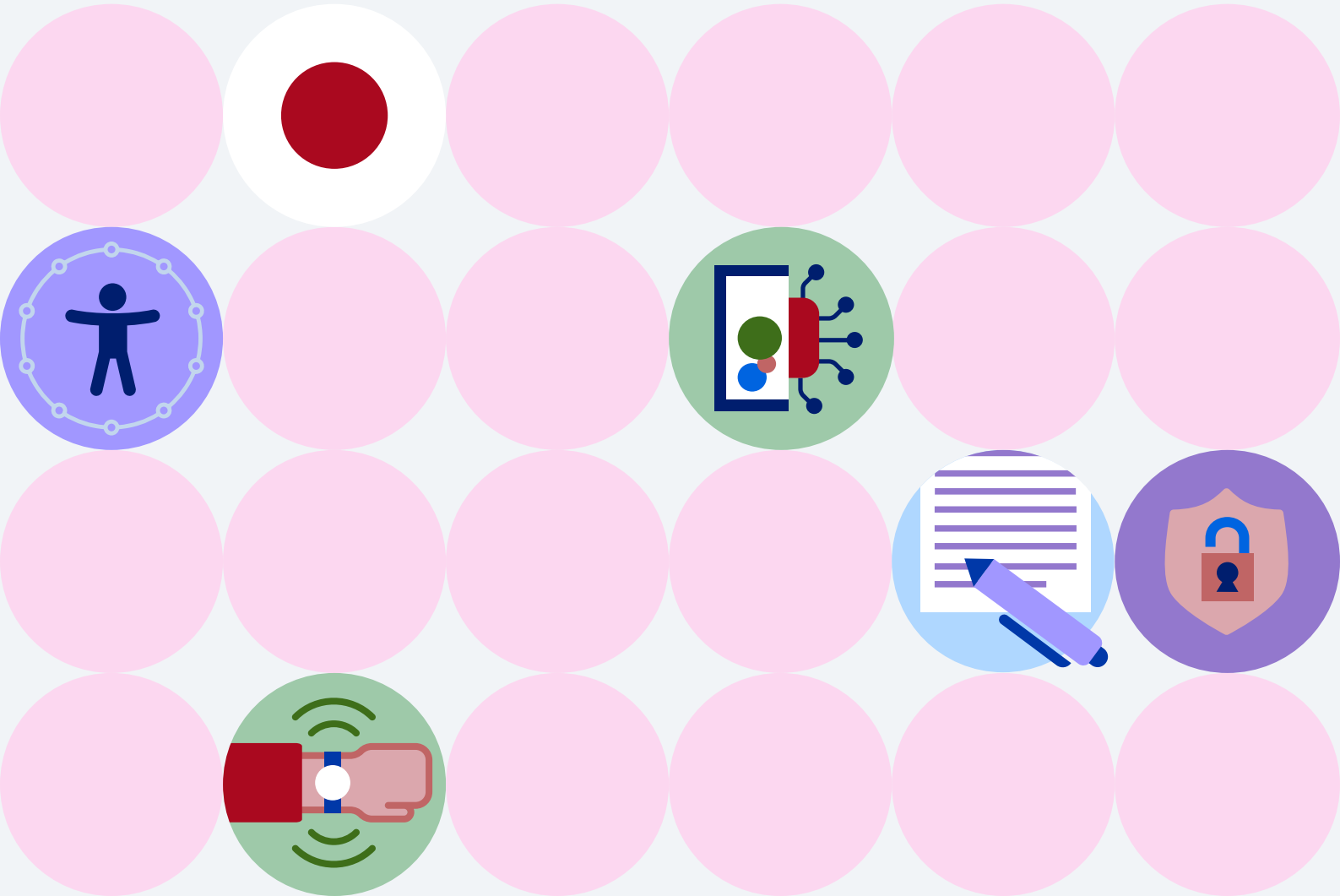
Open Loop | Meta

日本におけるAIおよびウェアラブル技術の責任あるイノベーションの推進

現行の法的指針を踏まえた課題と機会



目次

本プログラムおよび本報告書について 4

Open Loopについて 4
謝辞 5
序文 6

エグゼクティブサマリー 11

知見と提言 13
日本の政策への示唆 14

1 第1章 15

1.1 背景と目的 16
1.2 政策上の課題：AI搭載ウェアラブルデバイス時代における新たなデータカテゴリーの管理 16
1.3 Open Loop Japanの目標 17

2 第2章：調査結果、提言および機会 18

2.0 はじめに 19
2.0.1 本章におけるエビデンスについて 26
2.0.2 本プログラムのタイムラインと日本における法制度の動向 28
2.0.3 中心的な課題 29

2.1 知見1 – 日本のAIガイダンスは対象者に届いているが、参加者は法的拘束力のある義務への適合に関する疑問を解決するには不十分だと感じている 33
2.1.1 組織がすでに取り組んでいること 34
2.1.2 データが示すこと 35
2.1.3 組織が直面している課題 36
2.1.4 エコシステムへの示唆 38
個人情報保護委員会およびその他の政策立案者への提案 41

2.2 知見2 – 組織は、AI活動において個人情報を利用するためにどの程度まで非識別化を行う必要があるかの判断に苦慮している 44
2.2.1 組織がすでに取り組んでいること 45
2.2.2 データが示すこと 46
2.2.3 組織が直面している課題 46
2.2.4 エコシステムへの示唆 47
個人情報保護委員会への提言 48
その他の政策立案者への提案 49

2.3 知見3 – APPIにおけるAI出力およびモデルの分類は未解決のままである 50
2.3.1 組織がすでに取り組んでいること 51
2.3.2 データが示すこと 51
2.3.3 組織が直面している課題 51
2.3.4 エコシステムへの影響 54
個人情報保護委員会への提言 55

2.4 知見4 – 越境移転規則により参加者は日本国外でホストされるAIシステムの利用が妨げられており、クラウド規則は不確実性と躊躇を生じさせている 57
2.4.1 組織がすでに取り組んでいること 58
2.4.2 データが示すこと 58
2.4.3 組織が直面している課題 59
2.4.4 エコシステムへの示唆 62
個人情報保護委員会への提言 64
その他の政策立案者への提案 66

2.5 知見5 –ウェアラブルデバイスを規律するルールは現在策定中であり、決定的な問いは未解決である 67
2.5.1 本知見のエビデンスベース 68
2.5.2 参加者からの回答 68
2.5.3 新カテゴリーが求める要件と未解決の課題 69
2.5.4 フレームワークが発展を支援するか否かを決定する3つの問い 71
2.5.5 規制以外の制約：社会的受容 73
2.5.6 エコシステムへの示唆 74
個人情報保護委員会への提言 75
その他の政策立案者への提案 78

3 第3章：結論と今後のステップ 79
3.1 主要な知見の要約 80
3.2 日本の政策への示唆 85
3.3 今後の方向性 86

附録 88
I Open Loop Japanについて 89
i.i プログラムの趣旨 89
i.ii パートナー 89
i.iii 参加企業（コホート） 90
i.iv 調査方法 91
i.v 制約事項 93
II 主要概念と定義 95
注釈 97
参考文献 98

Open Loopについて

MetaのOpen Loopは、AIの専門家、政策立案者、企業をつなぐグローバルプログラムであり、新規または既存の政策、規制、法律、任意の枠組みに関する詳細なフィードバックを収集することで、AIおよびその他の新興技術に対する効果的かつエビデンスに基づく政策の策定を支援しています。

その目的は、新興技術に関するガイダンスおよび規制の質を向上させ、それらが理解しやすく、実務上実行可能であり、意図した成果の実現が見込めるものにすることです。

本報告書は、クリエイティブ・コモンズ 表示 4.0 国際ライセンスの下で提供されています。



謝辞

Open Loop Japanプログラムは、MetaがThe Future of Privacy Forum（FPF）およびAccenture Japanと連携して企画・運営しました。

本プロジェクトにおけるパートナーシップ、特に調査および運営面でのリーダーシップを発揮していただいたFPFの以下の皆様に感謝申し上げます。

- Josh Lee Kok Thong、アジア太平洋地域マネージングディレクター
- Dominic Paulger、アジア太平洋地域副ディレクター
- Bilal Mohamed、政策マネージャー
- Reina Sasaki、プロジェクトリサーチャー
- Lauren Koek、政策インターン
- Rachelle Faust、グローバルプライバシー担当シニアプロジェクトマネージャー
- Gabriela Zanfir-Fortuna、グローバルプライバシー担当バイスプレジデント

また、本プロジェクトの調査および運営面でご支援いただいたAccentureの皆様にも感謝申し上げます。

- Jimmy Sia、シニアリージョナルコマーシャルリード
- Isha Bhalla、シニアマネージャー
- Thomas Telandro、シニアマネージャー
- Kanji Endo、コンサルタント

最も重要なこととして、プログラム全体を通じてご参加いただいた以下の組織の皆様に感謝申し上げます。皆様のコミットメントと積極的なご参加がなければ、本報告書は実現しませんでした。

ベネッセコーポレーション
Citadel AI
Digital MICE
株式会社博報堂DYホールディングス
株式会社メルカリ
Schematching Inc.
株式会社テクノプロ
日本IBM株式会社
塩野義製薬株式会社

7社が匿名でプロジェクトに参加しました。

序文



先進的なAIとウェアラブル技術の融合により、パーソナライズされた体験、予防医療、そして日常的に利用する製品やサービスとのシームレスなデジタルインタラクションに向けた、まったく新しい可能性が開かれつつあります。しかしながら、こうした可能性には、身体由来データや生体データを含む新たなカテゴリーのデータをどのように収集、処理、保護すべきかという重要な問いも伴います。

これらの新興技術のガバナンスを適切に行うことは、単一の主体だけで達成できる課題ではありません。イノベーターに確実性を提供できるほど明確でありながら、急速な技術発展のペースに対応できるほど柔軟な、効果的かつエビデンスに基づくガイダンスが必要です。また、技術を開発する者と規制を担う者との間の緊密な協力も求められます。政策立案者と産業界が協働することで、包括的でリスクベースかつ実行可能であり、責任あるイノベーションを真に支援するガバナンスの枠組みを確保することができます。

日本はこれらの問いにおいてリーダーシップを発揮する独自の立場にあります。世界で「最もAIフレンドリーな国」になるという目標を掲げた日本は、2025年のAI推進法の成立や個人情報保護法（APPI）の改正を含む決定的な措置を講じ、イノベーションと効果的な保護のバランスを取るガバナンス環境の構築を進めてきました。この時期に下される選択は、日本国内のAIエコシステムを形作るだけでなく、アジア太平洋地域およびそれ以外の地域における規制アプローチにも影響を与えることになります。

このような背景のもと、私たちはFuture of Privacy Forum（FPF）およびAccenture Japanとの緊密なパートナーシップにより、Open Loop Japanプログラムを創設しました。これは、日本においてAI搭載ウェアラブル技術を開発・展開する企業が、この進化する規制環境にどのように対応しているかを、体系的かつエビデンスに基づくアプローチで理解することを目的としています。プログラムを通じて、私たちは日本で事業を展開する16社 および20名のAI・データ保護の第一人者と協働し、身体由来データや生体データを含む新たなカテゴリーのデータ処理に対して、 個人情報保護法（APPI）とAI事業者ガイドライン が実務上どのように適用されるか、また、どこでより明確性や一貫性が必要とされるかを検討してまいりました。

調査、インタビュー、および専門家会合を通じて、日本でAI搭載ウェアラブルを開発する企業が求めているのは、幅広い裁量ではなく明確なルールであることがわかりました。具体的には、非識別化のための実践的でリスクベースの基準 、識別可能性がない場合に学習済みモデルおよびその出力が個人データに該当しないという確信、事前に信頼できる越境移転メカニズム、そして生体データの新たなカテゴリーに対する実行可能な定義上の境界線です。その明確性が欠如している場合、企業は法令違反のリスクを冒すよりも、実現可能なユースケースの延期や縮小を選択すると述べています。本報告書は、これらの課題に対処すると考える提言を日本の規制当局および省庁に提供するものです。

今後数か月間にわたり日本のAIおよびデータガバナンスの枠組みの実施を形作る政策立案者および規制当局にとって、これらの知見と提言が価値あるも

序文

のとなることを願っております。さらに、個人を保護しながらイノベーションを可能にする形でAIおよび新たなデータカテゴリーを最善の方法で統治するにはどうすべきかという類似の問いに取り組んでいるアジア太平洋地域およびそれ以外の規制機関にとっても、本報告書が関心をお持ちいただけるものであることを期待しております。

最後に、Future of Privacy ForumおよびAccenture Japanのパートナーの皆様、惜しみなく知見をご提供くださった専門家グループの皆様、そして多大な時間と労力を本取り組みに投じてくださった企業の皆様に、心より感謝申し上げます。日本における責任あるイノベーション促進型ガバナンスの推進に向けた皆様のご尽力なくして、この取り組みは実現しませんでした。今後もこの重要な取り組みを共に継続していけることを楽しみにしております。

技術開発サイクルは短縮化し、加速しています。技術開発はその性質上、常に政策立案や規制を上回るペースで進んできました。しかしながら、AIやバイオメトリクスといった分野では、開発・導入のスピード、そしてその社会的影響の広さと深さにより、現行の政策や規制が目的に適っているかどうかについて懸念が表面化しています。このような状況下で、政府、産業界、学術界、市民社会の間の従来の役割分担は崩れ始めています。したがって、目的に適った規制の枠組みを構築するためには、これらのステークホルダーがいかに迅速かつ深く連携・協働し、政策・規制上のソリューションを共創できるかにますます依存するようになっています。

このような精神のもと、Future of Privacy Forum（FPF）はOpen Loop Japanプログラムのリサーチパートナーとしての役割を担いました。FPFは、原則に基づいた実践的なデータ保護、AI、デジタルガバナンスの実践を推進するグローバルな非営利団体として、産業界、学術界、公共部門のリーダーを招集し、責任あるイノベーションと規制遵守を支えるベストプラクティスの分析、ベンチマーキング、開発を行っています。私たちはOpen Loop Japanを志を同じくするプログラムとして、また関連するステークホルダーや広範なプライバシーコミュニティと関わる貴重な機会として捉えています。同様に重要なこととして、日本のデータ保護およびAIエコシステムにおける理解、リテラシー、責任あるイノベーション、そして最終的には信頼を深めるための機会であると考えています。

日本の政策枠組みに焦点を当てることは、重要かつ時宜にかなっています。日本の現在の時代精神は、技術的なブレークスルーを阻害しかねない硬直的な過剰規制を意図的に避けつつ、責任あるAI利用の文化を醸成したいという明確な意志によって特徴づけられています[1]。日本では、企業のAI導入が急増しており、5年前のわずか11%から今日では75%に達しています。同様に、日本のAI推進法（世界初の法律の一つ）が、「AI事業者ガイドライン」のような柔軟なソフトロー・フレームワークを活用しながら、イノベーションを慎重に優先していることにもそれは表れています。本プログラムでの私たちの取り組みが、日本の個人情報保護法（APPI）の改正（AIおよび統計処理に関する同意フレームワークの変更を含む）の成立と並行して進められたことも、

序文

日本を世界で最も「AI親和性の高い国」として位置付ける継続的な取り組みの中での本プロジェクトの時宜を得た性質を浮き彫りにしています。

しかしながら、経験豊富な政策立案者であればご存知のとおり、健全な政策や規制は、いかなる政策目標にとっても必要条件ではありますが、それだけでは十分ではありません。これらの政策や規制は、現場の実態にも同様に反映される必要があります。ここにおいて、FPFの客観的かつデータに基づく調査研究（調査、企業へのインタビュー、一次データの分析を含む）が、日本のAIおよびデータに関する枠組みの現場での適用と交差についてのより完全な理解に貢献できることを願っています。私たちは、これまでのすべての取り組みに対する深い敬意をもってこの研究に取り組んでおり、日本におけるAIの革新的かつ信頼性ある利用というビジョンに向けて貢献できることを光栄に思います。

参加企業の皆様、専門家グループのメンバーの皆様、コンソーシアムパートナーであるMetaおよびAccentureの皆様、そして何らかの形で本取り組みにご協力いただいたすべての方々に、心より感謝申し上げます。本報告書が、日本のAIおよびデータを取り巻く状況が形成され続ける中で、政策立案者や実務者にとって実践的な参考資料として役立つことを願うとともに、日本の皆様にとって信頼できるパートナーおよびリソースであり続けることを楽しみにしております。

Dan Hayden
Meta

序文



技術開発サイクルは短縮化し、加速しています。技術開発はその性質上、常に政策立案や規制を上回るペースで進んできました。しかしながら、AIやバイオメトリクスといった分野では、開発・導入のスピード、そしてその社会的影響の広さと深さにより、現行の政策や規制が目的に適っているかどうかについて懸念が表面化しています。このような状況下で、政府、産業界、学術界、市民社会の間の従来の役割分担は崩れ始めています。したがって、目的に適った規制の枠組みを構築するためには、これらのステークホルダーがいかに迅速かつ深く連携・協働し、政策・規制上のソリューションを共創できるかにますます依存するようになっています。

このような精神のもと、Future of Privacy Forum（FPF）はOpen Loop Japanプログラムのリサーチパートナーとしての役割を担いました。FPFは、原則に基づいた実践的なデータ保護、AI、デジタルガバナンスの実践を推進するグローバルな非営利団体として、産業界、学術界、公共部門のリーダーを招集し、責任あるイノベーションと規制遵守を支えるベストプラクティスの分析、ベンチマーキング、開発を行っています。私たちはOpen Loop Japanを私たちと理念を共有する取り組みとして、また関連するステークホルダーや広範なプライバシーコミュニティと関わる貴重な機会として捉えています。同様に重要なこととして、日本のデータ保護およびAIエコシステムにおける理解、リテラシー、責任あるイノベーション、そして最終的には信頼を深めるための機会であると考えています。

日本の政策枠組みに焦点を当てることは、重要かつ時宜にかなっています。現在の日本では、技術革新を阻害しかねない硬直的な過剰規制を避けながら、責任あるAI利用の文化を育てようとする姿勢が鮮明になっています[1]。日本では、企業のAI導入が急増しており、5年前のわずか11%から今日では75%に達しています。同様に、日本のAI推進法（この種の法律として世界でも先駆的なものの一つ）が、「AI事業者ガイドライン」のような柔軟なソフトロー・フレームワークを活用しながら、イノベーションを慎重に優先していることにもそれは表れています。本プログラムでの私たちの取り組みが、日本の個人情報保護法（APPI）の改正（AIおよび統計処理に関する同意フレームワークの変更を含む）の成立と並行して進められたことも、日本を世界で最も「AIフレンドリーな国」として位置付ける継続的な取り組みの中での本プロジェクトの時宜を得た性質を浮き彫りにしています。

しかしながら、経験豊富な政策立案者であればご存知のとおり、健全な政策や規制は、いかなる政策目標にとっても必要条件ではありますが、それだけでは十分ではありません。これらの政策や規制は、現場の実態にも同様に反映される必要があります。ここにおいて、FPFの客観的かつデータに基づく調査研究（調査、企業へのインタビュー、一次データの分析を含む）が、日本のAIおよびデータに関する枠組みの現場での適用と交差についてのより完全な理解に貢献できることを願っています。私たちは、これまでのすべての取り組みに対する深い敬意をもってこの研究に取り組んでおり、日本におけるAIの革新的かつ信頼性ある利用というビジョンに向けて貢献できることを光栄に思います。

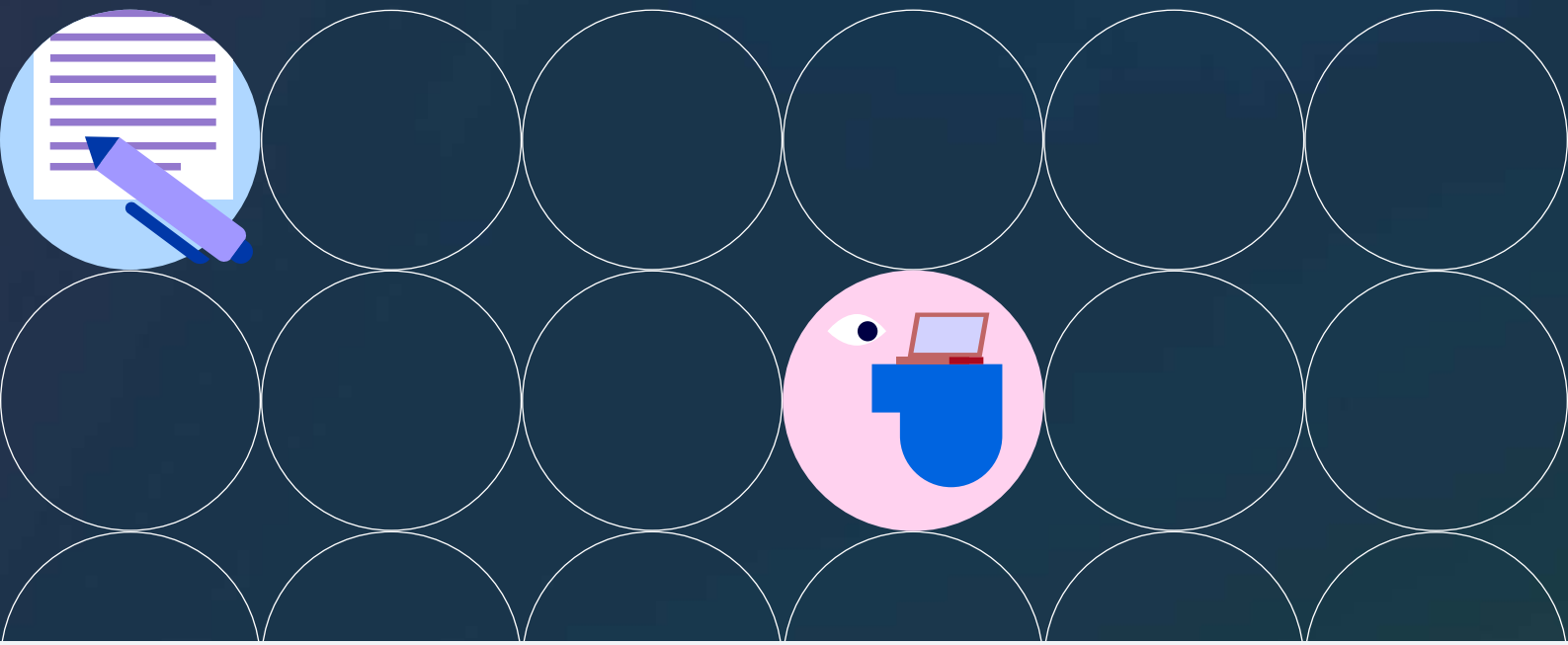
[1] https://www.bbc.com/news/articles/cwymw4434v7o

