2022年 日本：ステークホルダー・エンゲージメントプログラム
第４回（6月9日開催）

テクノロジーの進化と人権課題

プライバシーガバナンスの取組みによる企業価値向上

若目田 光生

株式会社日本総合研究所 創発戦略センター シニアスペシャリスト

若目田 光生（わかめだ みつお）

- 株式会社日本総合研究所
  創発戦略センター シニアスペシャリスト
  兼 リサーチ・コンサルティ ング部門 上席主任研究員
- 一般社団法人日本経済団体連合会
  デジタルエコノミー推進委員会 企画部会 データ戦略WG 主査
- 一般社団法人データ社会推進協議会 理事 利活用促進委員長
- 慶應義塾大学 グローバルリサーチインスティテュート 客員所員
- 文部科学省 科学技術・学術審議会 専門委員

1988年NEC入社。金融機関向けITソリューションのエキスパートとして、 大規模システムや新規サービスの開発を担当した後、全社のビジネスインキュベーション、ビッグデータ事業の立上げに従事。

AIやデータ利活用の推進に従事する反面、プライバシーや人権課題の重要性を強く認識、専門組織（デジタルトラスト推進本部）を立上げると共に社内外への発信、啓発、政策提言を開始。

現在は、 経団連データ戦略WG主査、データ社会推進協議会理事などの活動を通じ国のデータ流通政策に関わるとともに、日本総研において官民データ流通に関するコンサルティングに従事する。

テクノロジーの進化と人権課題

「エリーの個人情報オークション」

アップルが新CM　プライバシー保護は守りではなく差別化戦略

プライバシーは、基本的人権です。そして、Appleの中心にある大切な理念の一つです。あなたのデバイスは、毎日様々な場面で重要な役割を果たしていますが、どの体験を誰と共有するかは自分自身で決めるべきこと。私たちは、あなたのプライバシーを守り、自分の情報を自分でコントロールできるようにApple製品を設計しています。簡単なことではありませんが、それが私たちの信じるイノベーションだからです。

・Safariは追跡者からあなたを守ります。

・マップなら残る履歴は思い出だけ。

・写真アプリでは、あなたの写真を誰と共有するか、あなたが管理できます。

・Siriが学習するのはあなたが知りたいこと。あなた自身のことではありません。

・WalletとApple Payは、購入履歴を隠します。

・メッセージを見られるのは、送った人と送られた人だけ。

・ヘルスケアアプリなら、あなたの記録はあなただけのもの。

https://www.youtube.com/watch?v=T4bXwdyfb6Q

内定辞退率予測による差別的扱い

- リクルートキャリア社が提供している就活情報サイトとして有名な「リクナビ」。同サイトは、就活用「情報プラットフォーム」として機能し、全国80万人の学生が利用している。
- 就活学生が企業の情報収集をする際の閲覧履歴を収集し、AIが分析。
- 企業ごとに選考や内定辞退率を予測し、内定辞退率を五段階で算定し、学生の氏名と結びついたそのデータを就活学生側に十分な説明なしに、38社の企業に販売していた。
- 基本的には、事後分析用で採用判断には用いられていないとのことだが内定辞退率が高いとAIに「予測」された学生は、企業側から不利に（差別的に）扱われたのではないかとの懸念。
- 後日、個人情報保護委員会が個人情報保護法に基づきリクルートキャリアとリクルート社、及びサービス利用企業に対し是正勧告を、厚生労働省が職業安定法に基づき行政指導を行っている。
- 職業安定法3条　「何人も、人種、国籍、信条、性別、社会的身分、門地、従前の職業、労働組合の組合員であること等を理由として、職業紹介、職業指導等について、差別的取扱を受けることがない。」

顔識別機能付き防犯カメラの利用に関する国内外動向

①大阪ステーションシティ「ICT技術の利用実証実験」

- 2014年情報通信研究機構（NICT)はJR大阪駅一帯の商業ビル・公共空間において、監視カメラから取得する画像データと顔識別技術をもとに人流解析を行う実証実験を予定。準公共空間でのデータ取得や不正取得、実証実験の回避等の市民からの懸念を理由に延期となった。

②札幌市「札幌市ICT活用戦略」

- 札幌市が行う実証事業（2016～18年度）にて、個人の特徴や希望に合った情報を発信することにより効果的なマーケティングまたは防災、防犯対策等を目的として、顔識別カメラや人感センサー・デジタルサイネージ等のICT機器の設置を検討。顔識別カメラのプライバシー侵害や情報流出等の市民の不安が高まったことから、顔識別カメラは設置しない計画となった。

③渋谷書店万引対策共同プロジェクト

- 渋谷駅周辺の3書店が2019年7月より、書店内において発生する万引き、盗撮、器物損壊、暴行・傷害、公然わいせつに当たる犯罪の防止を目的として、個人情報保護法の「共同利用」に基づいて、参加店舗間で万引き等を実行した対象者等に関する情報を共有。

④JR東日本「不審者・不審物検知機能を有した防犯カメラの導入」

- JR東日本が東京オリンピック・パラリンピックを控えた2021年7月よりセキュリティ向上の取組として、首都圏の一部の駅に、不審者等の検知機能（うろつきなどの行動解析、顔識別技術）を有した防犯カメラを導入。

第1回犯罪予防や安全確保のためのカメラ画像利用に関する有識者検討会（資料３より引用）

https://www.ppc.go.jp/files/pdf/20220128_shiryou-3_doukou.pdf

顔識別機能付き防犯カメラの利用に関する国内外動向

EUのAI規則案

- 欧州委員会は2021年４月21日付でAI規則案を公表。
- 同規則案は、AIを①受容できないAI、②ハイリスクAI、③透明性義務を伴うAI、④極小リスク／リスクなしAIの４つのカテゴリーに分類した上で、使用方法について規定するものであり、①は原則禁止、②は要件と事前適合性評価の準拠を条件に許可、③は情報／透明性の義務を条件に許可、④は制限なし、という原則を規定している。
- 法執行の目的により公の場所において遠隔地からのリアルタイム生体識別システムを使用する行為は①として、一定の例外の除いて禁止されている。これ以外の遠隔地からの生体識別に使用することを目的としたAIシステムは②として、要件と事前適合性評価の準拠を条件に許可されている。

欧州評議会 顔認証に関するガイドライン

- 欧州評議会は2021年1月28日に、「Guidelines on Facial Recognition」（顔認証に関するガイドライン）を公表。
- 顔認証は、管理された環境下でのみ行われるべきであり、マーケティング目的や私的なセキュリティ目的のために、ショッピングモールのような管理されていない環境では、顔認証技術を使用すべきではないとしている。

顔識別機能付き防犯カメラの利用に関する国内外動向

世界プライバシー会議（GPA） 顔認証技術に関する決議

決議前文において、以下のとおり述べている（一部抜粋）。

- ✓ 顔認証技術の能力は重要であり、その潜在的な応用がセキュリティと公共の安全に利益をもたらす可能性がある。
- ✓ 顔認証技術は、広範な監視を可能にし、侵入的で、偏った結果を提供し、データ保護、プライバシー及び人権を侵害する可能性がある。
- ✓ 顔認証技術はユニークで永続的なセンシティブな生体情報に依存しており、個人に関する決定は潜在的に本人の認識や同意なく行われるため、適切な救済手段がなければ不利益をもたらす可能性がある。
- ✓ 個人を誤って識別又は認証する可能性若しくは識別又は認証できない可能性がある。
- ✓ 顔認証技術の利用が進化し、予期せぬ方法で利用されたり、他の技術的能力と結びつき、個人や社会の信頼に危害を加える可能性がある。
- ✓ 本人の認識又は同意なく様々な公開又は非公開ソースから情報が集められた大規模データセットが作成され、新しい又は予期せぬ文脈で商業的に利用することが可能である。
- ✓ 顔認証技術の広範な使用は、差別的効果を伴い、表現の自由や結社の自由といった基本的人権の行使に影響を与える可能性がある。

顔認証に関する世界の法制化動向

2019年5月、米国サンフランシスコ市では、警察含めた行政機関による顔認証の技術の利用を禁止する条例を可決。顔認証ツールによる犯罪者の検挙への活用ができな いことに。

フェイスブックがイリノイ州の生体認証情報プライバシー法に違反するとしてイリノイ州の住民が、 米国最高裁判所にて、フェイスブックに対する集団訴訟を起こす。

2019年、マサチューセッツ州で 複数の市で顔認証技術に関する禁 止条例が可決される。12月には3 つ目の行政であるノーサンプトン 市にてサーベイランスへの使用禁 止が可決。

2019年8月、スウェーデンの情報 保護局では、EUのGDPRへの違反 として顔認証技術を活用して学校 に対して初の罰金(20万クロー ネ)を科した。生徒と保護者から の同意は得ていたが、学校との力 関係が適切でない、との判断。

英国の情報関連当局にて、ロンドンにおける顔認証技術のライブ調査を始める。

2019年、EUが顔認証技術に対し てより厳しい法案の方向性の検討 を開始。2020年1月には、3年から5年の公的な場所(駅やスタジアム、ショッピングセンター等)での使用を仮に禁止する案が検討されている。

技術による人権侵害懸念に対するNGOの指摘

国・対象	概要
アメリカ （2018） 顔照合技術	アマゾンの顔認証システムに対し、法執行機関に利用されれば人権侵害となる恐れがあるとして、米自由人権協会（ACLU）など複数のNGOが販売中止を要求。人種によって認識の正確さに偏りがある点について「差別助長」との指摘。
カナダ （2019） スマートシティ	グーグル子会社のサイドウォーク・ラボが主導するトロントのスマートシティの計画中止を求めて、カナダ自由人権協会は国、州、市をに対し訴訟を起こした。「カナダはグーグルの実験用マウスではない」と公衆監視の強化を懸念。
アメリカ （2019） AI採用ツール	米人権NGO「EPIC」は、AIを使った企業向け採用支援ツールが「不公平で欺瞞的な」行為に当たるとしてFTCに調査を要求。偏った学習よるアルゴリズムが、白人や男性などの応募者を選ぶ可能性がより高くなる「差別助長」への懸念。
アメリカ （2018） 再犯スコア	ACLUや全米黒人地位向上協会（NAACP）など人権NGOが、AIで被告人の詳細プロフィールから予測する「再犯スコア」の使用に反対する声明文に署名した。既存のバイアスを拡大させ、特に低所得者などが再犯率が高いと評価されることへの懸念。

いわゆる炎上事案

JR大阪駅 市民の不安受け、顔認証の追跡実験を延期（2014年3月）

大阪ステーションシティ実証概要

- 2014年4月から2年間を予定
- 大阪駅ビル構内にカメラ92台を設置
- 独立行政法人情報通信研究機構NICT
- 通行人の顔映像を特徴情報に処理し、特徴情報で行動を追跡することにより、シティ内の人の流量や滞留の度合い等を把握し、災害発生時の安全対策等への利用可能性を検証する実証実験を計画。

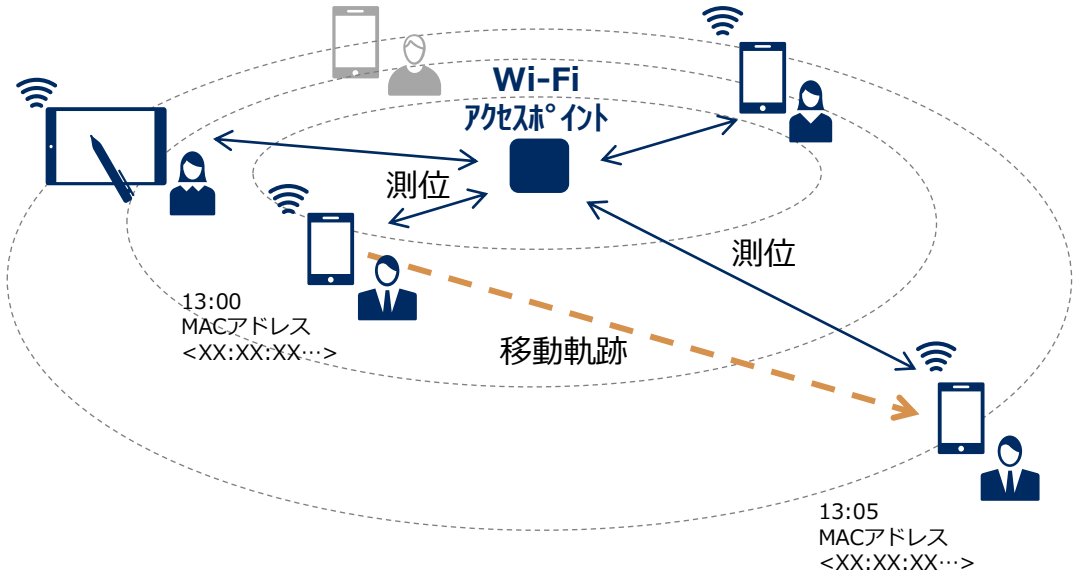
社会的批判と第三者委員会の提言

- 市民や有識者ら不安の声や中止の要請が寄せられ、実験は延期。第三者委員会を設置
- 第三者委員会の提言
  1. 実験手順や実施状況等を定期的に確認し公表すること
  2. 個人識別のリスクを市民に対して事前に説明すること
  3. 撮影を回避する手段を設けること
  4. 映像センサーの存在と稼働の有無を利用者に一目瞭然にすること
  5. 人流統計情報の提供に際しては委託契約又は共同研究契約を締結すること
  6. 安全管理措置を徹底すること
  7. 本実証実験に関して適切な広報を行うこと

識別できる情報への誘惑（例：MACアドレスの取り扱い）

Wi-Fiアクセスポイントによるセンシング

- Wi-Fi機能がONの状態のスマートフォン等の台数
- スマホ等の位置情報および動線
  （Wi-Fi電波強度、時間等から計測）



*例: グランフロント大阪における実証実験　http://www.festival-project.eu/ja/?p=1502

総務省「位置情報プライバシーレポート」

- MACアドレスは、単体では個人識別性を有しない
  （英数字の羅列（例：「A0：B1：C2:...」））
- しかし、同一ＩＤに紐付けて行動履歴や位置情報を集積する場合は、個人情報に準じた形で取り扱うことが適切

  ＜理由＞
  - 実質的に特定の個人と継続的に結びついている
    （原則として利用者側では変更困難なもの）
  - 同一ＩＤに紐付けて行動履歴や位置情報を集積する場合、プライバシー上の懸念がある

