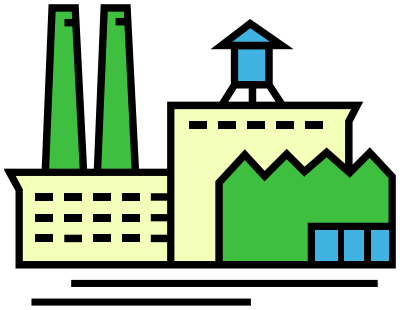
- 同社は、金沢市に会社工場を持ち、牛乳・ヨーグルト・清涼飲料水を製造して、北陸3県を中心に販売する会社であった。同社が販売店に販売した牛乳について、異臭がする旨のクレームがあったため、同社はこれを引き上げ、廃棄用冷蔵庫に保管していたが、これを新たに販売する牛乳製造に際して再利用した。

- その後、同社により製造された牛乳を飲んだ顧客である小中学校15校の児童生徒など400人あまりに食中毒が発生した。これを受けて金沢市は同社に無期限の営業停止命令を出し、同社は業務再開の目処が立たないことから、総会決議により解散し、廃業した。

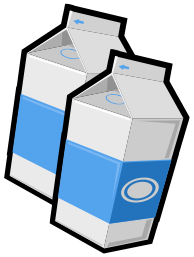
- 同社の資本金は1000万円。売上高は平成6年度の約15億円がピークである。解散時における同社の株主は、被告代表取締役、その妻およびその間の子ら2名の計4名であって、これらは被告と利益を共通にする親族であり、同社の解散に同意している。

判例における内部統制 -高木乳業事件②

ジャージー高木乳業事件（金沢地裁H15.10.6）
（名古屋高裁金沢支部H17.5.18）

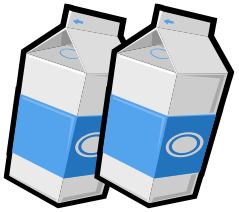


① 出荷



異臭!!

② 回収



③ 再利用

食中毒

判例における内部統制 – 高木乳業事件③

ジャージー高木乳業事件（金沢地裁H15.10.6）
（名古屋高裁金沢支部H17.5.18）

【原審の判断】

被告は担当部長の再利用行為を予見できた。

↓

直接の監督義務違反あり→任務懈怠

【控訴審の判断】

- 本件会社では，雪印乳業事件以後，金沢市保健所からの本件指導があって，一旦出荷された牛乳等製品についてはこれを再利用しないこととしていた。

↓

- そのことは朝礼等を通じて従業員にも周知させていた。

↑

- とすると、担当部長による本件再利用は，まことに異例。

↓

- よって、本件再利用を事前に予見することは困難。

↓

- よって、直接の監督義務違反なし。

↓

- しかしながら、被告は，これまでの本件会社における再利用が違法であることを知ったのであるから，本件会社の代表取締役として，直ちに同法に違反する再利用を廃止する措置を講ずるのはもとより，今後同様の違法な再利用が行われることのないようにするための適切な措置（再利用に関する取扱基準の策定，従業員に対する教育・指導等の徹底等）

判例における内部統制 – 高木乳業事件④

ジャージー高木乳業事件（金沢地裁H15.10.6）
（名古屋高裁金沢支部H17.5.18）

【控訴審の判断】（つづき）

監督義務違反と
内部統制構築義務違反

<u>を講じて，法令を遵守した業務がなされるような社内体制を構築すべき職責があった</u>

- 違法な再利用をしない社内体制を築くべき義務があったのに、しなかったことは、任務懈怠。

従業員の違法行為

監督義務違反では？

直接の
監督義務

職掌分担あり、予見可能性なし
（目を届かせるのはムリ）

内部統制
構築義務

では内部統制構築義務違反では？
（目が届かなければリスク管理体制で予防せよ！）

ガイドブックの核心部分

ガイドブックの構成

1. 本ガイドブックの位置づけ

2. ガイドブックの前提
- 2.1 Society5.0の時代における企業の役割
- 2.2 プライバシーの考え方
- 2.3 企業のプライバシーガバナンスの重要性

3. 経営者が取り組むべき三要件
- 3.1 プライバシーガバナンスに係る姿勢の明文化
- 3.2 プライバシー保護責任者の指名
- 3.3 プライバシーへの取組に対するリソースの投入