序文

参加企業の皆様、専門家グループのメンバーの皆様、コンソーシアムパートナーであるMetaおよびAccentureの皆様、そして何らかの形で本取り組みにご協力いただいたすべての方々に、心より感謝申し上げます。本報告書が、日本のAIおよびデータを取り巻く状況が形成され続ける中で、政策立案者や実務者にとって実践的な参考資料として役立つことを願うとともに、日本の皆様にとって信頼できるパートナーおよびリソースであり続けることを楽しみにしております。

Josh Lee Kok Thong
アジア太平洋地域マネージングディレクター、Future of Privacy Forum

エグゼクティブサマリー



Open Loop Japanは、日本が世界で「最もAIフレンドリーな国」を目指す中、日本のAIおよびデータガバナンスの枠組みが実際にどのように機能しているか、また、より明確化することでデータ保護と責任あるイノベーションの両立をどのように支援できるかについてのエビデンスベースを構築することを目的としました。本プログラムは、日本で先進的なAIシステム（AI搭載ウェアラブルデバイスを含む）を開発・導入する事業者 が、日本の3つの主要なAIガバナンスの枠組みに基づく要件にどのように対応しているかに焦点を当てました。

- **個人情報保護法**（**APPI**）- 個人情報保護委員会が所管する拘束力のある法律
- **人工知能関連技術の研究開発および活用の推進に関する法律**（**AI推進法**）- 日本におけるAI利用促進のための戦略的枠組みを定めていますが、民間事業者に対する義務は限定的です
- **AI事業者ガイドライン**（**Version 1.2**）- 経済産業省（**METI**）および総務省（**MIC**）が策定した自主的なガイドライン です

日本で事業を展開する16社 が、2026年6月から8月にかけて構造化されたバイリンガル調査に回答し、うち8社がフォローアップインタビューに参加しました。このエビデンスベースは、ウェアラブルデバイスに関する質問について、関連する専門知識を有する本プログラムの専門家グループのメンバー4名（業界専門家1名、学識経験者1名、日本を拠点とする法律実務家2名）からの書面による意見によって補完されました。

本調査全体を通じて、次の点が共通して見られました 。

1. **規制の不確実性はAI導入を妨げてはいないものの、その形態に影響を与えています。**規制の不確実性は、社内審査コストの発生、保守的なデフォルト設定、ユースケースの縮小または断念をもたらしています。また、同一の要件について組織ごとに異なる結論に至る状況を生み出しており、規制当局はその相違点を把握できていません。

2. **参加者が求めているのは義務の軽減ではなく、行動する前に適用できるルールです。**すなわち、事前に評価可能な基準、事例、モデル条項、およびチェックリストです。

3. **参加者の75%が、2026年のAPPI改正によりAIのための個人情報利用に対する障壁が建設的に軽減されると予想しています。**これは本調査において最も高い合意を示した項目です。

知見と提言

1 日本のAIガイダンスは広く参照されているものの、APPIコンプライアンスに関する疑問を解消するには至っていません

参加者16社中11社（69%）がAI事業者ガイドラインを参照していますが、追加の法的助言なしにAPPIの要件を確定するのに十分と考えているのはわずか1社（6%）でした。経済産業省および総務省は、事例、モデル条項、チェックリスト、およびガイドラインからAPPI上の義務への明示的な対応表を提供することが考えられます。個人情報保護委員会、経済産業省および総務省が連携し、サンドボックスや体系的な対話の仕組みを設けるとともに、法令に適合したAI導入事例を公表することが考えられます。

2 組織はデータをどの程度まで非識別化すべきか事前に確定できません

実用的かつリスクベースの匿名化基準は、本調査の参加企業が最も優先度の高い政策上の要望として挙げたものです（16社中10社、62%）。個人情報保護委員会は、組織が自ら評価できるリスクに応じた基準を公表し、匿名加工情報および仮名加工情報の制度を含め、当該基準を満たした場合に確保される法的地位を明示することが望まれます。

3 APPI上のAIモデルおよび出力の分類は未解決のままです

参加者の半数が、出力が個人情報を再構成または推論するリスクを指摘しています。個人情報保護委員会は、学習済みモデルがそれ自体としてはAPPI上の個人情報データベース等に該当しないことを確認することを検討すべきです。これは検索エンジンに関する既存の解釈および新たな統計作成の適用除外の前提と整合するものです。また、AIの出力から個人情報が推測されるリスクに対し、その程度に応じた措置についてガイダンスを発行することが望まれます。

4 越境移転の仕組みが事前に確定できません

16社中7社（44%）が、どの海外事業者または法域がAPPIを満たすか不明確であると回答し、16社中11社（69%）が、グローバル越境プライバシールール（CBPR）認証の効果について、2025年12月に個人情報保護委員会が示した明確化があるにもかかわらず、依然として確認を求めています。これは法律上の問題ではなく、情報が十分に行き渡っていないことの問題です。個人情報保護委員会は、グローバルCBPR認証の効果に関する明確化を周知し、認証に明確な便益を付与し、今後公表予定のモデル条項の法的効果を明示し、AIの処理パターンを踏まえてモデル条項を起草し、クラウド例外の取扱いを改めて明示することが望まれます。経済産業省および総務省は、AI・データの利用に関する契約ガイドラインを当該条項と整合させることが考えられます。

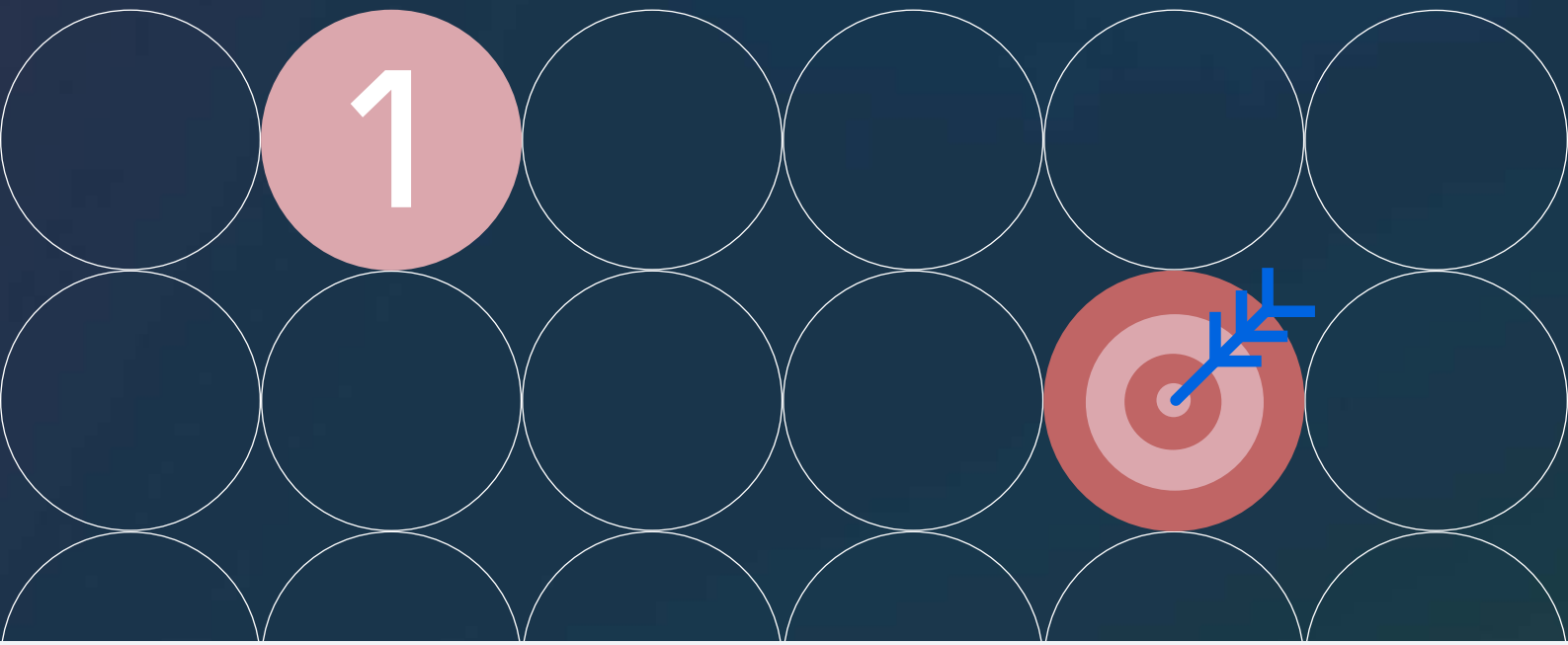
5 ウェアラブルデバイスを規律するルールは現在策定中です

施行準備期間中に、個人情報保護委員会は以下の点を明確にすることが望まれます：デバイスを装着することを選択し、収集される情報について説明を受けた者は、当該収集を容易に認識しているといえるか；個人を識別するための処理が決定的な要素となるか；どのモダリティが対象範囲に含まれるか；および録画の通知が後の認識処理にも及ぶか。全般的に、ガイダンスはメカニズムではなく条件を特定すべきであり、個人情報保護委員会および経済産業省は、周囲非利用者のデータを偶発的に取得する場合に、そのことを適切に知らせるための条件を設定することが考えられます。

日本の政策への示唆

参加者が求めていることのほぼすべてにおいて、追加の立法措置は必要ありません。特定された課題は解釈の問題であり、改正APPIの施行前の期間内に政令およびガイダンスで対応可能です。この期間が実質的な対応期間となります。十分に早く公表されたガイダンスであれば、システムや社内体制の設計に織り込むことができます が、施行直前に公表されたガイダンスではそれができません。また、複数の課題は省庁の所管を横断しており、個人情報保護委員会、経済産業省および総務省が連携して取り組むことが有益です。特に新たなAPPIの「特定生体個人情報」のカテゴリーについては、主要なリスクは規制不足ではなく、当該カテゴリーが規律することを意図したユースケースまで排除してしまうほど、早い段階で対象範囲を広く定めてしまうこと にあります。

第1章



1.1 背景と目的

日本のAIおよびデータガバナンスの枠組みの進展

日本は、「最もAIフレンドリーな国」となることを国家目標として掲げ、世界で最も意欲的にAIを導入する国の一つとしての地位を確立しています。この野心は、一連の重要な規制の進展に反映されています。2025年5月に成立したAI推進法は、AIの開発と実装に関する戦略的枠組みを確立するものです。現在進行中の個人情報の保護に関する法律（個人情報保護法、APPI） の3年ごとの見直しでは、新たな技術開発を促進するために日本のデータ保護の枠組みをどのように発展させるべきかが検討されています。また、AI事業者ガイドラインの継続的な改訂が行われており、これは企業が責任あるAI利用を実現するための指針を提供する、随時更新される文書です。AIガバナンスにおける日本のリーダーシップは国境を越えて広がっています。G7広島AIプロセスの議長国として、日本はAIガバナンスに関する国際的なアプローチの形成において影響力のある役割を果たしており、国内で行われる規制上の選択はアジア太平洋地域全体で大きな重みを持つことになります。

1.2 政策上の課題：AI搭載ウェアラブルデバイス時代における新たなデータカテゴリーの管理

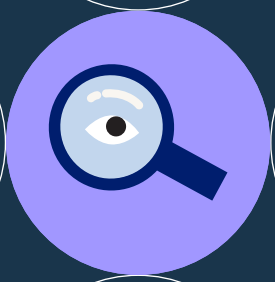
これらの規制の進展が交差する地点には、喫緊かつ十分に検討されていない政策上の課題があります。AI搭載ウェアラブル技術によって生成される新たなカテゴリーのデータに対して、既存および新興のガバナンス枠組みをどのように適用すべきでしょうか。スマートウォッチやフィットネストラッカーからAI搭載スマートグラスに至るまで、ウェアラブルデバイスは、ユーザーが求めるサービスを提供するために、身体由来データおよび生体データ の収集・処理を必要とする場合があります。AI機能によってこれらのデータからより高度で有用な推論を導き出すことが可能になるにつれ、現行の定義、処理の根拠、および効果的に適用し得るセーフガードの妥当性について疑問が生じています。日本でこれらの技術を開発・展開する企業は、個人関連情報の取扱い、外部送信規律、機微なデータのカテゴリーに関するものを含め、関連する義務が自社の製品やサービスにどのように適用されるかについて、不確実性の増大に直面しています。明確で実用的かつイノベーションを促進する指針がなければ、日本が大きな商業的可能性とグローバルスタンダードを確立する機会の両方を有するこの分野において、規制上の不確実性が意図せずイノベーションを阻害するリスクがあります。

1.3 Open Loop Japanの目標

Open Loop Japanは、構造化されたマルチステークホルダーの協働を通じて、この課題に取り組むことを目的として設計されました。AIおよびウェアラブル技術のエコシステム全体で活動する企業を、政策立案者、プライバシー専門家、学識者と結び付けることにより、本プログラムは日本のガバナンス枠組みの実践的な発展と実施に資するエビデンスに基づく知見を生み出しました。本プログラムには3つの中核的な目標があります。第一に、身体由来データおよび生体データを含む新たなデータカテゴリーに関連して、企業が現在どのように規制要件を解釈し実施しているかを把握すること。第二に、既存の枠組みが十分な明確性を提供している部分と、ギャップ、曖昧さ、または摩擦点が残っている部分を特定すること。第三に、データ保護と継続的なイノベーションという二つの目標を支える、実行可能でエビデンスに基づく政策提言を策定すること。政策と実践のギャップを埋めることにより、Open Loop Japanは、日本の規制アプローチがAI搭載ウェアラブル技術の責任ある開発と展開を意図せず阻害するのではなく、可能にすることを目指しています。

調査結果、提言および機会

2



2.0 はじめに

日本において、AIガバナンスは、個人情報の保護に関する法律（**APPI**）、および人工知能関連技術の研究開発および活用の推進に関する法律 （**AI推進法**）、およびAI事業者ガイドライン（バージョン1.2）などのAI固有の自主的ガイドラインの交差点に依拠しています。

APPIは技術中立的ですが、個人情報の利用に関する法的拘束力のある義務を課しています。生成AIモデルの訓練や精緻化に使用される非構造化データセットには個人情報が含まれていることが多く、また個人情報がAIシステムに直接提供される可能性があるため、この点はAIとの関連性が特に高いといえます 。さらに、2026年のAPPI改正により、AIガバナンスにおける個人情報保護委員会の役割が強化されました。内閣の改正法案概要によれば、統計情報の作成を目的とした同意要件の新たな免除規定は、統計情報の作成と位置付けられるAI開発にも適用されます。

AI推進法は日本におけるAIシステムの法的枠組みを確立していますが、民間事業者に対する義務は最小限であり、罰則もありません。

したがって、民間事業者が実際に遵守を求められる義務 は、主として個人情報保護委員会が所管するAPPI、および経済産業省（**METI**）と総務省（**MIC**）が共同で策定したAI事業者ガイドライン（バージョン1.2）などの自主的枠組みに見られます。

これらの枠組みは、規制の範囲、執行メカニズム、および基盤となる政策目的において大きく異なります。しかしながら、日本においてAIを開発または導入しようとする組織は、これら3つの枠組みすべてを同時に考慮しなければなりません。**したがって、組織がAI分野でイノベーションを起こし競争する能力を阻害しかねない規制上の摩擦を回避するために、これらが緊密に整合することが極めて重要です。**

本章では、これら3つの枠組みが交差する領域での活動について参加者から得られた意見を示します。これらの枠組みが意図どおりに機能している点、参加者間で期待される事項について異なる結論に達した点、および個人情報保護委員会、経済産業省、総務省、その他の日本の政策立案機関が要件およびガイダンスのより一貫した解釈を支援できる方法を特定します。

以下では、参加者のアンケート回答およびフォローアップインタビューに基づく5つの主要な知見を示します。調査方法の詳細については**§2.0.1**に記載しています。続いて、5つの主要な知見のそれぞれに至る結果の内訳を示します（**§2.1 - 2.5**）。各知見の最後には、日本の政策立案者に向けた関連する提言または提案 を記載しています。

知見 1 (§2.1)

日本のAIガイダンスは対象者に届いているものの、参加者は拘束力のある法的義務への準拠に関する疑問を解決するには不十分であると感じています

参加企業は、自主的なAIガイダンスを参照しているものの、このガイダンスの実施において課題に直面しており、さらなる法的解釈を必要とせずにAPPIなどAIに関連する拘束力のある法的義務への準拠に関する疑問を判断するには不十分であると報告しています。16社中11社（69%）がAI事業者ガイドライン（Version 1.2）を参照していると回答しましたが、追加の法的助言なしにAPPIが求める内容を判断できるほど明確であると回答したのはわずか1社（6%）でした。

参加者は日本のAIガイダンスの基礎となる原則を受け入れていますが、それを実務に落とし込むこと、または特定のベンダー契約が許容されるかどうかを判断することに困難を抱えています。参加者は、自らが直面する事例に適用できるモデル条項、チェックリスト、および事例があれば有益であるとの見解を示しました。

提案1

経済産業省および総務省向け：

> **AI事業者ガイドラインの次回改訂版において実践的なリソースを提供すること**

これには、事例、モデル契約条項、標準的なレビューチェックリストおよび業種別附属書、ならびにガイドラインから関係するAPPIの義務への明示的な対応表が含まれます。

提案2

経済産業省、総務省、個人情報保護委員会および省庁横断的な取組み向け：

> **サンドボックスを設置し、日本における法令に適合したAI導入 の事例集を公表すること**

組織は具体的な疑問を抱えていますが、回答を求めるための確立されたチャネルがありません。サンドボックスにより、本格導入前にアプローチを検証することが可能となります。対話経路により、特定の質問を規制当局に提示することが可能となります。事例集は、いかなる組織も単独では作成できない参照点を提供します。

知見 2 (§2.2)

一組織は、AI活動において個人情報を使用するためにどの程度まで非識別化を行う必要があるかを判断することに困難を抱えています

コホートの3分の1がAI活動において匿名化または集約されたデータを使用しています。しかしながら、参加者は、自らのデータ処理がAPPIの適用範囲外となる前に、非識別化の取組みがAPPIの匿名加工情報および仮名加工情報の基準を満たすかどうかを事前に判断することの困難さを挙げました。

提言1

> **組織がAI関連活動において個人情報を使用するためにどの程度まで非識別化を行う必要があるかについて、実践的かつリスクベースの基準を公表すること**

基準は、ユースケースのリスクに応じて調整され、組織自身が行動する前に評価可能であり、基準が満たされた場合にどのような法的地位が確保されるかを明示すべきです。ガイドラインには、データが正常に匿名化された場合と、そうでない場合を示す事例を含めるべきです。

提案3

経済産業省、総務省、個人情報保護委員会および標準化団体向け：

> **非識別化ツールに対する外部保証を確立すること**

参加者は、データを非識別化するために使用するツールが意図どおりに機能するかを検証できず、公表された基準に照らして評価する第三者機関も存在しません。文書化された十分なリスク評価を通じて、公表された基準を誠実に適用する組織のためのセーフハーバーを設ければ、そのような保証を提供できます。

知見 3 (§2.3)

APPIにおけるAI出力およびモデルの分類は未解決のままです

参加者の半数（50%）は、日本の既存のAIガバナンス枠組みでは、AIモデルに入力される個人情報、モデルが返す情報、または学習済みモデル自体に適用される義務がまだ確定していないと報告しています。各組織は異なる結論に達しており、ある参加者はこの問題を未解決のまま進めていると報告しています。

提言2

> **学習済みモデルおよびその出力は、識別可能性がない限り一般的に個人データに該当しないことを明確化するガイダンスの発出を検討し、出力からの推論リスクを最小化するためのガイダンスの発出を検討すること**

学習済みモデルがAPPIに基づく「個人情報データベース等」に該当するか否か、またそれに伴う義務が開発の連鎖のどこに位置づけられるかを確認すること。別途、出力が個人情報を露出するリスクに対して組織が講じうる措置（入力制御、展開前のテスト、ファインチューニングに使用されるデータの保持方法）を示すこと。

知見 4 (§2.4)

越境移転規則により、参加者は日本国外でホストされるAIシステムの利用を妨げられており、クラウドに関する規則は不確実性とためらいを生じさせています

コホートの半数弱が、どの海外プロバイダーおよび法域がAPPIの同等の保護および同等の措置に関する要件を満たしているかについて不確実性を報告しています。参加者は、データフローのマッピングやAIサービスプロバイダーとの移転契約の条件交渉における実務上の課題を挙げています。

提言3

越境移転メカニズムを事前に判断可能なものにすること

Global CBPR認証の効果に関する個人情報保護委員会の既存の明確化を周知し、この認証に明確なメリットを付与すること。

個人情報保護委員会が今後策定する越境データ移転のためのモデル条項を採用した場合の法的効果を明示し、AI処理パターンを考慮してこれを起草し、当該パターンに照らしてクラウドの例外を再確認すること。

提案4

経済産業省および総務省向け：

AIおよびデータの利活用に関する契約ガイドラインを個人情報保護委員会の（今後策定される）モデル条項と整合させること

個人情報保護委員会が今後策定するモデル条項は、移転元が個人情報の海外移転先から確保すべき事項を規定します。経済産業省の契約ガイドラインは、既にAIおよびデータに関する商業契約を扱っています。これらのモデル条項の起草時に両者を整合させることで、単一の契約で両方を満たすことが可能になります。

調査結果4（続き）

提案5

個人情報保護委員会および経済産業省向け（産業界と連携）：

> **プロバイダーによる（今後策定される）モデル条項の採用状況を可視化し、移転元が交渉ではなく確認によって対応できるようにすること**

当該条項を日本語と英語で併せて公開し、これを修正なく採用したプロバイダーの公的記録を維持することで、移転元の作業は、十分な交渉力がなく、有利に進められない可能性のある交渉を開始するのではなく、リストを確認することに変わります。

知見 5 (§2.5)

ウェアラブルデバイスを規律する規則は現在策定中であり、決定的な問題は未解決です

日本市場向けの高度なウェアラブルデバイスを開発または展開している参加者は1社のみであり、デバイスメーカーはいません。このような状況は、APPIの2026年改正で追加された「特定生体個人情報」という新たなカテゴリーに関するガイダンスへの継続的な需要と並存しています[2]。この新たなカテゴリーは、データが処理される目的ではなく、データが取得される条件によって範囲が定められています。この範囲がどのように適用されるか、特にデバイスの利用者本人と付随的にデータが取得される人々との区別については、政令によって定められます。

各組織は、構築に先立ちこの点についての明確化を求めているようです。

[2] 改正個人情報保護法第16条第5項において、「特定生体個人情報」は、「特定生体個人識別符号」を含む個人情報と定義されています。「特定生体個人識別符号」は、特別の技術を用いることなく、または多額の費用を要することなく取得でき、かつ本人が取得されていることを容易に認識できない態様で、身体の特徴を変換して得られたデータと定義されています。本報告書では一貫して「特定生体個人情報」の語を用います。改正法が主たる遵守義務を、この上位のカテゴリーに直接結び付けているためです。当該義務には、当該情報の取扱いに先立つ本人への通知、および当該情報の利用停止または第三者提供の停止の請求への対応が含まれます。

