

2024年11月28日 日本DPO協会 第33回個人情報保護セミナー

プライバシーとテクノロジーをめぐる議論の現在地

森・濱田松本法律事務所
弁護士 岡田 淳

森・濱田松本法律事務所

MORI HAMADA & MATSUMOTO

講師紹介



岡田 淳

Atsushi Okada

パートナー

第二東京弁護士会所属

米国ニューヨーク州弁護士会所属

TEL: 03-5220-1821

atsushi.okada@mhm-global.com

■ 主要な取扱分野

データ/プライバシー、知的財産権、TMT (Tech, Media, Telecom)
Fintech、ライフサイエンス、製造物責任、AI/自動運転/ドローン、
テクノロジー分野における紛争・M&Aなど

■ 著作・論文

- 個人情報保護法（商事法務、2024）
- AI事業者ガイドライン（第1.0版）（別冊NBL、2024）
- テクノロジー×著作権 理解を深めるキーワード（コピライト、2024）
- プラットフォームビジネスの法務〔第2版〕（商事法務、2022）
- 特許侵害訴訟〔第2版〕（中央経済社、2021）
- ヘルステックの法務 Q&A〔第2版〕（商事法務、2022）
- ダークパターンに関する一考察（上・下）（NBL、2023）
- AI・IoT・ビッグデータの法務最前線（中央経済社、2019）
- 実務担当者のための欧州データコンプライアンス
～ GDPRからeプライバシー規則まで（別冊NBL、2019）
- データ利活用のための政策と戦略（別冊NBL、2019）
- M&A法体系〔第2版〕（有斐閣、2022）
- ドローン・ビジネスと法規制〔第2版〕（清文社、2022）
- 自動運転・MaaSビジネスの法務〔第2版〕（中央経済社、2023）
- 資本業務提携ハンドブック（商事法務、2020）
- AI・データの利用に関する契約ガイドラインと解説
（別冊NBL、2018） 等、多数（いずれも共著）

■ 経歴

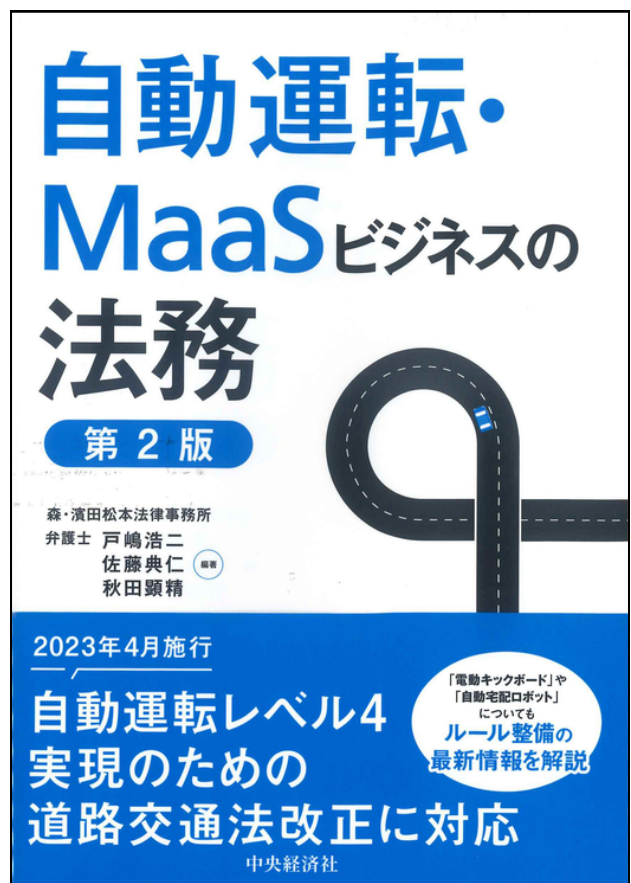
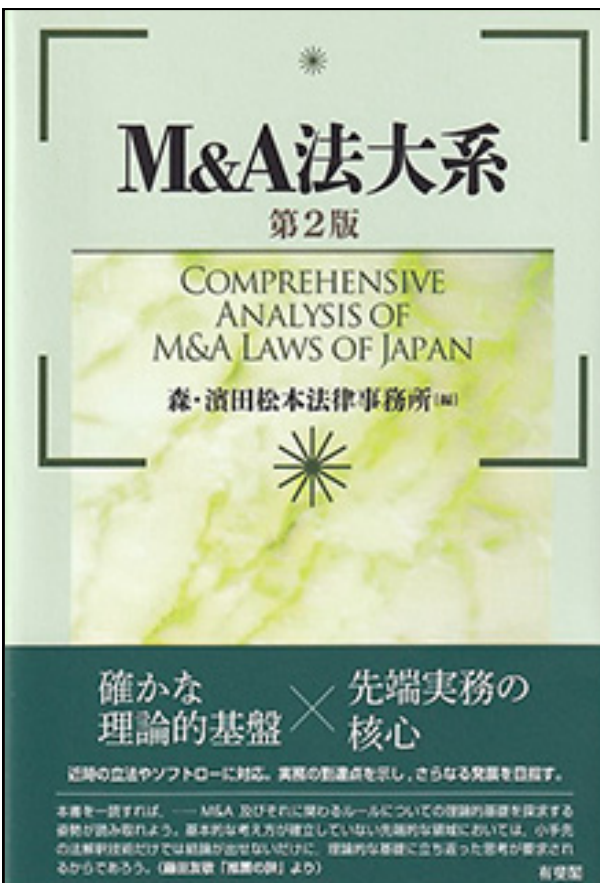
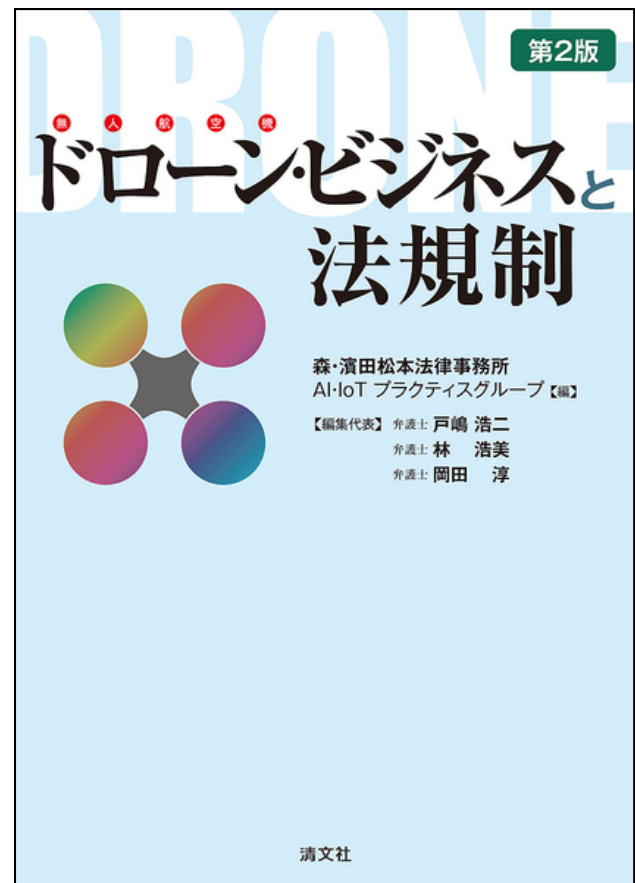
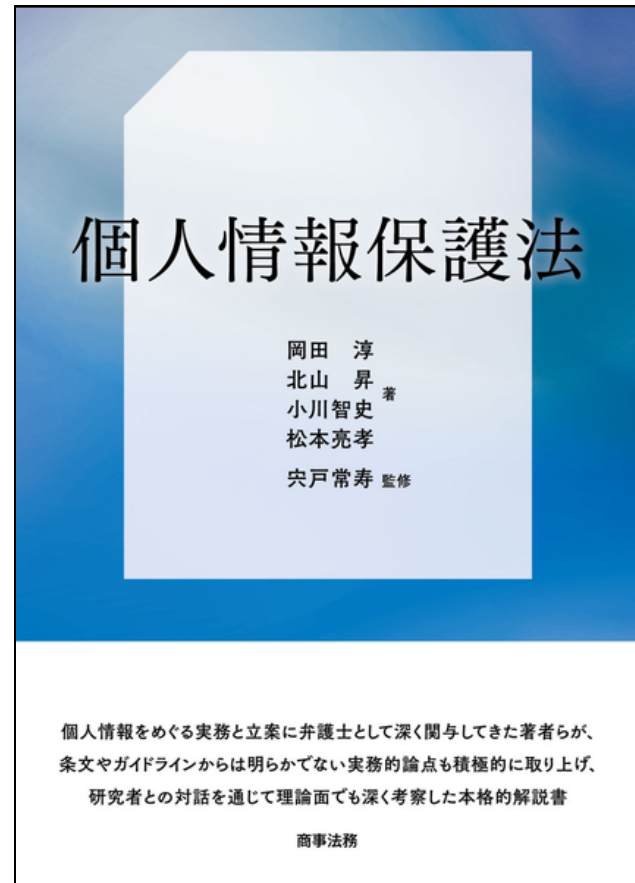
東京大学法学部卒業（2001年）
ハーバード大学ロースクール修了（2007年）
Weil, Gotshal & Manges法律事務所（シリコンバレー
オフィス）で執務（2007年～2008年）