ダークパターン

「ユーザーが無意識に、自身に不利な行動を取るように誘導するデザイン」オンラインサービスの進展し、日本では違法とは言えないが、ナッジによる行動変容などの施策含めサービスデザインとして慎重な対応が求められる。

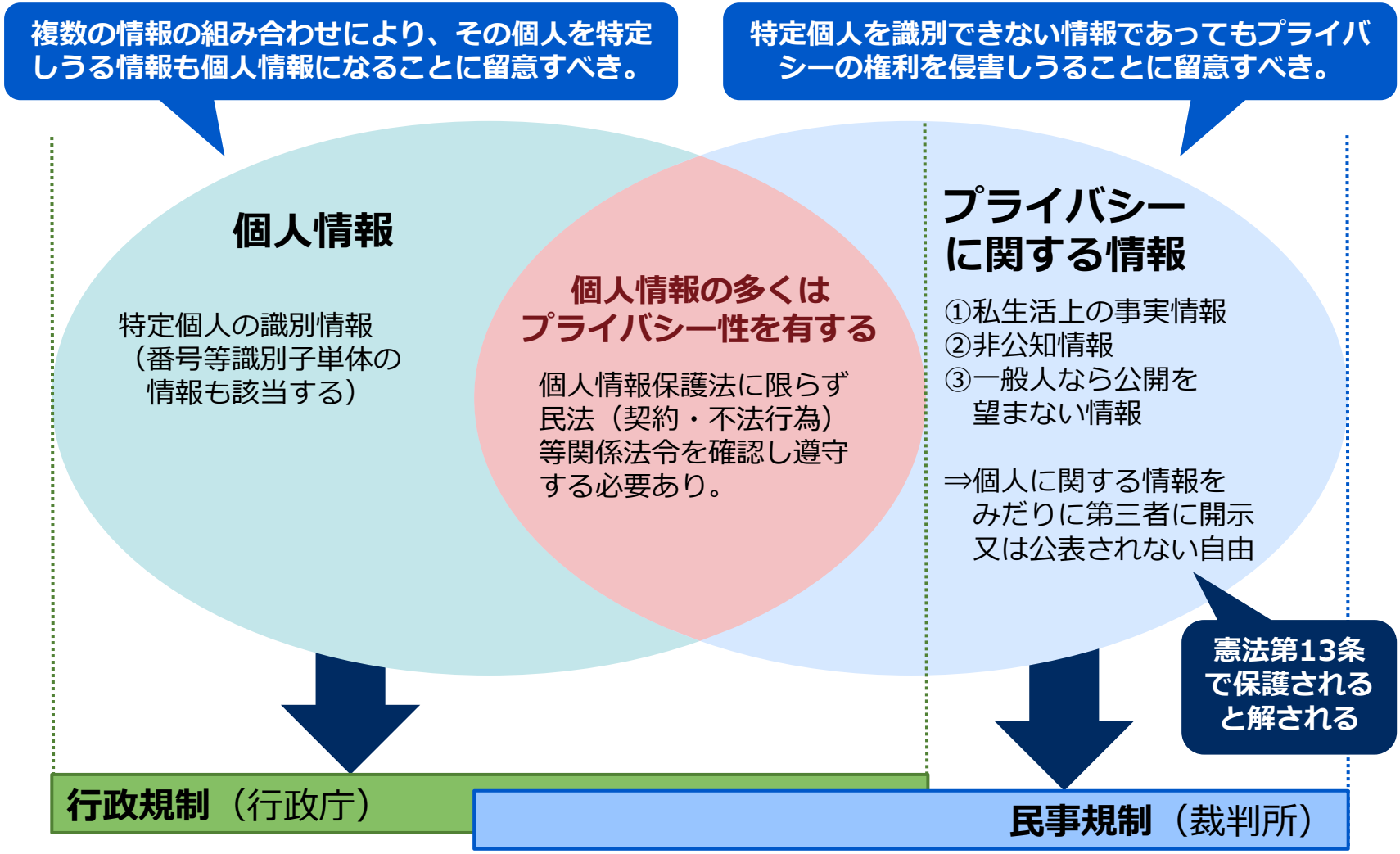
- **A. Sneaking（こっそり）**：ユーザーが気付かないうちに何かを買わせるやり方。定期購買であることがわかりにくい表示になっており、サブスクリプションに誘導するケースなど。
- **B. Urgency（緊急）**：ショッピングサイトなどで割引の期限を表示し、急いで買わないと損をすると思わせる手口。
- **C. Misdirection（誘導）**：購入するかどうかの選択画面で「Yes」を強調して「No」を押しにくくするなどのビジュアルインターフェイスや、個人情報の提供に関する説明文を二重否定などを多用した回りくどくわかりにくい文章にすることで、読まずにチェックを入れさせようとする手法。
- **D. Social Proof（社会的証明）**：「今このサイトを見ている人が○○人います」といった表示を行い、判断にプレッシャーをかける、虚偽の「お客様の声」を掲載する、お客様と称してAIが生成した人工の顔写真を掲載するなど。
- **E. Scarcity（欠乏）**：商品の在庫を少なく表示したり、期間限定であることを強調したりして、購買意欲を高める施策。「人気商品につき売り切れる可能性が高い」という文言など。
- **F. Obstruction（妨害）**：よくある例としては、キャンセルをしにくくする方法。サブスクリプションなどの解約希望者に対し、幾重にもページを経由させ、複雑な手続きを要求する方法など。
- **G. Forced Action（強制）**：ECサイトの閲覧に個人情報の入力を求めるなど、行動を強制する設計になっているもの。

技術の進化と人権懸念

魅力的な新技術であっても、多くは使い方を誤ると人権侵害につながるリスクがある。

- VIP検知
- 不審行動予測
- キャッシュレスデータ活用
- 視線検知、分析
- AI人事評価、人員配置
- 性別、年齢など属性推定
- 感情分析
- 教育ログ分析
- リモートワーク監視、働きぶり（集中力）可視化
- ドローンカメラ
- 人のデジタルツイン化

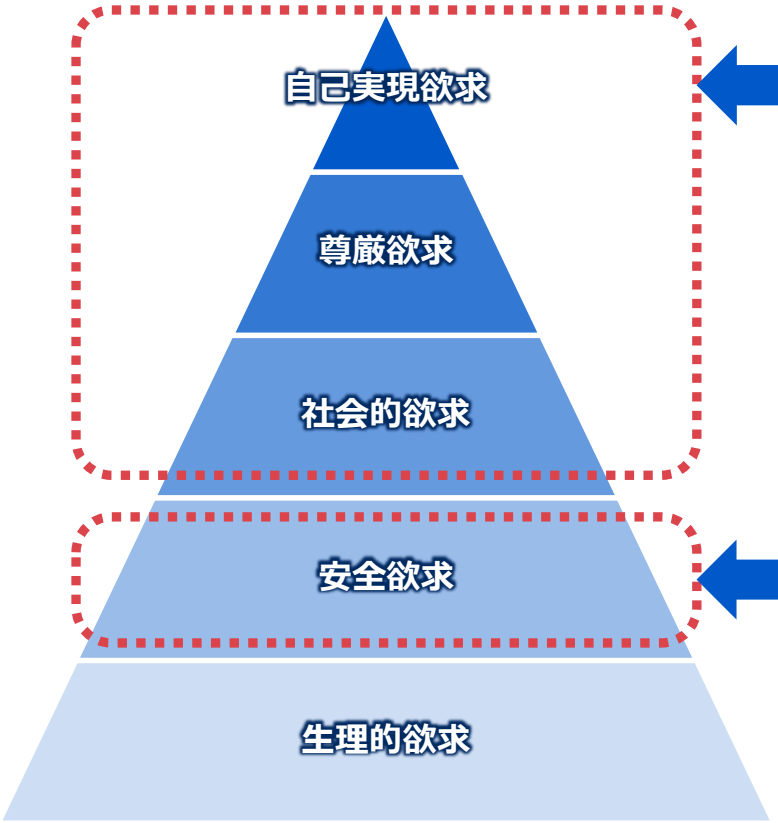
個人情報とプライバシーの違い



引用：個人情報保護法制の概要（新潟大学法学部　鈴木正朝教授）

情報セキュリティとプライバシーの違い

マズローの欲求五段階説



プライバシー対策

生活者の多様性への対応
国や地域、個人により求められる要素が異なる
（義務的要素もあるが、差別化要素、イノベーションとしての要素も大きい）

情報セキュリティ対策

サイバー犯罪から守る情報漏えいを防ぐ
（義務的・守備的要素が大きい）

技術の進化とグローバル目線の人権配慮の必要性

プライバシー保護としての配慮要素の拡大や、AIや顔照合技術、センシング施術などデジタルの進化と共にプライバシーに留まらないリスクへの対応が求められる。また、経済安全保障や環境など他の要件との関連も深く人材育成や組織役割やプロセス見直しも求められる。

- デジタルインクルージョン　弱者やマイノリティ、デジタルディバイドへの対応、プライバシー通念の多様性への対応
- 各国のデータ政策やガバメントアクセスの多様性への対応
- 優位的地位の乱用へ該当するリスクへの対応
- 業界やサービスにおける社会通念やレピュテーションへの対応
- 消費者の権利に対する配慮
- 国連「ビジネスと人権に関する指導原則」への対応
- 技術による人種差別懸念への対応
- コーポレートコミュニケーション、メディア報道の過程のリスクへの対応
- 環境や循環社会、公衆衛生、安全保障等の要請への対応

DX時代におけるプライバシーガバナンスガイドブック

企業によるプライバシーへの対応が求められる背景

＜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がある。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**プライバシー影響評価（PIA）の実施などの自主的取組が推奨**されている。

企業によるプライバシーへの対応が求められる背景

＜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。

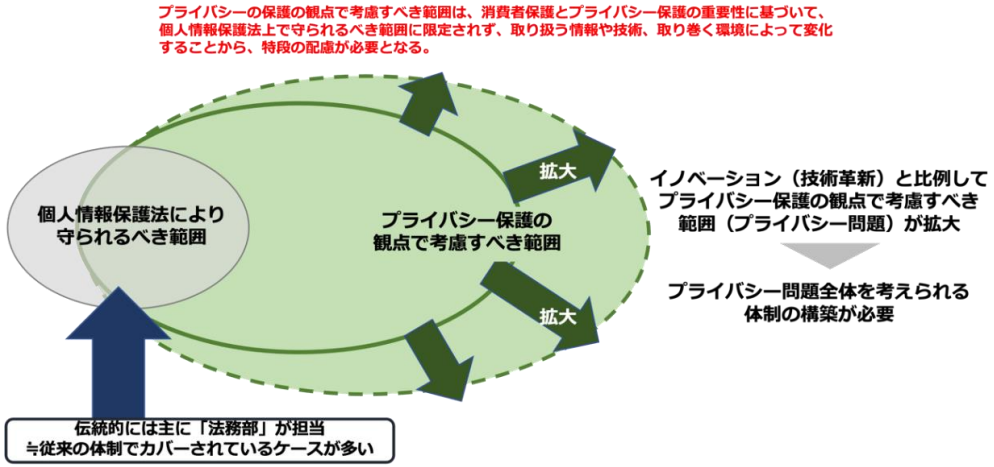
＜国内動向
：グローバルで活躍する国内企業の動き、個人情報保護法制度改正等への対応＞

- 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がある。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**プライバシー影響評価（PIA）の実施などの自主的取組が推奨**されている。

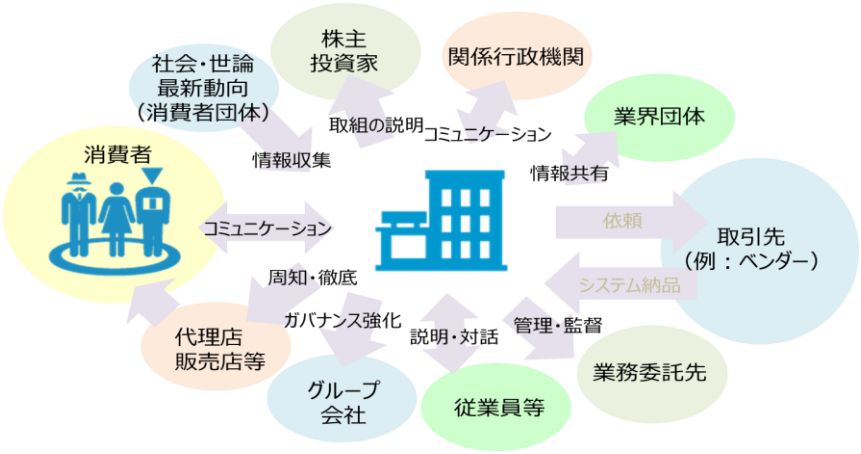
プライバシー対応に関する企業内ガバナンスの必要性

- 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

企業のプライバシーガバナンスモデル検討会（令和元年10月～）

	氏名（敬称略）	所属
座長	佐藤　一郎	国立情報学研究所
委員	板倉　陽一郎	ひかり総合法律事務所
委員	落合　正人	ＳＯＭＰＯリスクマネジメント株式会社
委員	クロサカ　タツヤ	株式会社企
委員	小林　慎太郎	株式会社野村総合研究所
委員	宍戸　常寿	東京大学大学院法学政治学研究科
委員	高橋　克巳	日本電信電話株式会社 NTT社会情報研究所
委員	林　達也	LocationMind株式会社／株式会社パロンゴ
委員	日置　巴美	三浦法律事務所
委員	平岩　久人	PwCあらた有限責任監査法人
委員	古谷　由紀子	公益社団法人日本消費生活アドバイザー・コンサルタント・相談員協会／サステナビリティ消費者会議
委員	村上　陽亮	株式会社KDDI総合研究所
委員	森　亮二	英知法律事務所
委員	若目田　光生	一般社団法人日本経済団体連合会／株式会社日本総合研究所