調査結果5（続き）

提言4

施行準備期間中に「特定生体個人情報」についてリスクベースかつ実用的な定義に関するガイダンスを提供すること

デバイスの装着を選択し、何が収集されるかを伝えられた人は、その収集を容易に認識できることを確認すること。個人を識別するための処理が決定的な要素であるかどうかを明確化すること。どのモダリティが対象範囲内にあるか、また技術の変化に伴い境界事例がどのように評価されるかを明示すること。記録のために行われた通知が、後の認識技術の適用にも及ぶかどうかに対処すること。全体を通じて、満たすべき条件を、その手段ではなく、特定すること。

提案6

個人情報保護委員会および経済産業省向け、施行準備期間中：

付随的な記録が適切に通知される条件を確立すること

デバイスが利用者以外の人々を記録する場合、組織はその人々に容易に連絡することができません。具体的な手段を規定するのではなく、解決策が満たすべき条件を示すこと：すなわち、近くにいる人が収集が行われていることを認識でき、追加情報を取得でき、異議を申し立てる手段を有すること。

2.0.1 本章におけるエビデンスについて

本章は、

2026年6月から8月にかけて参加16社が回答したバイリンガル形式の構造化調査、および

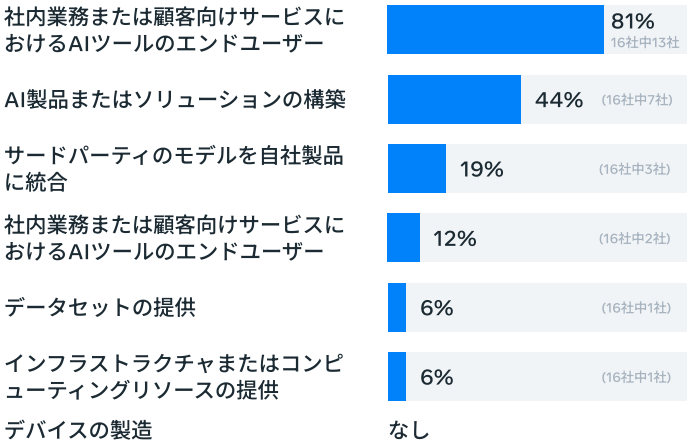
2026年8月を通じて参加16社のうち8社に対して日本語で実施したフォローアップインタビューに基づいています

総合すると、参加16社のコホートは、消費者向けヘルスケア、教育、電子商取引、エネルギー、食品・ライフサイエンス製造、電気機器製造、情報技術、製薬、人材サービス、広告、半導体、およびコンサルティングを含む多様な分野に及んでいます。本報告書では、すべての調査結果を集計して提示しており、個々の回答者または組織を特定することはありません。

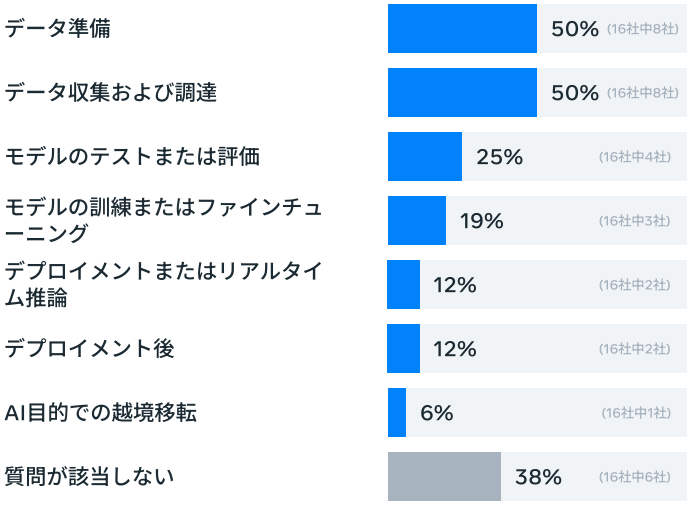
本コホートには、以降の調査結果を形作る2つの特徴があります。

第一に、本コホートはAIを構築するよりも、AIを導入する傾向があります

参加者は自らの役割を以下のように説明しました（参加者は複数の選択肢を選ぶことが認められていました）。



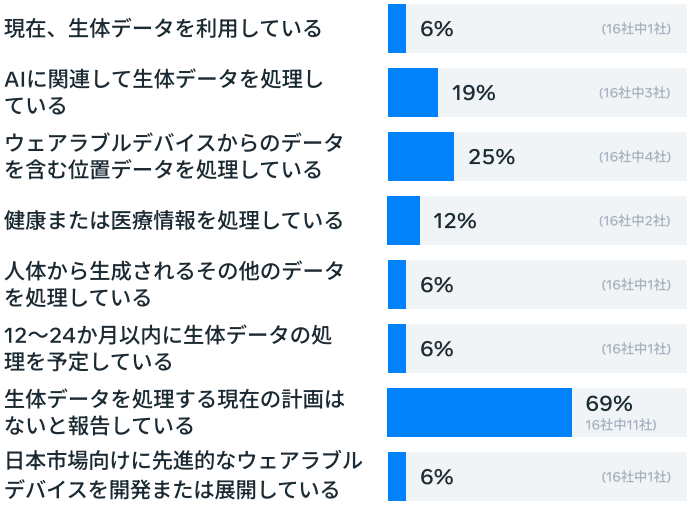
また、参加者はAIワークフローの最も初期の段階で個人情報を取り扱う傾向があります。



16社中5社の参加者（31%）は、AIに関連する個人情報を一切処理していないと回答しました。

したがって、本コホートが直面する課題は、AIモデルの訓練の仕組みではなく、組織がサードパーティのAIツールで使用するためのデータを収集・準備する段階、およびこれらのツールの導入に先立つガバナンス上の意思決定に集中しています。

第二に、本コホートの生体データ[3]およびウェアラブルデバイスで収集されたデータ[4]への関与は、皆無ではないものの、限定的です



[3] 本調査では、「生体データ」を、個人の身体的、生理学的または行動的特徴に関する特定の技術的処理から得られるデータであって、当該個人を一意に識別することを可能にするものと定義しました。個人情報保護法上、これは「個人識別符号」のカテゴリーに該当します。個人識別符号には、コンピュータによる認識のために身体の特徴を変換したデータ（顔認識データ、指紋など）が含まれます（個人情報保護法第2条および関係する政令）。

[4] In the survey, we defined **“wearable devices”** as electronic devices designed to be worn on the user's body or incorporated into clothing (e.g., smart glasses, AR/VR headsets, smartwatches, and health trackers). These devices are frequently equipped with advanced sensors (such as cameras, microphones, and accelerometers) and edge computing capabilities, enabling the continuous collection and processing of both user-specific body-based data and ambient environmental data.



参加者の政策改革に関する選好についての用語に関する注記

調査では、政策に関する選好について2つの別々の質問を設けました。

1. 1つの質問では、参加者に対し、自社のAI運用に最も有益な政策変更および支援メカニズムをランク付けするよう求めました。本章では、この質問への回答を「**政策要望ランキング**」と呼びます。
2. 別の質問では、日本の規制枠組みがより一般的にどのような優先事項を採用すべきかを、異なる表現の選択肢を提示する複数選択回答形式で尋ねました。本章では、この質問への回答を「**枠組みの優先事項**」と呼びます。

この区別は重要です。なぜなら、2つの質問は異なる選好に焦点を当てているからです。「政策要望ランキング」は、参加者が**自社の運用のために望むもの**を、その組織にとっての重要度順に反映しています。一方、「枠組みの優先事項」は、自社に影響するかどうかにかかわらず、**参加者が日本の枠組みに必要だと考えるもの**を記録しています。したがって、参加者はある問題を一方の質問では他方よりも高くランク付けする場合があります。

2.0.2 本プログラムのタイムラインと日本における法制度の動向

私たちがデータ収集を開始した時点では、APPIの改正法案はまだ国会で審議中でした。すなわち、個人情報の保護に関する法律等の一部を改正する法律案（第221回国会閣法第54号）（以下「**改正法案**」）です。この改正法案は、個人情報保護委員会によるAPPIの3年ごとの見直しにおける提言を実施するもので、2026年4月に閣議決定され、国会に提出されました。2026年6月中旬に開始した私たちの調査では、参加者に対し、提案された改正について質問しました。調査期間中に国会は改正法案を可決し、2026年7月17日に公布されました。新たな義務の大部分は、罰則に関する特定の「早期施行」規定を除き、2028年7月16日までに施行される予定です。

調査中に参加者が改正について期待を表明した場合、それらは成立した法律に対する評価ではなく、改正法案に対する期待であり、私たちはそのようなものとして報告しています。成立した改正法案は2026年4月に提出されたものと実質的に同一であるため、これは本調査の知見に重大な影響を与えるものではありません。それにもかかわらず、改正法案がまだ国会で審議中であった時点でも、16社中7社（44%）の参加者が改正案を参考にしていると回答しました。

改正法案成立後に実施したインタビューは、この点を再検討する機会となりました。参加者の見解は概ね変わっていないようでした。関心は法律本体から、その適用方法を決定する下位規則やガイダンスへと移行しており、日本国内の他の組織にAIサービスを提供している参加者の1社は、顧客から持ち込まれる内容にまだ顕著な変化は見られないと報告しました。

2.0.3 中心的な課題

参加者はAPPIの改正が自身の助けになることを期待しています。16社中12社（75%）が、改正によってAIの開発および展開における個人情報の利用に対する規制上の障壁が建設的に軽減されると予想しており、これは本調査全体で記録された中で最も高い合意率でした。したがって、本章は、業界がすでに進行中の改革を受け入れる姿勢にあるタイミングで発表されるものであり、私たちの提言もそれに応じて策定されています。すなわち、異なる内容を主張するのではなく、その改革を実際に効果あるものとするための方法を提案しています。

この期待は、現行の枠組みに対する、これと比べて明らかに肯定的とはいえない評価 と並存しています。 参加者は現行の枠組みが明確であるとは考えていません。

- AIモデルの学習に関するAPPIの要件が明確かつ曖昧さがないかについて尋ねたところ、16社中8社（50%）が否定し、16社中3社（19%）のみが肯定しました。
- AI推進法と自主的なガイドライン が合わせて規制上の期待を明確に示しているかについて尋ねたところ、16社中9社（56%）が否定し、ここでも16社中3社（19%）のみが肯定しました。
- APPIへの準拠を進める上での自主的なガイドライン の有用性について、16社中1社（6%）のみがガイドラインは準拠目的に十分明確であると回答しました。

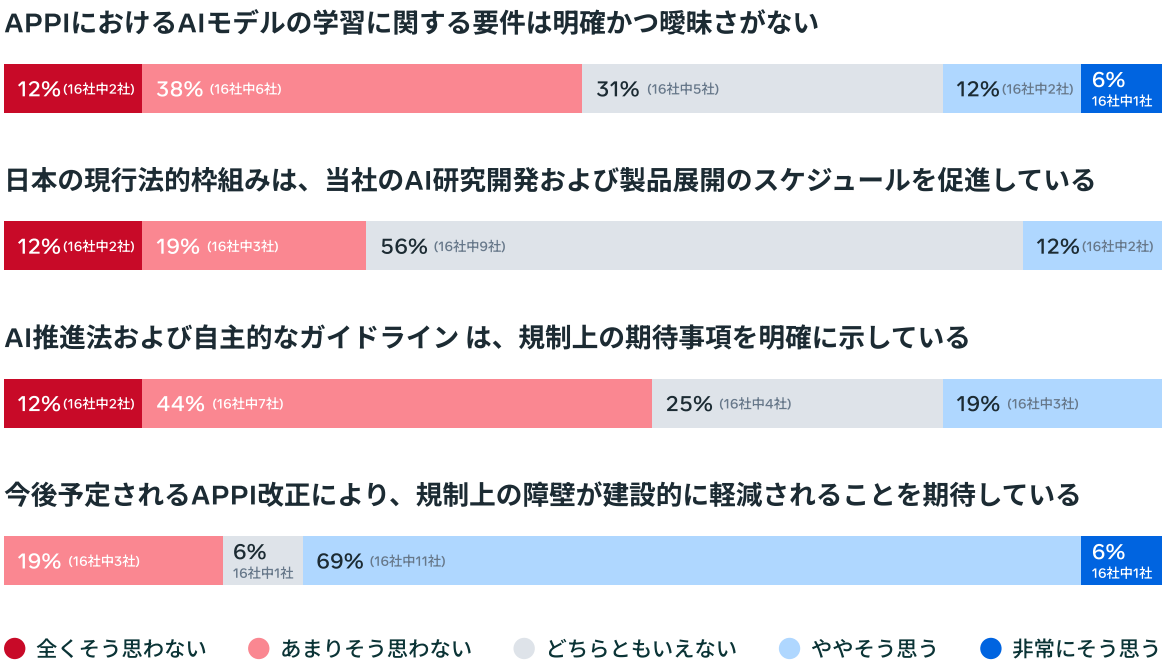
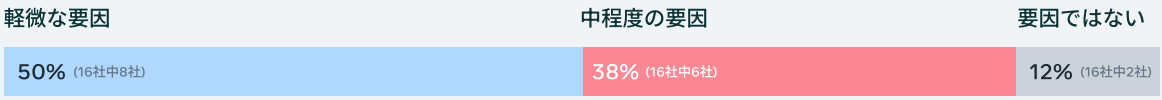


図2.1
現行の法的環境に対する認識（n=16）

しかしながら、このような規制の不確実性が、組織によるAIの開発・展開を妨げているわけではありません。参加者は、APPIまたはAI推進法に関する規制の不確実性が自社のAI開発または展開スケジュールにどの程度影響を与えたかについて、5段階で評価するよう求められました。

特筆すべきは、規制の不確実性を「重大な要因」または「主要な要因」と考えた参加者は一人もいなかったことです。参加者の回答は以下のとおりでした。



これらの結果は、本調査の参加者グループにおいて、規制の不確実性が製品のキャンセルや展開の中止につながるものではないことを示唆しています。むしろ、それは**社内審査コストの増加、保守的なデフォルト設定、合法性についての確定的な見解がないままの意思決定、および**概念実証（PoC） から実際の導入へ移行する際の障害という形で現れます。

2社の参加者が、コンプライアンス審査の負担について直接言及しています

- ある参加者は、APPI、AI関連ガイドライン、クラウドおよびベンダー管理、情報セキュリティおよび契約実務を考慮する必要があり、審査担当者と申請者の双方に大きな負担がかかっていると述べています 。同参加者の見解では、事業部門が必要としているのは、特定のAIツールが安全かどうか、職員がそこに個人情報や機密情報を入力してよいかどうか、海外のクラウドサービスや海外でホストされているAIモデルへの移転をルールがどのように扱うかを、迅速かつ一貫して判断できることです。
- 2番目の参加者は、自社のデータがAPPIの個人情報の定義に該当するかどうか、提案された利用が収集時に特定された目的を超えるかどうか、越境移転要件がどのように適用されるか、AIシステムが判断を下した場合に当事者間の責任がどこにあるかについて、曖昧さがあると報告しています。
- 3番目の参加者は、この作業の規模と、その中での困難の所在について説明しています。同参加者は、年間推定300〜400件のクラウドサービスの審査を実施しており、そのうち3分の1から4分の3がAIに関係しています。同参加者は、APPI、AI関連ガイドライン、クラウドおよびベンダー管理、情報セキュリティおよび契約実務の重複を課題として特に強調しました。これらのフレームワークはすべて同じ判断に関係しており、その結果、審査担当者は同じ領域を複数回確認しなければなりません。同参加者は、社内フローチャートを作成したものの、これは普遍的に適用できないと説明しています。各回答はユースケース、関係するデ

ータ、使用中のサービス、およびこれらの要素の組み合わせに依存しており、体系化することができていません。同参加者は、審査担当者が自身のスキルがその業務に十分かどうか疑問に思うことがあること、また審査を停止すれば事業が停滞してしまうため、組織としてできる限りの対応を続けていると付け加えました。

2社の参加者は、特に社内承認のスケジュールに言及しました

- 個人情報を伴うAIユースケースの社内承認にどのくらい時間がかかるかを尋ねたところ、ある参加者は、3つの機能：(1) セキュリティ、(2) プライバシー、(3) AIガバナンスにまたがり、2週間から1か月、時にはそれ以上かかると推定しました。
- 2番目の参加者は、自社の承認プロセスは長く、月単位で測定され、一部の提案は完全に断念され、どれだけ時間をかけても承認が得られないものもあると説明しました。同じ参加者は、審査能力はすでに他の法令に基づくコンプライアンスチェック（例として輸出管理を挙げました）に充てられており、その上にさらに個人データチェックを追加することは大きな負担になると指摘しました。

ある参加者は、社内能力の重要性を強調し、社内の専門知識があったことで、さもなければ6か月の無駄な作業になっていたであろうケースについて説明しました。

- 同参加者は、データブローカーからAPPIに準拠しているとして共通識別子ソリューションの提案を受けたことを説明しました。同参加者はそのソリューションを評価し、日本では使用できないと結論付け、その連携を中止することを推奨しました。約6か月後、そのソリューションが使用できないことが市場で明らかになりました。同参加者は、ガイダンスは明らかに許容されるものと明らかに許容されないものの例を列挙しているに過ぎず、その中間のケースについてはほとんど示されておらず、それらを評価する際に何に注意すべきかが示されていないと説明しました。むしろ、その判断は、同参加者自身のその分野への精通、同分野の他の専門家の見解、他の法域における規制アプローチに依拠していました。同参加者は、そのようなバックグラウンドを持たない同僚が同じ質問を検討するよう求められていたならば、同参加者の組織は、最終的に破棄されることになる連携交渉、契約書作成、開発作業に6か月を無駄にしていた可能性が高いと考えました。

2社の参加者は、法的な位置づけ が確定する前にAIを採用することへの懸念を特に提起しました

- ある参加者は、APPIの下での不確実性が、規制フレームワークがどのように解釈されるかについての楽観的な想定に基づいた事業設計につながっていると報告しています。同参加者はこれを事業リスクと考えています。インタビューでは、この点についてさらに詳しく説明し、過去の業界での論争を引用しました。そこでは、クッキーに関連するデータは個人情報に該当しないという想定の下で、雇用プラットフォームのトラッキングやデータブローカーの取り組みなどのビジネスモデルが設計されたものの、導入後に厳しい規制上および社会的な反発に直面しました。
- 2番目の参加者は、ファインチューニングされた生成モデルの社内利用について説明しながら、モデルに入力された個人情報をAPPIがどのように扱うか、またはモデルが返すものが個人情報に該当するかどうかを判断できないと報告しています。同参加者は、その疑問を解決しないままシステムを使用し続けていると報告し、その根拠で進めることが許容されるかどうかについて、広範な議論ではあまりにも注目されていないと考えています。
  同じ参加者は、調査回答においてこの点を直接指摘し、APPIに関する規制上の負担軽減は、AIモデルの開発、AIシステムの利用、およびAIを利用したことによって生じる個人情報の取扱いの3つについて別々に検討する必要があると主張しました。同参加者によれば、改革は1番目に対応していますが、2番目と3番目はあまり注目されていません。
- 3人目の参加者は、小規模組織の立場からの見解を述べました。現場業務を多く伴う同組織の事業分野において、多言語による顧客対応や業務管理など、AIによる複数の効率化の可能性を認識しています。しかしながら、法的な位置づけ の不確実性により、AIを導入するかどうかの判断において慎重にならざるを得ない状況にあります。また、中小規模の組織にとって、コンプライアンスを確認するためのコストが実質的な参入障壁として機能していることも指摘されました。

それにもかかわらず、未解決の法的根拠のままAI導入を進めることは、組織をリスクにさらし、個人が権利を行使するための確実な手段を失わせ、規制当局が業界慣行の変化を把握できなくなることを意味します。したがって、進むべき道は、既存のルールが何を求めているかについて、より明確にすることです。すなわち、改正がAIイノベーションを可能にすることを意図していた場合には、曖昧さを実行可能でイノベーションを促進する方向で解消する明確化（例えば、適切に非識別化されたデータ やモデル出力がAPPIの適用範囲外であることの確認）であり、ルール自体の緩和や厳格化ではありません。

2.1 知見 1
日本のAIガイダンスは対象者に届いているが、参加者は法的拘束力のある義務への適合に関する疑問を解決するには不十分だと感じている

AI推進法が重い義務的な規制を意図的に避け、「イノベーション優先」の方針を重視していることから、自主的なAIガイダンス（AI事業者ガイドライン（第1.2版）など）は、組織のAI活動のガバナンスやAPPIなど他の拘束力のある枠組みの解釈を形成する上で、引き続き重要な役割を果たしています。この文脈において、日本のガイドラインは稀有かつ顕著な成果を達成しています。組織が実際にそれらを活用しているのです。



(16社中11社の参加者)

69%

がAI事業者ガイドライン（第1.2版）を参照しています



(16社中3社)

19%

が、これらのガイドラインを日常のAI業務において最も影響力のある単一の枠組みとして扱っています。



(参加企業1社)

6%

APPIのような法律が自社のAI活動に何を求めているかを、さらなる法的解釈なしに確立するのに十分であると考えている

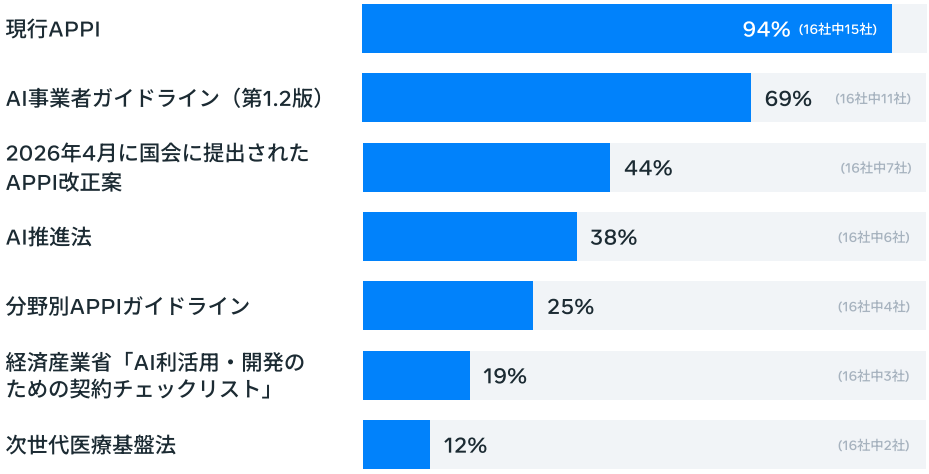
ガイダンスがルールではなく原則を示している場合、それらの原則を審査担当者が適用できるものに変換する作業は各組織に委ねられており、参加者は社内ガイドラインの作成、チェックリストの構築、レビュー時間という形でそのコストを負担しています。