■ 主な活動

- 2010年 立教大学 法学部 講師（特許法、商標法）
- 2011年 青山学院大学 経営学研究科 客員教授（著作権法）
- 2012年 一般社団法人発明推進協会 模倣被害対策アドバイザー
- 2015年 日本弁理士会 特定侵害訴訟代理業務研修講師（不競法）
- 2017年 経済産業省 AI・データ契約ガイドライン検討会 委員
- 2018年 東京大学 政策ビジョン研究センター 客員研究員
- 2019年 内閣府 スマートシティ分野アーキテクチャ検討会議委員
- 2019年 一般社団法人日本DPO協会 顧問
- 2019年 東京大学 未来ビジョン研究センター 客員研究員
- 2021年 経済産業省 AIガバナンス・ガイドラインWG 委員
- 2022年 特許庁 工業所有権審議会 試験委員
- 2023年 自由民主党 AIの進化と実装に関するPT WG 委員
- 2023年 内閣府 AI戦略会議 委員
- 2023年 東京都 文章生成AI利活用ガイドライン 有識者委員
- 2023年 内閣府 AI時代の知的財産権検討会 委員
- 2023年 経済産業省 AI事業者ガイドライン WG 委員
- 2023年 AIガバナンス協会 アドバイザー
- 2024年 一般社団法人ダークパターン対策協会 理事
- 2024年 日本ディープラーニング協会 法と技術の検討委員会 委員

■ 受賞歴等

- Chambers Asia-Pacific (TMT, IP), Chambers Global (IP) で高評価
- Legal 500 Asia Pacific (TMT, IP) で高評価
- ALB Asia Super 50 TMT Lawyersに選出
- IAM Patent 1000 / IAM Global Leadersに選出
- World Trademark Review 1000に選出
- Asia IP Top 50 IP Experts of Japanに選出
- Asialaw Leading Lawyersに選出
- Best Lawyers in Japanに選出
- Who's Who Legalに選出
- 日本経済新聞の企業法務・弁護士調査で高評価
- 週刊東洋経済の弁護士ランキングで高評価



1

はじめに

テクノロジーとプライバシーを取り巻く諸課題

AI・IoTの進展に伴い、問題は多様化・複雑化している

個人情報法制定時の ガバナンスモデルの想定

限定的なデータ活用

消費者はサイバー空間からの
逃避が可能

消費者は、自己のデータが
どう利用されるかを想像し
やすい

技術発展に伴う変化

- 広汎なデータ収集
- AIによるプロファイリング
- 生成AIによるハルシネーション

- AI・サイバー空間が日常に浸透
- 消費者は逃避が困難に

- 消費者による認識に限界
- 情報の非対称性が顕著に

現在のガバナンスモデル で解決すべき課題

- 多様なサービス・レイヤー
での利活用
- よりセンシティブなデータ

プライバシーリスクにかかわ
らず利用せざるを得ないサー
ビスが増加

自己情報のコントロールが一
層困難となり、企業や技術に
対する不信が増加

一律のルールベースのデータ保護法
でも最低限の対応ができていた？



- 問題の多様性に応じた対応も必要に
- データ活用への信頼性・透明性もよ
り強く求められるように

これまでの個人情報法の主な特徴

対象情報の区分

- 個人情報、個人データ、保有個人データ
- 要配慮個人情報とそれ以外
- 様々な種類の非個人情報

処理行為の区分

- 一定の類型について原則**同意**が必須
(個人データの第三者提供、要配慮個人情報の取得)
- それ以外は、**利用目的中心主義**

主にルール・ベース

- 対象情報や処理行為に応じて、OKな行為とNGな行為を線引き
- プリンシプル・ベースでの規律は少ない

主に手続的規律

- **予防的措置**として遵守すべき手続に主眼
- 事後処理は民法上の不法行為等に委ねる
(不明確で過剰な事後規制には謙抑的)