4. プライバシーガバナンスの重要項目
- 4.1 体制の構築
  - 4.1.1 プライバシー保護責任者の役割
  - 4.1.2 プライバシー保護組織の役割
  - 4.1.3 事業部門の役割
  - 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
- 4.2 運用ルールの策定と周知
- 4.3 企業内のプライバシーに係る文化の醸成
- 4.4 消費者とのコミュニケーション
  - 4.4.1 組織の取組の公表、広報
  - 4.4.2 消費者との継続的なコミュニケーション
  - 4.4.3 問題発生時の消費者とのコミュニケーション
- 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
  - 4.5.1 ステークホルダーやビジネスパートナーへの対応
  - 4.5.2 プライバシー問題の情報収集
  - 4.5.3 その他の取組

5.（参考）プライバシーリスク対応の考え方
- 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
- 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）
- 5.3 プライバシーリスク評価（PIA）

6.（参考）プライバシー・バイ・デザイン

7. おわりに

参考文献
検討体制

3.経営者が取り組むべき三要件

1. 本ガイドブックの位置づけ

2. ガイドブックの前提
- 2.1　Society5.0の時代における企業の役割
- 2.2　プライバシーの考え方
- 2.3　企業のプライバシーガバナンスの重要性

3. 経営者が取り組むべき三要件
- 3.1　プライバシーガバナンスに係る姿勢の明文化
- 3.2　プライバシー保護責任者の指名
- 3.3　プライバシーへの取組に対するリソースの投入

4. プライバシーガバナンスの重要項目
- 4.1　体制の構築
  - 4.1.1　プライバシー保護責任者の役割
  - 4.1.2　プライバシー保護組織の役割
  - 4.1.3　事業部門の役割
  - 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
- 4.2　運用ルールの策定と周知
- 4.3　企業内のプライバシーに係る文化の醸成
- 4.4 消費者とのコミュニケーション
  - 4.4.1　組織の取組の公表、広報
  - 4.4.2　消費者との継続的なコミュニケーション
  - 4.4.3　問題発生時の消費者とのコミュニケーション
- 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
  - 4.5.1　ステークホルダーやビジネスパートナーへの対応
  - 4.5.2　プライバシー問題の情報収集
  - 4.5.3　その他の取組

5.（参考）プライバシーリスク対応の考え方
- 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
- 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）
- 5.3　プライバシーリスク評価（PIA）

6.（参考）プライバシー・バイ・デザイン

7. おわりに

参考文献
検討体制

3. 経営者が取り組むべき三要件

- ガイドブックにおいては、プライバシー保護とデータ利活用を単に二項対立ではなく、**プライバシーに配慮しながらデータ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を位置付け。
- その上で、①プライバシー保護への取組が個々の**サービスや製品の品質を高め**ることと同じであり、ひいては**企業価値の向上**につながる、②不適切なプライバシー問題に関する取組は**内部統制の構築義務違反として経営責任**につながる、という両面から、**経営陣がプライバシーガバナンスの構築を行う必要性を明確化。**
- かかる観点から、経営陣が取り組むべき**具体的な要件として三要件を提示**している。

＜経営者が取り組むべき三要件＞

要件１：プライバシーガバナンスに係る姿勢の明文化

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

3. 経営者が取り組むべき三要件

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。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。

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

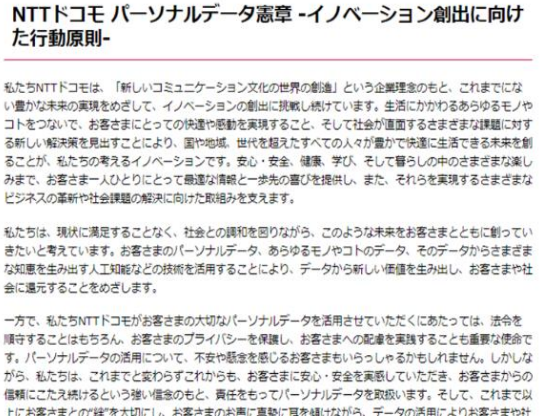
3. 経営者が取り組むべき三要件

要件１：プライバシーガバナンスに係る姿勢の明文化

- **企業が**それぞれの企業理念の下、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、商品やサービスの品質を向上させ、社会からの信頼の獲得、ひいては企業価値向上に繋がる**。
- 経営者はプライバシー問題への取組を経営上の重要事項の1つと認識し、**プライバシー保護の軸となる基本的な考え方や姿勢を明文化し、組織内外に知らしめることが必要**。
- 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。公表することで消費者やステークホルダー（株主、取引先等）からの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に取り組むことへのアカウンタビリティ確保が求められる。
- 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など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