2.1.1 組織がすでに取り組んでいること

参加者は、AI活動においてどの国内の枠組みを参照しているかを尋ねられました。そのリストは、法的位置付けが大きく異なる2つの文書にまたがっています。

1. APPIなどの拘束力のある法律
2. 個人情報保護委員会などの規制当局が発行する解釈ガイダンス
3. 法的拘束力はないものの解釈目的で参照される可能性のある自主的なガイドライン

参加者は複数の選択肢を選ぶことができました。回答は以下のとおりです。

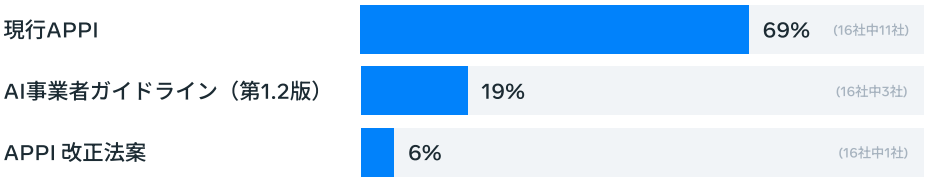


APPIへの参照は16社中15社（94%）とほぼ普遍的であり、これはAI活動における個人情報を規律する拘束力のある枠組みとしての地位を反映しています。AI事業者ガイドライン（第1.2版）が16社中11社（69%）で続いており、単独では法的拘束力を持たないにもかかわらず高い参照率となっています。注目すべきは、AI推進法は技術的には拘束力があるものの、16社中6社（38%）にしか参照されていない点です。これは、同法が確立するより広範な政策枠組みの下で発行された任意のガイダンスよりも少ない数字です。

これは驚くべきことではないかもしれません。AI推進法は、AIの開発と利用を促進するための政府のアプローチを定め、民間事業者には直接的な罰則のない拘束力のない「努力義務」のみを課しています。その執行は間接的であり、政府はガイドラインを公表しなければならず（第13条）、AIが市民の権利を侵害する場合には調査を行い、事業者に指導を行うことができます。

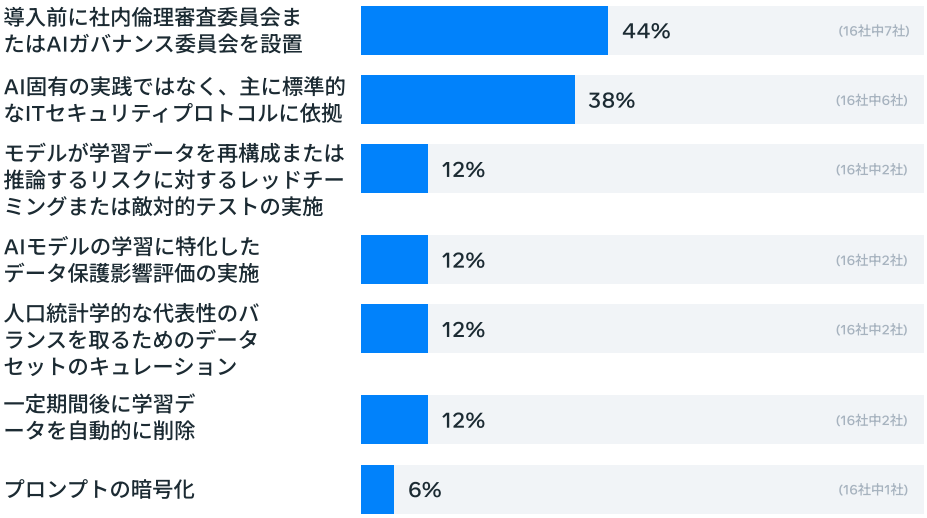
しかしながら、日常のAI活動において、AI推進法は組織が参照できる具体的なルールを比較的少なくしか提供していません。したがって、実務上の状況は、法的地位が大きく異なる2つの文書間での役割分担となっています。AI活動に関わる法的拘束力のある義務はAPPIに存在し、それらの活動がどのように行われるべきかについての期待は任意のガイダンスに示されています。

参加者はまた、日常のAI業務に最も影響を与えている単一の枠組みはどれかについても尋ねられました。



一部の参加者、特に国際的に製品やサービスを提供している参加者にとっては、外国の法的枠組みも実質的な基準として機能しています。ある参加者は、責任ある実践に関する質問に対し、日本の法令等ではなく、EU一般データ保護規則（**GDPR**）および米国の分野別規制への準拠を挙げて回答しました。

参加者は、以下の方法で独自のガバナンスプログラムを構築していると報告しています（参加者は複数の選択肢を選ぶことが可能でした）：



2.1.2 データが示すこと

自主的なAIガイダンスを参照することと、それに基づいて行動できることは同じではありません。そのため、本調査では、AI事業者ガイドライン（第1.2版）などの自主的なAIガイダンスが、参加者がAI活動においてAPPIなどの「ハードロー」をどのように遵守すべきかを判断する上で、どの程度役立っているかを尋ねました。

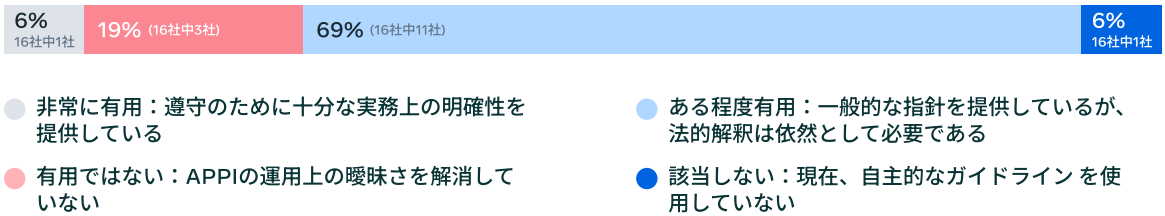


FIGURE 2.2
AIにおけるAPPI遵守を進める上での自主的なガイドライン の有用性（n=16）

参照状況の数値と照らし合わせると 、これは本調査で最も注目すべき結果の一つです。これは、自主的なAIガイダンスが対象者に届いているように見えること——16社中11社（69%）がそれを読んでおり（図2.2参照）、16社中3社（19%）がそれを主要な参照先としている——を示していますが、それを十分と考える参加者は少ない（この場合、わずか1社（6%））ことも示しています。16社中14社（88%）が、ガイダンスに加えて法的助言が必要であるか、またはガイダンスが直面している問題を解決していないと回答しました。

同様に、16社中4社（25%）が、APPI遵守をAI推進法および自主的なガイドライン の要件と整合させることを、直面したコンプライアンス上の課題として挙げました。16社中5社（31%）が、APPI上の義務とAI推進法の整合を「政策要望ランキング」の対象として選択し、16社中5社（31%）が「枠組みの優先事項」としても選択しました。

2.1.3 組織が直面している課題

本調査では、組織が直面している3つの課題を特定しました。

参加者が述べる最初の課題は、具体化と実装 です

ガイダンスはリスクを特定していますが、これらのリスクを管理するための軽減策の特定は各組織に委ねられています。

- ある参加者は次のように的確に述べました。日本の自主的なAIガイダンスは、AIシステムへの個人情報および機密情報の入力、組織が検索拡張生成を統合する際の重要情報の開示、およびプライバシー侵害に注意を喚起しています。しかしながら、当該ガイダンスを自社の業務に反映させるためには、追加の社内ガイドラインやチェックリストを準備する必要があります。
- 別の参加者は、このギャップを埋めるための潜在的な方策を提案しました。これらの方策には、例えば、組織が実務上実施可能なリスクベースの基準、標準化された契約書および標準チェックリスト、ケーススタディ、サンドボックスの要請などが含まれ、機動性を維持しながら安全性を確保するものです。

組織は、AIシステムにおいて個人データを適切に取り扱うという原則を全面的に受け入れながらも、特定のベンダーとの取り決めが許容されるかどうか判断できないことがあります。モデル契約条項や、担当者がユースケースを承認する前に確認すべき事項を明記したチェックリストなどの実務的なリソースは、当該事案に直接適用されるため、このギャップを埋めることができます。

インタビューにおいて、ある参加者は、企業がガイダンスを待つ間に業務が停滞しかねない不確実性について述べました。この参加者によれば、APPI改正の公布から新たな義務が発効するまでの現在の期間は、前回のAPPI改

正や電気通信事業法に基づく外部送信規律の導入など、過去の規制改革と同様の課題をクライアントにもたらしているとのことでした。いずれの場合も、クライアントの新要件への対応は法務・コンプライアンス部門に限定され、データを利用したい事業部門は行動できない状態に置かれ、大半の組織はパブリックコメント手続きの結果が出るのを待つという姿勢に落ち着きました。この参加者は、現在も同様のパターンが見られ、組織は再びパブリックコンサルテーションの結果と、それに続く下位規則やガイダンスが改正APPIの実務上の適用方法を確定させるのを待っている状況にあると指摘しました。

この説明は、新たな改正の公布から施行までの期間が空白期間ではないことを浮き彫りにしています。すなわち、この期間こそが、改正がどのように適用されるかを決定する下位規則やガイドラインが実際に策定される時期なのです。この参加者の証言によれば、組織はこれらの規則やガイドラインが出るまで行動を控えています。したがって、猶予期間は、ガイダンスが義務発効の直前ではなく、十分に早い段階で提供され、組織が内容を消化できる場合に最も有用となります。

第二の課題は、ガイダンスが、組織がガバナンスを求められている技術に必ずしも追いついていないことです。

特に、 エージェント型AI （自律的に一連の行動を計画し実行するシステム）は、調査回答において最も明確な例として挙げられました。このようなシステムに対して既存のコンプライアンス体制が適切かどうかについては、参加者の間で見解が分かれました。

- 16社中6社の参加者（38%）は、APPIの要件は、文言上、自ら処理を決定するシステムへの適用方法を明確にしておらず、その答えを導き出すには既存のガイダンスに記載されている内容を超えた追加の法的解釈が必要であると考えています。
- 16社中5社の参加者（31%）は、AIエージェントが処理する個人情報について、適切な通知を行い、同意を取得する方法をまだ検討中であると明示しました。
- これらを合わせると、16社中8社（50%）がこれらのいずれか、または両方を未解決の課題として特定しました。
- 一方、16社中2社（12%）のみが、既存のAPPIコンプライアンス対策で自律型エージェントの動作をすでにカバーしていると考えています。ただし、インタビューにおいて、この2社のうち1社はその見解を限定しました。その評価は自身の所管内のシステムには当てはまるものの、組織内の他の部署で自身の把握範囲外において使用されているAIツールがあれば、回答が変わる可能性があることを認めました。

両方の立場を取った参加者はいませんでした。したがって、同様の立場にある組織が同じ法律を読みながら、現在行っていることで十分かどうかについて正反対の結論に達しています。

さらに16社中5社（31%）が、 エージェント型AI の開発または導入を全く行っていないと回答しました。大半はこの質問に対して他の選択肢を選んでいなかったため、調査だけではその理由は明らかになっていません。しかしながら、この選択肢を選んだ参加者の1社は、自由記述の回答において、 エージェント型AI ツールを社内で開発・運用しており、エージェントが自律的に社内データベースを参照して顧客サポートの問い合わせに対応するユースケースをテストしていると述べました。この参加者は、現行のAPPIの枠組みでは、エージェントが自らの判断でデータにアクセスする場合の「取得」および「利用」の解釈について追加の明確化が必要であると付け加えました。

インタビューでの回答は、組織が直面する課題についてさらなる説明を提供しました。

- ある参加者は、AI事業者ガイドライン（第1.2版）はエージェント型AIについて、用語の定義以上の指針をほとんど提供していないと考えています。
- 2社の参加者が、組織がAIエージェントを制御する能力について懸念を示しました。1社は、自社でのエージェント使用について述べ、実際には完全な制御を達成することは困難であると述べました。エージェントは特定の行動をとらないようにという指示を無視したり、明示的なガードレールを独自に迂回したりする可能性があり、効果的な法的制御を極めて困難にしています。もう1社は、AIの導入について顧客に助言を行っており、エージェントが組織の想定する制御の範囲を超えて動作する可能性への懸念が高まっており、また顧客も、このリスクを管理できるとの保証をより強く求めるようになっていると報告しました。

インタビューの回答は、この困難がエージェントにとどまらないことも示唆しています。ある参加者は、日本のAIガイダンスは生成AIを中心に構成されている一方、組織が実際に得ている価値は生成モデルと従来の機械学習を組み合わせることから生じていると指摘しました。この参加者は、フィジカルAIがこのギャップをさらに広げると考え、ガイダンスはAIとは何かについてより広い視点に基づく必要があると提案しました。

2.1.4 エコシステムへの示唆

上記**§2.1.1**で述べたとおり、日本のAIガバナンスの枠組みは現在、責任あるAIの実践とはどのようなものか、どのようなリスクに注意すべきか、AIシステムの適切なガバナンスとは実際に何を意味するかを組織に示すために、自主的なガイドライン に依拠しています。参加者の経験によれば、彼らはこのガイダンスを読みますが、その後、ガイダンスが自組織に何を求めているかを解明するために、弁護士に指示を出し、社内委員会を招集する必要があります。これにより、コスト負担に格差が生じます。例えば、デジタルトランスフォーメーション部門やITガバナンス部門を持つ大企業は、スタートアップなどと比較して、これらの追加コストをはるかに容易に吸収できるためです。

調査はまた、組織によってAIガバナンスへの取り組み方が異なることを示しています。調査では、参加者は複数の実践を選択でき、最も一般的な2つは相互に排他的ではありませんでした。



- がガバナンス委員会を設置しています
- が主に一般的な情報セキュリティの実践に依拠しています
- が両方を選択しました
- いずれも選択しませんでした

一般的なセキュリティの実践に依拠している組織の中には、AI製品を構築したり、自らモデルを開発したりしているところもあり、1組織は生体データや健康データを処理しています。2つのグループを分けているのは、規模や技術的な洗練度ではなく、その組織がAIには情報セキュリティガバナンスとは異なるガバナンスが必要であるという結論に至っているかどうかです。

主に一般的な情報セキュリティの実践に依拠しているある参加者は、その理由を直接説明しました。同組織のデータセキュリティ対策は生成AIよりも前から存在しています。そのため、AIを独立したリスクカテゴリーとしてではなく、多くのツールの1つとして捉えており、AIツールに入力されるデータには、他の外部提供サービスに入力されるデータと同じ管理策を適用しています。この参加者は、自組織はAIモデルを大規模に開発しておらず、AIツールのユーザーとしての立場は他のソフトウェアサービスに対する立場と実質的に異ならないと付け加えました。

この回答は、企業がこの技術をどのように分類するかというアプローチの違いから、重要な示唆が生じることを示しています。組織は、AIを独自のガバナンスを必要とする新しいカテゴリーとして扱うことも、既にガバナンスを行っているカテゴリーの新たな一例として扱うこともできます。各組織が独自に運用上の解釈を構築する場合、日本はAPPIがAIシステムに何を求めているかについて、様々な民間部門の解釈を抱えることになり、規制当局が観察・追跡することが困難な、著しく異なるAIガバナンスの実践が生じる可能性があります。

ガイダンスを使いやすくするために何が必要かと尋ねたところ、参加者は非常に具体的な回答を示しました。

- ある参加者は、政府省庁の慣行に例えながら、**より分かりやすい要約**の作成を求めました。法令が制定される際、所管省庁は通常、法令の条文、詳細なスライド資料、および要点を素早く伝えるための1ページの概要を公表します。この参加者は、AIと個人情報に関するガイダンスにも同様の手法を適用すべきであると提案しました。
- 2人目の参加者は、顧客から最も頻繁に寄せられるAIガバナンスに関する質問は、**日常業務で使用できるスプレッドシート形式のチェックリスト**があるかどうかであると述べました。この参加者は日本の2つの文書を比較し、チェックリストの形式に近い方がより有用または適用しやすいと指摘しました。
- 3人目の参加者は、**ガイダンス自体を文書ではなくインタラクティブなツールとして提供すること**を提案しました。小規模な組織でチェックリストを記入するのは通常、専門家ではなく総務担当者や部門の代表者であり、実際に製品を開発する人々向けに設計されたツールの方が利用される可能性が高いと指摘しました。同参加者は、企業の機能別にガイダンスを差別化することも提案しました。すなわち、事業開発チームが確認すべき事項と、どの時点で経営層やコンプライアンス部門にエスカレーションすべきかを明示するというものです。
- 4人目の参加者は、既存のガイダンスにおけるギャップについて説明しました。そのギャップは参加者自身も解消できていないものです。この参加者はAI対応状況の評価資料を保有していますが、それらは断片化しています（例：ウェブサービス、アプリケーションなど別々に存在）。参加者はこれらすべてを単一のフレームワークで網羅しようと試みていますが、日本には同等のものが存在しないことが分かりました。参加者が求めたのは、複雑なAIサービスを評価できる包括的なチェックリストまたは基準でした。すなわち、リスク評価を組み込み、導入前に満たすべき基準を明示し、すぐに利用できるものです。また、そのような資料の作成方法に関わる要件も追加しました。AIはサービスの主要機能ではなく、その中の一つのコンポーネントであることが多いため、フレームワークはAIの関与レベルに応じてスケールし、すべてのサービスを同様に扱うのではなく、各ケースで何が必要かを特定する必要があるとしました。

同参加者は、標準的な資料の限界についても言及しました。チェックリストは組織が最低基準を満たしていることを示すことはできますが、特定の企業の状況には適合しない可能性があります。参加者は、補完として事例研究を提案しました。

- 5人目の参加者は、AIを開発するのではなく利用する組織の観点から同様の意見を述べました。参加者の評価では、エンドユーザーとしてAIを導入・利用する組織に特化した実践的なガイダンスが不足しており、小規模な組織にはAPPIが自分たちに何を求めているかを把握するためのリソースが限られています。参加者の要望は、エンドユーザー組織向けの簡潔な越境チェックリストと、自社の分野におけるAI活用に関する業種別ガイダンスでした。

個人情報保護委員会およびその他の政策立案者への提案

提案1

経済産業省および総務省向け：

> **AI事業者ガイドラインの次回改訂版 において実践的なリソースを提供すること**

経済産業省の既存の「AI・データの利用に関する契約ガイドライン」を補完するため、組織は業務に直接適用できる追加の実践的リソースにアクセスできると有益です。これには、具体的な事例、モデル契約条項、標準的なレビューチェックリスト、業種別付属書などが含まれ得ます。特に、AI事業者ガイドライン（バージョン1.2）のガイダンスとAPPIに基づく対応する法的義務との間の明示的なマッピングがあれば、組織は単一の内部レビューで両方のフレームワークに対応できるようになります。AI事業者ガイドラインは、エージェント型AIに関するより充実したガイダンスがあるとさらに有益です。

提案2

内閣、AI戦略本部、経済産業省、総務省、および個人情報保護委員会向け ：

> **革新的なアイデアを検証するサンドボックスを設置し、規制当局と産業界が新規または複雑なコンプライアンスの問い合わせについて議論するための構造化された対話経路を整備し、日本における法令に適合したAI導入の事例研究を公表すること**

これら3つの施策は、同じギャップに対して異なる方向からアプローチするものです。組織は新しいアプローチが受け入れられるかどうかを事前に確認することができず、ガイダンスが回答していない問題について法的助言を依頼する以外に確認する方法がありません。

革新的なアイデアを検証するサンドボックス

16社中3社（19%）の参加者が、本格展開前にコンプライアンスアプローチを検証するためのサンドボックスを選択しました。そのうち1社は、そのような環境で許可されるべき内容を具体的に示しました。すなわち、同一企業グループ内の組織が、各移転について個別の取り扱いを必要とせずに単一のAI開発プロジェクトのためにエンティティ間でデータを共有すること、および無関係な組織が定義された開発目的のためにデータをプールすることです。

機会2（続き）

APPI改正法案により追加された新たな統計作成に関する例外規定は、この多くを可能にするものと考えられます。この規定は、両当事者が当該活動に関する所定の情報を公表し、書面による合意がその根拠に基づいて提供が行われることを記録している場合、同意なく統計目的で第三者に個人情報を提供することを許可します。引き続き有用なのは、組織がコミットする前に、提案された協力が例外規定の範囲内に該当するかどうかを確認できる管理された環境です。具体的には、何を公表すべきか、合意書に何を記録すべきか、そして利用目的の制限と再移転の制限が複数当事者のプロジェクトにどのように適用されるかについてです。

体系的な対話の枠組み

参加者は一貫して、自らが抱える疑問と入手可能な回答との間にギャップがあると述べました。これに対処するため、参加者はガイダンスに追加するのではなく、それを補完する措置を提案しました。具体的には、特定の質問を提出し、その回答を信頼できるチャンネルの設置です。

- ある参加者は、個人情報保護委員会との事前相談の拡充を求めました。これにより、組織は問題が発生した後ではなく、適切なガバナンス措置を実施する前に検討できるようになります。同参加者は、ほとんどの小規模組織は大手コンサルティング会社や法律事務所に依頼する余裕がないと指摘しました。
- 2番目の参加者は、規制当局との業界ラウンドテーブルを政策要望の第2位に挙げ、そのようなフォーラムに期待することを説明しました。それは、AIシステムを提供する組織が、使用したデータ、その処理方法、および結果として得られるシステムへの信頼がどのように確保されているかを透明な形で開示することです。
- 3番目の参加者は、Open Loop Japanプロジェクト自体が産官学連携のモデルであると指摘しました。同参加者は、政府がこのフォーラムを主導することを提案し、その成功には分野横断的な連携が不可欠であると強調しました。この取り組みの根拠は明確です。公の議論はしばしば規制強化に傾きがちですが、焦点はむしろイノベーションの可能性を拡大することに置かれるべきです。何もしないことがしばしば最も抵抗の少ない道であることから、保守的な規制に傾く心理的傾向が繰り返し見られます。したがって、同参加者は、国および学術機関を含むマルチステークホルダー環境を求め、エコシステムに対してより建設的で実現可能な方向性を確立できる場を望みました。

これらの意見に共通するのは、組織が回答できない疑問が新規かつ具体的であるということです。特定のベンダー契約が許容されるか、提案された識別子ソリューションが日本で使用可能か、特定の受領者に対して所定の非識別化の水準 で十分かといった疑問です。ガイダンスは質問の類型に対応します。対話の枠組みは個別事例に対応し、組織が行動方針を決定する前にそれを行うことができます。