■オブザーバ
個人情報保護委員会、経済産業省 知的財産政策室、総務省 情報通信政策課、デジタル庁

■事務局
経済産業省 情報経済課、総務省 消費者行政第二課、一財）日本情報経済社会推進協会（JIPDEC）

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

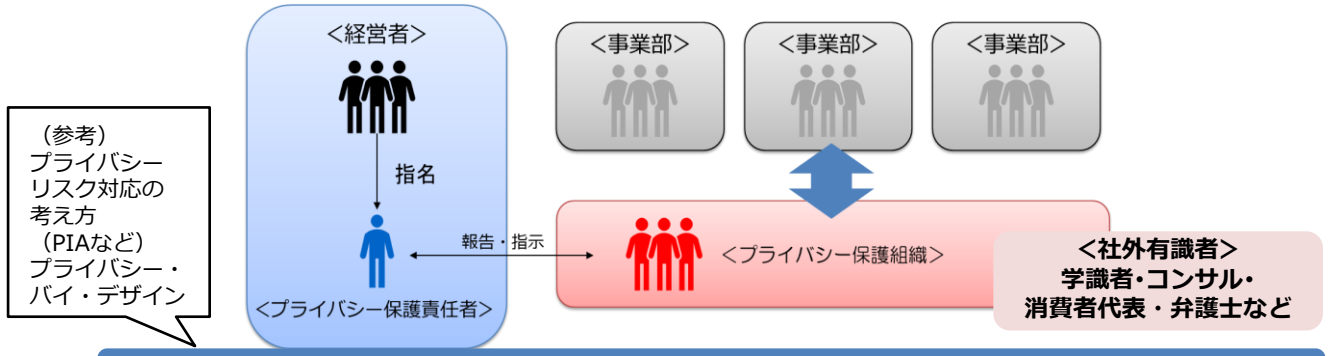
【対象読者】パーソナルデータを利活用した製品・サービスを提供し、消費者のプライバシーへの配慮を迫られることが想定される企業や、そのような企業と取引をしているベンダー企業等であって、
①**企業の経営陣**または**経営者へ提案できるポジションにいる管理職**等
②データの利活用や保護に係る事柄を総合的に管理する部門の責任者・担当者　など

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

重要項目（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

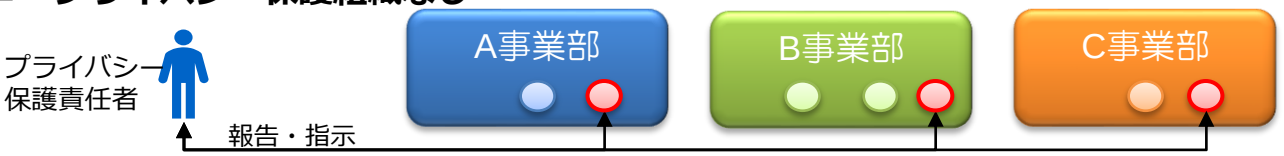
- 企業内の各部門から新規事業やサービス内容に関する**様々な情報を集約**し、**プライバシー問題が消費者や社会に発現するリスクを見つける**。そのために、各部門と日頃から接点を持つとともに、プライバシー保護組織の存在を企業内に周知徹底する必要がある。
- プライバシー問題は、個人的な感じ方の相違や、社会受容性がコンテキストや時間の経過で移り変わることから、**常に関連する情報を収集**する。
- **対象事業の目的を実現**しつつ、プライバシーリスクに対応するために、**多角的に対応策を検討**する。
- 新規事業や新規技術を開発する部門とともに、**他部門と円滑な連携を図ることが重要。**
- **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。

重要項目（体制の構築）

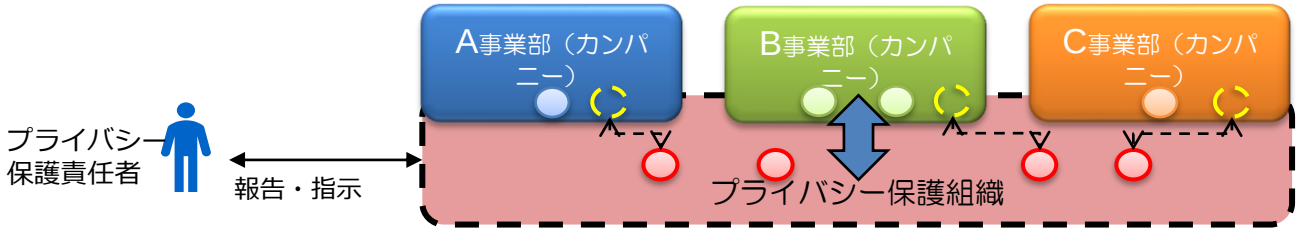
- 企業によって設置する形態は異なる。専任者の確保が困難な場合には**兼務の従業員のみで保護組織を構成するなど、自社のリソースに合わせて実効性のある組織を構築することが大切**。
- プライバシー保護組織が機能するためには、多角的な観点からなされる検討内容を取りまとめ、**複数部署の間に立って調整できる人材が不可欠**。こうした人材を配置することに加え、**プライバシー保護は高い専門性が必要であることを念頭に、中長期的な視野で人材を育成することが必要**。

<プライバシー保護組織の企業内での位置づけの例>

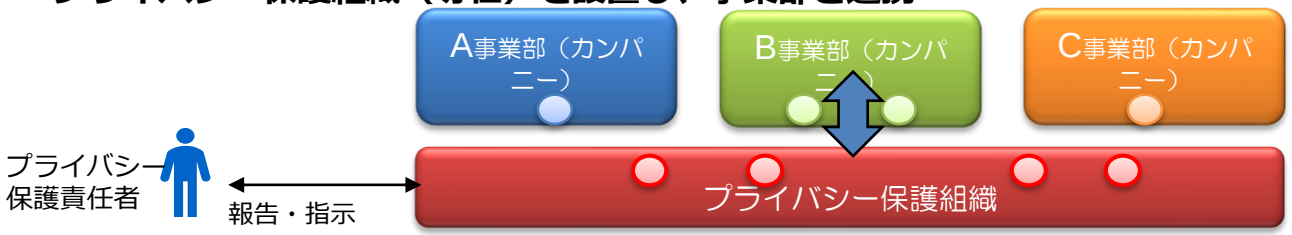
■ **プライバシー保護組織なし**



■ **プライバシー保護組織（兼務）を設置し、事業部と連携**



■ **プライバシー保護組織（専任）を設置し、事業部と連携**



重要項目（体制の構築～運用ルールの策定と周知）

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。

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。

重要項目（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

重要項目（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。

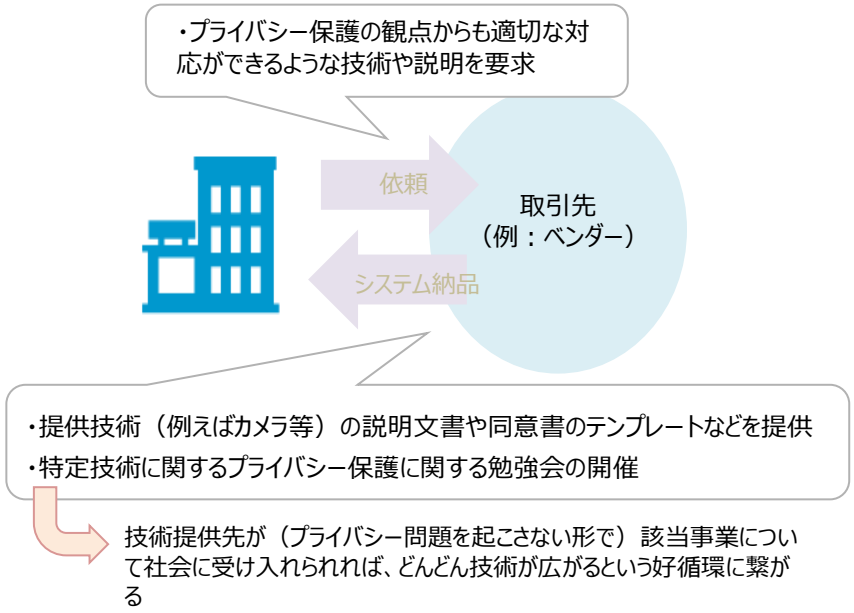
○問題発生時の消費者とのコミュニケーション

- 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。

重要項目（その他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。

重要項目（その他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。

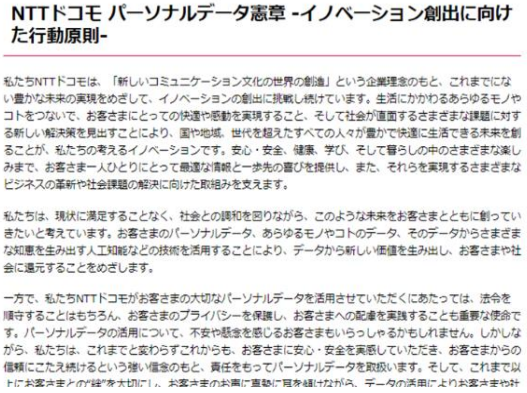
（参考）プライバシーガバナンスに係る取組の例

○プライバシーガバナンスに係る姿勢の明文化

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

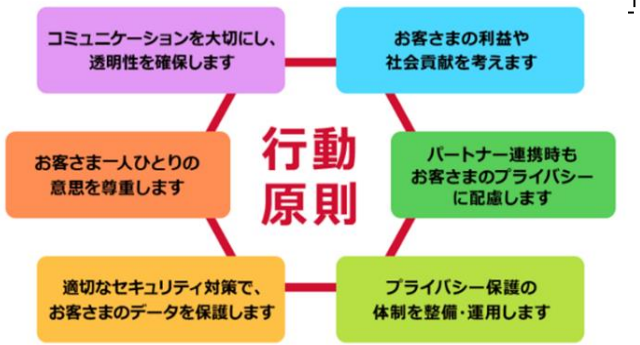
株式会社NTTドコモでは、「パーソナルデータ憲章―イノベーション創出に向けた行動原則―」を作成し、公表している。このパーソナルデータ憲章は、NTTドコモが「新しいコミュニケーション文化の世界の創造」という企業理念の下、これまでにない豊かな未来の実現をめざして、イノベーション創造に挑戦し続けていること、社会との調和を図りながら、未来をお客様と共に創っていきたいと考えていること、パーソナルデータの活用に当たり法令順守はもちろん、お客様のプライバシーを保護し、配慮を実践することも重要な使命であることなどを宣言し、行動原則として6つの原則を提示している。


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



（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

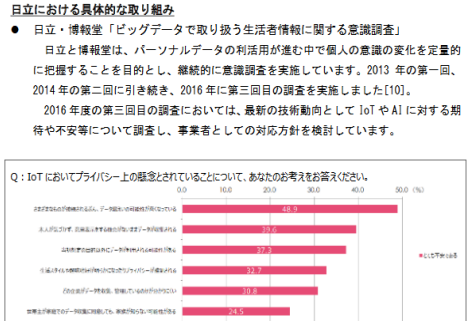
株式会社NTTドコモは、お客様自身のデータの提供先と種類の確認・変更、データ取扱いに係る同意事項の確認などの機能を提供している。

（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

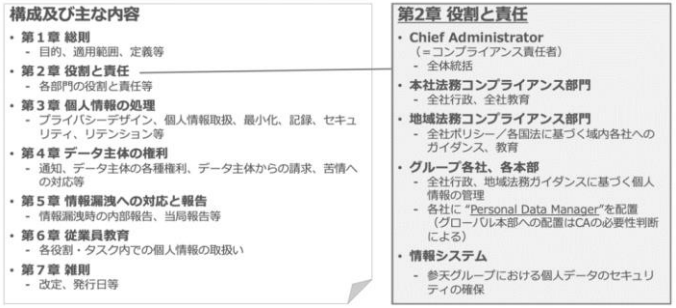
（参考）プライバシーガバナンスに係る取組の例

○体制の構築

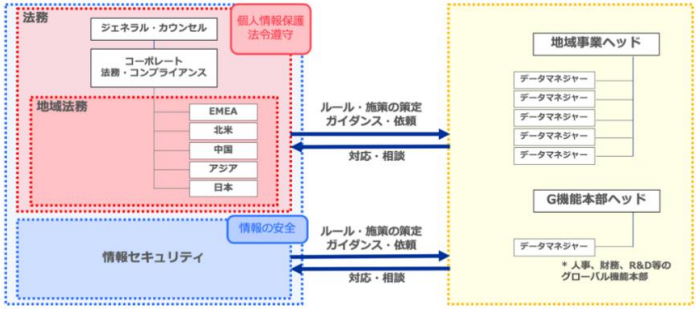
プライバシーガバナンスを機能させるには、各部門の情報を集約し、事業におけるプライバシー問題を見つけるとともに、対象となる事業の目的の実現とプライバシーリスクマネジメント を可能な限り両立させるために、対応策を多角的に検討することが必要となる。上記を実現するため、指名されたプライバシー保護責任者を中心として、中核となる組織を企業内に設けることが望ましいと考えられる。