プライバシーとの関係

- 個人情報の取扱いに関する私法上の権利利益の内容・
範囲を直接確定し保護するものではない

テクノロジーと、個人情報法の解釈

急速な技術進歩に、法解釈が追い付かない状況

生成AIの利活用

個人情報委の「注意喚起」（2023.6.2）は出されたものの、残る課題は多い

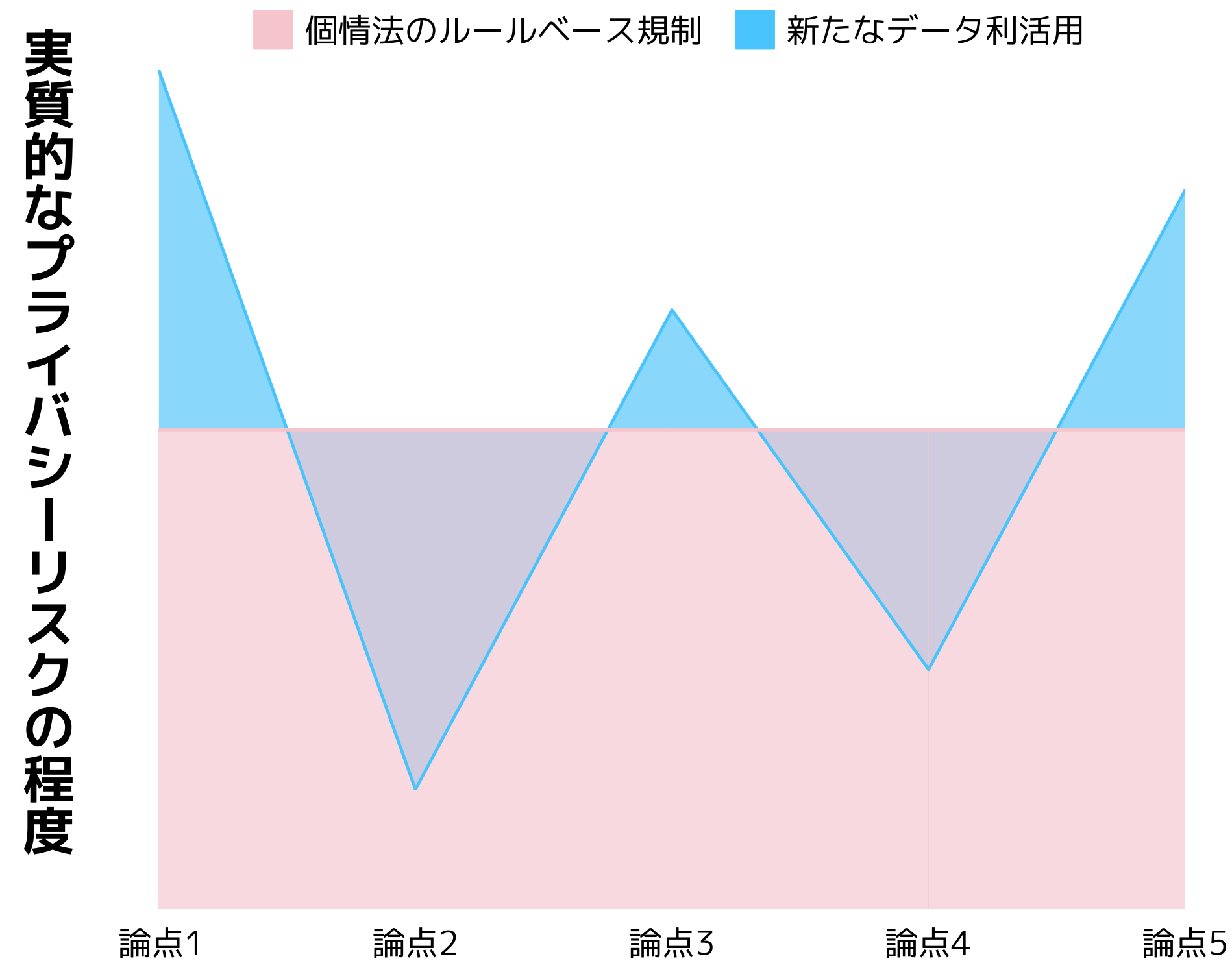
- クラウド例外の範囲は？
- 要配慮個人情報の取得規制との関係
- 利用目的規制と汎用AIの関係
- ハルシネーション対応への限界
- 複数事業者からの委託をどう整理？

プライバシーテック（PETs）

様々なテクノロジー（**秘密計算**、**差分プライバシー**、**合成データ**、**連合学習**など）が注目を集めているが、個人情報法上の整理は十分でない

- 「個人情報」の該当性
- 安全管理措置との関係
- 漏えい報告と「高度な暗号化」

実質的なプライバシーリスクと、ルールベース規制のギャップ



2-1

個人情報・個人データの概念: 試行錯誤の歴史

「個人情報」と関連する概念: 法改正とその限界（混乱？）

情報通信技術の発展、ビッグデータ時代の到来をふまえて改正が重ねられてきたが…

個情法の
制定

「個人情報」:

- 生存する個人に関する情報であって、
- **個人識別性**を満たすもの（**容易照合性**がある場合を含む）

H27改正
①

「個人識別符号」概念の導入:

- 2条2項1号/2号において限定列挙
- 民間サービスに係る符号は規定されず

H27改正
②

「匿名加工情報」概念の導入:

- 規制緩和？（むしろ規制強化にすらみえる…？）
- グレーゾーンの解消という目的の達成は疑わしい？

R2改正
①

「仮名加工情報」概念の導入:

- 個人情報に該当する／しない場合、事業者の主観による違い
- 当初想定ユースケース（機械学習用データセット等）の妥当性？

R2改正
②

「個人関連情報」概念の導入:

- 新たな情報の類型を定義し、その提供行為の一部のみ規制するアプローチ = 個人情報の定義を拡大するアプローチは採用せず

「**準個人情報**」（仮称）を
類型化し、個人情報等の範
囲を拡大することが議論さ
れていたが…

- **加工基準**の分かり難さ
- **主観要件**の分かり難さ
- **実務的ニーズ**に即した
制度への組替が必要？

端末識別子の利用を念頭
に、「提供元において非個人
データ、提供先において
個人データ」の場面に対応

「個人データ」の該当性をめぐる議論の難しさ

主に、第三者提供、開示・訂正等請求権の文脈で問題に

「個人情報」と「個人データ」の区別をめぐる幾つかの論点

開示請求権 東京地裁 R4.6.10	検索エンジンによる 検索結果	生成AIによる 出力結果
銀行の顧客が、自らの銀行口座への銀行従業員のアクセス履歴の開示を求めた 顧客情報の日常的な管理のために必須とはいえないとして、「個人情報データベース等」に該当しないと判示した 控訴審は、個人識別性の要件を満たさない（「個人情報」でない）と判示 ➡ 開示請求権は及ばない	立法当時の政府見解、通説は原則として該当性を否定 - 体系的に個人情報としての索引が付されておらず他の情報と混在 - 但し、個人情報だけを選別して検索できれば該当する可能性あり ➡ 検索結果の提供は、個人データの第三者提供に該当しない	該当性を否定する考え方が一般的 体系的に個人情報としての索引が付されておらず入力された内容に応じて都度確率的にもっともらしい出力を生成しているにすぎない ➡ 出力結果の提供は、個人データの第三者提供に該当しない

他方で、近時の規則やGLの改正では、両概念の境界線がかえって曖昧になった面も…

- **安全管理措置**：「個人情報であって、当該個人情報取扱事業者が個人データとして取り扱うことを予定しているものの漏えい等を防止するために必要かつ適切な措置も含まれる。」
- **漏えい等報告**：「個人情報であって、個人データとして取り扱われることが予定されているものを含む。」（規則7条3号）