機会2（続き）

公表された事例研究

参加者16社中2社（12%）が、日本における法令に適合したAI導入 を示す事例研究またはベンチマークを選択しました。標準的な資料を使いやすくするために何が必要かを尋ねたところ、ある参加者は、チェックリストは組織が最低基準を満たしていることを示すことができるが、特定の企業の状況に適合しない可能性があると指摘し、その補完として事例研究を提案しました。これらは控えめな数字ですが、この要望は単独の組織では作成できないものに関するものです。

2.2 知見 2
組織は、AI活動において個人情報を利用するためにどの程度まで非識別化を行う必要があるかの判断に苦慮している

コホートにおいて加重選好度で最も高い「政策要望」は、APPIの下で十分な匿名化と見なされるものに関する、実用的で客観的かつリスクベースの基準です。エビデンスによれば、参加者は個人情報の識別可能性を低減するための措置を講じる意思があります。しかし、組織はAPPIにおける匿名加工情報および仮名加工情報の基準を満たすために、データをどの程度まで非識別化する必要があるかを事前に判断することに困難を抱えています。この不確実性に直面し、一部の組織はこれらの規定に依拠することを断念しており、その結果、APPIの匿名加工情報および仮名加工情報の制度が提供するよう設計された柔軟性を放棄している可能性があります。

2.2.1 組織がすでに取り組んでいること

一部の参加者は、AI関連活動において使用する個人情報の識別可能性を低減するための措置を講じています。参加者の約3分の1（16社中5社、31%）は、AI目的には匿名化または集計済みデータのみを使用しています。

AI開発を委託する第三者に個人情報を提供する場合、参加者は以下のような措置を組み合わせて適用しています。

- **暗号化：**データを保護しますが、APPI上の取扱いを変えるものではありません 。
- **非識別化処理 ：**法定基準を満たさないもの。
- **匿名加工情報への変換：**3つの選択肢のうち、データを正式にAPPIの適用範囲外とする唯一の方法です。

参加者はこれらを組み合わせて適用することがありますが、必ずしも一貫しているわけではありません。

インタビューにおいて、ある参加者はこれに対するアプローチを説明しました。状況に応じてこれらの技術のいずれかを適用することがありますが、データの取扱いを変える ためにいずれかに依拠することはありません。同参加者の基本的な前提は、個人データはどれほど加工されても個人データのままであるというものであり、したがって第三者にデータを提供する際には、当該情報すべてがAPPIに基づく義務の全範囲に服するものとして取り扱っています。

2人目の参加者も同様の立場を示しました。当該参加者によると、その組織では仮名化および匿名化のプロセスが整備されており、プロジェクトごとに必要と考えられる措置を適用しているとのことです。それにもかかわらず、当該データについてはAPPIに基づく義務の全範囲が適用されるものとして引き続き取り扱っています。当該参加者は、これが法律の要求事項に関する熟慮された解釈ではなく、意図的な過度の慎重さであることを明確に述べました。

確定できない基準に対するこれら2つの対応の背景にある理由は理解できます。しかしながら、その実際的な効果は、APPIの匿名加工情報および仮名加工情報の制度が提供するよう設計された柔軟性と利点を放棄することになります。

別の観点として、プライバシー強化技術（PETs）は、このコホートにおいて依然として優先度が低い状況にあります。調査における政策関連の質問全体を通じて、PETsに関するより詳細な規制ガイダンスを求めたのは16社中1社（6%）のみであり、PETsの導入に対するインセンティブを求めたのは16社中3社（19%）でした。これは、参加者が説明する困難の性質を考えると注目に値します。PETsは、特定の処理操作が何を達成するかを主張するのではなく、実証することを可能にするまさにその種の技術です。PETsがこれほど注目を集めていないという事実は、制約が利用可能な技術の不足ではなく、**それらの技術の出力を測定するための外部基準が存在しないことにあることを示唆しています。**

2.2.2 データが示すこと

調査では、参加者に対し、AI業務に最も有益となる政策変更および支援メカニズムをランク付けするよう求めました。16社すべてがランク付けを完了し、加重選好度により結果をスコア化しました。

APPIに基づく「十分な匿名化」に関する実用的、客観的、リスクベースの基準は、加重選好度で1位となりました。16社中10社（62%）がこれを選択し、16社中4社（25%）が1位にランク付けしました。他のいずれの選択肢も、これ以上の選択数または加重スコアを獲得しませんでした。

また別に、APPIの下で直面したコンプライアンス上の課題について尋ねたところ、16社中8社（50%）の参加者が、データがAPPIの適用範囲外となるためにどの程度まで非識別化する必要があるかを判断する際の課題を特定しました。16社中8社（50%）はまた、匿名化の柔軟で実用的、文脈に基づき、リスクに比例した定義を「枠組みの優先事項」として選択しました。

2.2.3 組織が直面している課題

APPIには、匿名加工情報および仮名加工情報に関する加工基準がすでに含まれています。しかしながら、参加者からは、必要とされる加工の程度、適用されるデータセット、許容される受領者、および許可される目的など、いくつかの運用上の不確実性が報告されています。

1点目は、匿名化の実質的な閾値です

ある参加者は、AI開発の実施を委託する第三者にデータを提供する前に、データを暗号化、匿名化、または仮名化していると報告しています。しかしながら、当該参加者の見解では、この加工をどの程度まで行う必要があるのか、また、そもそも必要であると仮定した場合、なぜ必要なのかは、これまで明確に示されたことがありません。当該参加者は、この点について大幅により具体的な検討が必要であると考えています。

2点目は、基準の性質です

2人目の参加者は、AIの利用を妨げない形式で、APPIの下でデータを使用する前にどの程度まで非識別化する必要があるかについて、実用的かつリスクベースの観点から明確化することを求めています。これは、組織が過度に保守的にならず、適切なガバナンスの下でデータ利用を促進できるようにするためであると明示的に述べています。

3点目は、保証です

十分に起草された基準であっても、組織がその基準を満たしていることを外部の第三者が確認できなければ、ほとんど価値がありません。3人目の参加者はその懸念に直接言及し、匿名化または仮名化製品が意図したとおりに機能することを実証できるソフトウェア、およびそのようなツールを保証する公的または第三者の認定機関がどこであるかについての明確化を求め、基準およびチェック項目を事前に公表することを求めました。

これら3つの困難の影響は累積的です。匿名化の閾値を決定できず、どのように評価されるかを予測できず、それが満たされたことの外部確認を得られない組織は、独自の基準を設定し、誤った場合の結果を負担せざるを得ません。

2.2.4 エコシステムへの示唆

ここでの要望は、基準を引き下げることではなく、確定可能な基準を求めるものであり、ある参加者は、対処を望むリスクとして、匿名化の閾値が不明確であるために組織が過度に保守的になることを明確に述べました。

参加者は不確実性に対してさまざまな方法で対応しており、最も顕著な2つの対応は、正反対の方向を指しながらも同じ効果を生み出しています。一部の組織は、AI業務を匿名化または集計されたデータに限定し、より豊富になり得るデータ をAPPIの適用範囲に持ち込むことを控えることで、APPIの適用範囲外にとどまっています。他の組織は、データがAPPIの適用範囲から出ることは決してないと想定し、すべてのデータを一貫して個人データとして取り扱っています。どちらも、事前に確立できない匿名化の閾値に対する合理的な回答であり、どちらも何かを放棄しています。前者はデータの分析的価値を放棄し、後者は法定制度が提供するよう設計された柔軟性を放棄しています。

いずれのアプローチも、どこに境界線があるかについての共通理解を生み出すものではありません。匿名化の閾値が事前に決定できず、事後にも検証できない場合、同じルールに直面する組織が同じデータについて実質的に異なる判断に至り、個人の保護は、その個人のデータを取り扱う組織がどの判断を採用したかに依存することになります。

個人情報保護委員会への提言

提言1

> **AI関連活動において個人情報を利用する前に、組織がどの程度まで非識別化を行う必要があるかについて、実践的かつリスクベースの基準を公表すること。**

閾値はリスクに応じたものであるべきであり 、利用可能なデータを縮小させる過度に保守的なデフォルトを避け、基準を満たした場合の法的効果を明示することで、組織が事前にそれを信頼できるようにすべきです（例：セーフハーバー）。

最も価値あるものとするためには、組織がそれらの基準を事前に適用できる必要があります。上述のとおり、参加企業が述べた主要な課題は、関連する閾値を満たしているかどうかを事前に確認できないということです。

以下の3つの要素により、そのようなガイダンスは実効性のあるものとなります。

データの閾値をユースケースのリスクレベルに連動させること

内部分析、パートナーとのデータ共有、および公開に対して単一の基準を設けると、内部利用には厳格すぎるか、公開データには緩やかすぎるものとなることが避けられません。これらの異なるユースケースを区別することで、それぞれが提示し得るリスクに基準を調整することが可能になります。参加者は、基準が実践的で、リスクベースであり、達成可能であることを求めました。実務上、これは最低限、基準が組織自身で容易に評価できる要素（例：データを受け取るのは誰か、受領者がどのような他のデータを保有しているか、およびその二つを照合して個人を識別できるかどうか）に基づくべきであり、再識別のリスクに焦点を当てるべきであることを意味します。さらに、形式の面では、基準は組織が解釈・適用を求められる高次の原則ではなく、組織が容易に照合できる形式をとることが考えられます。

APPIの匿名加工情報および仮名加工情報の制度の法的効果について、わかりやすいガイダンスを提供すること

データを匿名加工情報に変換することで組織が何を得られるか、仮名加工情報から何を得られるか、そしていずれの基準も満たさずにデータを処理した場合にそのデータの法的位置づけがどのように変わるかを説明すること。これにより、組織は最も保守的な解釈をデフォルトとするのではなく、二つの制度を意図的に選択できるようになります。

提言1（続き）

基準を満たした場合の法的効果を明示すること

参加者は、その投資がどのような法的位置を確保するか分からないまま、非識別化に投資しています。ガイダンスは、基準が満たされた場合に何が変わるかを示すべきです：そのデータを同意なく第三者に提供できるか、取得時に特定された目的を超えて利用できるか、そして引き続き適用される義務があるとすれば何か。これがなければ、組織はデータをさらに処理するコストと、そうすることによる便益を比較衡量する方法がありません。

その他の政策立案者への提案

提案3

経済産業省、総務省、個人情報保護委員会、および標準化団体向け：

非識別化ツールに対する外部保証を確立すること

基準を公表するだけでは、組織は自らのコンプライアンスを自己認証することになります。ある参加者は外部保証の必要性を強調しました。匿名化および仮名化を正確に実行する ことが実証されたツールも、そのようなツールを公表された基準に照らして評価する公的または民間の機関も見つからないとのことです。

セーフハーバーを設ければ、この問題に直接対処できます：公表された基準を誠実に適用した組織は、後の評価が異なる結論に達したとしても保護されることになります。これにより、組織は自らの判断を超えた確信の根拠を得ることができます。

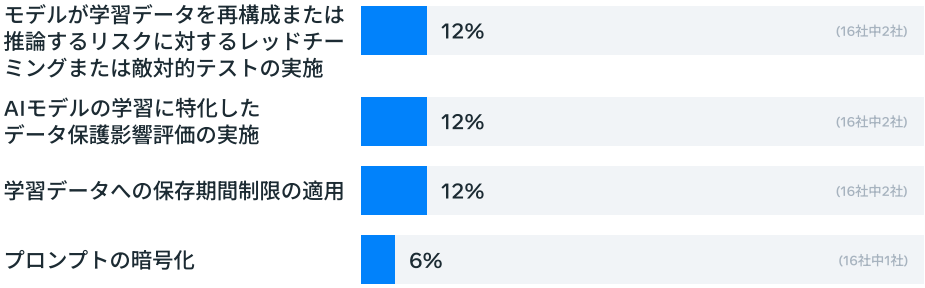
非識別化は急速に進展する分野であり、データを非識別化する技術とそれを復元する手法の両方が進歩し続けており、ツールに対する固定的な評価は、見直されるよりもかなり前に最先端の状況を反映しなくなる可能性があります。したがって、いかなる保証の仕組みも、改訂されることを前提に設計されるべきであり、多くの組織がすでに取得している国際認証（ISO/IECやSOC規格など）を重複させるのではなく、それらを認めるべきです。

2.3 知見 3
APPIにおけるAI出力およびモデルの分類は未解決のままである

調査において最も頻繁に挙げられたコンプライアンス上の課題の一つは、生成AI出力が個人情報を再構成または推論するリスクです。この背景には、学習済みAIモデルおよびその出力のAPPIにおける位置づけが不明確であるという問題があります。2社の参加者が独立して、これを自社の業務に影響を与える未解決の問題として特定しました。1社は、この不確実性にもかかわらず展開を進めていると報告しています。

2.3.1 組織がすでに取り組んでいること

一般に、参加者は「**出力関連リスク**」– 生成AI出力が個人情報を再構成または推論する可能性があるリスク – を、さまざまなツールや技術を用いて管理しています。



これらの対策に加え、調査結果の全体像からは、組織が生成AIを社内環境に限定する、機微情報を扱わない業務に限定する、またはAIワークロードに関連して匿名化された情報のみを使用するといった制限措置によってリスクを管理している可能性が示唆されています。

2.3.2 データが示すこと

16社中8社（50%）の参加者が、AI関連活動においてAPPIの下で直面する不確実性およびコンプライアンス上の課題として、出力関連リスクを挙げています。これにより、出力関連リスクは、匿名化と並んでこうした課題の中で同率1位となっており（**知見2**参照）、越境データ移転（16社中7社、44%）を上回っています （**知見4**参照）。

2.3.3 組織が直面している課題

2社の参加者がこの問題を詳細に説明しましたが、それぞれ異なる観点からアプローチしています。

> **ある参加者は、社内で生成AIを使用するために特定のモデルをファインチューニングし、その成果を組織全体に展開していると説明しています**

しかし、この参加者は、モデルが返す出力が個人情報に該当するかどうかについて不確実性を示しました。参加者は、この問題を解決しないままシステムの使用を継続していると説明しました。

インタビューにおいて、参加者はこの点についてさらに詳しく説明しました。AIシステムが返す情報の位置づけに関して、個人情報保護委員会からの裁定、ガイドライン、Q&A、または評価基準は存在しません。その結果、自社の立場が許容されるものかどうかを判断できませんでした。また、出力が組織が保有する個人データと解釈された場合、その出力を第三者に提供すること自体に本人の同意が必要となり、出力の使用方法が制限されることになると述べています。

リスクを社内でどのように管理しているかを尋ねたところ、参加者は、プライバシーを侵害する情報が出力に現れた場合の対応について、詳細なガイダンスを発行していないと述べました。これはより徹底的に対処したいと考えているものの、まだ実現できていない課題であると説明しました。

別の参加者は、APPIにおける学習済みAIモデルの法的分類について言及しています

これは、APPIにおける「個人情報」、「個人データ」、および「保有個人データ」という独自の区別に関わる問題です。

APPIの第2条第1項において、「個人情報（personal information）」は、生存する個人に関する情報であって、特定の個人を識別できるすべての情報を包含する、より広範で基礎的なカテゴリーです。「個人情報」に対する義務は透明性と範囲に焦点を当てており、事業者は収集目的を明確に定義し、その明示された目的の範囲内で利用を制限することが求められます。

一方、「個人データ」（personal data）は「個人情報」の部分集合です。APPIの第16条第3項（第16条第1項における「個人情報データベース等」（personal information database）の定義に基づく）によれば、「個人データ」は、検索可能なデータベースに編集され体系的に整理された個人情報のみを指します。「個人データ」に対する義務はより厳格です。事業者は、堅牢なセキュリティ対策を実施し、第三者への提供について同意を取得し、データ漏えいを報告しなければなりません。

事業者が「個人データ」（personal data）の開示、訂正、追加、削除、または利用停止を行う権限を有している場合、その個人データはAPPIの第16条第4項において「保有個人データ」（retained personal data）に分類されます。このレベルでは、事業者は本人の権利に対応しなければならず、個人はデータへのアクセス、またはデータの訂正もしくは削除を法的に請求することができます。

この参加者は、個人情報保護委員会による生成AIサービスの利用に関する注意喚起（2023年6月公表）を、大規模言語モデル（LLM）がAPPIの「個人情報データベース等」の定義に該当することを示唆するものと解釈して

います。参加者は、個人情報保護委員会の公式見解では、検索エンジンは個人情報を検索するために体系的に整理されていないため、この定義から除外されていると指摘しました。LLMも同様にそのような目的で整理されていないため、LLMもこの定義から除外されるべきであると参加者は推論しています。しかし、参加者は、注意喚起以降の実務において、そうしたLLMが「個人情報データベース等」に該当するものとして扱われていることを確認しています。LLMが個人データに該当するかどうかの解釈は国際的に異なっており、参加者は日本においてこの点に関する明確なガイダンスが必要であると考えています。

参加者は、LLMが「個人情報データベース等」に該当する場合、「保有個人データ」としての開示、訂正、または利用停止のAPPIに基づく請求に対して、組織がどのように対応すべきかが不明確であることを強調しました。その解釈が定まっていないため、参加者は事業設計の方向性を定めることができない状況にあります。

インタビューにおいて、参加者は、導入事業者 が開示、訂正、利用停止の請求に対応することは現実的ではないと考えました。導入事業者 は単にそれを可能にする形式でモデルを保持していないためです。したがって、開示および訂正に付随する義務は、実務上、基盤モデルの開発者が負わざるを得ないことになります。

この参加者はまた、APPIにおける個人情報、個人データ、保有個人データの区別は日本のAPPIに特有のものであるため、通常グローバルに事業を展開する基盤モデルの開発者が、一つの法域にのみ存在する区別のためにコンプライアンス体制を構築する可能性は低いと考えました。参加者の評価によれば、この義務は履行するインセンティブがほとんどない当事者に課されることになり、個人と対峙する導入事業者 は対応することができないことになります。

これらは、関連のない業界の2名の独立した参加者が、同じギャップについて述べたものです。2番目の説明は、これが単なる分類の問題を超えるものである理由も示しています。学習済みモデルが保有個人データを含む個人情報データベース等に該当する場合、APPIの開示、訂正、利用停止の権利がそれに適用されます。しかし、モデルの重みに対する削除請求を実現する方法を特定できた参加者はいませんでした。参加者は、現時点では権利と技術が一致していないように見えると認識しています。

2.3.4 エコシステムへの示唆

APPIに関連するAIモデルおよび出力の分類が未解決であることの結果として、組織は本来であればAIを活用していたであろう状況において、その機会を見送っています。

参加者はこのことを直接説明しています。ある参加者は、その枠組みがどのように適用されるかに関する業界ガイダンスが出されるまで、生成AIの利用を自社の業界の規制品質枠組みの対象外の業務に限定しています。別の参加者は、従業員データを含む社内ユースケースがあるものの、進展していません。16社中5社（31%）の参加者はAI関連の業務を匿名化または集計されたデータに限定しており、16社中5社（31%）はAIに関連して個人情報を一切処理していません。ある参加者は、自組織内の障壁は法的なものではなく心理的なものであると説明しました。スタッフが個人情報を広く解釈し、リスクが高すぎるという想定のもとでAIに関わるものをすべて除外するため、有用なアプリケーションが誰かが評価する前に放棄されてしまうというものです。

モデルおよびその出力の未解決の状態は、これに直接寄与しています。自社のモデルが返すものが個人情報に該当するかどうかを判断できない組織は、どのような義務がそれに付随するかを判断することができず、慎重な対応としてはユースケースを狭めるか、構築しないことになります。2名の参加者は未解決の状態のまま継続しましたが、これには組織にとっても、どの解釈が採用されるかによって立場が左右される個人にとっても、独自のリスクが伴います。しかし、この証拠に基づくと、より一般的な対応は自制であるようです。

根本的な問題については、現在の実務が想定するよりも限定的な解釈が成り立つという合理的な議論があります。ある参加者がそれを説明しました。公式解釈では、検索エンジンは個人情報の検索のために体系的に構成されていないため、APPIに基づく「個人情報データベース等」に該当せず、学習済みモデルもそのように構成されていません。この推論に基づけば、モデルは定義の対象外となります。そうであれば、重要なのはモデルに何が含まれているかではなく、特定の出力が個人を識別するかどうかです。同じ参加者は、個人情報保護委員会の2023年6月の注意喚起以降の実務は逆の方向に傾いており、解釈は国際的に異なると指摘しました。これを解決することで、組織はリスクが実際に発生する地点、すなわち出力に取り組みを集中させることができるようになります。

個人情報保護委員会への提言

提言2

> **学習済みモデルおよびその出力は識別可能性がない限り一般的に個人データに該当しないことを明確化するガイダンスの発行を検討し、出力からの推論リスクを最小化する措置について、実務的なガイダンスを提供すること**

新しい統計作成の例外規定は、活動の出力自体が個人に関する情報ではない場合にのみ適用され、AI開発がその定義に含まれると扱われる根拠は、学習済みモデルが個人の記録ではなく統計的パターンを表すということです。学習済みモデルがそれ自体としては個人に関する情報ではないことを確認することは、したがって、モデルの扱いを、例外規定がすでに基づいている前提と整合させることになります。

APPIに基づくLLMの法的分類を確認すること

学習済みモデルがそれ自体ではAPPIに基づく個人情報データベース等に該当しないこと、およびその出力は個人を識別する場合にのみ個人データであることを確認するガイダンスは、参加者が最も解決できなかった問題を解決することになります。この推論は、個人情報保護委員会自身の既存の解釈において利用可能です。検索エンジンは個人情報の検索のために体系的に構成されていないため定義の対象外となり、学習済みモデルもそのように構成されていません。これを確認することで、モデルの扱いを類似の技術の扱いと整合させることができ、出力が誰かを識別する場合には重要な義務が引き続き適用されるため、個人に対する保護が低下することはありません。

ガイダンスは、開発およびデプロイのチェーンにおいて義務がどこに位置づけられるべきかについても対処する必要があります。ある参加者は、モデルが個人情報データベース等に該当する場合、開示および訂正の義務は、導入事業者 ではなく開発者が負うべきであると指摘しました。導入事業者は、技術的にこれらの請求に応じることができないためです。

中間生成物への対応

統計作成に係る適用除外における除外要件—出力が個人に関する情報であってはならないという点—は、学習済みモデルについては明確です。しかし、埋め込み、特徴ベクトル、モデルの活性化値、その他類似の中間生成物については、それほど明確ではありません。これらは統計的関係性を表すものですが、原理的には特定の学習データに紐づけられる可能性があります。この適用除外に依拠する組織は、そうした中間生成物を生成または保持することが当該要件と整合するかどうかを把握する必要があります。これは、参加者がモデル出力について提起したのと同じ問題であり、パイプライン上の異なる段階で生じるものですが、実務上この適用除外にどこまで依拠できるかを左右することになります。