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。



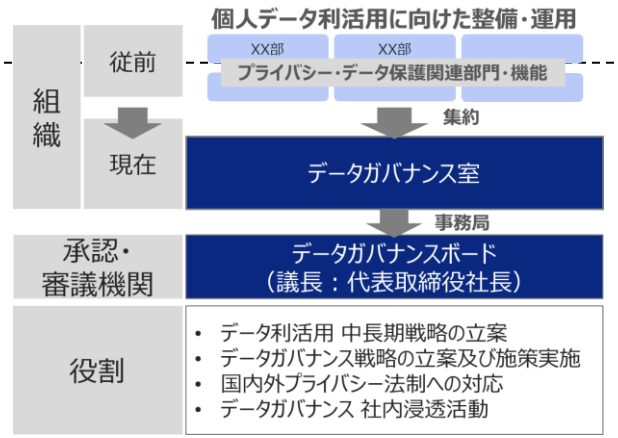
Global Data Privacy Policy（出典）（社内資料）



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）

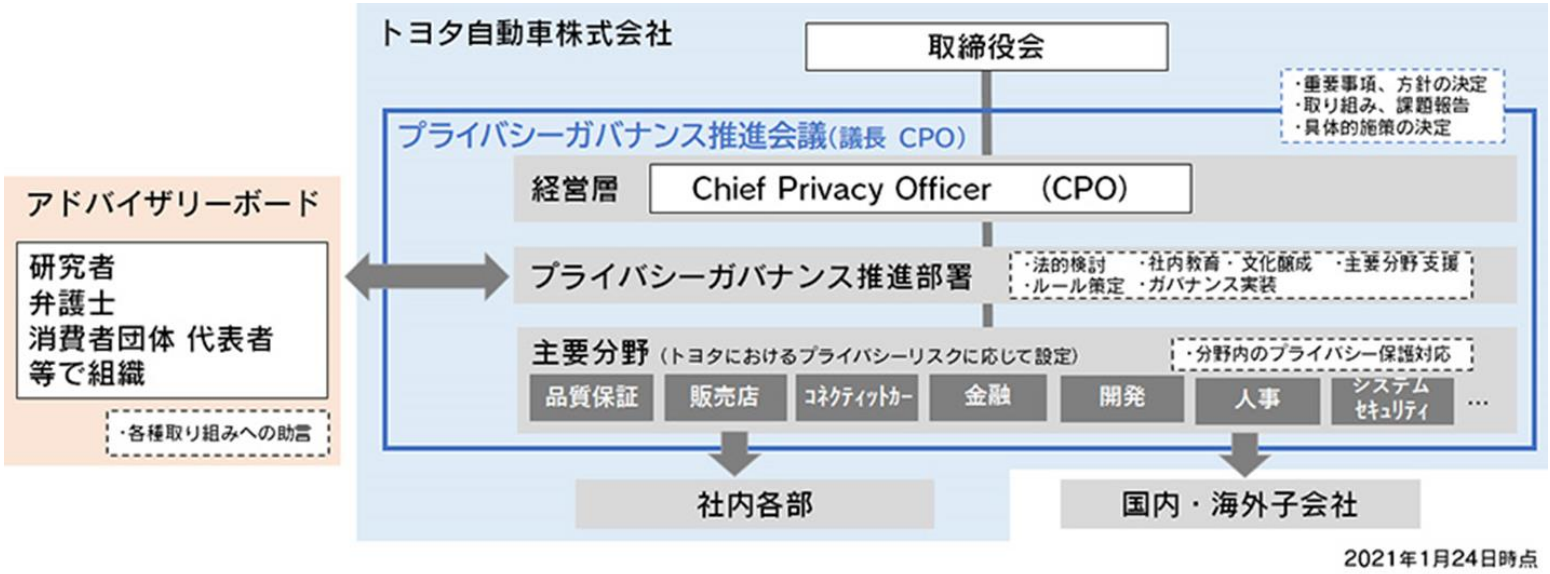
（参考）プライバシーガバナンスに係る取組の例

○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/

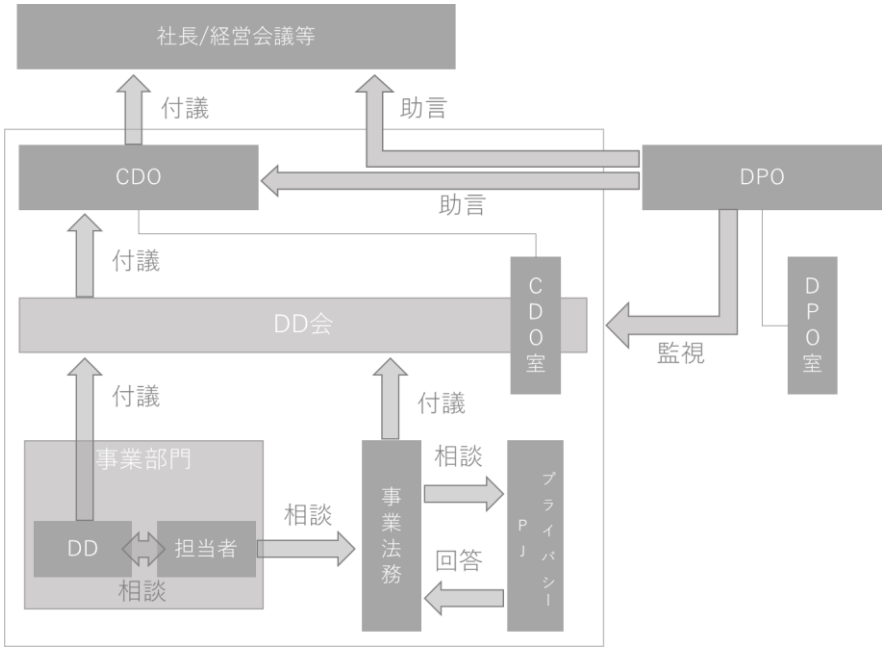
（参考）プライバシーガバナンスに係る取組の例

○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）

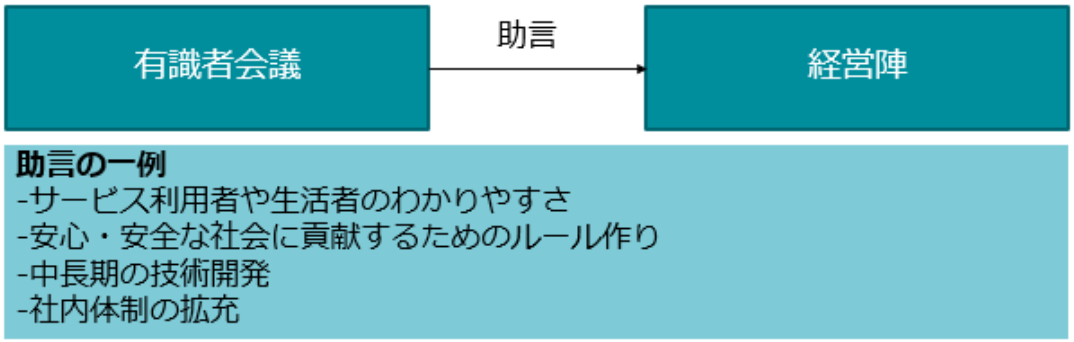
（参考）プライバシーガバナンスに係る取組の例

○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

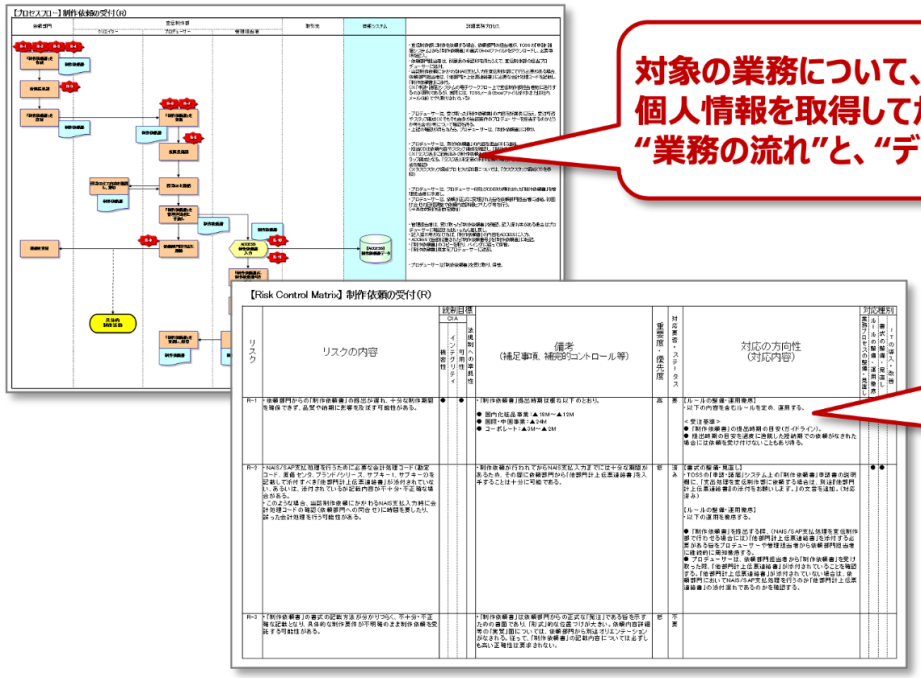
（参考）プライバシーガバナンスに係る取組の例

○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）

（参考）プライバシーガバナンスに係る取組の例

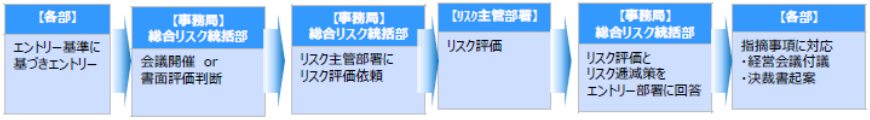
○プライバシー影響評価（PIA）

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】

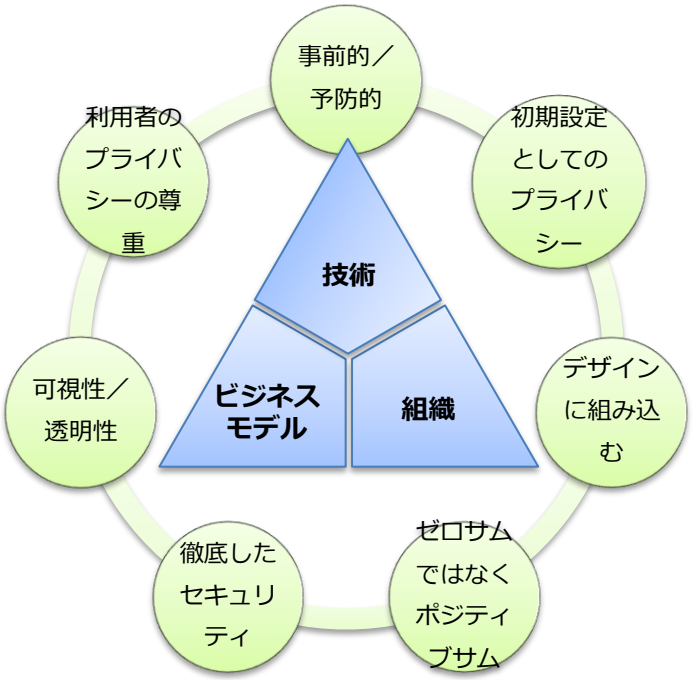
#	原則	基準
1	経緯（コンテキスト）の尊重	お客様に不安を抱かせない、予期できる範囲で利用すること
		お客様がパーソナルデータを提供した際の経緯（コンテキスト）に沿って、本人の期待と合致する形態で利活用を行うこと
2	個人によるコントロール	お客様に、自分のデータをコントロールする機会（どのように利用されるかについて関与する機会）を確保すること
		サービスに応じて、オプトイン・オプトアウトを適切に使い分けること
3	明確でわかりやすいポリシー	お客様に、何のデータをどのように使うかわかりやすく伝えること
4	プライバシー・リスクの大きさに応じた対策	データ種別ごとのプライバシー性、デー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

（参考）プライバシーガバナンスガイドブック　関連資料について

「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」の
関連資料は、以下ウェブサイトからダウンロードいただけます。ぜひご覧ください。

■「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」の公表

- 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ver1.2」を策定しました
  https://www.meti.go.jp/press/2021/02/20220218001/20220218001.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ver1.2」の公表
  https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000140.html
- IoT推進コンソーシアムWebサイト「企業のプライバシーガバナンスモデル検討会」ページからの公表
  http://www.iotac.jp/wg/data/govenance/

■「プライバシーガバナンスに関する調査結果（詳細版）」の公表

- 経済産業省ニュースリリース
  プライバシーガバナンスに関する調査結果（詳細版）を公開しました
  https://www.meti.go.jp/press/2021/03/20220318014/20220318014.html
- 総務省ニュースリリース
  プライバシーガバナンスに関する調査結果の公表
  https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000145.html
- JIPDECニュースリリース
  「プライバシーガバナンスに関する調査結果」の公開
  https://www.jipdec.or.jp/topics/news/20220318.html

■講演資料やパネルディスカッションのレポートの公表

- 「2021年度経済産業省・総務省・JIPDEC共催　企業のプライバシーガバナンスセミナー」
  第１回イベントページ（2021年7月20日）
  第２回イベントページ（2021年9月14日）
  第３回イベントページ（2022年2月25日）

技術と人権課題に対する取り組み事例

東京都の取組み（東京データプラットフォーム）

東京都が2022年度スタートを目指し取り組んでいる「東京データプラットフォーム」はプラットフォーム構築に先立ち、運営する組織が扱うデータの収集や提供・利活用に係る基本的な考え方（ポリシー）を検討

東京データプラットフォームの目的・名称

データ利活用推進のため、データ提供者・利用者をつなぐ基盤となり、流通の加速を通じて、都民のQOL向上を目指します

TDPF 東京データプラットフォーム

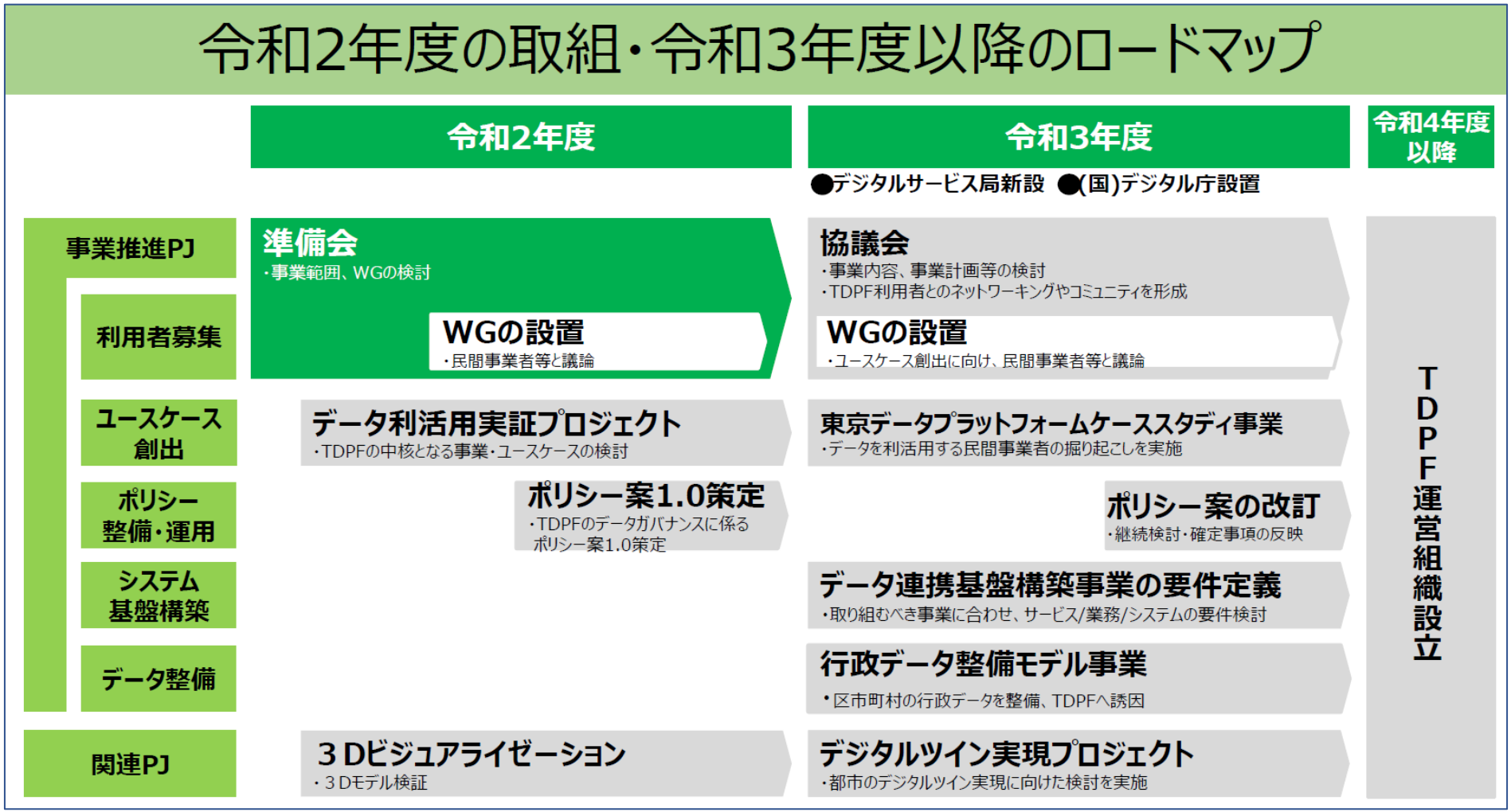
Tokyo Data Platform

略称：TDPF

「官民連携データプラットフォーム」について、
今年から新たな名称・略称を使用し、推進

https://www.digitalservice.metro.tokyo.lg.jp/society5.0/dpf_suishin_01.html
東京データプラットフォーム協議会　第1回推進会議　事務局資料より引用