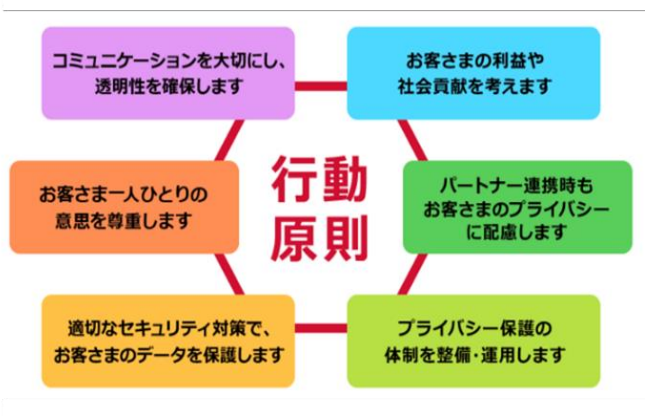
株式会社NTTドコモでは、「パーソナルデータ憲章―イノベーション創出に向けた行動原則―」を作成し、公表している。このパーソナルデータ憲章は、株式会社NTTドコモが「新しいコミュニケーション文化の世界の創造」という企業理念の下、これまでにない豊かな未来の実現をめざして、イノベーション創造に挑戦し続けていること、社会との調和を図りながら、未来をお客様と共に創っていきたいと考えていること、パーソナルデータの活用に当たり法令順守はもちろん、お客様のプライバシーを保護し、配慮を実践することも重要な使命であることなどを宣言し、行動原則として6つの原則を提示している。


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



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

3. 経営者が取り組むべき三要件

要件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明文化した内容の具体的な実践が不可欠。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（プライバシー保護責任者）として指名し、経営者が姿勢を明文化した内容を実現するための責任を遂行させる**ことが必要。
- 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権限も与える**必要がある。
  - プライバシー保護責任者は、**GDPRでいうところの、強い独立性が担保されているデータ保護オフィサー（DPO）とは必ずしも同じものとは限らず**、役員が担うこともありうる。
- 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。

要件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、明文化した姿勢の実践のため、**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の構築や、十分な人員の配置、人材の確保・育成等を実施することが必要。
- プライバシーに係る対応は、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。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、**必要な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。

4.プライバシーガバナンスの重要項目（4.1~4.3）

1. 本ガイドブックの位置づけ

2. ガイドブックの前提
- 2.1　Society5.0の時代における企業の役割
- 2.2　プライバシーの考え方
- 2.3　企業のプライバシーガバナンスの重要性

3. 経営者が取り組むべき三要件
- 3.1　プライバシーガバナンスに係る姿勢の明文化
- 3.2　プライバシー保護責任者の指名
- 3.3　プライバシーへの取組に対するリソースの投入

4. プライバシーガバナンスの重要項目
- 4.1　体制の構築
  - 4.1.1　プライバシー保護責任者の役割
  - 4.1.2　プライバシー保護組織の役割
  - 4.1.3　事業部門の役割
  - 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
- 4.2　運用ルールの策定と周知
- 4.3　企業内のプライバシーに係る文化の醸成
- 4.4 消費者とのコミュニケーション
  - 4.4.1　組織の取組の公表、広報
  - 4.4.2　消費者との継続的なコミュニケーション
  - 4.4.3　問題発生時の消費者とのコミュニケーション
- 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
  - 4.5.1　ステークホルダーやビジネスパートナーへの対応
  - 4.5.2　プライバシー問題の情報収集
  - 4.5.3　その他の取組

5.（参考）プライバシーリスク対応の考え方
- 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
- 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）
- 5.3　プライバシーリスク評価（PIA）