提言2（続き）

出力からの推論リスクを最小化する措置について、実務的なガイダンスを提供すること

ステータスの問題が解決すれば、実質的な作業は出力段階に移りますが、組織が最も対応に苦慮しているのがこの段階です。16社中8社（50%）が、生成AIの出力が個人情報を再構成または推論するリスクを指摘しており、これは匿名化と並んで今回の調査で最も多く挙げられた課題でした。一方、これに対する措置を講じている組織ははるかに少なく、モデルが学習データを漏洩または再構成することに対するレッドチーミングや敵対的テストを実施しているのは16社中2社（12%）、学習データに保存期限を設けているのも16社中2社（12%）に留まっています。

参加者が述べるギャップは具体的です。ある参加者は、入力として個人情報を入力しないようスタッフに指示するポリシーを定めているものの、出力にプライバシーを侵害する情報が現れた場合の対処方法についてはガイダンスを発行しておらず、対処すべきと考えていながらもまだ対応できていないとのことでした。別の参加者は、出力に含まれる個人情報に類似し得るものはすべて検証しなければならないと報告しました。また、別の1社は注意喚起レベルの警告を発しており、その懸念は、組織が十分に認識しないままデータが取り込まれ、内部で使用される可能性があるという点にあります。

ガイダンスは、組織が採用できる措置を特定し、それぞれの措置についてリスクに見合った水準を示すものであれば、最も有用なものとなります。今回のコホートの証拠に基づけば、関連する措置には以下が含まれます。

- **入力制御**—システムに入力できる内容を制限すること、および組織自身のデータでモデルをファインチューニングする場合のそのアプローチの限界を明示すること
- **学習データの記憶および再構成に関する導入前テスト**—16社中2社（12%）が既にこれを実施しているものの、適切なテストとは何かを示す明確な基準がないため、リスクに見合ったテストの水準を示すこと
- **ファインチューニングデータの保持および削除の実務**、およびデプロイされたモデルが再現できる内容に対するその影響
- **出力の取扱い**—出力に個人情報が現れた場合に組織が行うべきこと（第三者提供が発生したかどうかを含む）
- **入力データでの再訓練の回避**—ある参加者は、入力データで再訓練される生成AIシステムにはデータを入力せず、そうしたシステムを避けていると述べました。それが必要なのか、あるいは契約上の保証で十分なのかは、ガイダンスで解決できる問題です。

2.4 知見 4
越境移転規則により参加者は日本国外でホストされるAIシステムの利用が妨げられており、クラウド規則は不確実性と躊躇を生じさせている

知見　越境データ移転の要件は、AI の開発または導入に関する意思決定に実際に影響を及ぼしていると参加者が報告した主要な分野です。コホートの半数弱が、APPIの同等の保護および相当措置の要件をどの海外プロバイダーおよび法域が満たしているかについて不確実性があること、また、これらを特定のベンダー契約に適用することの困難さを報告しています。16社のうちGlobal Cross-Border Privacy Rules（**CBPR**）の枠組みを使用している参加者はありませんが、16社中11社（69%）は、それを変える可能性のある単一の明確化を特定しています。それは、日本のデータ移転元がGlobal CBPR認証を取得している受領者に対し、他の法的根拠や他の法的手続き・要件を満たすことなく個人情報を移転できることを個人情報保護委員会が確認することです。

2.4.1 組織がすでに取り組んでいること

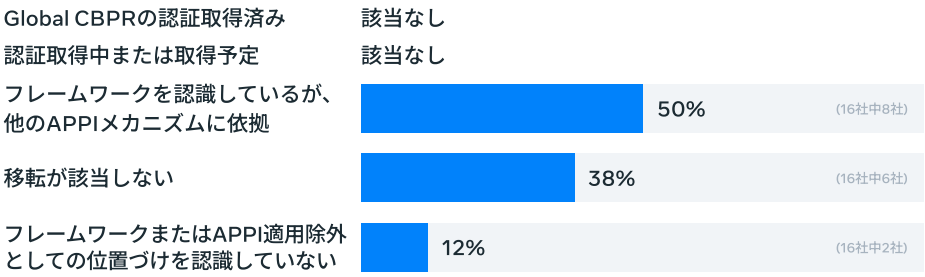
16社中4社（25%）がAI処理のために海外のクラウドインフラにデータを移転しており、16社中1社（6%）がAIワークフローの越境移転段階で特に個人情報を取り扱っています。

参加者は、日本国外への個人情報の移転について適切な法的メカニズムを特定することに困難を感じています。

APPIの第28条に基づき、これらのメカニズムには以下が含まれます。

- 「**十分性認定**」は、個人情報保護委員会がAPPIと同等の保護を提供していると指定した法域[5]への個人情報の移転を、追加の制限なく組織に認めるものです。
- そうした指定がない場合は、受領者が移転後の個人情報を保護するための**相当措置**を講じていることを確認するか、または必要な情報を提供した上で**本人の同意**を取得すること。

参加者には、国境を越えて個人情報を移転する組織向けの国際認証フレームワークであり、「相当措置」要件を満たし得るGlobal CBPRについても、各自の立場を共有するよう求めました。



2.4.2 データが示すこと

16社中7社（44%）が、直面したコンプライアンス上の課題として越境移転に関する明確性を挙げており、これは全体で直面した課題の上位3つに入っています（上記参照）。

この文脈で直面した具体的なコンプライアンス上の課題について、参加者の回答を以下の図2.4に示します。

[5] 現在は、欧州経済領域および英国です。

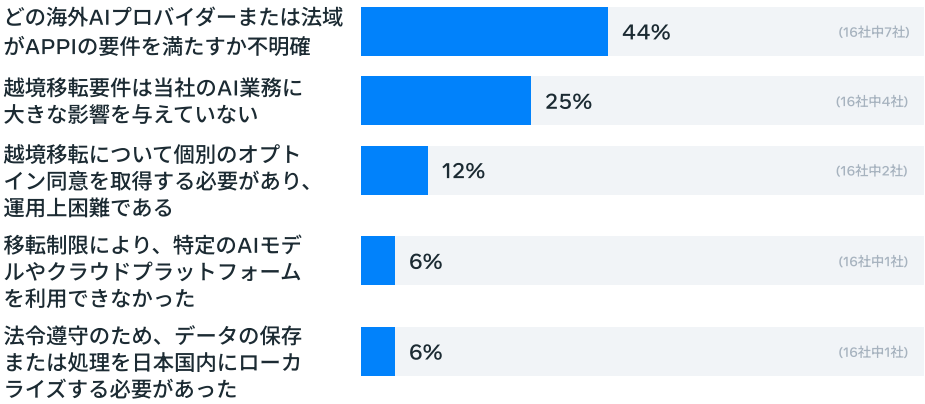


図2.4
APPIの越境移転要件がAI関連業務に及ぼす影響（n=16、複数選択可）

不明確さが法域の十分性認定に関するものか、個々のプロバイダーが講じる措置に関するものかを尋ねたところ、ある参加者は両方であると回答しました。データ保護へのアプローチは国や地域によって異なり、データをグローバルに移転する際にそれらの違いを調整することは困難です。また別の問題として、各受領者が実施するセキュリティ措置も様々であり、それらの違いも管理する必要があります。この参加者は、これらを2つの別個の課題として説明しました。

政策上の要望に関する質問では、参加者はAIに関するより分かりやすい移転ルールを求めました。

- 16社中6社（38%）が、AI文脈における越境データ移転のための合理化された相互運用可能なフレームワークを「優先政策要望」として選択し、16社中2社（12%）がこれを15の選択肢の中で最優先に位置づけました。
- 16社中8社（50%）が、グローバルなAI協力を可能にする合理化された移転ルールを「枠組みの優先事項」として選択しました。

2.4.3 組織が直面している課題

ある参加者の説明では、3つの区別可能な困難が特定されています。

事実関係

個人情報がベンダーのサービスに入った後、実際にどこに流れるのか（どの再委託先が処理し、どの国で事業を行い、サービスがログに保存するか当該リクエストへの対応の範囲を超えて利用するか）を、サービス説明書に記載されている内容とは別に把握すること。

契約面および技術面

それらのデータの流れを、APPIの相当措置要件を満たす契約条件および技術的・セキュリティ措置に反映させること。

商業面

組織が必要な契約条件を取得できるかどうかは、プロバイダーに対する交渉力に依存しますが、大手AIプロバイダーが交渉に応じることはほとんどありません。

また、この参加者がコホート内で比較的大規模な組織の一つであることも注目に値します。これは、交渉力の制約が小規模な組織に限定されないことを示唆しています。

2人目の参加者は、APPIの移転規則自体が技術的な現実と整合していないと考えています

現在では、単一の利用目的を達成するためであっても、個人情報が複数の事業者間を移動し、処理されることが日常的に必要とされています。この参加者の見解では、困難はAPPIの構造に起因しています。APPIは各事業者を個別に規制しているため、各事業者は自らの立場を独立して評価し、複数の事業者が単一の目的に寄与している場合であっても、処理チェーン全体としての評価は行われません。この参加者は、これをGDPRと対比しました。同参加者の説明によれば、GDPRは組織ではなく処理操作を中心に構成されており、義務はある時点でどの主体がデータを保有しているかではなく、データに対して何が行われているかに追随します。この参加者の説明では、APPIのアプローチの下では、各事業者が自らの担当部分についてのみ判断するため、チェーン全体にわたる保護が調整されていません。さらに、義務はリスクに比例してではなく、組織の境界において最も重く課されるため、同一の目的で使用される同一のデータであっても、受け渡しのたびに新たな要件が発生します。

インタビューにおいて、3人目の参加者は、日本の組織がサービスについて最初に尋ねる質問は、データセンターが日本国内に所在しているかどうかであると報告しました

同様に、4人目の参加者は、データを日本国内にローカライズするという具体的な決定について説明しました。

- この参加者は、特定の業務上の会話を録音しており、その録音の文字起こしが必要でした。当時最も性能の良い文字起こしサービスは、米国に拠点を置く組織によって提供されていました。録音は業務上の会話であったため、必然的に双方の参加者の名前が含まれており、海外に資料を送信する前にすべての名前の出現箇所をマスキングすることは実用的ではありませんでした。この参加者は、代わりに性能の低い国内提供のサービスを使用しました。
- 同じ参加者は、自社の一般的な方針を次のように説明しました。やむを得ない理由がない限り、日本国内のクラウドサービスのみを使用しています。その理由は、海外のサービスプロバイダーへの移転は、たとえその契約がサービス契約であっても本人の同意が必要であり、その同意を得ることは実務上困難であるためです。この参加者は、国内でアクセスできないサービスを事実上除外しています。

上記の議論は、APPIの移転規則がそもそも適用されることを前提としています。これもまた不確実性の領域として挙げられました。

5人目の参加者は、AIサービスの利用が、個人情報保護委員会のQ&A 7-53におけるいわゆる「クラウド例外」に該当しうるかどうかを問題提起しました

この規定の下では、プロバイダーが個人情報を自らの目的のために取り扱わない場合、個人情報保護委員会は、クラウドサービスプロバイダーへの特定の個人情報の移転を第三者への個人情報の提供（APPIの下では一般に本人の同意が必要）とはみなしません。この参加者は、この例外は日本独自のものであり、解釈が困難であると述べました。クラウド例外がAIサービスの利用に適用される場合、推論APIの呼び出し、ベンダープラットフォームでのファインチューニング、外部インデックスを介した検索、ログの保存など、通常のAI活動のかなりの量が、APPIの越境移転規則の対象とならない可能性があります。したがって、**図2.4**における不確実性の一部は、移転規則をどのように満たすかについての不確実性ではなく、移転規則が適用されるかどうかについての不確実性を含んでいる可能性があります。

6人目の参加者は、分析のより早い段階で生じる関連した不確実性を特定しました

それは、海外から提供されるAIサービスにデータを送信することが、そもそも越境移転に該当するかどうかという問題です。その困難はプロンプトの内容に関するものです。従業員が、海外のプロバイダーが運営するLLM APIに顧客情報の要約を送信した場合、その参加者は、それがどの程度個人情報の提供に該当するのか判断できませんでした。この参加者は、エンドユーザーとしてAIを使用する組織に向けた実務的なガイダンスを、判断フローチャートや具体的な質問と回答の形式で求めました。自社の業務で繰り返し生じる質問として、データが個人情報でなくなるまでにどの程度まで非識別化する必要があるか、およびAPIへのデータ送信が第三者への提供に該当するかどうかを挙げました。

7人目の参加者は、AIの導入により業界の慣行が変化したと指摘しました

SaaS（Software-as-a-Service）の文脈で、以前は個人情報が海外のサーバーに移転されるかどうかに細心の注意を払っていた多くの組織が、現在ではAIに対して、その経験がなかったかのようにアプローチしていると観察しました。

これに対して、Global CBPRの結果は際立っています。上記**§2.4.2**で述べたように、参加者の過半数がAIのためのより簡素な移転規則を求めており、まさにそれを提供するために設計された認証フレームワークであるGlobal CBPRはすでに存在しています。しかし、16社の参加者のうち、Global CBPR認証を保有している、または取得を目指している企業は一社もありませんでした。

認証によって何が達成されるかについての不確実性がこのギャップを説明しているかもしれません。16社中11社の参加者（69%）が、日本のデータ提供元の事業者が

Global CBPR認証を保有する受領者に対し、他の法的根拠や他の法的手続きまたは要件を遵守することなく個人情報を移転できることを個人情報保護委員会に確認するよう求めました。これらの結果は、個人情報保護委員会が2025年12月に**APPIガイドライン（外国にある第三者への提供編）**の改正を通じて、APPIの下でのGlobal CBPRシステムの位置づけを明確化したことを考慮すると、注目に値します。これは、政策上の明確化がより幅広い組織にとってアクセス可能ではなかったことを示唆しており、法律の問題ではなく周知の問題であることを意味しています。

しかしながら、参加者はまた、日本においてCBPR認証の普及が限定的である理由についても見解を共有しました。

- ある参加者は、CBPR認証の明確な価値提案が欠如していることを指摘しました。明確なメリットがなければ、組織には認証を取得する動機がないとのことでした。同参加者は、そのようなメリットを構成する2つの要素を挙げました。1つは特定の要件の免除、またはインシデント発生時の責任の判断・配分方法の変更であり、もう1つは政府やユーザーの間でフレームワークがより広く認知され、認証を受けた組織がより安全であると理解されることです。2点目について、同参加者は、そのような理解を共有する人が十分に増えれば、それだけで認証を取得する価値が生まれると述べました。
- 別の参加者は、障壁は法的効果ではなくキャパシティにあると指摘しました。認証を取得することと、それを維持することは別の問題です。維持するには組織がまだ確立していない内部システムが必要であり、現時点ではそれを構築することを正当化するリターンが見えていません。同参加者は消費者に直接AIサービスを提供していないため、認証の価値は事業の展開次第であるとのことです。同参加者の見解では、この計算を変えるのは取引先からの圧力であり、取引先の組織がそうした認証を保有していれば、自らも取得することがほぼ避けられなくなるとのことでした。

2.4.4 エコシステムへの示唆

これらの回答を総合すると、知識の問題ではなく、適用の難しさが浮かび上がります。規則や指定は公表されています。参加者のキャパシティを消費しているのは、データの流れを追跡し、これらの実態に沿った条項を起草し、プロバイダーと交渉することです。参加者は、新しいベンダーやサービスごとに同じ評価を実施しなければならないと報告しています。これらの義務を吸

収するのに最も適した立場にあるのは、専門のプライバシー機能を有する組織であり、これは**知見1**がガバナンス実践において特定した不均一性を反映しています。

また、参加者がAPPI第28条の遵守に異なるアプローチを採用し、業務への影響が大きく異なると報告していることも注目に値します。16社中4社（25%）は重大な影響がないと報告し、16社中2社（12%）は現在、移転ごとに個別の同意を取得しており、16社中1社（6%）は処理を日本国内に移転しています。組織が獲得できる契約条件がその交渉力に依存する場合、データがどの程度保護されるかは、データの機微性ではなく、提供元の事業者の商業的な力に左右される可能性があります。

特にGlobal CBPRに関しては、参加者が誰も保有していない既存の認証メカニズムは、誰も望んでいないものではなく、むしろその価値と法的な取扱いがより明確化され、認知されることで恩恵を受け得るものです。

個人情報保護委員会への提言

提言3

越境移転メカニズム（例：モデル条項、Global CBPR認証）をより採用しやすく、事前に判断可能なものにすること

個人情報保護委員会が2026年国際戦略において、日本からの個人情報の移転に関するモデル契約条項を策定するとのコミットメントを歓迎いたします。

参加者は2つの異なる問題を述べています。1つ目は、利用可能なメカニズムが、移転を完全に回避するという代替手段よりも採用が難しいことです。2つ目は、メカニズムを採用した場合でも、その法的効果が事前に判断できないことです。両方に対処する必要があり、それぞれ異なる措置が求められます。

メカニズムの採用を容易にすること

1. **Global CBPR認証の効果に関する政策の明確化を周知すること**
   2025年12月に行われた個人情報保護委員会のガイドライン改正により、Global CBPR認証の法的効果はすでに明確化されています。しかしながら、この政策の明確化にもかかわらず、組織がAPPIに基づく他の移転メカニズムや法的要件に関与することなく、Global CBPRに依拠して国境を越えてデータを移転できるという明確な声明は、調査において最も要望の多い政策介入の1つとなっています。16社中11社（69%）がこれを具体的に求めました。この数字自体が、規則の内容ではなく、可視性に関する証拠です。すでに行われた明確化を、その対象となる組織がまだ求めているということは、意図した対象者に届いていないことを意味します。16社中2社（12%）のみがフレームワークに馴染みがないと回答しましたが、認証を取得している、または現在取得を目指している組織はありません。これは法的な問題ではなくコミュニケーションの問題であり、その解決策も複雑ではありません。

2. **Global CBPR認証の採用に対するインセンティブを提供すること**
   Global CBPR認証の法的効果の明確化は重要ですが、組織にGlobal CBPR認証の取得を促すための出発点に過ぎません。§2.4.3で述べたとおり、参加者は認証取得に対する2つの異なる障壁を特定しました。

   （1） 認証を保有することによるメリットが認識されていないこと、および
   （2） リターンがまだ見えていない中で認証を維持するために継続的なキャパシティが必要であることです。

   いずれの参加者もフレームワーク自体には異議を唱えていませんでした。困難な点は、認証がまだ、他の要件の免除、何か問題が発生した場合の責任の帰属方法の変更、または市場でのより広い認知など、認証取得を正当化するために組織が示せるものを確保していないことです。

   認証プロセスの簡素化と有効期間の延長は、参加者が指摘する維持管理の負担を軽減します。組織が誠実かつ相当の注意を払って行動した場合、認証の対象となる処理に対するセーフ

提言3（続き）

ハーバーを設けることも、明確な価値提案となります。また、多くの組織はすでに隣接する分野をカバーする国際認証（例：ISO/IEC 27701）を保有しています。それらの認証がすでに満たしているGlobal CBPR要件のマッピングを公開し、同じ要件をカバーしている場合に既存の監査証拠の活用を認めることで、認証コストを低減できます。

普及は自己強化的である可能性もあります。ある参加者は、取引先が認証を保有していれば、自社も認証を取得することがほぼ不可避になると指摘しました。これは、少数の大規模な購入者またはプロバイダーの間での採用が、個々の組織に直接提供されるインセンティブよりも普及促進に効果的である可能性を示唆しています。

3. **（今後策定される）モデル条項のプロバイダーによる採用を可視化する**
   モデル条項は、プロバイダーがそれを受け入れる場合にのみ、参加者が指摘する制約を緩和します。ある参加者は、組織が取得できる条件はその交渉力に依存し、大手AIプロバイダーはほとんど交渉に応じないと報告しています。条項を日本語と併せて英語でも公開し、修正なしで採用したプロバイダーの公的記録を維持することで、提供元の事業者の作業は交渉を開始することからリストを確認することへと転換されます。



移転メカニズムの法的効果を事前に判断できるようにすること

1. **モデル条項を採用することの法的効果を明示する**
   すなわち、それらを使用することで相当措置要件が満たされるか、また提供元の事業者が追加で証明すべき事項があるとすれば何かを明らかにします。これにより、組織が設計段階でそれらに依拠できるか、それとも各案件で助言を得なければならないかが決まります。

2. **AI処理パターンを考慮して（今後策定される）モデル条項を起草する**
   参加者が述べた取り決めに対応するため、条項は再委託先の連鎖およびAIワークフローを特徴づける処理パターン（推論APIコール、ベンダープラットフォーム上でのファインチューニング、外部インデックスに対する検索、ログ保持を含む）をカバーする必要があります。

3. **相当措置のプロバイダーレベルでの評価に関するモデル基準を公表する**
   組織が認証に依拠しない場合、海外プロバイダーとの契約前に確認すべき事項に関するガイダンス—提供元の事業者がGlobal CBPR認証を持たない場合にどのような文書で十分か、再委託先の連鎖をどこまで追跡すべきか、適切な回答とはどのようなものか—は、特に専門のプライバシー担当機能を持たない組織にとって有用です。

3. **AIが実際に生成する処理パターンに照らしてクラウド例外を再明示する**
   （推論APIコール、ベンダープラットフォーム上でのファインチューニング、外部インデックスに対する検索、ログ保持など）。これは利用可能な最も価値の高い明確化の一つです。なぜなら、日常的なAI処理の大部分を規定し、移転ルールがそもそも適用されるかどうかを決定するからです。少なくとも1名の参加者が解釈できないと報告しています。

その他の政策立案者への提案

提案4

経済産業省および総務省向け：

> 「AI・データの利用に関する契約ガイドライン」を個人情報保護委員会の（今後策定される）モデル条項と整合させる。

私たちは、データおよび学習済みモデルにおける権利配分に関して当事者に参照点を提供する経済産業省の「AI・データの利用に関する契約ガイドライン」を歓迎します。

本ガイドラインは商業当事者間の契約を対象としています。個人情報保護委員会のモデル条項は、APPIを満たすために提供元の事業者が海外の受領者から確保すべき事項を対象とする予定です。海外AIプロバイダーと契約する組織は両方の文書に同時に関与することになり、参加16社のうち3社（19%）がすでに経済産業省の「AI利活用・開発に関する契約チェックリスト」を参照しています。両者を整合させ、重複する部分についてどちらが優先するかを示すことで、単一の契約と単一の社内審査で両方を満たすことが可能になります。

提案5

個人情報保護委員会および経済産業省向け（業界との連携）：

> （今後策定される）モデル条項のプロバイダーによる採用を可視化し、提供元の事業者が交渉ではなく確認できるようにする

モデル条項は、プロバイダーがそれを受け入れる場合にのみ、参加者が述べた制約を緩和します。ある参加者は、組織が取得できる条件はその交渉力に依存し、大手AIプロバイダーはほとんど交渉に応じないと報告しています。その参加者はコホート内で最大規模の組織の一つであり、この制約が小規模組織に限定されないことを示しています。