東京都の取組み（東京データプラットフォーム）



https://www.digitalservice.metro.tokyo.lg.jp/society5.0/dpf_suishin_01.html
東京データプラットフォーム協議会　第1回推進会議　事務局資料より引用

東京データプラットフォームのポリシー概要

【ポリシー】「ポリシー案1.0」の概要

準備会での議論や実証プロジェクト等の取組に基づいて、「ポリシー案1.0」を策定

昨年度の策定範囲

準備会や実証プロジェクト等

「ポリシー策定委員会」からの提言も踏まえながら「準備会」、「WG」を通じて事業概要の大枠を策定

- TDPF事業におけるプリンシプル
- 事業概要 (データ流通推進・データ整備)
- 取り扱いデータ範囲
- トラストアンカー※型での実施

ポリシーから必要に応じて提言 ⇄ 準備会決定事項を共有

ポリシー

準備会や実証プロジェクトでの検討内容に基づいた「ポリシー案1.0」を策定

- **プライバシーステートメント**での**対象情報をパーソナルデータとし、対象者をデータ提供者・利用者及びデータ主体**と規定 法令 契約
- **トラストアンカー型で実施**をしていく際に必要となる、**データ提供時・利用時の基本的なルール**を規定 法令 契約
- TDPFが**データ整備の委託を請け負った場合に関する基本的なルール**を規定 等 法令 契約 技術

ポリシー案1.0の構成

官民連携データプラットフォーム **データガバナンス指針**	• パーソナルデータ保護とサイバーセキュリティ確保に加え、**積極的なデータ利活用のために運営組織が取り組むこと等**を規定
官民連携データプラットフォーム **プライバシーステートメント**	• 対象とする情報**(パーソナルデータ)**、対象者**(データ提供者・利用者及び個人)**を定め、原則**オプトアウトでのパーソナルデータの第三者提供をしない**方針等を規定
官民連携データプラットフォーム **コンプライアンス指針**	• **各種の関係法令の遵守**、運営組織の**透明性を保つための体制の確立**、**データプラットフォームに係るコンプライアンス研修**の運営組織内で**実施**等を規定
官民連携データプラットフォーム **規約**	• サービス利用に関する**入退会の基本内容**及び**データ提供時・利用時の基本的なルール**等を規定
官民連携データプラットフォーム **情報セキュリティポリシー**	• 東京都サイバーセキュリティ基本方針に準じ、**データプラットフォーム事業者としてデータ流通時に留意する対策・最新のセキュリティに対する情報収集**をしていくこと等を規定

※個人、法人、機器などのサイバー空間の存在（ID） の認証（審査・登録・発行・管理など）を担う機能のこと
官民連携データプラットフォームでは、TDPFがデータ提供者とデータ利用者を審査することや、データの管理をすることなどによって、トラストを担保し、保証すること

https://www.digitalservice.metro.tokyo.lg.jp/society5.0/dpf_suishin_01.html
東京データプラットフォーム協議会　第1回推進会議　事務局資料より引用

トヨタ自動車株式会社

企業分類		
企業規模	大	中小
主な事業がBto	B	C

事業概要等

トヨタ自動車は、豊田自動織機を源流とする自動車会社である。近年は、CASE（Connected/Autonomous/Shared＆Services/Electric）と呼ばれる新たな潮流の中、モビリティカンパニーへの変革をかかげ、コネクティッドサービスや自動運転、その他移動に関する様々なモビリティサービスを通じて豊かな社会づくりへの貢献を目指している。

クルマづくりを通じて培われてきた「お客様第一」という信念は、プライバシー保護の観点においても変わらず、国際社会の一員として、国内外の法令を遵守するとともに、お客様のプライバシーの尊重や適切な保護に努めている。

<プライバシーに関する企業の取組>

1. Chief Privacy Officer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、取り組んでいる。
- 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。

2. コネクティッドカーデータに関するホワイトペーパー公開による取組の公表

- コネクティッドカーから取得するデータの利活用・保護の取組についてホワイトペーパーを開示し、トヨタが目指す姿、データ取得・利活用の流れ・データ保護の取組や活動事例を示しいる。
  https://toyota.jp/pages/contents/tconnectservice/contents/pdf/toyota_datapolicy.pdf

3. 車載カメラ画像の取扱いに関する消費者とのコミュニケーション

- トヨタの先進安全システムや高度運転支援システムを搭載している車両の一部より取得する車載カメラの画像の取扱いについて、WEBサイトでの説明（Q&A等）を通じて、カメラに映り込む可能性のある消費者とのコミュニケーションを図っている。
  https://faq.toyota.jp/category/show/515?site_domain=default

トヨタ自動車の取組み

「車載カメラによる走行環境画像の取得と利用について」

https://global.toyota/jp/sustainability/privacy/on-board-cameras-initiatives/

- トヨタが車外画像データを取得することについて、「自分も映り込むことがあるのか？」「映り込んだ自分の画像が何に利用されるのか？」「自分のプライバシーは大丈夫なのか？」といった個人の不安への対応。
- 車外画像データの取得と利用におけるトヨタの思い「全ての人により安全で自由な移動を」

  「車外画像データには、お客様が実際に車両を運転する道路・交通環境の情報が含まれています。これらは、試験場では得ることのできない情報です。実際の道路・交通環境を知ることで、トヨタは、より実際の道路・交通環境に合った、より安全なクルマやシステムの開発を加速させることができるほか、交通インフラの改善に資するサービスの開発など、社会をより便利・より安全にするための取り組みにつなげることができます。」

- 個人情報保護・プライバシー尊重への取り組み
  - ✓ 取得する社外画像のイメージを動画で提供
  - ✓ 取得する車両や、実施プロジェクトの違いにより利用目的や取得するタイミング、場所が異なる為、それぞれの利用目的や画像データの取得タイミング等の詳細について個別に丁寧な説明。（①一部のお客様の車両より取得する車外画像データ、②試験車の車載カメラより取得する車外画像データ、③各種実証実験において取得する車外画像データ）
- 具体的取り組み例
  - ✓ 車外画像データの取り扱いに関するの情報の適時適切な公表（ウェブサイト）
  - ✓ 車外画像データに対するアクセス制限やアクセスログの管理
  - ✓ 車外画像データに映り込む人や車両のナンバーを個別に検索できない形式での保管
  - ✓ 車外画像データに映り込んだ人や車両について個別に追跡したり、その行動特性や移動傾向などを分析したりすることの禁止
  - ✓ 社外への提供に際して、利用目的に応じたモザイク処理やトリミングなどの匿名化処理

日本電気株式会社

企業分類		
企業規模	大	中小
主な事業がBto	B	C

事業概要等

社会公共、社会基盤、エンタープライズ、ネットワークサービス、グローバルをグループの主要事業とする。

NECグループが共通で持つ価値観であり、行動の原点を、「NEC Way」と定める。

「Purpose（存在意義）」「Principles（行動原則）」と、一人ひとりの価値観・ふるまいを示した「Code of Values（行動基準）」「Code of Conduct（行動規範）」で構成され、企業としてふるまう姿を示し、NEC Wayの実践を通して社会価値を創造する。

<プライバシーに関する企業の取組>

1. デジタルトラスト推進本部設置

- AIによる社会価値創出にチャレンジしており、法制度・倫理・社会受容性など総合的観点からケアする専門組織として、2018年10月にデジタルトラスト推進本部を設置し、人権リスクへのマネジメント体制を構築した。
- デジタルトラスト推進本部は、コーポレートスタッフの経営企画機能の一つとして位置づけ、顔認証技術などを事業活動として正当に、人権プライバシー侵害なく、顧客価値に変えることをミッションとして、CDOの下に配置した。
- デジタルトラスト推進本部、コンプライアンス推進部、サスティナビリティ推進本部が、プライバシーに関わる統括を違う切り口で推進している。

2. プライバシーに対してAIと人権という観点からの取組を実施

- 2019年4月「AIと人権に関するポリシー」（ https://jpn.nec.com/press/201904/images/0201-01-01.pdf）を策定した。
- 2019年までは個人情報保護・プライバシーとしていたが、それ以降はAIと人権という広い枠組みの中でプライバシーを扱う。

3. サステナビリティレポートの発行

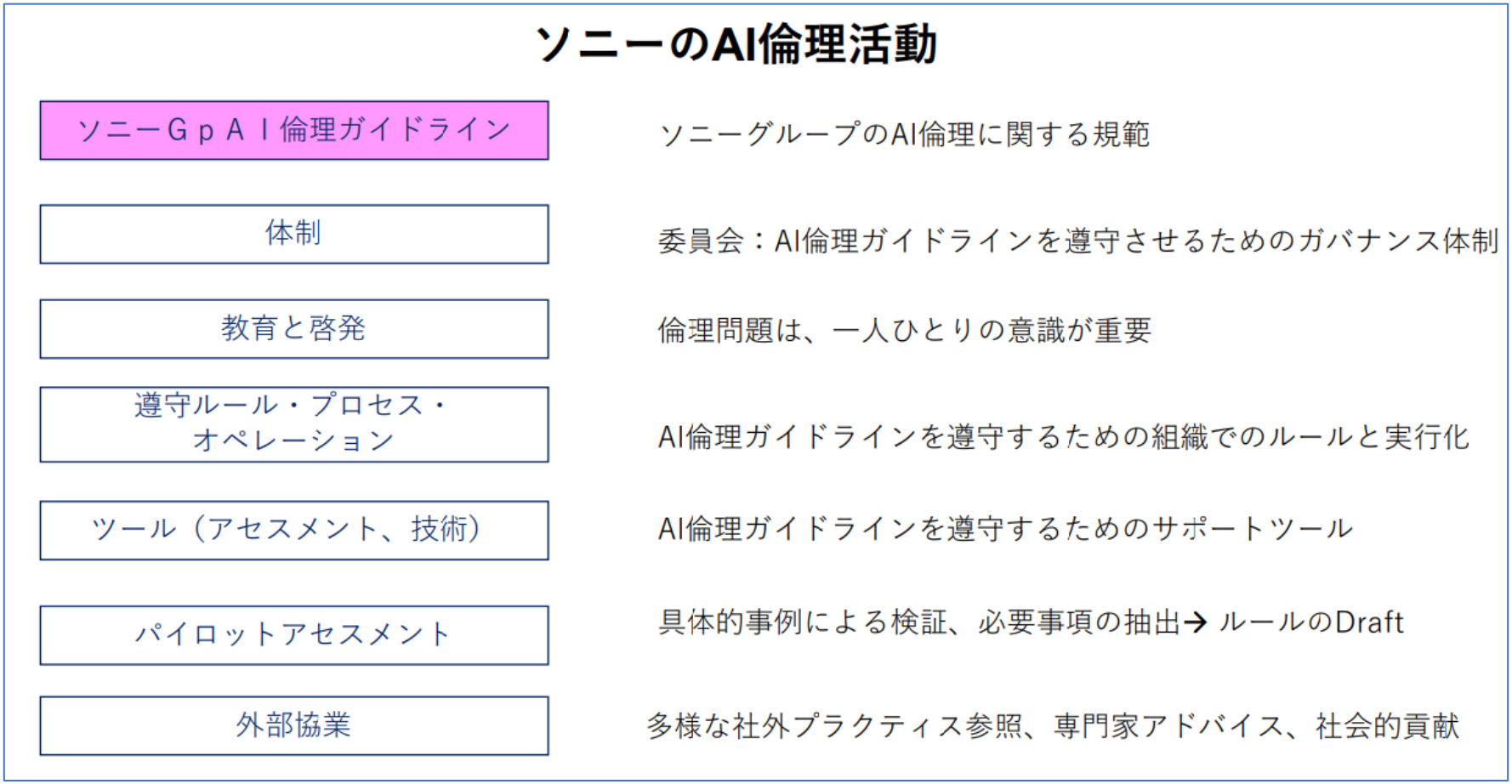
- ESG的な活動について、統合レポートと、サステナビリティレポート（ https://jpn.nec.com/csr/ja/report/index.html）を発行し、プライバシーについても年度の活動を公表している。
- 新たな中核として社会貢献をテーマに掲げ、デジタルトラスト推進本部に加え、2021年4月からサステナビリティ推進室を本部として、人権やESG、サステナビリティに係る全社のレポーティングを統括している。

4. 外部有識者との対話

- 外部の有識者との対話（デジタルトラスト諮問会議）を設置。諮問委員会では、専門家・消費者団体・人権について、コンサルを行っているNGOなどの知見も得て、活動に活かす。2019年から半期に一回実施。