6.（参考）プライバシー・バイ・デザイン

7. おわりに

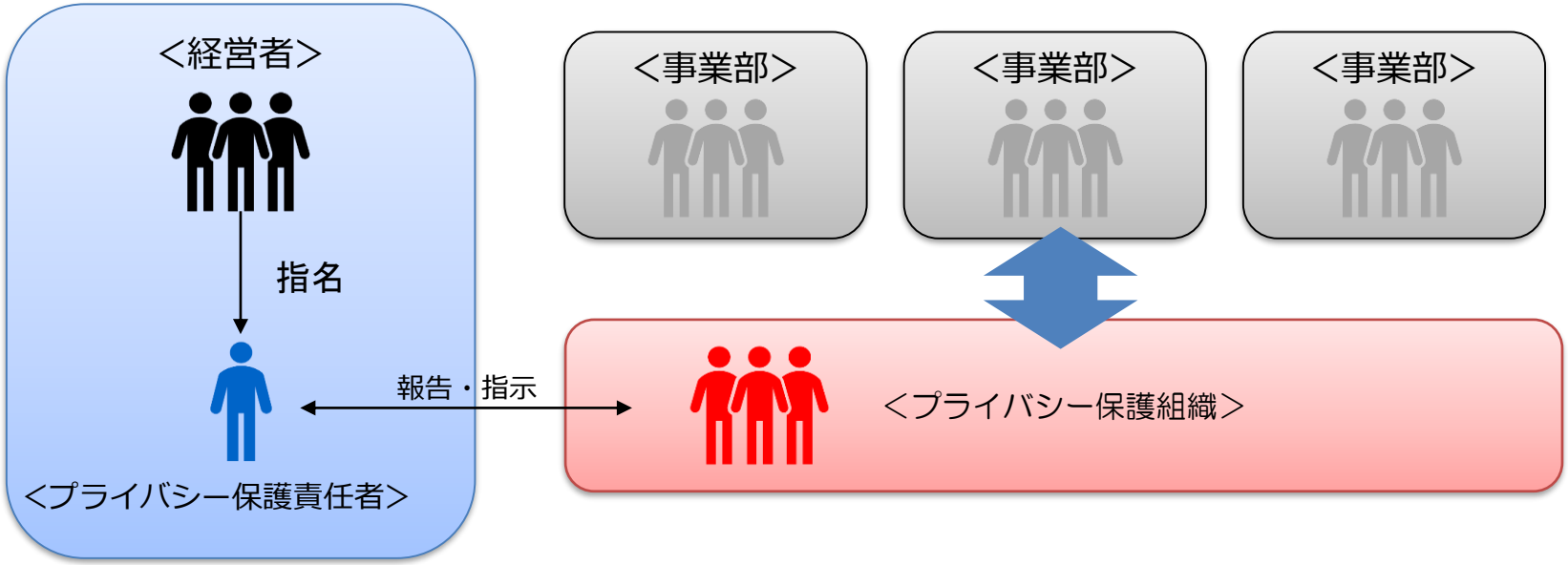
参考文献

検討体制

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の機能として、**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発見することが求められる**。さらに、**対象となる事業の目的達成とプライバシーリスクマネジメントを両立**するために、**対応策の多角的な検討**が必要。

■ **プライバシー保護責任者の下で、中核となる組織を企業内に設ける**ことが望ましい（＝**「プライバシー保護組織」**）。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の醸成や、社外有識者などからの関連情報の収集、多角的な対応策の検討を遂行する**ことができる。



4．プライバシーガバナンスの重要項目（4.1体制の構築）

プライバシー保護責任者の役割

- プライバシー保護責任者は、**経営者が明文化した姿勢等の実践のための方針の確立及び体制の構築を進め、当該方針の実施を徹底**する。
- 経営者に対し報告を行い、経営者が明文化した内容と合致しているかを絶えず確認する。

プライバシー保護組織の役割

- 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**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見つける**。そのために、各部門と日頃から接点を持つとともに、プライバシー保護組織の存在を企業内に周知徹底する必要がある。
- 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、**常に関連する情報を収集**する。
- **対象事業の目的を実現**しつつ、プライバシーリスクに対応するために、**多角的に対応策を検討**する。
- 新規事業や新規技術を開発する部門とともに、**他部門と円滑な連携を図ることが重要**。
- **プライバシー問題が発生した場合の初動や**、その後の再発防止策の策定等の**事後対応について**、事業部門と連携して情報を集約・検討し、**プライバシー保護責任者へ報告・指示を仰ぐ**。
- 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、活用**できるようにしておく。

4.1 内部監査部門や第三者的組織の体制構築

- **内部監査の体制を構築**するなど、**独立した立場からモニタリング・評価**することで、社内の取組を徹底し、**社外からの信頼を更に高める**。
- また、**第三者的な立場の外部の有識者からなるアドバイザリーボード、諮問委員会などを設置**し、評価・モニタリングを受けることも検討すべき。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ることも可能。