条項を日本語と併せて英語でも公開することで、海外プロバイダーが翻訳を依頼することなく採用することを促進します。修正なしで採用したプロバイダーの公的記録を維持することも、提供元の事業者の作業を、交渉力が限られる可能性のある交渉を開始することからリストを確認することへと転換するのに役立ちます。

地域間の相互運用性こそが、プロバイダー側の採用を商業的に合理的なものとします。複数のアジア市場にサービスを提供するプロバイダーは、市場ごとに交渉するのではなく、単一の条項セットを採用できます。そして、最も恩恵を受ける提供元の事業者は、個々の交渉力が最も弱い組織です。

2.5 知見 5
ウェアラブルデバイスを規律するルールは現在策定中であり、決定的な問いは未解決である

参加16社のうち、日本市場向けに先進的なウェアラブルデバイスを開発または展開しているのは1社のみであり、ウェアラブルデバイスを製造している企業はありませんでした。それにもかかわらず、生体データに関する定義の明確化は、調査において参加者の政策優先事項の第3位にランクされました。APPI改正法案は、APPIに「**特定生体個人情報**」という新たなカテゴリーを導入しましたが、これはデータが最終的に何に使用されるかではなく、データがどのように取得されるかに焦点を当てています。本セクションでは、この新たなカテゴリーが日本国内におけるウェアラブル技術の発展を適切に支援できるかどうかに影響を与える3つの主要な問いを検討します。すなわち、データが処理される目的が当該カテゴリーの適用に影響を与えるかどうか、および記録のために提供された通知が、その後の当該記録への認識適用にまで及ぶかどうかです。また、正式な法的枠組みの外にある制約、すなわち特定の環境において特定のデバイスやセンシングシステムが使用されることを一般市民が受け入れるかどうかについても検討します。

2.5.1 本知見のエビデンスベース

この特定の知見は、本報告書の他の知見と比較して、より限定的なエビデンスベースに基づいています。

参加16社のうち15社（94%）が、日本市場向けに先進的なウェアラブルデバイスを現在開発、展開、または展開を計画していないと調査で回答しました。この質問は、調査においてフィルターとして機能しました。これにより、15名の参加者は、AIにおけるウェアラブルデータの使用、マルチモーダルデータ収集、周囲の非利用者のプライバシー慣行、およびAPPIが他のフレームワークと交差する際のコンプライアンス上の課題に関する後続の質問をスキップしました。1社のみが現在日本でウェアラブル技術を展開していると回答し、その結果、調査の当該セクションを完了しました。その回答は**§2.5.2**に詳述されており、データ全体に反映されています。

そのため、調査結果を補完するために、関連する専門知識を有するプログラムの専門家グループの4名のメンバーから追加の書面による意見を求めました。このグループには、1名の業界専門家、1名の学識者、および日本を拠点とする2名の法律実務家が含まれていました。各専門家には同一の4つの主要な質問が提示され、加えて各自の専門分野に特化した5番目の質問が個別に用意されました。専門家の回答は匿名で報告されており、本文中に記載される箇所では専門家の意見として明確に識別されています。これらの専門家の意見は、本章で提示される定量的な数値からは除外されています。専門家には、単に当方の予備的な知見に対するコメントを求めるのではなく、規制枠組みに関する独自の評価を依頼しました。専門家の見解が参加者から得た回答と異なる場合には、その相違を明示的に強調しています。

2.5.2 参加者からの回答

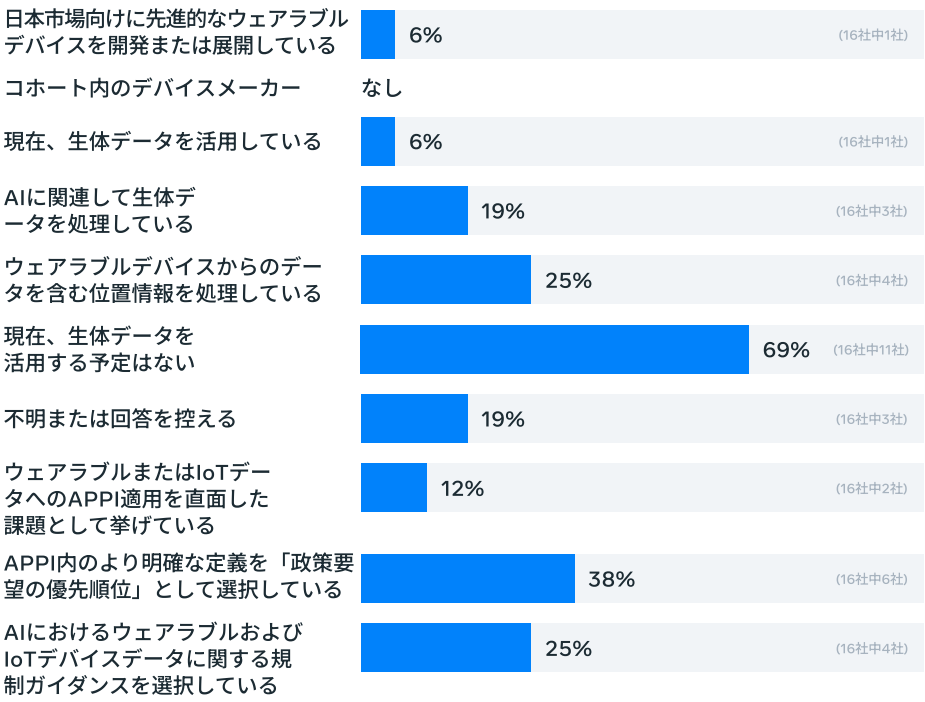


図2.6
生体データおよび身体由来データへの関与（n=16）

ガイダンスへの需要は実務に先行しています。参加者16社中2社（12%）のみが、ウェアラブルデバイスまたはモノのインターネット（IoT）デバイスからのデータにAPPIを適用する際に実際の問題に直面しています。それにもかかわらず、参加者16社中6社（38%）が、生体データに関するAPPI内のより明確な定義を、自社の事業に最も有益となる重要な政策変更として選択しています。参加者16社中4社（25%）が、ウェアラブルおよびIoTデバイスデータに対応する規制ガイダンスを具体的に選択しています。参加者16社中2社（12%）が、15の選択肢の中でこのガイダンスを最優先事項として位置づけています。ある参加者は、その順位付けが、自社組織の現在のニーズに特有の優先事項を反映したものではなく、日本の枠組みが全般的に必要としていると考える事項を表したものであることを明らかにしました。

ウェアラブルデバイスを展開している参加者は、ウェアラブルデバイスから収集した氏名、個人識別子、生体データ、および位置情報を処理していると示しています。同社は、AIワークフローの3つの異なる段階（AIモデルの学習およびファインチューニングを含む）において個人情報を取り扱っています。同社のデバイスが収集するマルチモーダルデータは、視線および眼球追跡データ、ならびに視覚的な周囲環境と空間データを捉える映像で構成されています。同社は、今後2年以内にウェアラブルデバイスデータをAI開発に使用し始めることを見込んでいます。

この参加者の枠組みに対する評価は、特に肯定的です。調査への回答において、同社は、APPIがデバイスを利用していない周囲の人々からの個人情報収集に関する明確なガイダンスを提供していること、および個人情報保護委員会のガイダンスがウェアラブル特有のプライバシー問題に対処するのに十分であることに、ある程度同意しています。さらに、同組織は、常時稼働の環境センサーを通じて収集された「特定生体個人情報」の利用目的について、事前に個人に通知することが運用上実現可能であることに強く同意しています。

参加者は、**ウェアラブル生体データおよびAI生成による健康推論データを対象とする具体的なガイドライン**を要望しました。これらのガイドラインにおいて、取得されたデータ、推論されたデータ、および学習目的で使用されるデータを明確に区別し、それぞれのカテゴリーに対して個別の同意要件および利用条件を設けることを求めました。

2.5.3 新カテゴリーが求める要件と未解決の課題

「特定生体個人情報」の新カテゴリーは、2つの累積的な基準に基づいています。第一に、**特別の技術または多額の費用**を要せずに個人の身体的特徴を取得できることが必要です。第二に、当該データの取得が行われていることを本人が容易に認識できないことが求められます。詳細については、今後公布される政令において規定される予定です。

個人情報保護委員会は、新カテゴリーの施行に関する概要案を公表しました。2026年8月、個人情報保護委員会事務局は、今後公布される政令、委員会規則、ガイドライン、およびQ&A文書において規定される具体的な規制事項を示す概要案を発出しました[6]。顔特徴データ等に関する規律のセクションにおいて、この概要は、新データカテゴリーに対する3つの主要な効果を提案しています。第一に、事業者はこのデータの取扱いに関する一定の情報を周知しなければなりません。第二に、本人がデータの利用停止を正式に請求するために満たすべき法的要件が緩和され、本人がそのような請求を行うプロセスが簡素化されました。第三に、このデータを第三者に提供する前にオプトイン同意を取得しなければならず、APPIのオプトアウトメカニズムへの依拠は禁止されています。

[6] https://www.ppc.go.jp/files/pdf/260717_kaiseihounitsuite.pdf

また、この概要は、周知義務および緩和された利用停止請求権に対する例外の設定、ならびに本人の意図に沿った取得であるため本人の権利利益を害しない取扱いに対する特定の適用除外の設定も検討しています。

現時点での見通しとして、当該カテゴリーの当初の範囲は顔特徴データに限定されると考えられます。専門家らは、個人情報保護委員会の説明資料および立法議論の双方が、ビデオカメラを使用した顔特徴データの収集にほぼ専ら焦点を当てていることを指摘しました。これに基づき、専門家らは、規制の範囲は当面、顔の特徴に厳密に限定される可能性が高く、ウェアラブルデバイスの包含は不確実であると評価しています。したがって、専門家らは、**今後公布される政令において、他の形態の特定生体個人情報がこの新カテゴリーに該当するか否かを明示的に規定することを推奨します。**

専門家らは、特別の技術または多額の費用を要しない収集に関する規定が、主要な困難の原因であると特定しました[7]。「特別の技術」の規定に関して、ある専門家は、この用語の固定的な定義を設けることは非現実的であると考えました。今日特別とみなされる技術が3年から5年以内に完全に時代遅れになる可能性があり、新しい形態が継続的に出現し、規制当局が定義を継続的に更新することは不可能であるためです。その専門家は、「高リスクをもたらす可能性が高い」処理に対するデータ保護影響評価に関する欧州データ保護会議のガイドラインで採用されているアプローチを採用することを提案しました。その専門家は、この枠組みにおける「新技術」という柔軟な概念が、実行可能なモデルを提供し得ると示唆しました。技術的なバックグラウンドを持つ第二の専門家は、独立して同じ結論に達しました。その専門家は、技術の正確な形態を規制することにかなり反対しており、代わりに、ガイダンスにおいて技術の機能的側面およびその使用の具体的条件を特定し、新技術の出現に応じて規則を更新するためのメカニズムを明示することを推奨しました。

専門家らは、「多額の費用」の規定がさらに大きな困難を呈すると考えました。ある専門家は、費用は相対的なものであると説明しました。中小企業にとって多額とみなされる金額が、大企業にとっては多額でない場合があります。さらに、価格は時間とともに変動するため、今日閾値内にある技術が、後に閾値外になる可能性があります。例えば、契約更新時に割引を受けた場合などです。この専門家の見解では、**閾値を定量的に表現することは不可能です。**代わりに、規制当局が境界線を決定する際に関連する**定性的要素を特定すること**が極めて重要です。

実務家は法的助言を行う上での課題に直面しています。ある専門家は、個人情報保護委員会の2026年8月の概要に言及しつつ、すべての規制要素の具体的内容が完全に解釈に委ねられた状態にあると指摘しました。その結果、日本の法務実務家は、このような状況下で関係者に助言を行うことに困難を感じています。

[7] https://ec.europa.eu/newsroom/article29/items/611236

2.5.4 フレームワークが発展を支援するか否かを決定する3つの問い

① デバイスの装着を選択した本人は、収集を容易に認識できるか？

データが「特定生体個人情報」に該当するかどうかの基準の一つは、個人が取得が行われていることを容易に認識できるかどうかです。表面上、これは大きく異なる二つの集団、すなわちデバイスの装着を選択した本人と、装着していない周囲の人々の双方に適用され得ますが、この規定は両者を区別していません。これにより、ウェアラブルデバイスのメーカーやこれらのデバイス上で動作するアプリケーションの開発者に適用される義務の範囲が決定され、製品発売の数年前に行われる設計上の意思決定に影響を与えることになります。

この問題について独立して意見を求めた3名の専門家は、同じ見解に達しました。専門家らは概ね、自発的にデバイスを装着し、利用規約等を通じてそのデータ取扱慣行について十分な開示を受けた個人は、取得を容易に認識していると合理的にみなし得るという点で一致しています。

個人情報保護委員会の2026年8月の概要では、この同じ実務上の結果を達成するための別の方法が示されています。この概要では、取得の状況から、データの取扱いが個人の権利利益を害しないことが明らかである場合について、緩和された利用停止権の例外を提案しています。これは、取扱いが本人の意思に反しないことを理由として特に適用されます。デバイスが何を収集するかについて明示的に説明を受けた上でデバイスの装着を選択した人は、まさにこの例外の自然な適用対象となります。

② 処理の目的は重要ですか？

「特定生体個人情報」という新たなカテゴリーは、データが何に使用されるかではなく、どのように取得されるかによって範囲が定められています。これは意図的な設計上の選択と思われますが、主にデータが個人を識別するために処理されるかどうかに焦点を当てる他の法域の枠組みとは、日本のアプローチを区別するものとなっています。

このような範囲設定の結果、個人が識別されない多くの処理であっても、このカテゴリーに該当し得ることになります。そのような処理の例としては、利用者が画面上の項目を選択するための視線追跡、デジタルインターフェースの幅広いユーザー操作のためのジェスチャー検出、疲労の兆候が見られる際にドライバーに警告を発する車内機能などが挙げられます。

この問題が今重要である理由は、個人情報保護委員会の説明資料では個人を識別するために設計されたデバイスやソフトウェアを参照してこのカテゴリーを説明してい

ますが、法定の基準では目的について全く言及されていないためです。その枠組みが政令やガイダンスに反映されるかどうかは未解決です。

ここで専門家の回答は大きく分かれており、その相違は有益な示唆を与えています。

- ある専門家は、規制上の懸念は、特に個人を識別するために設計されたデバイスやソフトウェアに重点が置かれているように見えると考えています。この専門家は、個人を識別するという積極的な目的が決定的な規制要素となるかどうかを、政令または関連するガイダンスで明確にすることが極めて適切である可能性があると示唆しています。
- 2人目の専門家は、個人を識別することを意図しない一時的な処理は、識別目的で特に使用される生体データとは別に検討される可能性が高いと考えています。ただし、この専門家は、そのようなデータであっても、個人に関する他の識別情報と紐付けることが可能な場合には、依然として個人情報に該当し、したがってAPPIの適用を受けると指摘しています。
- 3人目の専門家は、保持されたデータは後に他の目的で使用される可能性があり、また、表明された目的が現在の処理に引き続き適用されていることを個人や政府が確認することは困難であるという理由から、目的を分類の基準とすることについて、他の専門家ほど確信を持っていませんでした。この見解では、より信頼性の高い管理はアーキテクチャ上のものであり、開発者はデータが保持される期間とデータがデバイスから外部に送信されるかどうかを明示すべきであり、これによりシステム設計がオンデバイス処理に向かうことをこの専門家は予想していました。

③

録画のために与えられた通知は、その後の認識処理の適用にまでおよびますか？

ある参加者が、インタビュー中にこの特定の複雑な問題を提起しました。この参加者の説明によれば、撮影に対する基本的な同意を取得することと、その映像に対して事後的に顔認識、歩容認識、またはその他の高度な認識を適用することは、全く異なる処理の層を表しています。この参加者は、これらの層は現行法では別個のものとして扱われていないと指摘しました。

ある専門家も別途同様の結論に達し、標準的な映像記録に対する個人の当初の同意が、その後の顔認識その他の高度な認識技術の適用にまで自動的に及ぶと法的に結論づけることは極めて困難であると主張しました。利用者に提供された当初の説明が、個人識別、顔特徴データの作成、およびデータベースとの照合を具体的に網羅して

いた場合、その後の利用はその範囲内に安全に収まる可能性があります。しかしながら、個人が単に記録されることのみを告知され、その記録がその後個人識別や行動追跡に使用される場合、当該処理は通常、個人が合理的に予期し得た範囲を超える可能性があります。この同じ専門家は、特定生体個人情報を収集する際には特定の情報を提供しなければならないため、データ主体は有効な同意を行う前にこれらの事項について告知を受ける必要がある可能性が非常に高いと指摘しています。この必須開示事項には、処理の事実、その正確な目的、および変換される身体的特徴の具体的な詳細が含まれます。

2.5.5 規制以外の制約：社会的受容

日本において組織がウェアラブルデバイスを成功裏に開発・展開できるかどうかに最も大きな影響を与える要因は何かという質問に対し、専門家らは正式な法的枠組みの完全に外側にある強力な要因を挙げました。

ある専門家は、個人の映像記録が日本において特に懸念される話題であると説明しました。この専門家は、こうした強い社会的懸念への配慮を、日本の消費者が期待する極めて高い製品品質の要件に直接組み込む必要があると考えました。この専門家の評価として、製品設計が完了した後にのみ法令遵守を検討する組織は、必然的に商業的に失敗する製品を生み出すことになります。

2人目の専門家は、全く同じ文化的背景を指摘し、日本のスマートフォンに義務的なシャッター音が存在するのは、まさに盗撮に関する社会的懸念のためであると述べました。その結果、日常的な場面で画像を撮影するあらゆるデバイスには、可聴信号や明るいインジケーターライトなどの物理的な仕組みが普遍的に期待されています。

3人目の専門家は、作用している独特の社会的力学を的確に要約しました。日本では、専門家が当初提起した非常に具体的な懸念が一般市民に極めて急速に広がり、重大かつ圧倒的な社会的批判へと急速に発展することがあります。この専門家は、APPIが法的にこれらを義務付けていないにもかかわらず、厳格なリスク評価の実施およびマルチステークホルダー協議プロセスの実行を事実上必須として扱うべきであると助言しました。また、この専門家は、組織はこれらの評価のわかりやすい概要を公表すべきであり、そこには特定されたリスク、製品設計に直接組み込まれた具体的な軽減措置、および一般利用者向けの極めて実用的なガイダンスとよくある質問を詳述すべきであると考えました。

この文化的背景は、第2.5.2節で記録された極めて限定的な業界の関与をどのように読み解くべきかに直接関係しています。規制上の立場が明らかに未確定のままであり、参加者がその確定を待っているのは当然のことです。しかしながら、専門家の証言に基づけば、すべての規制上の問題を完璧に解決した組織であっても、製品展開を完全に阻止しうる大きな社会的制約に直面することになります。

2.5.6 エコシステムへの示唆

この領域に規制が存在しないわけではありません

日本の政策立案者が直面する主要な問題は、既存の規制介入が技術開発を支援するよう調整されているかどうかです。APPIは現在、確立された個人識別符号の概念を通じて生体データに適用されています。2026年の改正では、特定生体個人情報の専用カテゴリーが正式に追加されます。医療・保健分野には分野別の枠組みが適用され、AI事業者ガイドラインはAIシステムにおけるかかるデータの利活用に関する指針を提供しています。

詳細はまだ提供されておらず、不確実性を生じさせています

4人の専門家のうち3人の回答が、表現は若干異なるものの、全く同じ構造的な命題に収斂しています。彼らは、政令および個人情報保護委員会規則は、満たされなければならない運用条件と規制の境界を設定する上で関連する質的要素のみを規定すべきであると主張しています。規制当局は、特定の技術形態を規定したり、必然的に時代遅れになる固定的なリストを作成したりすることを避けなければなりません。ある専門家はこの論理を通知の問題に直接適用しました。この専門家は、個人情報保護委員会は、要件がどのように実施されなければならないかを指示するのではなく、どのような機能的条件が満たされなければならないかに完全に焦点を当てるべきであると述べました。このアプローチは、民間部門の主体が最も適切な技術的ソリューションを開発する余地を意図的に創出するものです。

当調査で記録された要望はそれに応じて解釈されるべきです

調査参加者は、投資を確定する前に政府が明確なルールを確立することを明示的に求めています。専門家の証言に大きく基づけば、これらの組織は、新しいカテゴリーが正確に何を対象とするか、どのような具体的な運用基準に依拠するか、および基盤となる技術が時間の経過とともに変化するにつれて境界がどのように評価されるかを正確に説明する、明確で原則に基づいた声明から恩恵を受けることになります。

個人情報保護委員会への提言

提言4

施行準備期間中に「特定生体個人情報」に関するリスクベースかつ実行可能な定義上の指針を提供すること

特定生体個人情報（specific biometric personal information）の専用カテゴリーを設けるAPPI改正を歓迎いたします。また、この新規定を実施するための下位規範が策定される際の包括的な体系を個人情報保護委員会が公表したことも強く歓迎いたします。さらに、その策定過程の各段階において、個人および事業者から建設的な意見を積極的に求めるという同委員会の表明された姿勢を称賛いたします。

5つの具体的な明確化により、この枠組みは、日本においてウェアラブル技術を開発・展開する組織にとって非常に実用的なものとなります。

第一に、デバイスの装着を選択し、そのデバイスが何を収集するかを告知された者は、その収集について容易に認識していることを確認すること

私たちが相談したすべての法律専門家が、それぞれ独立してまさにこの見解に達しました。将来のガイダンスでは、どのような種類の通知が法的に十分であるかを明確に示す必要があります。なぜなら、認識は、単にデバイスを装着するという物理的行為から生じるのではなく、どのようなデータが収集されるかを個人が根本的に理解することから厳密に生じるものだからです。付随するガイダンスは、この新しいカテゴリーに該当しないデータがAPPIの一般的な義務の対象であり続けることも確認すべきです。

第二に、個人を識別する目的での処理が決定的な要素であるかどうかを明確にすること

当方の2名の法律専門家の解釈に基づくと、個人情報保護委員会の主たる規制上の懸念は、個人を識別するために特別に設計されたデバイスおよびソフトウェアに向けられているように見受けられます。この解釈を正式に確認することで、当方の参加者の一人がウェアラブルデバイスを展開する際に回答できなかったまさにその運用上の疑問が完全に解決されることになります。これにより、個人が一切識別されない完全に無害な処理を、新しいカテゴリーの完全に外に安全に位置付けることもできます。このアプローチは、そのようなデータすべてを、個人に関する他の識別情報と紐付けられる限りにおいて、APPIの一般的な義務に厳密に服するものとして正しく位置付けます。