以上のような個人情報／個人データ／保有個人データという**3層構造の是非**や、**個情法が対象とすべき情報の範囲設定**をめぐっては、様々な議論がある

2-2

「通知＋同意」モデルをどう考えるべきか

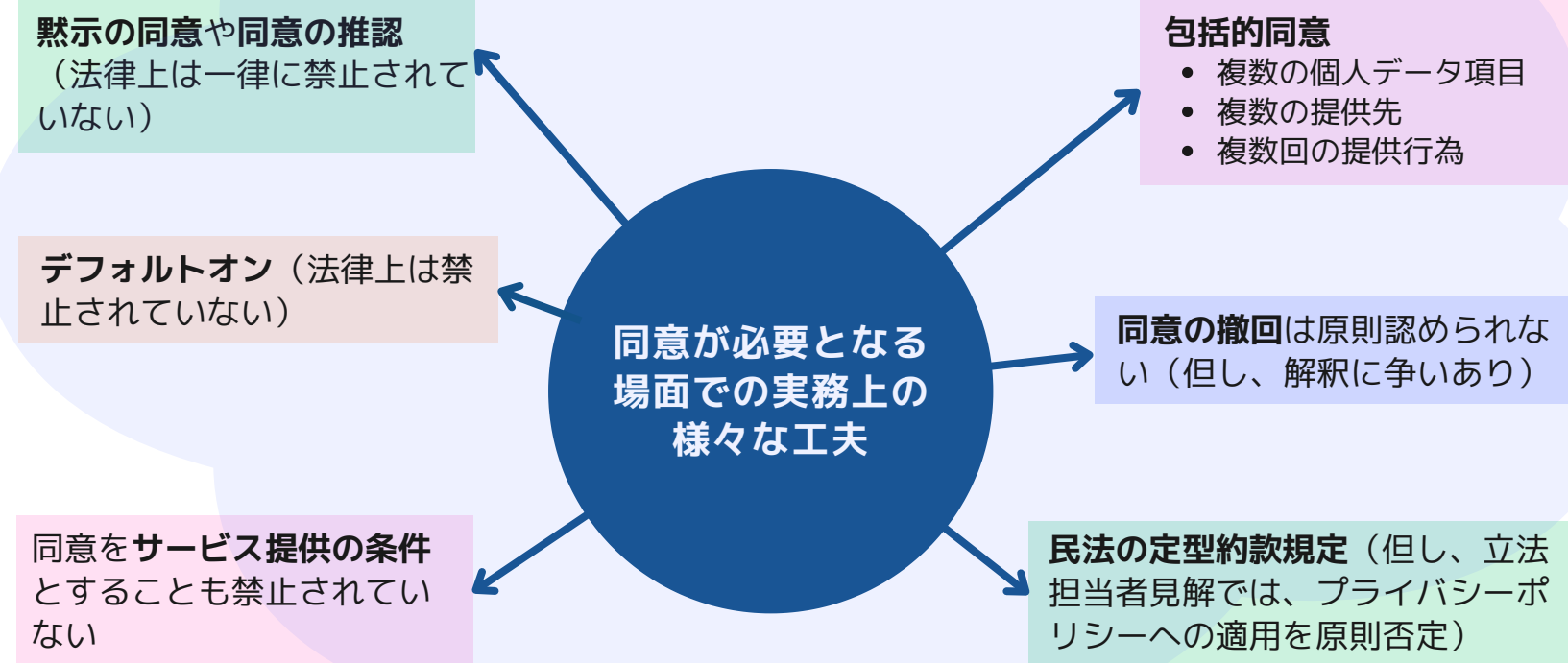
「通知と同意」モデルの限界？

これまでの個人情報法：ルールベースでの手続的規律に主眼を置いてきた

- 一定の類型（ex.個人データの第三者提供）で同意を要求。その他は利用目的中心主義
- 予防措置として遵守すべき手続に重点 ▶ 事後処理は、民法上の不法行為等でカバー

「同意」概念の柔軟な解釈

解釈上の工夫により、実務上の支障を防止？



いわゆる「クラウド例外」のなし崩しの拡大？

個人情報委Q&A7-53: クラウドサービス提供事業者が、**当該個人データを取り扱わないこととなっている場合**には、「提供」に該当しない

- 契約条項によって当該外部事業者がサーバに保存された個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合等

「クラウド例外」がカバーする範囲は事実上拡大してきた印象。
例えば、

- 非常時や緊急時にベンダによるデータへのアクセスを例外的に合理的範囲で許容する条項が規定されていても、問題ないと解される
- 生成AIの文脈で、個人情報委の「注意喚起等」(2023.6.2)は、利用事業者が入力する個人データをAI事業者が「機械学習に利用しないこと」が担保されていれば、クラウド例外に依拠できる趣旨に読める

以上のような解釈上の工夫の一方で、**近時の個人情報法改正：実体的規律の整備も充実してきた**

- R2改正が、**不適正利用の禁止（19条）**を追加

同意概念の形骸化と、同意疲れの問題

個人情報全体のフレームワークとの関係を考慮する必要性

日本では、「**個人データ**」「**第三者提供**」「**同意**」の各概念につき、実務上の支障を回避するため、ガラパゴス的な解釈をパッチワーク的に積み重ねてきた結果、**同意概念の形骸化**をはじめ、世界の潮流との整合性も取れなくなっている？

また、第三者提供規制の例外としての「**共同利用**」や「**委託**」については、書かれざる解釈上のルールの占める割合が大きく、混乱を生む要因にもなっている

他方で、日本法における同意概念等を単純に厳格化すればよいわけではない：

- ▶ これまで個人情報法が設定してきたルールそのものの妥当性の検証が必要？
- ▶ 真に本人が関与すべき範囲をどのような方向で精査すべきか？

同意や第三者提供の法的位置づけは、各国法によって異なる

- **GDPR**: 第三者提供は処理行為の一環にすぎず、また同意は様々な適法化根拠のうちの一つにすぎない
- **CPRA**: 第三者提供についてオプトイン同意中心主義を採用しているわけではない
- **日本**: 第三者提供につき本人同意原則を定めているため、同意の有効性をある程度柔軟に認めなければ、他の適法化根拠に依拠できない結果、合理的な範囲での個人データ処理まで過度に制約されることになり、実務上の運用としてワークし難い

また、**同意疲れ (consent fatigue)** の問題もある

AI・IoT時代における同意の難しさ

IoTの進展等に伴い、従来典型的に想定されていた同意取得の場面とは異なる配慮が求められるケースも増えている。

例えば、コネクテッドカーを通じたデータ利活用の場面では、

- **契約者**が利用規約に同意するだけでは、**家族や友人**が運転する場合のプライバシーへの配慮が不十分ではないか
- **運転者**がディスプレイを通じて同意するだけでは**同乗者**のプライバシーへの配慮が不十分ではないか
- ライドシェアの場合どうなるのか

また、**世帯プライバシー**の問題も顕在化しやすい。

AIについても、プロファイリングによる推測、隠れたバイアス（公平性の問題）、ハルシネーションなどの問題はあるが、アルゴリズムから明確に予測することは難しく、将来的な問題点の可能性について把握した上での実効性ある同意がどこまで可能なのか、という問題はある。

2-3

データ利活用についての制度的検討の本格化

データ利活用につき、体系的・横断的に検討する必要性

データ保護との「二項対立」ではないことを正しく認識すべき

AIやデータ利活用の正の効果を最大化するとともに、負の効果を抑止する

- 個人情報とはもとより、非個人情報も含めた横断的な検討
- 個人情報法の守備範囲と、特別法の守備範囲をどう切り分けていくか

2024.11.12 デジタル行財政改革
会議（第8回）資料より抜粋:

(今後の取組)

- デジタル行財政改革の下で、
2024年内に検討会を立ち上げ、検討を行い、2025年夏を目途に、我が国のデータ利活用制度の在り方についての基本的な方針を策定する