ソニーグループのResponsible AIへの取り組み

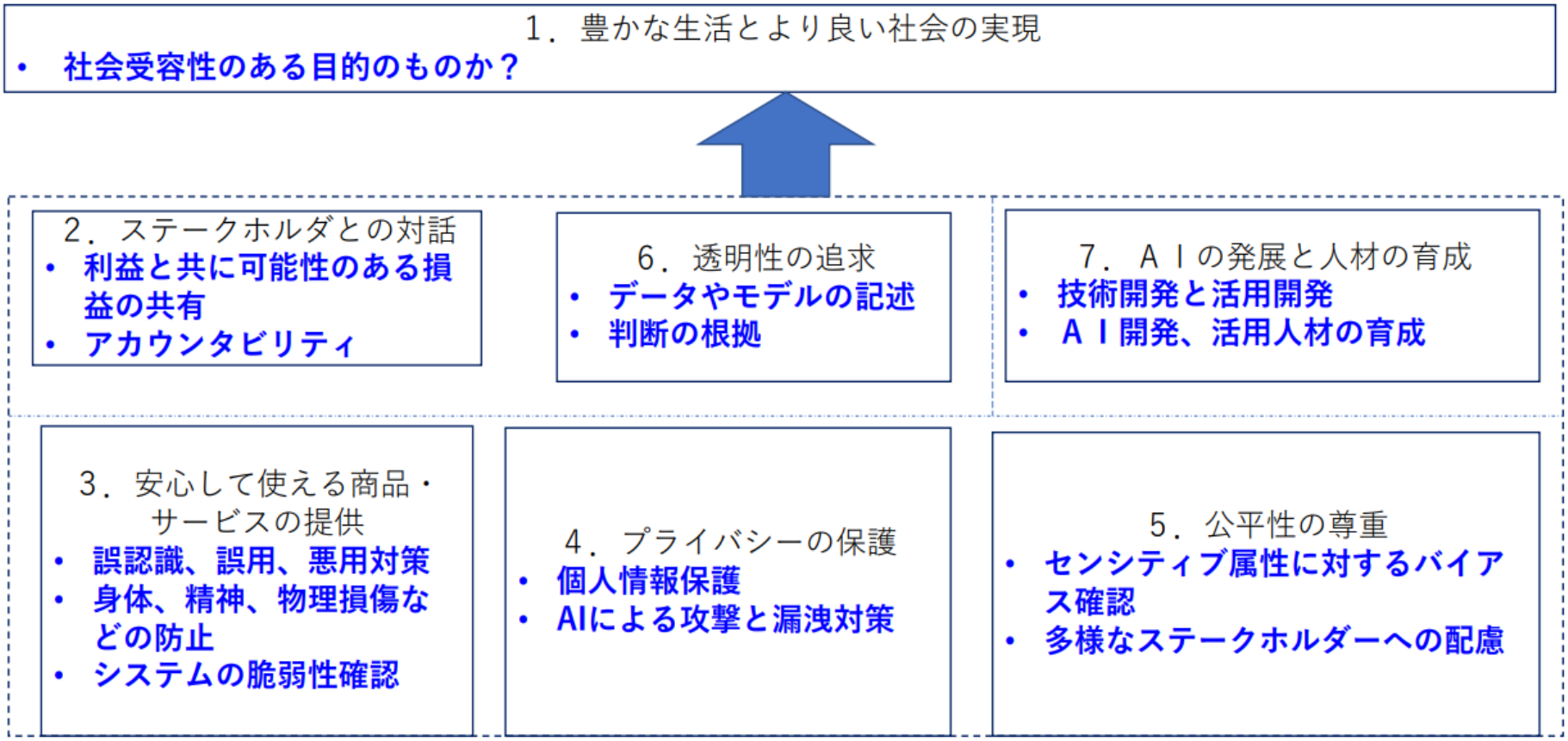
ソニーグループは単にガイドラインの策定に留まらず、体制、教育、サポートツール、AI倫理関連技術開発とソリューション提供まで、総合的に整備している



出所ソニーグループ：https://www.soumu.go.jp/main_content/000736981.pdf　より引用

ソニーグループのResponsible AIへの取り組み

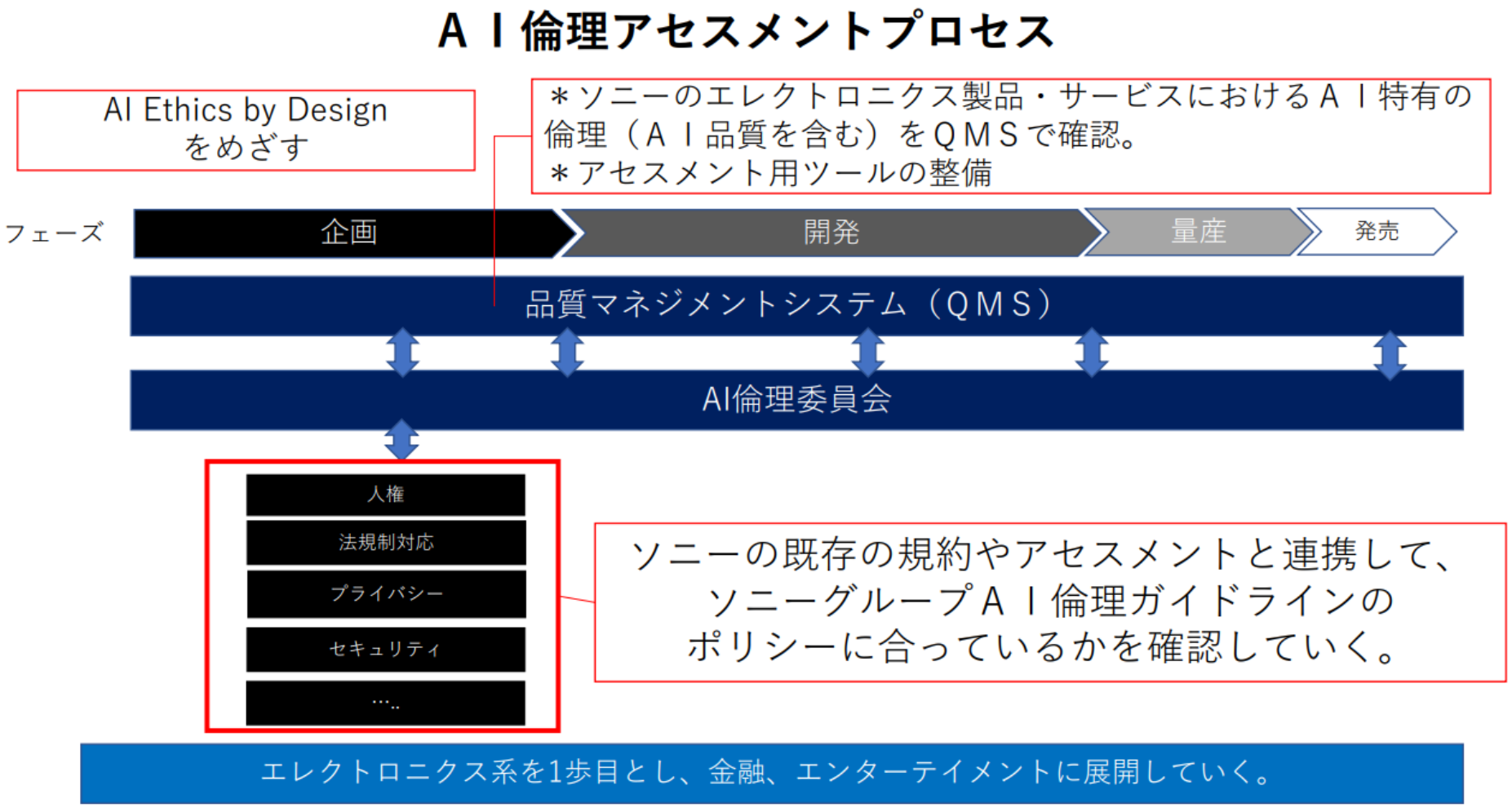
遵守ルール・プロセス、オペレーション
--アセスメント＝ガイドラインに沿っているか？



出所ソニーグループ：https://www.soumu.go.jp/main_content/000736981.pdf　より引用

ソニーグループのResponsible AIへの取り組み

ソニーグループは、エレクトロニクス製品にこれまで適用していた品質マネジメントシステム（QMS）に、AI倫理の審査・評価を追加。倫理＝製品やサービスの品質要件として、競争力につなげている。



出所ソニーグループ：https://www.soumu.go.jp/main_content/000736981.pdf　より引用

コンビニ業界における検討の具体例（経産省事業）

- コンビニの省人化、無人化の大きな課題が、酒・たばこの販売時の対面による年齢確認プロセスである。顔認証、AIによる年齢推定などのデジタル活用への期待が大きいが、他方、制度的、技術的課題やプライバシー懸念などの受容性課題の解決が重要。
- 本事業ではデジタル活用による年齢確認の自動化を「デジタル成人認証」と称し、上記課題への対策の要諦をガイドラインに取りまとめ、省力化店舗の加速に道筋をつけることが狙いとなる。

コンビニの成長基盤の危機	売上げの伸び悩み、人手不足による店舗運営の困難化、人件費の高騰による運営コストの上昇
リテールテックを活用した次世代モデルへの期待	キャッシュレス決済端末やセルフレジ導入に代表される省力化店舗施策
年齢確認業務が省力化の課題	酒・たばこ販売における対面による年齢確認プロセスがセルフ化の推進の妨げとなっている
デジタル活用による年齢確認の自動化（デジタル成人認証）への期待	ICカード認証、年齢推定技術、顔認証技術などの技術による成人認証の適正性の確保

コンビニ業界における検討の具体例（経産省事業）

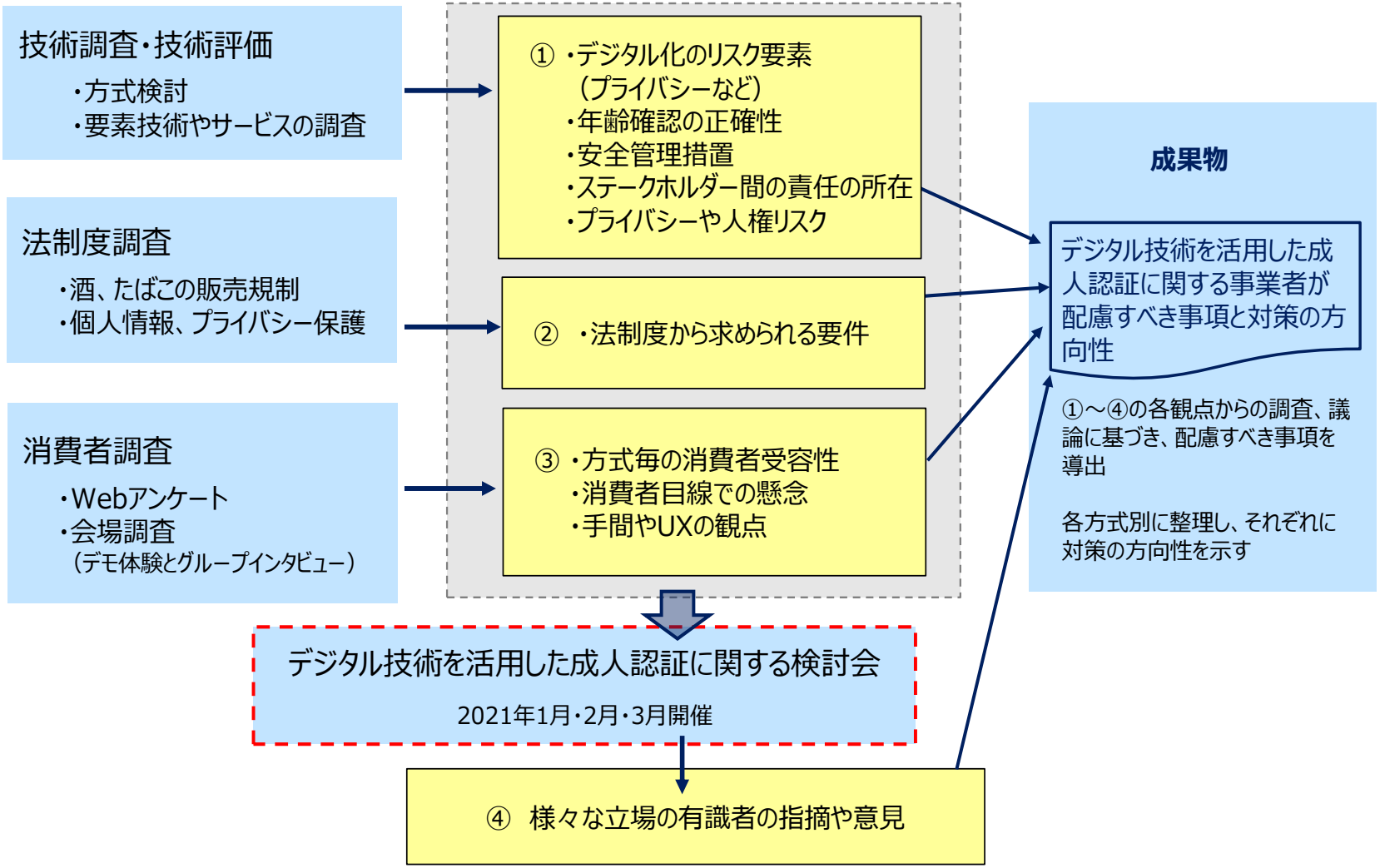
- 成人認証の方式として、以下の3つの方式が案として考えられる。
- これらの案をもとに、対象とするユースケース・検討スコープを議論し、方式の整理・検討を進めていく

	方式名称	特徴
方式①	ICカード認証方式	• たばこの自動販売機のTASPOのように、ICカードをかざす方式 • 事前に書類等で本人確認・身元確認を行う • なお、ICカードの代わりにスマホのアプリの利用も考えられる
方式②	顔認証方式	• 購入時に顔認証等を行い、事前登録している成人認証の情報を取得して確認する方式 • ※先行している実証事例から考え、今回は生体認証の中でも特に顔認認証を想定
方式③	年齢推定方式	• レジ併設のカメラを用いて、顔画像から年齢を推定する方式 • 事前登録は基本的に不要 • なお、推定の誤差による救済措置などの検討も必要となる

コンビニ業界における検討の具体例

デジタル成人認証の導入に関する配慮事項と対策の方向性

検討プロセス



デジタル成人認証の導入に関する配慮事項と対策の方向性

１．デジタル成人認証の導入に関する共通的な配慮事項

(１)配慮すべき3つの基本的要素

基本的要素1：未成年者（20歳未満の者）の誤認防止

- 認識技術の精度、不正利用、生年月日を取得する元情報の信頼性などが起因して、誤って20歳未満の者に酒・たばこを販売してしまうリスクを回避すること。

基本的要素2：利用者の個人情報とプライバシーの保護

- 個人情報保護に関する法令の遵守を前提として、幅広い消費者のプライバシー意識や受容性へ配慮することによりプライバシー侵害リスクを回避すること。
  - ✓ データの最小化（必要最小限のデータの取得、成人認証後の不必要データの即時廃棄、生年月日を成人であるか否かのフラグで管理するなど）
  - ✓ 店舗におけるプライバシー保護（周囲からのプライバシー配慮など）
  - ✓ 消費者への適切な通知（HPや店頭、メディアなどでの事前通知など）
  - ✓ 適正利用（同意のない他情報との紐付けや目的外利用、店舗スタッフによる活用の制限など）
  - ✓ 苦情受付や各種問い合わせ体制の整備
  - ✓ 個人情報やプライバシー保護に関する加盟店の啓発、教育や支援（プライバシーポリシーの雛形やマニュアルの提供など）