4.2 運用ルールの策定と周知

- 構築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、プライバシー保護責任者やプライバシー保護組織によってプライバシーリスクが把握され、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。
- 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 。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ともに、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。
- 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を実質的に機能させていくためには、プライバシーリスクに適切に対応できる企業文化を組織全体で醸成することが不可欠。**企業に所属する従業員一人一人が、当たり前のようにプライバシーに関する問題意識を持ち、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望ましい**。

■ このような企業文化を根付かせるためには、経営者やプライバシー保護責任者が発信し続けるなど、継続的な取組が必要。こうした取組は、社内の専門人材育成の基盤となる。

＜企業文化の醸成に係る取組の例＞

- ✓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、部署異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）の対象とする

4．プライバシーガバナンスの重要項目（4.4消費者とのコミュニケーション）

1. 本ガイドブックの位置づけ

2. ガイドブックの前提
- 2.1　Society5.0の時代における企業の役割
- 2.2　プライバシーの考え方
- 2.3　企業のプライバシーガバナンスの重要性

3. 経営者が取り組むべき三要件
- 3.1　プライバシーガバナンスに係る姿勢の明文化
- 3.2　プライバシー保護責任者の指名
- 3.3　プライバシーへの取組に対するリソースの投入

4. プライバシーガバナンスの重要項目
- 4.1　体制の構築
  - 4.1.1　プライバシー保護責任者の役割
  - 4.1.2　プライバシー保護組織の役割
  - 4.1.3　事業部門の役割
  - 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
- 4.2　運用ルールの策定と周知
- 4.3　企業内のプライバシーに係る文化の醸成
- 4.4 消費者とのコミュニケーション
  - 4.4.1　組織の取組の公表、広報
  - 4.4.2　消費者との継続的なコミュニケーション
  - 4.4.3　問題発生時の消費者とのコミュニケーション
- 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
  - 4.5.1　ステークホルダーやビジネスパートナーへの対応
  - 4.5.2　プライバシー問題の情報収集
  - 4.5.3　その他の取組

5.（参考）プライバシーリスク対応の考え方
- 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
- 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）
- 5.3　プライバシーリスク評価（PIA）

6.（参考）プライバシー・バイ・デザイン

7. おわりに

参考文献
検討体制

4．プライバシーガバナンスの重要項目（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の実施においては、消費者と継続的にコミュニケーションを行う必要がある。**消費者や社会の受け止めの変化を常に把握**するとともに、**平時の取組や**、実際の**問題発生時の対応**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。

○組織の取組の公表、広報（次頁事例①）

- **企業のプライバシー問題への考え方や、リスク管理のあり方を取りまとめ、社外に公表**。（例：**透明性レポート**）
- パーソナルデータを活用した**新規プロジェクトの実施方針や内容を、事前に公表するケースも増えている。消費者からのコメントを受け付け、検討・反映してから、事業開始するという取組も一般化しつつある**。

○消費者との継続的なコミュニケーション（次頁事例②・③）

- **機能追加や利用規約等の改訂のタイミングで、プライバシーリスクへの対応がどのように変化したのか、迅速に、分かりやすくWebサイト等でお知らせ**する。**情報更新時には利用者へのプッシュ通知を行う**など、**企業から消費者への積極的なアプローチを継続**することが大切。
- プライバシーは変化しうるため、**消費者の意識について、各種消費者との接点から把握するよう努める必要**がある。**プライバシー問題に係る意識調査等を継続的に行い、取組に反映させる**ことも一つの方法。

○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た場合に備え、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**。
- 漏えい等の実害を受けた消費者に対しては、**発生している事象の内容・原因・対応状況などを、謝罪と共に分かりやすく伝える必要**がある。
- **二次被害発生のおそれがある消費者に対しては、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、個別の通知を行う**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ため、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。

4．プライバシーガバナンスの重要項目（4.4消費者とのコミュニケーション）

企業における取り組み事例

事例①：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

事例②：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。

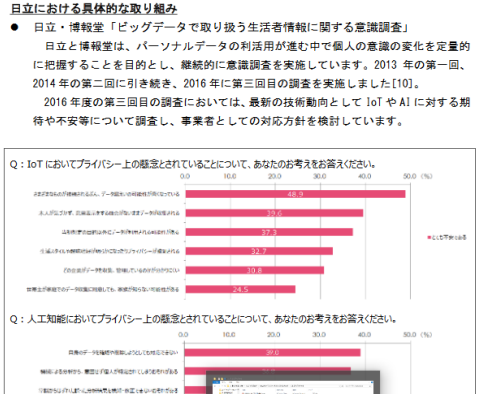
（出典）https://datadashboard.front.smt.docomo.ne.jp/