出典: 2024年11月12日同会議資料3「デジタル
行財政改革の今後の取組方針について」

データ利活用：EUと日本のデジタル関係の法制度の整備						
	データ関係			競争政策関係	AI関係	サイバーセキュリティ関係
	データ保護の法的強化 各分野におけるデータ利活用に影響	データ利活用の法的強化 ①個人起点（一次利用）、②社会起点（二次利用）等でのルール整備が進展 ※GDPRと整合的な形でEHDS法等は整備				
EU	GDPR (2016)	データスペース構想 (2020) 国や組織を超えてデータを連携できる空間に関するルールや仕組みを整備する構想。ヘルスケア、産業・製造等の9分野を指定	データガバナンス法 (2021) オープンデータ以外の政府のデータ共有促進 データ法 (2023) 民間の非個人データ (IoT等) の共有促進 EHDS法 (医療・2024) ・ヘルスデータ基盤の構築 ・ヘルスデータ(仮名化・匿名化済)の第三者提供に同意不要 ・医療機関からのデータ提出義務 PSD3（金融決済・検討中） ※PSD2は2015に成立 金融データアクセスの枠組と連携したPSD2の改正	デジタル市場法 (2022) 競争可能で公正な市場の確保	デジタルサービス法 (2022) 消費者と企業へ安全なオンライン環境を創出	EU AI法 (2024) 人間中心のAI開発政策の具体化
						サイバーレジリエンス法 (2024) デジタル要素を含む製品への水平的なサイバーセキュリティ要件の整備
日本	個人情報保護法	日本では、一部の対応※にとどまる。 ※次世代医療基盤法・銀行法等		PF透明化法 スマホ競争促進法	電気通信事業法等で一部対応 検討中	サイバーセキュリティ基本法をはじめ、各種ガイドライン等で対応 (IoTセキュリティ適合性評価制度 (JC-STAR) ※2025.3制度開始予定)

(続) 2024.11.12 デジタル行財政改革会議での議論

尖戸構成員資料からの抜粋：

…本会議の下でデータ利活用制度についての基本的な方針を検討することとなったことを歓迎する。その上で、

- (ア) データ共有の促進に当たって、データ保有者間のデータの提供・連携、データ連携基盤の設置等の様々な方策が考えられるところ、それぞれのメリットやリスク、コストの分担、分野ごとの特性等に合わせた検討が必要であること
- (イ) これまで、個人情報保護法などの情報を保護する規律の外はデータ利活用は法的に自由であるとの建前であったにもかかわらず、現実にはデータ利活用が進まなかった要因を丁寧に分析し、必要であれば積極的な促進のための規律をも検討すべきこと
- (ウ) EUで個人データを保護するGDPRを前提としつつ、それと整合的な形で医療データの利活用のための制度が本年春に整備されるなど、海外における全体的なデータ政策の急速な展開を踏まえつつ検討すべきこと
- (エ) 既存のデータの利活用にとどまらず、とりわけ本会議が目指すデジタル行財政改革に必要なデータの生成・加工のあり方についても検討すべきこと
- (オ) データ利活用が個人や社会にとっての「**データによる自由**」の実現に奉仕し、データ利活用によって生じるリスクをアジャイルに分析しその低減を可能にするために必要なガバナンスを、データ利活用に関わる主体や社会全体において構築すること

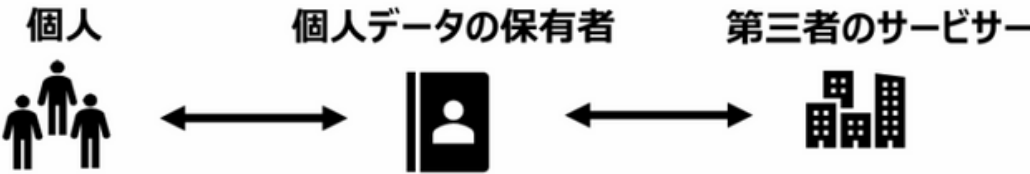
を検討の視点に含めるべきものとする。

個人起点・社会起点のアプローチと、重要分野の例

データ利活用：重要分野のデータ利活用の課題の例

【データ利活用に関する主なアプローチ】

①個人起点でのデータアクセス



- 個人の同意の上で自らのデータを第三者に提供
- 自らに最適化した商品やサービスの提供を受けられる

②社会起点でのデータ利活用



- 個人データを集積して社会課題の解決に活用
- 公益実現、経済発展とともに個人にも利益が還元

【データ利活用が重要と考えられる分野の例】

	医療	教育	金融
データ利活用の進展状況	• 医療DXの推進に関する工程表に基づいた取組を推進（全国医療情報プラットフォームの創設等）	• GIGAスクール構想の下、1人1台端末の実現、個別／協働学習を可能にするデジタル教材の普及	• 銀行法APIによりフィンテック事業者による新たなサービスの提供
データ利活用の論点	• 利用可能な医療データの充実、電子カルテ等の共通化	• 初等中等教育段階のアーキテクチャやID管理の実現方策の検討、次世代校務DX環境の整備（学習系・校務系データ等の連携）	• クレカ、電子マネー等の各種決済データへのAPI連携の検証・検討（セキュリティ上のリスクがあるスクレイピングからの脱却）
データ利活用のメリット	• 個人はどの医療機関でも自らの診療情報を参照できる • 創薬の研究開発に活用できる（EUではコロナワクチンの経験も議論に反映）	• 個別最適な学び・協働的な学びの一体的な充実につながる • 校務負担の軽減・学校の働き方改革につながる	• 各種決済サービスの利用にあたり手数料の低減を期待できる • 個人や中小企業が効率的に家計・会計の管理ができる

18

出典：2024年11月12日同会議資料3「デジタル行財政改革の今後の取組方針について」

2-4

**交錯する法領域と、
重層的なレイヤーでのアプローチによる相互補完
～ダークパターンへの取組みを例として～**

ダークパターンとは？

統一的な定義はないが、SPSI改定案（後述）によれば、

- サービスの利用者を欺いたり操作したりするような方法又は利用者が情報を得た上で自由に決定を行う能力を実質的に歪めたり損なったりする方法で、ユーザインタフェースを設計・構成・運営すること

特集 消費者を欺くダークパターンとは
特集 1 ダークパターンとは

OECD（経済協力開発機構）は2022年に「ダーク・コマーシャル・パターン（Dark commercial patterns）」^{※3}と題したレポートを刊行しました。このレポートにまとめられている類型化をもとに、ダークパターンを紹介しましょう。

1. 行為の強制（Forced Action）
特定の機能にアクセスさせるために、何かを強制的に行わせようとする。

- 必須であると偽り会員登録をさせる。
- サービスにおいて不必要な範囲までの個人情報の開示を強制する。
- 消費者の同意なく連絡先情報を抽出する。

図1 「行為の強制」の例。商品を開覧したいだけなのに、会員登録を求められた

2. インターフェース干渉（Interface Interference）
情報をフレーミングする（切り出す）ことによって、企業にとって都合のよい行為の実行を促す。

- 重要な情報を視覚的に不明瞭にする。
- 企業にとって都合のよい選択肢をデフォルトの選択肢にする。
- 虚偽の高値に対して割引した値段を表示する。

図2 「インターフェース干渉」の例。ある選択肢が他の選択肢と比べて目立っている

3. 執拗な繰り返し（Nagging）
企業にとって都合のよい行為を行うよう消費者に繰り返し要請する。

- 通知や位置追跡機能を有効にするようしつこく要求する。

図3 「執拗な繰り返し」の例。「はい」「あとで回答する」のように、拒否する選択肢がないポップアップが何度も表示される

4. 妨害（Obstruction）
ある行為を諦めさせる意図で、タスクの流れやインタラクションを必要以上に困難にする。

- サービス登録の容易さに比べて、解約を困難にする。
- アカウントや個人情報の削除を困難または不可能にする。
- 異なる条件や単位で商品を提示することによって価格の比較を困難または不可能にする。