基本的要素3：安全管理措置

- 組織的、人的、物理的、技術的それぞれの要素における安全管理措置を講じ、情報漏えい対策を徹底すること。

デジタル成人認証の導入に関する配慮事項と対策の方向性

２．取組みを効果的にするための4つの視点

視点1：バイ・デザイン の視点

- 企画段階から配慮すべき３つの基本的要素について検討し、サービス仕様や運用設計、システム設計などにその対策を組み込み、デジタル技術を活用した成人認証導入のリスクを未然に回避すること。加えて、運用においては継続的なモニタリングを行い、定期的な見直しや改善を行うこと。

  ✓サービスの企画段階から配慮事項に基づいた要件定義を実施し、対策に必要なリソース（予算や体制）を確保すること。

  ✓データの取得から廃棄まで、ライフサイクル全体におけるリスクを把握し、対策を講じること。

  ✓リスク分析結果に応じ、プライバシー影響評価　（Privacy Impact Assessment）など実効性のある対策を検討すること。

  ✓環境の変化、消費者意識の変化等に対する継続的なモニタリングと対策の定期的な見直しを行うこと

２．取組みを効果的にするための4つの視点

視点2：顧客中心の視点

- コンビニを利用する顧客の価値観、来店動機、デジタル習熟度など多様性に配慮したサービス設計を行い、受容性を高めること。また、新しい技術や、理解しにくい仕組みに対しては不安を感じる生活者の目線に立ち丁寧な説明を心がけること。
  - ✓容易な操作で迅速にサービスが利用できるユーザーインタフェースを基本とすること。
  - ✓わかりやすい手続きでサービスの利用停止ができること。
  - ✓利用規約や個人情報の取扱いに係る通知・同意取得については、要諦が一目で直感的に理解しやすい表現に努め、求めに応じ詳細な情報を提供する等の工夫をすること。
  - ✓スマートフォン操作やデジタル技術へ抵抗感がある顧客を想定したサポート体制の整備、及びマニュアルの整備やスタッフへの教育を行うこと。
  - ✓段階的導入により、サービスの受容性や配慮事項の効果や課題を洗いだし、改善しながら導入拡大すること。
  - ✓採用した方式や技術に対し利用意向が低い顧客、またはサービスを受ける前提を充足しない顧客（例えば、運転免許証を保有しない、利用する携帯キャリアが対象ではない等）が他の手段で酒・たばこを購入できること。

視点3：役割・責任の明確化の視点

- 配慮すべき３つの基本的要素の検討において、加盟店（オーナー）始め、デジタル技術を活用した成人認証サービスに係る全ての関係者と、役割分担や責任の所在について明確にすること。
  - ✓ 複数事業者が関与する場合であっても、未成年者の誤認、プライバシー侵害、情報漏えい等のリスクに対し、役割・責任が明確化され、サービス全体、システム全体として漏れの無い対策が実施されること。（問い合わせや苦情窓口、事故対応や万一の際の損害賠償、契約の在り方などについて事業者間で取り決めること。）
  - ✓ 20歳未満の者で無いことを確認する主体（酒類販売業者等）、個人情報保護法における規律の主体（個人情報取扱事業者）の異同を、顧客が明確に把握できること。

視点4：社会全体の視点

- デジタル技術を活用した成人認証が広く受容されることを目指し、社会全体の利益や効率化を考慮して配慮事項の検討や対策を実施すること。
  - ✓ 積極的な情報発信やコミュニケーションを通じ、コンビニ利用者、地域社会、加盟店（オーナー）など全ての関係者で取り組みの意義を共有し、社会のコンセンサス獲得に努めること。
  - ✓ デジタル技術を活用した成人認証の導入による効率化を、サステナブルな成長の基礎となる協調領域と位置づけ、仕様やガイドライン、啓発活動の在り方などを検討すること。
  - ✓ 酒・たばこの販売や提供に係る他の事業者や業態への拡大、あるいはネット販売など新たな提供形態への拡大など、安心、効率、公平な社会の実現に向けた働きかけを行うこと。

（参考）「空港での顔認証技術を活用したOne IDサービスにおける個人データの取扱いに関するガイドブック」

・空港におけるOne Idサービスは顔認証技術とID連携を土台としているサービス。
・留意事項3原則、配慮事項として具体的な対応方法3点を示し、今後空港オペレータが同種のサービスを導入する際の、実質的サービスやシステムの非機能要件となっている。

ガイドブック策定の背景

国土交通省では、航空需要の増大や、人手不足等の課題に対応しつつ、世界最高水準の空港利用者サービスを提供していくため、「FAST TRAVEL（ファストトラベル）」を推進し、首都圏空港では、空港会社等において顔認証技術を用いた搭乗手続きであるOne IDサービスの導入準備を進めている。

【目 的】
One IDサービスで利用する個人データは、生体情報である顔画像情報を含むが、顔画像情報は不変性が高く本人の意思によらない取得が容易な識別子であり、強い追跡機能を有することから、導入に際しては、旅客に利用目的や情報管理について十分な理解と納得を得ることが求められる。

【取 組】
個人情報保護関係法令の遵守に加え、さらに社会的受容性を高めるために、プライバシー保護の観点での具体的な対応を踏まえた内容として、個人データの取扱いに関して事業者が配慮すべき事項をとりまとめたガイドブックを策定。

「One ID 導入に向けた個人データの取扱検討会」

（R1.10.30設置、全４回開催）

One IDサービスにおける個人データの取扱いについては、有識者を含む検討会を設置し、ガイドブック策定に向けて検討。併せて、パブリックコメントを実施。

（構成員） ◎：座長
◎森 亮二　英知法律事務所 弁護士
菊池 浩明　明治大学 総合数理学部 専任教授
鈴木 正朝　新潟大学 大学院 現代社会文化研究科・法学部教授
理化学研究所AIP
若目田 光生　株式会社日本総合研究所
リサーチ・コンサルティング部門 上席主任研究員
佐藤 洋子　一般財団法人 日本消費者協会
消費生活コンサルタント
篠原 治美　公益社団法人 日本消費生活アドバイザー・コンサルタント・相談員協会 個人情報保護特別委員会委員長

国際航空運送協会（IATA）
日本航空株式会社
全日本空輸株式会社
成田国際空港株式会社
東京国際空港ターミナル株式会社
成田国際空港航空会社運営協議会
東京国際空港航空会社運営協議会

（オブザーバ）
個人情報保護委員会事務局
関西エアポート株式会社
中部国際空港株式会社

ガイドブックの概要

【対象者】：One IDサービスの導入を検討している空港会社等の事業者

（１）One IDサービスの運用における留意事項

・個人データの利用目的を搭乗手続き※に係る利用に限定。
※国際線出発手続きで、チェックイン、手荷物預け入れ、保安検査場入口、航空会社ラウンジ入口、搭乗ゲートの全てもしくはいずれか（出国審査を除く）

・顔認証の利用は希望する旅客のみとし、従来通りの手続きも存置。

・個人データは原則24時間以内に消去。定期的に監査を実施。

（２）One IDサービスの導入において、事業者が旅客との適切なコミュニケーション体制を構築する上で特に必要とする配慮事項

①事前告知・公表
利用目的や情報管理について旅客から十分な理解を得られるよう、One IDサービスの概要や手続き方法、利用目的等について、適切な内容、手段、場所、周知期間を踏まえて旅客への事前告知・公表を実施すること。

②旅客からの同意取得
One IDサービスの利用についての同意と、空港会社・航空会社間での個人データの提供にかかる同意の取得に際しては、旅客に対して、サービス内容や個人データの流れ等を容易に理解できるよう、説明すること。

③旅客からの個人データに関する苦情・相談等の受付
旅客からの個人データに関する苦情・相談等に対して適切に対応できるよう、受付手段、受付時間、対応言語を設定すること。

https://www.mlit.go.jp/report/press/kouku19_hh_000096.html　国土交通省広報資料より引用

プラットフォーマのプライバシー重視の動き（マイクロソフト）

◆ Satya Nadella CEO の声明

「6 つのプライバシー原理にフォーカスすることで皆様の信頼を得られるように努力しています。」

- 管理: 使いやすいツールや明確な選択肢を提供することでプライバシーを管理できるようにします。
- 透明性: 情報に基づいた意思決定を行えるよう、データ収集と使用に関して透明性を徹底します。
- セキュリティ: 信頼のうえご提供いただいたデータを強力なセキュリティと暗号化で保護します。
- 強力な法的保護: プライバシーに関する地域の法規制を遵守し、基本的人権としてプライバシーを法的に保護します。
- コンテンツに応じたターゲットの非実施: ユーザーのメール、チャット、ファイル、その他の個人用コンテンツはターゲット広告に利用しません。
- 皆様への利点: 当社がデータを収集する場合、皆様のお役に立て、より良いエクスペリエンスを提供する目的で使用いたします。

◆ 顔認識テクノロジに関する行動規範

- 公正性： あらゆる人々を公正に扱う顔認識テクノロジの開発と展開を行います。
- 透明性： 顔認識テクノロジの能力と限界について文書化し、明確に伝えます。
- 説明責任： 顔認識テクノロジが重大な影響を及ぼす用途では、人間による適切なコントロールが行われるようお客様を支援していきます。
- 差別的使用の禁止： 顔認識サービスが違法な差別に使用されることを利用規約により禁止します。
- 通知と同意： 民間セクターのお客様に対して顔認識テクノロジの展開における通知と明確な同意を奨励します
- 合法的監視： 警察権力による監視の状況において人々の民主主義的自由が確保されるよう支援し、その自由が損なわれると考える目的では顔認識テクノロジを使用しません。

技術と人権課題に対する政策動向

2022年４月28日 未来のインターネットに関する宣言

令和4年4月28日、「未来のインターネットに関する宣言」立ち上げイベントが対面及びテレビ会議のハイブリッド形式で開催された。同イベントには、米国主催の下、初期パートナー国（日、豪、加、EU、英）及び賛同国等が参加し、「未来のインターネットに関する宣言」を発表

（ビジョン）

デジタル技術は、信頼性があり、自由で公正な商取引を可能にする方法で生産、使用、運営されるべきであり、個々のユーザー間の不公平な差別を避け、効果的な選択を確保し、公正な競争を促進し、イノベーションを奨励し、人権を促進・保護するとともに、以下のような社会を育成するものである。

- 人権と基本的自由、及び全ての個人の幸福を保護、促進する
- アクセスの増加、利用可能性及びデジタルスキルの向上等を通じて、全ての人がどこにいてもインターネットに接続できる
- 個人と企業が、自身が使用するデジタル技術の安全性と機密性について信頼することができ、彼らのプライバシーが保護されている
- あらゆる規模の企業が公正で競争的なエコシステムの中で、それぞれの強みによって革新し、競争し、繁栄することができる。
- インフラが、安全で、相互運用性、信頼性及び持続可能性を持って設計されている。
- 技術が、多元主義、表現の自由、持続可能性、包摂的な経済成長及び地球規模の気候変動に対する闘いを促進するために使用されている。

2022年４月28日 未来のインターネットに関する宣言（原則）

（4）デジタルエコシステムに対する信頼

- サイバー技術が可能とする犯罪を含むサイバー犯罪に対抗し、悪意のあるサイバー活動を抑止するために協働する。
- 政府および関係当局による個人データへのアクセスが、法律に基づき、国際人権法に従って行われることを確保する。
- 公共の安全の保護と適用される国内法および国際法に整合して、個人のプライバシー、個人データ、電気通信の秘密、エンドユーザーの電子機器上の情報を保護する。
- 消費者、特に弱い立場の消費者を、オンライン詐欺やその他の不当な行為、およびオンラインで販売される危険で安全でない製品から保護することを推進する。
- ネットワーク・セキュリティのための技術的および非技術的要素を含むリスクベースの評価に基づき、信頼できるネットワーク・インフラおよびサービスの供給者を推進し、利用する。
- 秘密裏に行われる情報操作キャンペーンを含め、選挙インフラ、選挙および政治プロセスを弱体化させるためにインターネットを使用することを控える。
- 企業や起業家がそれぞれの強みに基づいて競争できるよう、貿易と競争可能で公正なオンライン市場を促進する、ルールに基づくグローバルなデジタル経済を支持する。
- インターネットとデジタル技術の環境負荷を可能な限り削減しながら、気候変動対策と環境保護のために技術の効果を最大化するために協力する。

（5）マルチステークホルダーによるインターネットガバナンス

2022年４月28日 未来のインターネットに関する宣言（原則）

（1）人権及び基本的自由の保護

- 世界人権宣言を含む人権、法の支配、正当な目的、非恣意性、効果的な監督、透明性の原則を、オンライン・オフラインの双方で尊重
- オンラインの安全性を推進し、性的あるいはジェンダーに基づく暴力、さらには児童の性的搾取を含むオンライン暴力と闘い、インターネットをすべての人、とりわけ女性、子供、若者にとって安全で安心できる場所とするための取組強化
- 性別、ジェンダー、性的自己認識、人種、肌の色、民族的・社会的出自、遺伝的特徴、言語、宗教・信条、政治的・その他の意見、少数・先住民族の一員、財産、出生、障害、年齢、性的指向による差別を受けず、すべての人にとって安全かつ公平なインターネット利用を推進
- 社会的スコアカード、その他の国内社会統制や犯罪前の拘束や逮捕等の仕組みの開発を含め、国際人権原則に沿わない違法な監視、弾圧、抑圧のためにインターネットやアルゴリズムツールや技術を悪用、乱用することを控える。

（2）グローバル（分断のない） インターネット

（3）包摂的かつ利用可能なインターネットアクセス

- 個人や企業が、必要とする場所で、利用可能で包摂的かつ信頼性の高いインターネットへのアクセスを促進し、世界中の全ての人々がデジタル変革の恩恵を受けられるよう、世界中のデジタルディバイドを解消するための取組を支援する。
- 個人がデジタルディバイドを克服し、安全にインターネットに参加し、デジタル経済の経済・社会的潜在力を実現できるよう、デジタル・リテラシー、スキル習得、能力開発を支援する。
- 多様な文化や多言語のコンテンツ、情報、ニュースのオンラインでのより高い露出機会を促進する。オンラインで多様なコンテンツの露出は、多元的な公論に貢献し、社会における一層の社会的・デジタル的包摂を促進し、偽情報や誤情報に対する強靱性を高め、民主的プロセスへの参加を増大させる。