事例③：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



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

4．プライバシーガバナンスの重要項目（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）

1. 本ガイドブックの位置づけ

2. ガイドブックの前提
- 2.1　Society5.0の時代における企業の役割
- 2.2　プライバシーの考え方
- 2.3　企業のプライバシーガバナンスの重要性

3. 経営者が取り組むべき三要件
- 3.1　プライバシーガバナンスに係る姿勢の明文化
- 3.2　プライバシー保護責任者の指名
- 3.3　プライバシーへの取組に対するリソースの投入

4. プライバシーガバナンスの重要項目
- 4.1　体制の構築
  - 4.1.1　プライバシー保護責任者の役割
  - 4.1.2　プライバシー保護組織の役割
  - 4.1.3　事業部門の役割
  - 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
- 4.2　運用ルールの策定と周知
- 4.3　企業内のプライバシーに係る文化の醸成
- 4.4 消費者とのコミュニケーション
  - 4.4.1　組織の取組の公表、広報
  - 4.4.2　消費者との継続的なコミュニケーション
  - 4.4.3　問題発生時の消費者とのコミュニケーション
- 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
  - 4.5.1　ステークホルダーやビジネスパートナーへの対応
  - 4.5.2　プライバシー問題の情報収集
  - 4.5.3　その他の取組

5.（参考）プライバシーリスク対応の考え方
- 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
- 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）
- 5.3　プライバシーリスク評価（PIA）

6.（参考）プライバシー・バイ・デザイン

7. おわりに

参考文献
検討体制

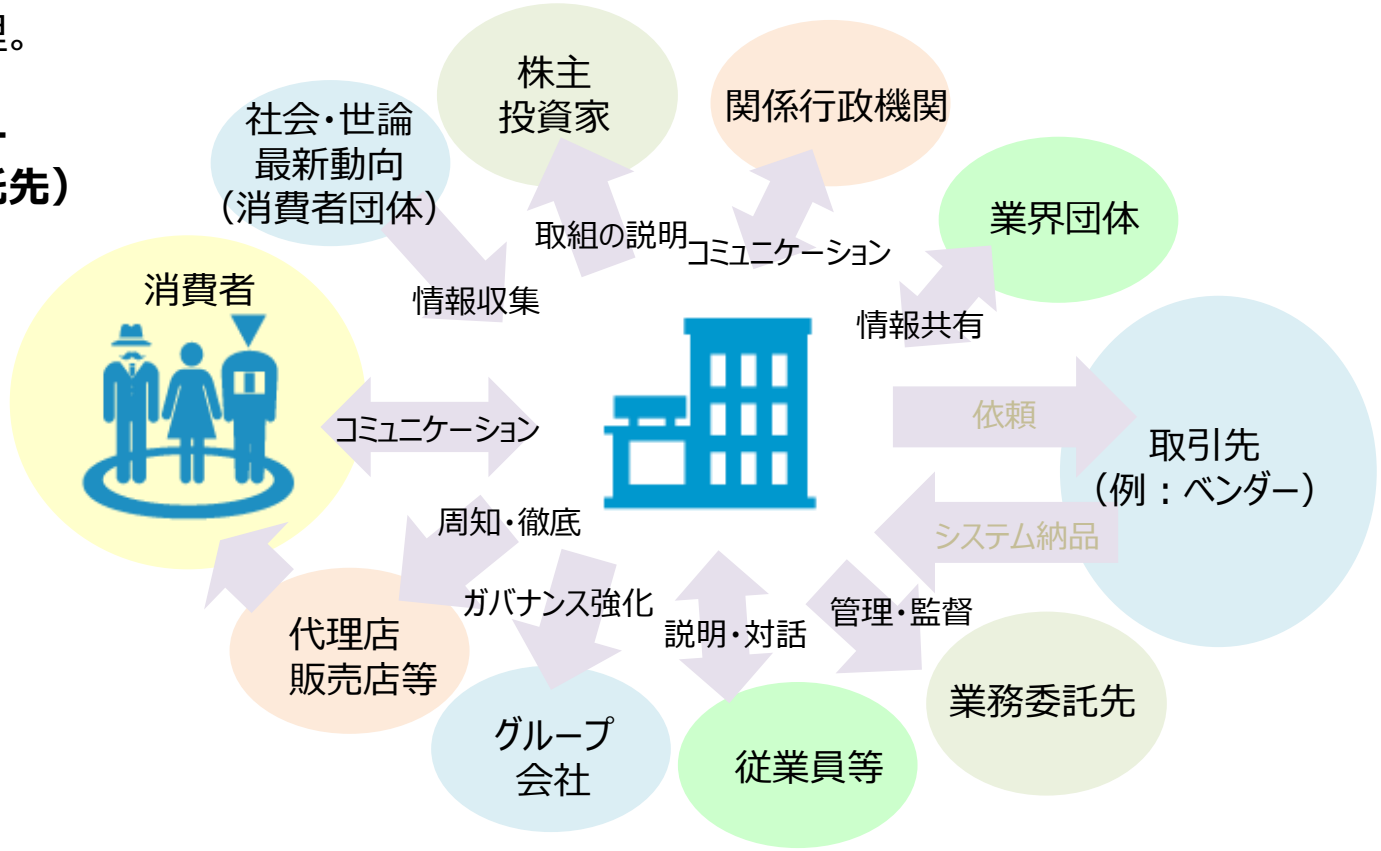
4．プライバシーガバナンスの重要項目（4.5その他のステークホルダーとのコミュニケーション）