図4 「妨害」の例。退会／解約に手間や時間がかかる

5. こっそり（Sneaking）
消費者の意思決定に関連する情報を隠したり、偽装したり、告知を遅らせようとする。

- カートに商品をこっそり追加する。
- 消費者の明確な同意を得ずに、トライアル期間後に契約を自動更新する。

※3 OECD Digital Economy Papers, No.336 (2022) <https://www.oecd.org/digital/dark-commercial-patterns-4415e846-en.htm>

国民生活 2024.3 ②

特集 消費者を欺くダークパターンとは
特集 1 ダークパターンとは

図5 「こっそり」の例。定期購入なのに1回だけの購入であるかのように表示されている

図6 「社会的証明（Social Proof）」の例。他の消費者の行動に関する通知をする

図7 「緊急性（Urgency）」の例。割引期間の終了をカウントダウンタイマーによって表示する

図8 ダークパターンに至る3つのトレンド

●ダークパターンが生まれるしくみ

ダークパターンが生まれた背景
「Dark Patterns: Past, Present, and Future」(脚注2)では、ダークパターンに至る3つのトレンドが挙げられています(図8)。これらを順に解説しましょう。

(1) 小売業における欺瞞的な慣行
ダークパターンの問題に先立って、心理学的効果を利用して顧客の意識を誘導するようなアプローチは商慣習として一般的になっていました。例えば、「サイコロジカルプライシング(心理的価格付け)」と呼ばれる、99円や1999円といった価格設定の戦略はよく知られています。人々は100円といわれるよりも99円といわれたほうが心理的に安く感じる傾向があります。また、異なる単位で比較させたり、二重の割引率を提示することで消費者を混乱させ、より高い価格の商品へ誘導するような施策も、スーパーマーケットの店頭などでよく見られます。このような小さな施策が、ダークパターンを許容してしまうような倫理観を構築している、と前述のナラヤナンらは指摘しています。

(2) 公共政策における「ナッジ」
これに加えて、公共領域から始まった「ナッジ(Nudge)」の影響が挙げられています。ナッジとは、「ひじで突つく」という意味ですが、まさにちよっとひじで突つくように人に行動を変えるきっかけを与え、気づかぬうちに行動変容をもたらすような施策を意味します。

(出典) Arvind Narayanan, et al., Dark Patterns: Past, Present, and Futureの図をもとに筆者作成

国民生活 2024.3 ③

出典: 2024.3 国民生活 特集
「ダークパターンとは」(長谷川敦士)

ダークパターン: 日本国内での法規制

ダークパターンを正面から**横断的・包括的に規制した法律はまだ無い**

- 違法と適法の境目が曖昧であり、グラデーションのある概念であることの難しさ
 - はっきり嘘はつかないが、心理学的効果を利用して顧客の意識を誘導することをどう捉えるか
- 但し、特定の類型の行為については、事実上既に個別に規制されているものもある**

特定商取引法

通信販売での広告や申込画面で一定の表示を義務付け

▶サブスクの規制強化（2022.6～）

- 提供するサービスの期間、回数等
無期限や自動更新の場合、その旨も
- サービス料金
有料サービスへの切替時期など
- キャンセル・解約に関する事項
解約方法や条件を明示

景品表示法

優良誤認・有利誤認表示を禁止

▶ステマの規制強化（2023.10～）

- 一般消費者が事業者の表示であることを判別することが困難な表示を、
不当表示として規制

広告であることを分かりやすく表示
する必要がある

ダークパターン: 欧米での法規制

横断的な規制と、個別の規制のそれぞれが存在する

- 新たな法律を導入するアプローチ
- 従来から存在する法律をダークパターンの文脈でも積極的に活用するアプローチ

欧州

デジタルサービス法: オンラインプラットフォームにおけるダークパターンの利用を明示的に規制

- オンラインプラットフォーム事業者は、サービス利用者を欺いたり操ったり、サービス利用者が情報に基づく自由な決定を行う能力を実質的に歪めたり損なったりする方法で、オンラインインターフェイスを設計、構成、運用してはならない。

GDPR: 個人情報保護の文脈で、ダークパターンに関するガイドラインを公表

不公正取引行為指令(UCPD): 消費者保護の文脈で、ダークパターンに言及するガイダンスを公表

米国

FTC法: 「不公正又は欺瞞的な行為・慣行」を広く禁止

- Epic Gameの事例（ダークパターンによる課金誘導）
- Amazonの事例（複雑な解約プロセス、係争中）

カリフォルニア州のCCPA: 個人情報保護の文脈で、ダークパターンによる同意を無効とした

- 規則で、ダークパターンに該当する可能性のある行為を列挙
 - オプトアウトをするのに、オプトイン同意を取得する場面よりも多くのステップを要求する
 - Yes と Ask me laterの選択肢
 - 本来関係ないはずの利用目的への同意とバンドルする

ダークパターン対応の、今後あるべき姿は？

日本でも、消費者法、個人情報保護法（例：不適正利用）、独占禁止法などの既存の法律の抽象的な条項を今後当局がより柔軟に活用していく可能性はある

他方で、法律で全て対応することには限界があることも事実

▶ **国・民間の様々なレイヤーでのアプローチ**が相互補完的に機能することが必要に

総務省：利用者情報に関するワーキンググループ報告書案

スマートフォン プライバシー セキュリティ イニシアティブ

2024.10.17「消費者法制度のパラダイムシフトに関する専門調査会 中間整理」

- 「消費者の自律的な意思決定を支援する仕組みにおいては、消費者団体を始めとする多様な団体の活躍が期待される。例えば、**ダークパターンにより自律的な意思決定をゆがめるという問題**や情報、時間、関心・アテンションが奪われるという問題のように**実害を感じにくい**、あるいは**経済的な損失の発生に至らない問題**については、消費者本人では気づきにくいいため、消費者の意見を集約してあるいは消費者利益の観点から活動（提言）する組織が、モニタリングしていくことが必要である。」

SPSI改定案からの一部抜粋

1.2.1.6. ダークパターン回避の対応

- 利用者利益の保護を図るため、サービスの利用者を欺いたり操作したりするような方法又は利用者が情報を得た上で自由に決定を行う能力を実質的に歪めたり損なったりする方法で利用者情報の取扱いを行わないことが望ましい⁴⁹。

【補足】

ダークパターンの具体的な事例は、例えば以下の場合が考えられる⁵⁰。

- アプリケーションの利用開始後に利用者情報の取得・利用をオプトアウトすることが可能であるにもかかわらず、利用開始時には同意を拒否する選択肢が提示されず、デフォルトで同意をすることとなっている場合。
- 同意を取得する場合の操作に比べ、同意を撤回する場合の操作が煩雑になっている場合、又は同意を撤回する方法に容易に到達することができない場合。
- 同意の取得画面において、同意ボタンが目立つように表示されており、拒否するボタンが表示されていない又は目立たない形で表示されている場合。
- 利用者が一度拒否したにもかかわらず、同意が得られるまで繰り返し同意取得画面を掲出する場合。
- 同意の取得画面又はその直前の画面において、利用者情報の取得・利用に同意することによるメリット又は同意しないことによるデメリットのみを強調し、同意へ誘導している場合。
- 同意取得時に、利用者に対して金銭等のインセンティブを提示することにより、同意へ誘導している場合。
- 同意取得時に、後で同意を撤回する方法が用意されている旨説明していたにもかかわらず、実際には同意を撤回する方法が用意されていない場合。情報の取得範囲を利用者が設定できるようにしている場合において、より多くの情報を取得する選択肢がデフォルトで選択されている場合。