2022年5月11日　G7デジタル大臣声明

- ロシアによるウクライナへの軍事進攻を強く非難。通信インフラを含むデジタルインフラについて、サイバー上の脅威に対する認識の向上と共有、サイバー対策に関する協力の拡大を含め、サイバー・レジリエンスを向上させることに合意。
- デジタルソリューションが環境保護の強化と温室効果ガス排出のネットゼロ達成に貢献できることを再確認。その一方で、データセンターや通信ネットワークなどのデジタル技術やサービスの利用の増加に伴うエネルギーや資源の需要を高めており、専門家やステイクホルダーとの対話を通じ、デジタル技術をより良く活用するための方法を模索。
- オープンで民間企業主導の自発的かつコンセンサスベースによるデジタル技術標準化に対するG7協調の更なる強化に合意。22年9月開催予定のハイレベルマルチステイクホルダーイベントを歓迎。
- Data Free Flow with Trust（DFFT：信頼性ある自由なデータ流通）はイノベーション、繁栄、その他の民主主義的価値を支えるものであることを確認。また、共有する民主主義的価値観と、DFFTの利益を制限する措置に対処する決意を再確認し、デジタル保護主義に反対。DFFTを促進すべく、将来の相互運用性を促進するため、共通理解を深め、既存の規制アプローチと手段の間の共通性、補完性及び収斂の要素の特定に向けた取り組むための努力を強化することに合意。
- プラットフォーム規制を含むデジタル競争問題に関する国際的な協力の深化。22年秋開催予定のG7政策決定者間の議論を支援。G7競争当局間の継続的な情報・経験の交換を歓迎。
- オンラインの安全性を向上させ、インターネット上の違法・有害なコンテンツや活動を削減するというコミットメントを再確認。22年秋のマルチステイクホルダーダイアログを歓迎。
- 電子的移転可能記録の促進のための法的枠組みの設計や電子貨物輸送情報及び文書の交換に関する官民専門家の対話を継続。21年G7で合意した電子的移転可能記録に関する協力をさらに進め、国際貿易における情報のデジタル化の促進の取り組みを支援。

2022年5月11日　G7デジタル大臣声明

- 15. 我々は、カービス・ベイでの 2021 年の G7 首脳会議において、我々の地球を保護するという目的に対する我々のコミットメントを再確認し、環境保護の強化と温室効果ガス排出ネットゼロの達成にデジタルソリューションが貢献できることを強調する。同時に、我々は、データセンターや通信ネットワークなどのデジタル技術やサービスの利用の増加に伴うエネルギーや資源の需要の高まり、及びデジタル機器やデバイスの生産、使用、廃棄が環境に与える影響を認識する。
- 22. 我々は、我々が共有する民主主義的価値と、DFFT の利益を制限する措置に対処する決意を再確認し、デジタル保護主義に反対する。データガバナンスに対する我々の多様なアプローチを認識しつつ、我々は、機会を活用し、特にセキュリティ、プライバシー、データ保護及び知的財産権の保護に関連して生じる課題に対処するために、引き続き協力する。
- 32. 我々は、オンライン上の市民、特に最も影響を受けやすい脆弱な人々、特に女性や子どもを保護すべきである。我々は、プラットフォーム・プロバイダー及びその他の関連企業に対し、法的義務に加え、既存のルールを遵守し、安全なオンライン環境を促進するための自主的な取組を強化するよう求める。違法・有害なオンラインコンテンツや活動に対抗するための彼らの決定や措置は、世界、国、地域レベルで透明性があり、理解しやすく、一貫性をもって利用規約に沿った形で適用され、表現の自由など、オンラインでの人権や基本的自由を尊重したものであるべきである。

おわりに

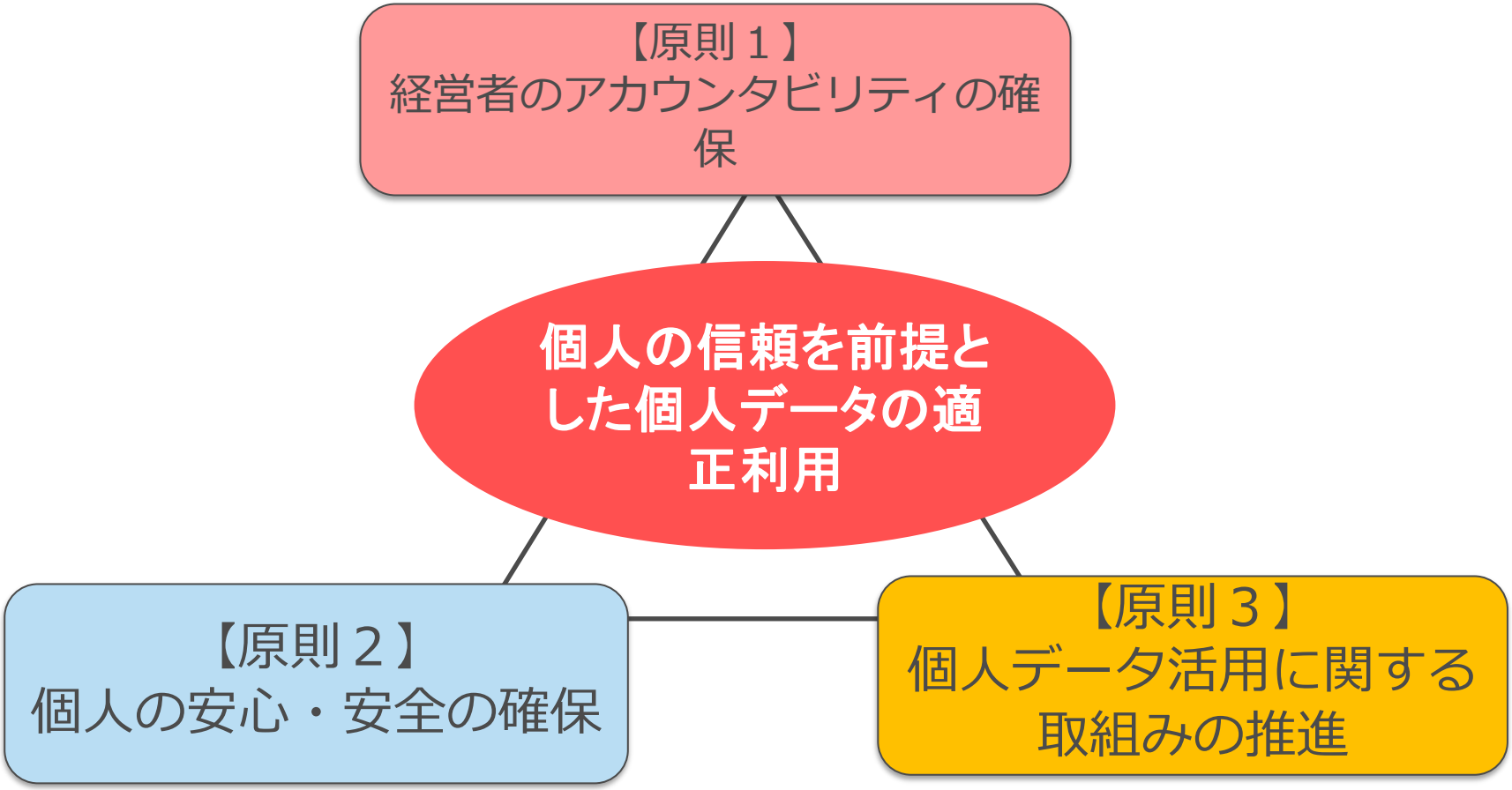
経団連 個人データ適正利用経営宣言

- 様々な社会課題を解決して**人間中心の社会を目指すSociety 5.0を実現するためには、個人の信頼を前提とした個人データの活用を進めることが不可欠**
- しかし、個人の権利利益の侵害やサイバーセキュリティをめぐる内外事案の発生等により、**個人データ活用に向けられる眼はこれまでになく厳しくなっている**

▼

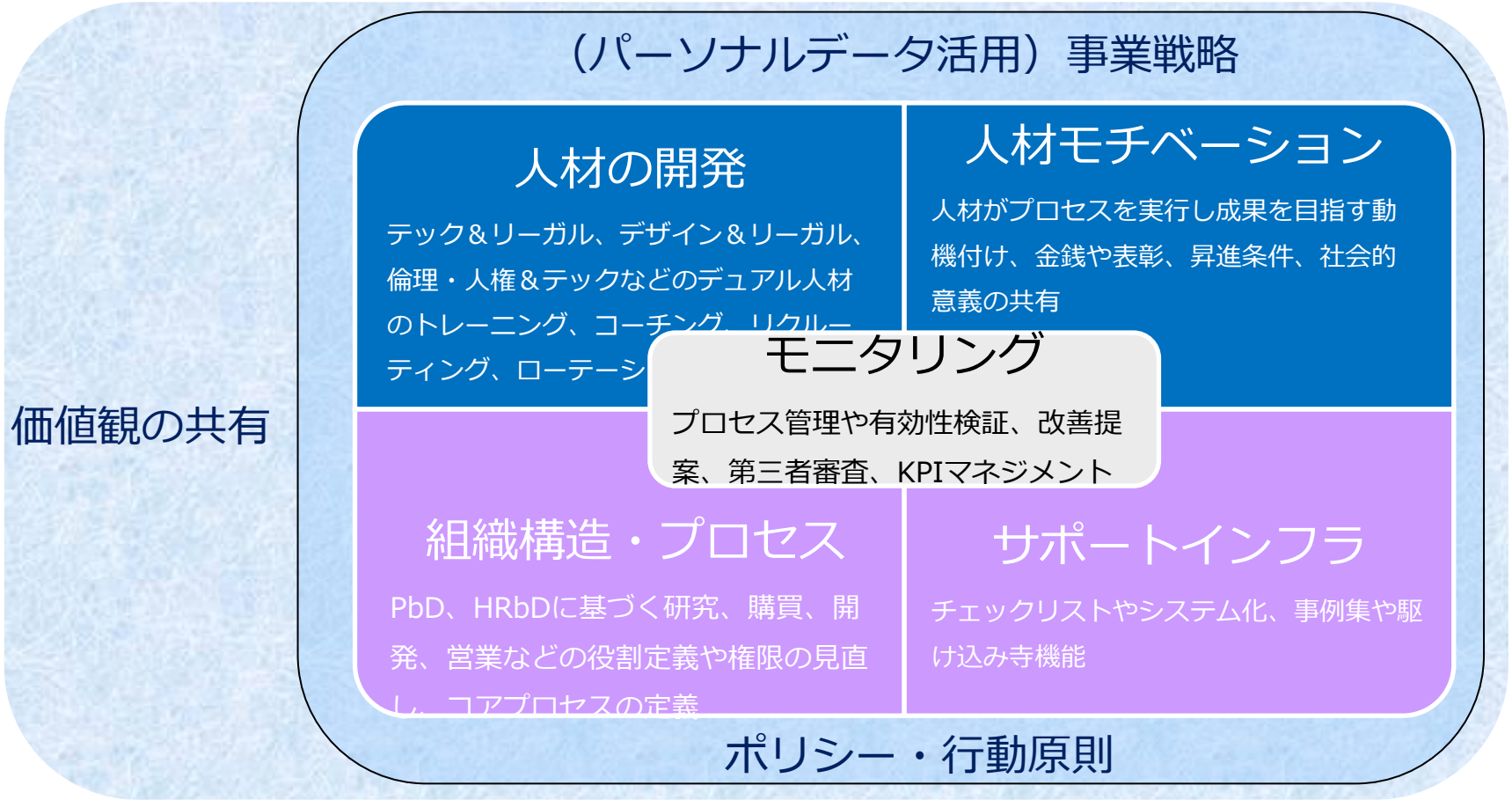
- 経営者は、個人データの保護やサイバーセキュリティ対策が、事業リスクの低減のみならず、**個人の安心・安全を獲得することで中長期的な企業価値の創造に寄与することを認識し、これらを事前に組み込んだ個人データ活用に主体的に取り組むことが必要**
- 個人データの適正な利用に向け、経済界として３つの原則を実践することを宣言

経団連 個人データ適正利用経営宣言



プライバシーのガバナンスと事業強化の両立に向けて（企業の在り方）

「個人データ適正利用経営」とは、形式的なのポリシー策定やガバナンス強化を指すのではなく、業務を回す仕組み、人を動かす仕組み、それらをモニタリングし改善する仕組みが総合的に整備されたプラットフォーム実現を意味する。



CSV（Creating Shared Value）経営とプライバシー

ＣＳＶとは、戦略論のマイケル・ポーターが提唱した新しい経営モデル。企業は社会課題への対応を、慈善や非営利の事業ではなく本業として経営戦略に組みこむことで、経済価値を同時に増大できるという考え方。

デジタル技術の進歩によって、意図的でない場合も含め、プライバシー侵害、新たな差別や排除など人権課題は、AI時代の新たな社会課題といえる。

「誰一人取り残さない」持続可能で多様性と包摂性のある社会の実現というSDGsの趣旨にも合致した人類共通の目標であり、それを防ぐ技術やサービスの開発を行うことや、それを経営戦略に組み込むことが、結果的に企業の経済価値を増大させる。

経済的成長と社会的成長の両立を目指すＣＳＶの３つのレバー

１．社会的課題を解決する次世代製品・サービスの創造と事業化
２．自社を取り巻くバリューチェーン全体の生産性の改善や育成
３．事業を展開する地域でインフラ整備や雇用の確保といった地域生態系の構築

テクノロジーと人権に関し、今後越えるべきハードル

- コンプライアンス疲れへの対応（グローバル、経済安全保障、環境など）
- 縦割りと形式主義からの脱却、ガイドライン主義からの脱却
- 企業や従業員の評価とインセンティブの在り方
- 業界という枠組みの再考とバリューチェーン毎
- デザインアプローチとプライバシーガバナンスの連動
- アジャイルガバナンスの実践
- サステナビリティ部門、法務部門などプロフェッショナルスタッフへの期待と役割の再定義

本資料は、本日の発表資料として取りまとめました。本資料に記載している情報、意見等は、資料作成時点における公開情報または非公開情報を元にした研究員個人の判断に基づくものであり、正確性、完全性を保証するものではありません。

本資料に関しますお問い合わせ、ご確認は下記までお願いいたします。

〒141-0022

東京都品川区東五反田2-18-1大崎フォレストビルディング
株式会社日本総合研究所

創発戦略センター シニアスペシャリスト
若目田光生

wakameda.mitsuo@jri.co.jp