■ ステークホルダーと継続的にコミュニケーションをとり、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**。

○ステークホルダーへの対応

以下についてそれぞれ整理。

（1）ビジネスパートナー
（取引先・業務委託先）
（2）グループ企業等
（3）投資家・株主
（4）関係行政機関
（5）業界団体
（6）従業員等



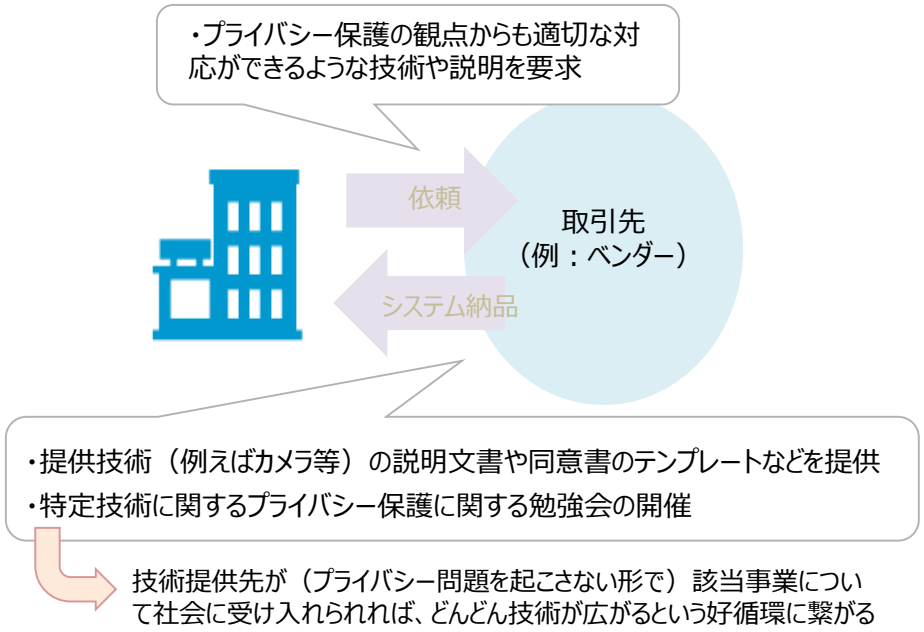
4．プライバシーガバナンスの重要項目（4.5その他のステークホルダーとのコミュニケーション）

（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も含めてプライバシー問題に適切に対応しなければ、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・対応することが望ましい。**

■ **発注側は、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）に要求。取引先は、発注側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の提供や、発注側の理解を深めるための勉強会の開催**も有効。発注側のサービスがプライバシー問題を起こさず社会に受容されることで、取引先の技術もさらに普及するという好循環につながる。



■ 業務を他社に委託する場合、**問題が生じたときには委託元にも責任が発生**。適切な対応ができる委託先を選び、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。同時に、委託元のプライバシーへの取組を高めるよう、委託先の協力も重要。プライバシー問題の発生時には委託元が顧客や消費者に対して真摯に対応する必要がある。

4．プライバシーガバナンスの重要項目（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）

（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も意識する必要がある**。
- 海外に拠点がある場合には、国ごとに対応が必要であることに注意。

（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、コストではなく先行投資として評価する傾向**がみられる。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を明確に説明することがますます求められる。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に。