一般社団法人ダークパターン対策協会の取組み①

- 消費者が正しい判断を行えるようにする一つの目安として、誠実なWebサイトを審査・認定し、改ざんできないロゴマークを付与する仕組みを提供するとともに、消費者の方々にダークパターンに関する注意喚起やロゴマークの普及啓発活動を行う。
- 誠実なWebサイトの認定について、出来ていない事象を広義のダークパターンと捉え、**非ダークパターン認定**
(Non-Deceptive Design Accreditation : NDD認定)
(仮称) という名前で検討中。

11/13に正会員を募集開始。
有識者、政府関係者も参加する制度・
ガイドライン構築分科会で1月をめど
にガイドライン、チェックリストを策
定し公開することを目指している。
2025年7月から審査を開始できるよう
準備を進めている。

悪質誘導「ダークパターン」対策、協会が優良企業を認定

情報通信・ネット + フォローする

2024年10月2日 14:47

保存

あA 印刷 メール n X f 共有

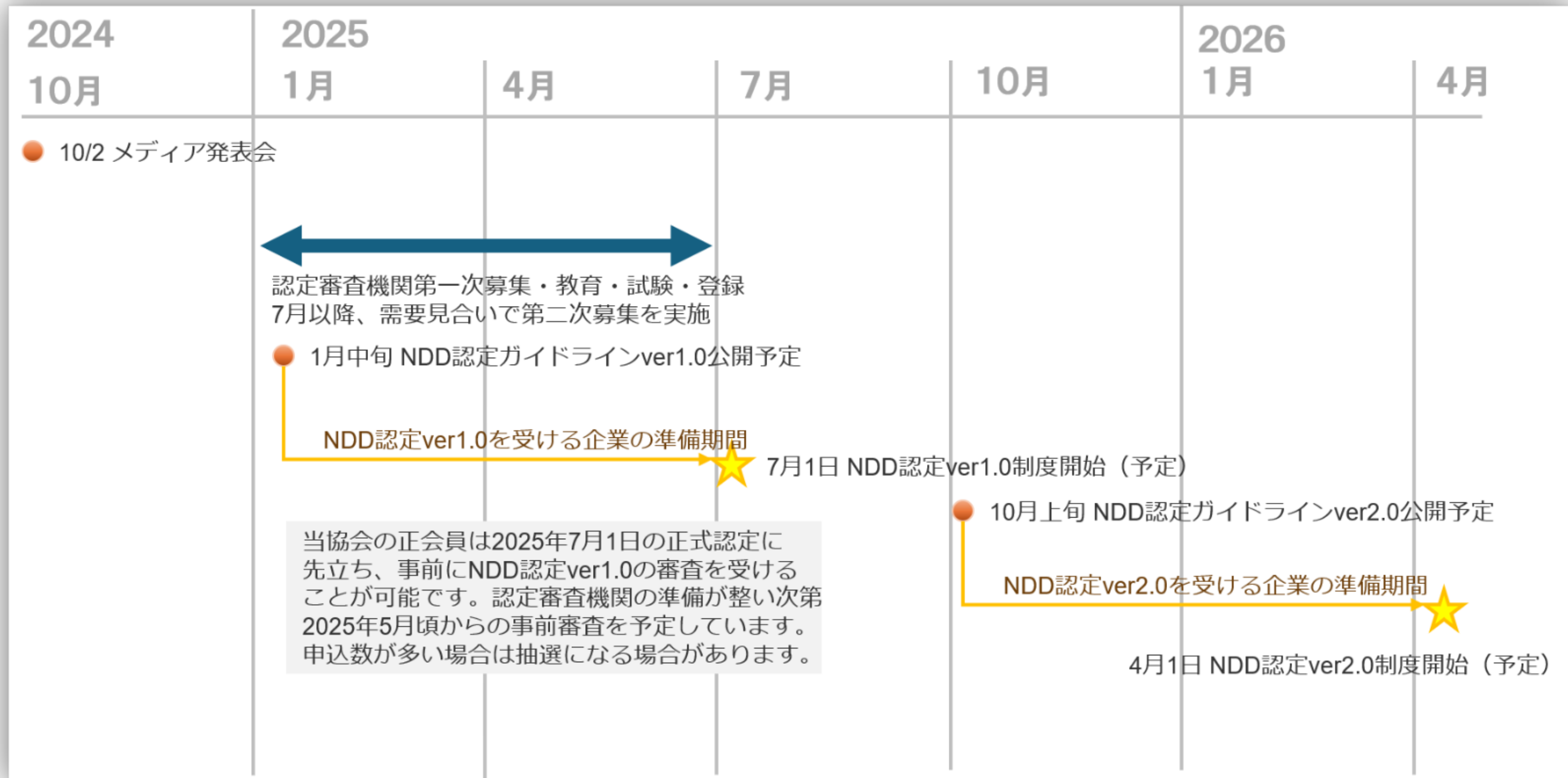


設立会見には北島康介さん（左から3人目）らが出席した（2日、東京都目黒区）

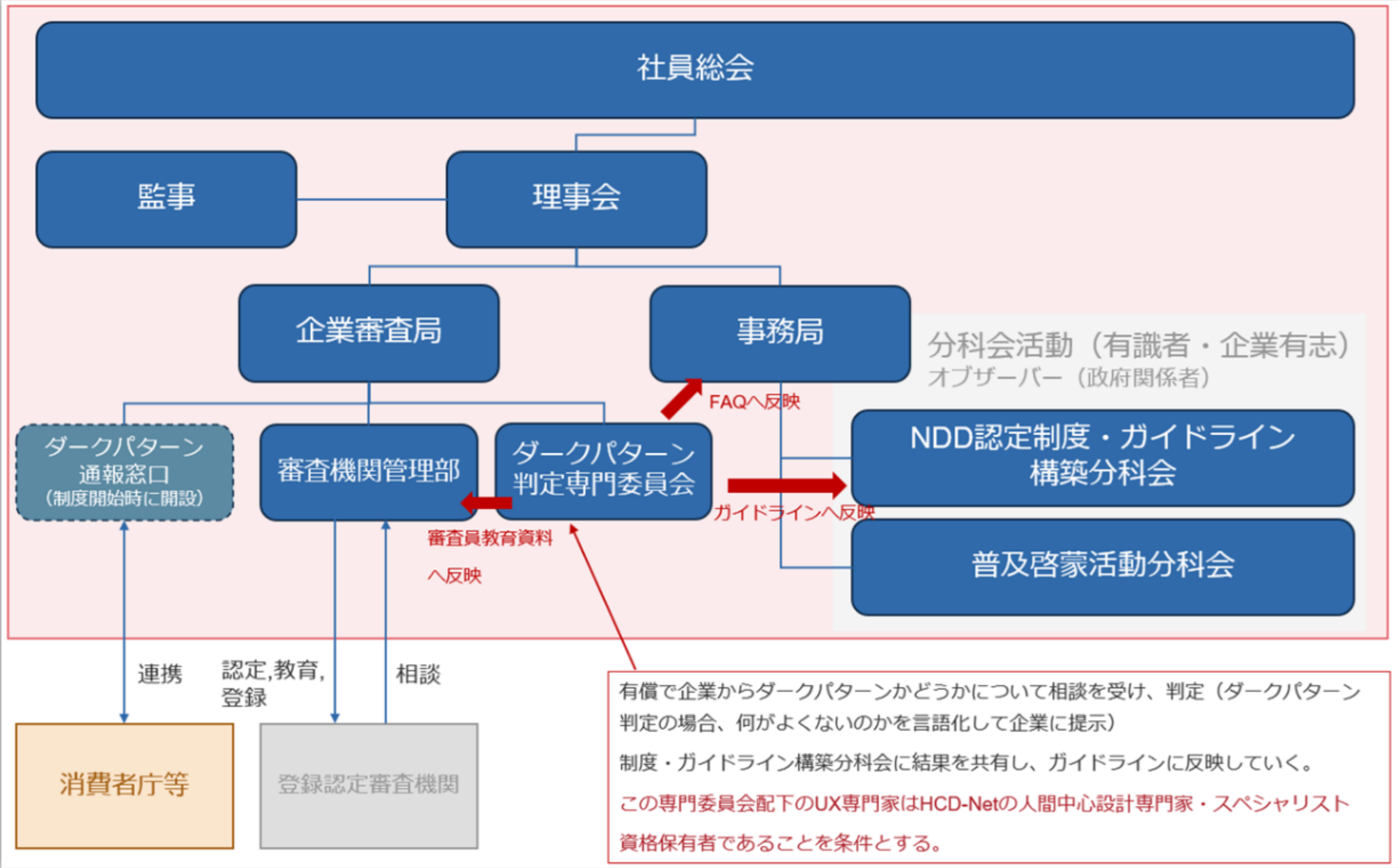
ウェブサイトなどの利用者を本来の意思に沿わない選択肢に誘導する「ダークパターン」の被害低減を目指す団体が2日、東京都内で記者会見を開いた。利用規約の同意画面などが消費者に配慮されているかどうか、企業を認定する制度を2025年7月にも始める。国内の年間被害額は最大1兆7000億円規模とみられ、消費者への浸透を図る。

出典: 2024.10.2 日本経済新聞

ダークパターン対策協会の取組み②（スケジュール案）



ダークパターン対策協会の取組み③（審査体制・プロセス案）



3

おわりに

個人情報・消費者法が転換期に：事業者求められる役割は？

これからの個人情報法は、どうあるべきか？

- **自己決定・同意**のコンセプトをどのように位置付けるか
- **実体的規律**をどう適切に運用していくか
- **プリンシプル・ベース**の規律についてどのように考えるべきか
 - 規制すべきものが規制されず、逆に規制緩和してもよい規制が残ったままとなっていないか
 - 規制や執行の不備を埋めるとともに、事業者の**自発的なガバナンス**を促すことはできるか

2024.10.16 個人情報委「個人情報保護法のいわゆる3年ごと見直しの検討の充実に向けた視点」

2024.10.17 消費者委員会「消費者法制度のパラダイムシフトに関する専門調査会 中間整理」

2024.9 一般社団法人ダークパターン対策協会の設立

法律に書かれていることを守るという伝統的な法務・コンプラマターではなく、ユーザー目線で横断的なリスク判断を**主体的に選択し実践する経営マター**としての要素が一層強まる

- ▶ 個人情報法に頼りすぎない、期待しすぎないことも大切に
- ▶ 正直者が損をしないような取組みなども、相互補完的に作用することが望ましい

「個人情報保護法のいわゆる3年ごと見直しの検討の充実に向けた視点」

以下では参考までに、主要項目の一部のみ要約

1

個人データの利用の適正性を本人の関与により規律しようとする仕組みの実効性

- 自律的ガバナンスを重視する現行制度の考え方
- 利用目的の特定、データ処理の説明のあり方
- 実体的ルールを設けることにより、本人の関与による規律に依存しないアプローチ
- プロファイリング等につき本人の権利保護の実効性
- 本人がより能動的に関与し得る仕組み

2

個人の権利利益への直接的な影響が想定されない個人データの利用に対する規律の考え方

- 統計的利用などにも、本人の関与を通じて適正な利用を確保するという仕組みは求められるか？

3

個人データの第三者提供を原則として禁止する仕組みの妥当性

第三者提供を禁止する必要のない類型はあるか？

- 一般的・汎用的な分析に限定される場合
- 本人が、第三者提供を躊躇するとは想定されない場合
- 提供後も本人の権利利益の保護が図られる状態が保証される場合

4

取扱い態様の多様化の下における、データの適正な取扱いに係る義務を負うべき者の在り方

- クラウド、AIなど、データベースの構築・処理のプロセスについて第三者に依存するケースが拡大

5

守られるべき個人の権利利益の外延

- 端末識別番号やCookie情報等についても、従前の住所等と同様に、個人の権利利益を保護する上で注目すべきデータ類型であるとの視点をどう捉えるか

6

個人データそのものの特徴に起因する考慮要因

- 要配慮個人情報の規律は引き続き妥当か
- 容易に取得され、長期にわたり本人の追跡の手掛かりとなるなど、リスクの増大を助長する種類のデータにつき、特別な規律を課すべきか

最後にご紹介: 日本ディープラーニング協会での取り組み

詳細は今後公開予定

2024/11に「**法と技術の検討委員会**」を設立して、検討を開始

- 法律家から5名、技術者・ビジネスサイドから5名で構成

以下、「**設立趣旨**」より一部抜粋：

- 「近年の生成AIの急速な発展に伴い普及が急速に進むAIの利活用にあたっては、個人情報保護法や著作権法などの様々な法令に留意する必要がありますが、**これらの法令が制定された当時には想定されていなかったような態様でのデータの取得や利用が可能になっており、法解釈が明確でないものも少なくありません。**また、**法的リスクに加えて、AIを活用する企業のレピュテーションやAI倫理等の観点からも、判断に迷う問題もあります。**企業としては、このような未知の問題に対してリスクを適切に判断し、リスクをとるか否かを判断する必要があります。リスクを過小評価すると法令違反やレピュテーションの毀損が生じえますが、**リスクを過大評価するとイノベーションの障害となり、海外企業に先行を許すことにもなります。**
- **本委員会は、AIに関する法律・技術・ビジネスの専門性を有する委員が議論して議論内容を公表すること、及び議論内容を踏まえて積極的にAI利活用の前例を作出することを目的として立ち上げられました。**
(中略)
- **日本は、企業が法的リスクに対して保守的な対応をとる傾向にあり、また、訴訟が起こりにくく、司法によるルール形成プロセスが他国と比べて十分とはいえないなどの要因から、AIなどの新しい分野に積極的に取り組むことが容易ではありません。**そのような状況において、**本委員会の取り組みは、AIの開発・ビジネスにおける新しい標準を作る活動として非常に重要な意義を持つと考えております。」**