（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。

（5）業界団体

- 業界によっては、**事業の健全な発展を図り、消費者の理解を醸成するため**、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。
- **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**。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。

（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にも配慮が必要**。他方で、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や、従業員に関する情報の漏えいのリスクも存在。
- このため、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。
- 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。

5.（参考）プライバシーリスク対応の考え方～6．（参考）プライバシー・バイ・デザイン

1. 本ガイドブックの位置づけ

2. ガイドブックの前提
- 2.1　Society5.0の時代における企業の役割
- 2.2　プライバシーの考え方
- 2.3　企業のプライバシーガバナンスの重要性

3. 経営者が取り組むべき三要件
- 3.1　プライバシーガバナンスに係る姿勢の明文化
- 3.2　プライバシー保護責任者の指名
- 3.3　プライバシーへの取組に対するリソースの投入

4. プライバシーガバナンスの重要項目
- 4.1　体制の構築
  - 4.1.1　プライバシー保護責任者の役割
  - 4.1.2　プライバシー保護組織の役割
  - 4.1.3　事業部門の役割
  - 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
- 4.2　運用ルールの策定と周知
- 4.3　企業内のプライバシーに係る文化の醸成
- 4.4 消費者とのコミュニケーション
  - 4.4.1　組織の取組の公表、広報
  - 4.4.2　消費者との継続的なコミュニケーション
  - 4.4.3　問題発生時の消費者とのコミュニケーション
- 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
  - 4.5.1　ステークホルダーやビジネスパートナーへの対応
  - 4.5.2　プライバシー問題の情報収集
  - 4.5.3　その他の取組

5.（参考）プライバシーリスク対応の考え方
- 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
- 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）
- 5.3　プライバシーリスク評価（PIA）

6.（参考）プライバシー・バイ・デザイン

7. おわりに

参考文献
検討体制

以下Webサイトより「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」の本文及び概要資料を公表しています。

- 経済産業省ニュースリリース
「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」を策定しました
https://www.meti.go.jp/press/2020/08/20200828012/20200828012.html

- 総務省ニュースリリース
「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」の公表
https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000098.html

- IoT推進コンソーシアムホームページ
http://www.iotac.jp/wg/data/govenance/

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の概要

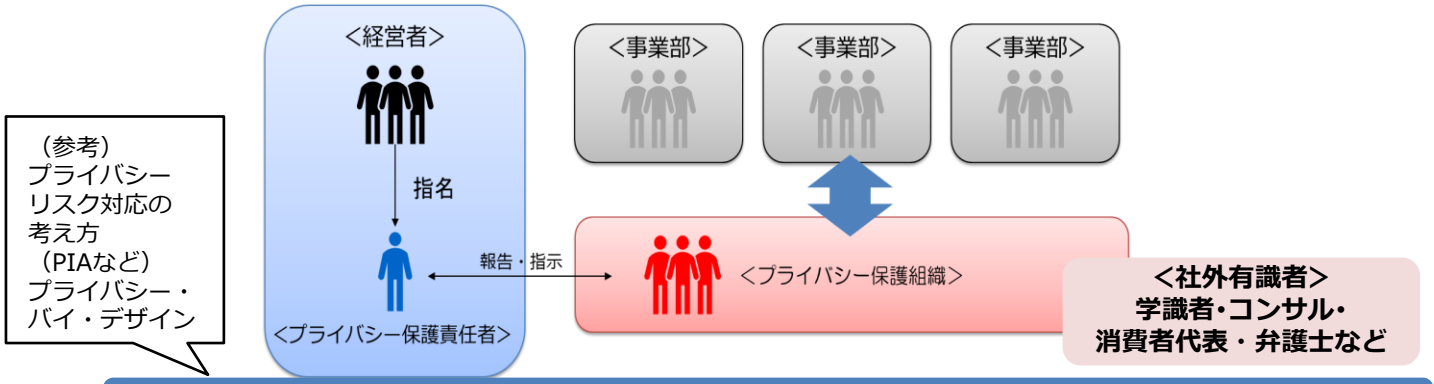
【対象読者】パーソナルデータを利用した製品・サービスを提供し、消費者のプライバシーへの配慮を迫られることが想定される企業や、そのような企業と取引をしているベンダー企業等であって、
①**企業の経営陣**または**経営者へ提案できるポジションにいる管理職**等
②**データの利活用や保護に係る事柄を総合的に管理する部門**の責任者・担当者　など

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

ご清聴ありがとうございました