提言4（続き）



第三に、どのモダリティが対象範囲に含まれるか、また技術の変化に応じて境界事例がどのように評価されるかを明示すること

当方の専門家は、現在の規制上の示唆から、新しいカテゴリーの実施は当初、顔の特徴データに焦点を当てる一方、ウェアラブルデバイスの位置付けは不明確なままであると評価しています。当方の専門家は、政令において、他の形態の特定生体個人情報がこのカテゴリーに該当するかどうかを明示的に記載し、業界が仮定や推論のみに依拠しないようにすることを推奨しています。加えて、純粋に定量的な基準は、取得に特別の技術が必要となる場合や、多額の費用が発生するかどうかを判断するには不適切である可能性があります。当方の専門家が説明したように、何が特別の技術に該当するかは時間とともに急速に変化し、何が多額の費用に該当するかは、誰がいつそのコストを負担するかによって異なります。当方の4名の専門家のうち3名は、これらの境界を確立するために関連する正確な質的要素と、評価がどのように更新されるかを詳細に示す正式なメカニズムを、ガイダンスで明示するよう求めました。ある専門家は、欧州データ保護会議のデータ保護影響評価に関するガイドラインで採用されている、「新技術」という適応可能な概念に基づく柔軟なアプローチが、実用的なモデルとして機能し得ると提案しました。



第四に、取得とその後の認識処理との関係、および周知義務が発生する条件について対応すること

完全に合法的に記録されたセンサーデータまたは映像に、後から高度な認識アルゴリズムが適用される場合があります。専門家の証言に大きく基づくと、記録に関する当初の通知は、通常、法的にはその後の処理にはおよびません。個人が単に記録されることを告知されただけの場合、識別または行動追跡のための後の使用は、個人が合理的に予期し得た範囲を超える可能性があります。したがって、認識技術の後の適用が想定される場合に、収集前に何を開示しなければならないかをガイダンスで明示することは有用です。ある専門家によれば、これには、特定生体個人情報が収集される際に法律がすでに提供を求めている事項が含まれる可能性が高いとのことです。ガイダンスは、データがローカルデバイス上でのみ処理され、使用後直ちに削除され、外部に一切送信されないシナリオにおいて、規制上の義務が一切適用されるかどうかについても、明確に対処しなければなりません。ある専門家は、このまさにシナリオを、すべての通知要件を安全に緩和できる有効な条件として直接提案しました。このアプローチは、法的コンプライアンスを単なる書類上の開示作業に矮小化するのではなく、製品の基本設計の中核的な特性とするための、最も明確な利用可能な道筋を示しています。

提言4（続き）

第五に、運用上の条件がどのように技術的に満たされるべきかを正確に指示するのではなく、どのような運用上の条件が満たされなければならないかを明示すること

この種のガイダンスは、達成すべき成果を明示し、それをどのように達成するかを業界に委ねる場合に最も効果的に機能します。ある専門家が述べたように、これは規制当局に詳細な技術的ガイダンスを提供することが期待されるべき分野ではありません。これらのシステムを構築する組織がそれらを最もよく理解しており、自社の製品に適したソリューションを開発するのに適した立場にあります。別の専門家は、異なる方向から同じ結論に達しました。日本固有の技術要件はデバイスコストを増加させることになり、これは、メカニズムではなく条件を中心に構成されたガイダンスが、規制上および商業上の両方の目的に資することを示唆しています。

手続きについて。 これらの重要な問題は、政令、個人情報保護委員会規則、および進行中のパブリックコメント手続きを通じて決定されることになります。私たちの包括的な調査で特定された主要なリスクは、規制の不足ではなく、むしろ時期尚早な過度の広範性です。商業的な実務が十分に成熟する前に厳格な基準が定められ、識別リスクが全くない無害な処理を誤って捕捉するほど広範に設定された場合、規制は、このカテゴリーが本来規律するために創設された革新的なユースケースそのものを排除することになります。

その他の政策立案者への提案

提案6

個人情報保護委員会および経済産業省に対し、施行準備期間中に：

付随的な記録が適切に通知される条件を確立すること

APPIは、特定生体個人情報が収集される際に一定の事項を本人の知り得る状態に置くことを求めています。データを取得される本人がデバイスの利用者である場合、これは簡単です。購入時または登録時に通知することができます。データを取得される本人がデバイスがたまたま記録した人物——通行人や、利用者の後ろに立っている人——である場合、事業者はその人が誰であるかを知らないため、その人に連絡する方法がありません。一般向けの告知を公表することで、この義務を形式的に満たすことができるかもしれません。しかし、ある専門家が指摘したように、自分のデータが収集されたことを全く知らない個人は、どの公表された告知を参照すべきか知ることができません。

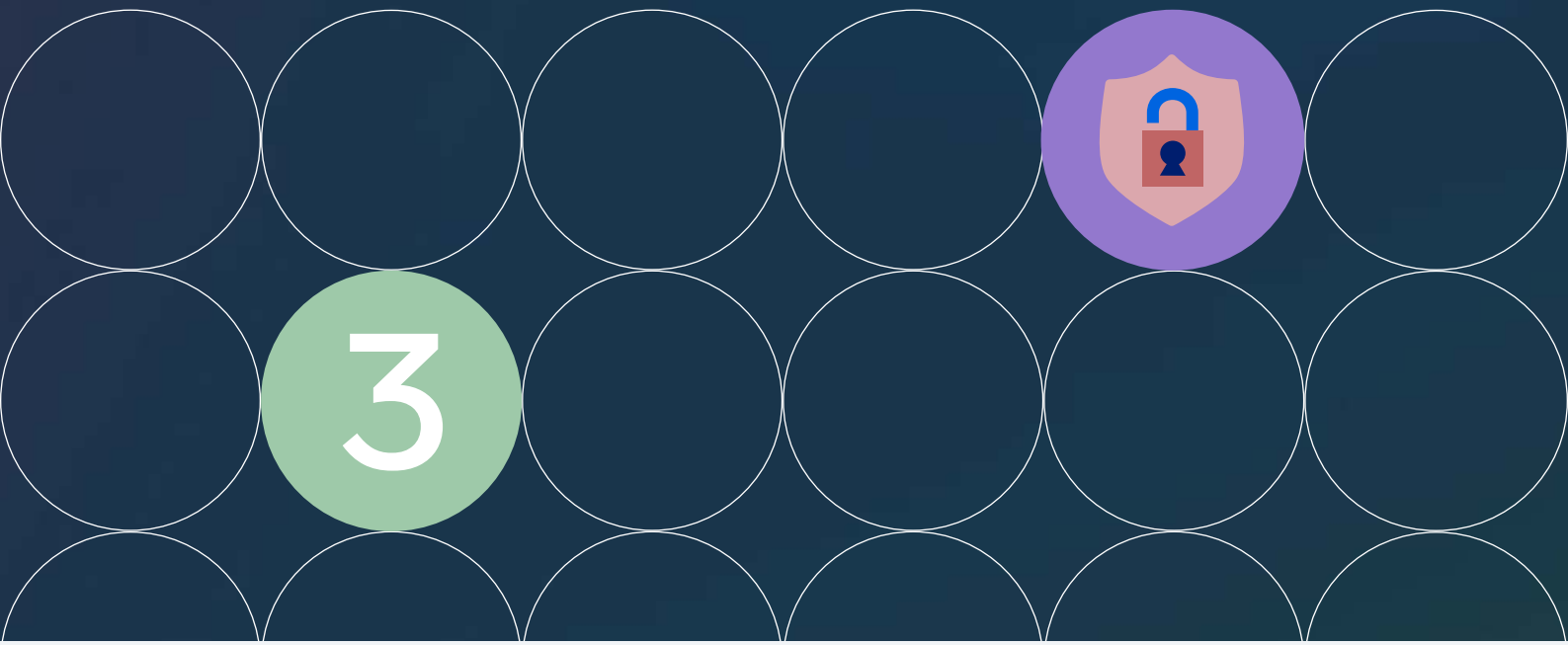
特定の技術的メカニズムを義務付けるのではなく、個人情報保護委員会と経済産業省は、提案されるいかなる解決策も満たすべき条件を共同で示すことができます。これらの条件は、近くにいる人がデータ収集が行われていることを容易に認識できること、希望すればより詳細な情報を容易に入手できること、および異議を申し立てる実効的な手段を有していることを義務付けるべきです。民間企業は、これらの広範な条件が技術的にどのように満たされるかを正確に決定するのにより適した立場にあるかもしれません。

例えば、私たちの専門家は、デバイスの動作状態をハードウェア自体に直接明示的に表示することを含め、すでに活発に議論されている幅広い革新的なアプローチについて説明しました。開発者は、近くにいる人が認識できる視覚的な表示や、一定の間隔で繰り返される明確な音声通知を使用することもできると提案しました。専門家は、傍観者により大きな透明性とコントロールを提供できる可能性のある、その他の将来的な仮説的アプローチの範囲についても議論しました。私たちの専門家の見解は、規制当局は解決策が満たすべき条件を示すべきであるが、技術的な設計と実装は業界に委ねるべきであるというものでした。

ある専門家は、明示的に述べる価値が非常に高い追加の条件を提案しました。この専門家は、データがローカルデバイス上でのみ処理され、即座に削除され、外部に送信されることが一切ない場合、義務的な通知要件を適用する必要がない可能性があると提案しました。

第3章

結論と今後のステップ



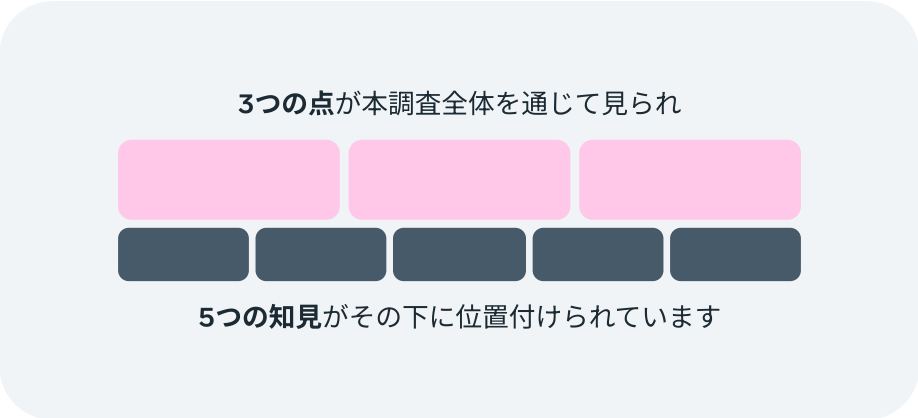
3.1 主要な知見の要約

本プログラムは、これらの分野を規律する法律自体が変化しつつある時期に、日本で事業を展開する組織がAIイノベーションとデータ保護が交わる領域で、どのように対応しているかを理解することを目的として開始されました。16社が構造化されたバイリンガル調査を完了し、8組織がフォローアップインタビューに参加しました。

調査の公開からインタビューの終了までの間に、国会は個人情報の保護に関する法律（**APPI**）の重要な改正を可決しました。これらの改正のうち2つは、本報告書で取り上げた問題に直接関係しています。

- 1つ目は、「統計作成等」に関する同意の新たな免除であり、公に開示された要配慮個人情報の取得と、統計目的での第三者への個人情報の提供の両方を許容するものです。これらの場合に個人の同意を求める代わりに、この免除は、組織が統計作成活動に関する所定の情報を継続的に公表することを求めています。改正法案の内閣の概要によると、「統計作成等」はAI開発にもおよびます。
- 2つ目は、「特定生体個人情報」の新しいカテゴリーであり、特別の技術や多額の費用を要せずに身体的特徴を取得できるかどうか、および個人が取得が行われていることを容易に認識できるかどうかを基準として決定されます。この新しいカテゴリーの個人情報は、透明性要件、第三者への開示に関するより厳格な基準、および情報が違法に取り扱われていない場合であっても個人が利用または提供の停止を求める権利の対象となります。

改正法は2026年7月17日に公布され、新たな義務の大部分は2028年7月16日までに施行されます。両規定の実務上の範囲は、本稿執筆時点では公表されていなかった政令および個人情報保護委員会規則によって定められることになります。



観察事項 1

業界は改革に期待しています

参加者16社中12社（75%）が、2026年のAPPI改正によりAIにおける個人情報利用に対する規制上の障壁が建設的に軽減されると予想しており、これは本調査全体で記録された中で最大の合意率でした。改正法案可決後に実施したインタビューでも、この期待は実質的に変わっていないことが確認されました。したがって本報告書は、業界からのフィードバックが最も有用となる改革プロセスの時点に到達しています。すなわち、主たる法律は確定し、その適用方法を決定する下位規則およびガイダンスはまだ策定中であり、それらを適用しなければならない組織は既に遵守に何が必要かを検討しています。

観察事項 2

参加者はより軽い義務を求めているわけではありません

調査およびインタビュー全体を通じて、参加者は主に、行動する前に適用できる規則、すなわち事前に評価可能な基準、事例、モデル契約条項、チェックリストを求めていました。より実質的なことを求める参加者がいた場合、それは通常、現行規則で禁止されていることを行う許可ではなく、学習済みモデルが個人情報データベース等に該当するかどうかといった法的解釈の問題を規制当局が解決することでした。ある参加者は、執行の縮小ではなく、より広範な執行を求めていました。

観察事項 3

規制の不確実性はAI導入を止めてはいませんが、その形態に影響を与えています

AIの開発または導入に関する意思決定において、規制の不確実性を「重大な」または「主要な」要因と評価した参加者はいませんでした。しかしながら、本報告書では、規制の不確実性が社内レビューコスト、保守的な対応、合法性についての確定的見解のないまま行われる意思決定、および縮小されるか全く試みられないユースケースを生み出していることが確認されました。直接的な結果として、組織は法律がそれを許可していることを事前に確認できないため、合法であった可能性のあるデータのユースケースを断念しています。より広範な結果として、組織は同じ要件について異なる結論に達し、それらの結論が収束するメカニズムも、規制当局も、組織間でどの点の解釈が異なるのかを把握できません。

このような背景を踏まえ、第2章で示す5つの知見は以下のとおりです。

知見 1

日本のAIガイダンスは対象とする受け手に届いていますが、参加者は法的拘束力のある義務への遵守に関する問題を解決するのに十分とは考えていません

AI推進法は民間組織に努力義務のみを課しているため、AIユースケースを進めてよいかを決定する組織にとって、法的帰結をもたらす問題はAPPIが何を要求しているかです。自主的なAIガイダンスは広く参照されており、参加者16社中11社（69%）が「AI事業者ガイドライン」を参考にしており、16社中3社（19%）がそれを最も影響力のある単一のフレームワークとして扱っています。しかしながら、追加の法的助言なしにAPPIが何を要求しているかを確認するのにそのガイダンスで十分と考える参加者は1社（6%）のみであり、16社中14名（88%）はそれに加えて法的助言を必要とするか、直面する問題を解決できないと考えています。各組織は様々なガバナンスフレームワークを独自に調整することを余儀なくされ、社内ガイドラインの作成、チェックリストの構築、レビュー時間という形でそのコストを負担しています。

知見 2

組織は、AI活動で個人情報を利用するためにどこまで非識別化しなければならないかを確認することに困難を抱えています

十分な匿名化の水準を判断するための、実務的・客観的でリスクに基づく基準を示すことは、参加企業が最も高い優先順位を付けた政策要望です。16社中10社

（62%）がこれを選択し、16社中4社（25%）が第1位としました。16社中8社（50%）が実務上の困難に遭遇しています。2名の参加者は、法定制度への依存を完全にやめ、すべてのデータを一貫してAPPIの適用範囲内として扱っていると述べました。これは事前に確立できない閾値に対する合理的な対応ですが、APPIの匿名加工情報および仮名加工情報制度が提供するよう設計された柔軟性を放棄するものです。

知見 3

APPIにおけるAI出力およびモデルの分類は未解決のままです

参加者16社中8社（50%）が、生成AI出力が個人情報を再構成または推論し得るリスクを挙げ、参加者が遭遇したコンプライアンス上の課題の中で同率1位となりました。その下には、学習済みモデルがAPPIにおける個人情報データベース等に該当するかどうかについての未解決の問題があり、2名の参加者が独立して提起しました。問題が未解決の場合、より一般的な対応は自制です。組織はユースケースを縮小するか、構築しません。

知見 4

越境規則により、参加者は日本国外でホストされているAIシステムを利用できず、クラウド規則は不確実性と躊躇を引き起こしています

参加者16社中7社（44%）が、どの海外プロバイダーまたは法域がAPPIの要件を満たすかについて不確実性を報告しており、これは参加者が構築したものを変更したと述べた分野です。参加16社のうち、Global CBPR認証を保持または取得しようとしている者はいませんが、16社中11社（69%）が、認証された受領者への移転が他の根拠なしに合法であることの確認を求めています。個人情報保護委員会が2025年12月にその立場を明確化したため、これは法的な問題ではなく、既に示された明確化が十分に周知・認知されていないという問題です。

知見 5

ウェアラブルデバイスを規律する規則は現在策定中であり、決定的な問題は未解決です

参加16社のうち、日本市場向けに先進的なウェアラブルデバイスを開発または導入しているのは1名のみであり、デバイスを製造している者はいません。それにもかかわらず、参加者は生体データに関する定義の明確化を政策要望の第3位に挙げており、問題に遭遇した後ではなく、構築する前に規則を求めています。2026年改正は、データの利用目的ではなく取得方法によって範囲が定められる特定生体個人情報という新たなカテゴリーを創設し、その内容は施行までの準備期間中に政令および個人情報保護委員会規則によって確定されます。

本報告書は、当該カテゴリーがウェアラブルデバイスにどのように適用されるかを決定する3つの論点を特定し、それらに回答するため専門家からの追加的な意見を求めました。

① デバイスの装着を選択した者がそのデータ収集を容易に認識できるものとして扱われるかどうか

私たちが相談したすべての法律専門家は、デバイスが何を収集するかを事前に説明された装着者は‘、当該カテゴリーの対象外となる可能性が高いと考えました。

② 処理の目的が重要かどうか

2名の専門家は、個人情報保護委員会の説明資料を個人を識別することを目的として設計されたデバイスを対象としたものと解釈し、これにより、識別を目的としない通常のデータ収集（例：視線追跡、ジェスチャー制御、疲労検知）はカテゴリーの対象外となると考えました。一方、3人目の専門家は、保持されたデータは後に他の用途に使用される可能性があるため、目的はカテゴリー分類の不安定な根拠であると注意を促しました。

③ 録画に対して行われた通知が、その後当該映像に認識技術を適用することにまで及ぶかどうか

ある専門家は、元の説明が識別について具体的に言及していない限り、及ばないと考えました。

これら3つの論点はいずれも未解決であり、3つすべてが現在策定中のAPPI 2026年改正に関する施行規則およびガイドラインに委ねられています。私たちは、個人情報保護委員会が施行までの期間中に各論点を解決し、充足手段ではなく充足すべき条件を明示し、技術の変化に伴い境界事例がどのように評価されるかを示すことを推奨します（提言**4**参照）。

第4の制約は、法的枠組みの完全に外側に位置しています。私たちの専門家は、特定のデバイスが特定の場所で使用されることに対する社会的受容が、製品が市場に到達するかどうかを決定する上で、いかなる法的論点よりも重要である可能性が高いと考えました。

第2章の提言は、本改正の実施に向けられています。これらは、新たな義務が発効する前に組織が回答を必要とする論点、および回答が利用可能となる形式——公表された基準、具体的な事例、モデル条項、設計段階で適用できる程度に限定的に規定された政令条項——を特定しています。異なる規則を主張するものではありません。

3.2 日本の政策への示唆

これらの結論は、4つの点で日本の政策に関係しています：

どのような手段が必要か

いつまでに策定される必要があるか

何を対象とする必要があるか

そして誰が策定する必要があるか、という点です

参加者が求めるもののほぼすべては、追加の立法を必要としません

本報告書で特定された論点——データがAPPIの対象外となるためにはどの程度まで非識別化される必要があるか、モデルが返す内容にどのような法的地位が付与されるか、提供元の事業者は海外の提供者をどのように評価すべきか、新たな生体情報カテゴリーの範囲はどのように定められるか——は解釈の問題です。政令およびガイドラインを通じて、改正APPIが発効するまでの期間内に回答を得ることができ、次の見直しサイクルを待つ必要はありません。

施行までの期間が実質的な対応期間です

参加者は、行動を起こす前に下位規則およびガイドラインを待っていると述べていますが、これは適用がまだ確定していない改正に対する合理的な対応です。しかしながら、施行までの期間を待機に費やすことは、その期間を活用したことにはなりません。組織が内容を理解し、開発に反映するための時間を十分に確保できるよう、早期に公表されたガイダンスであれば、それに沿った開発が可能になりますが、義務が発効する直前に公表されるガイドラインはそれを可能にしません。

いくつかの論点は組織の境界を越えています

業種別ではなくカメラやセンサーを軸としたガイドラインは、個人情報保護委員会、経済産業省、および総務省が協力して行動することを必要とします。ある参加者は、ソフトウェア、ハードウェア、およびデータ政策に関する所管が異なる省庁に分かれているため、各省庁が個別に策定したガイドラインは、3つすべてを組み合わせた製品に容易に適用できないと指摘しました。

促進的な枠組みは、展開だけでなく開発にも対応する必要があります

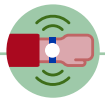
本報告書の多くは、導入するAIシステムに規則を適用する組織に関するものです。コネクテッドデバイスを開発する組織にとっては、そもそも日本での開発を枠組みが支援するかどうかがより早い段階の問題となります。これは、製品が市場に到達するかなり前に生じる事項に左右されます——例えば、開発者が設計段階でデバイスが生成するセンサーデータにどの義務が適用されるかを判断できるか、データを取得される人々がその取得を認識できるものとして扱われるか、同意した参加者から収集した開発データをデバイスが実行するモデルの学習に使用できるか、そしてその回答が複数年にわたるプログラムを通じて維持されるか、といった事項です。今回の参加者の証言に基づけば、これらのいずれも現時点では確信をもって回答することができません。

3.3 今後の方向性

本調査で明らかにできなかったこと

3つの問いが未解決のまま残っています。

1. 参加者が述べた困難が、主として規則自体に起因するものなのか、それとも組織の規則解釈能力に起因するものなのかという点です。
2. 同一の要件を読んだ組織が実際に異なる実質的結論に至るかどうかという点です。組織によって業務の進め方が異なること、また一部の組織は未解決の前提のまま進めていることは示しましたが、すべての参加者に共通のシナリオを提示してこの点を直接検証することはしませんでした。
3. これらの要件がその保護目的を達成しているかどうかという点です。これは規制対象組織への質問では答えられない問いであり、個人からのエビデンス、苦情データ、または規制当局からのエビデンスが必要となります。



ウェアラブルデバイスに関するエビデンスベース

本調査のアンケートにはフィルター質問が含まれており、16社中15社の参加者がウェアラブルデータ、マルチモーダル収集、および周囲の非利用者のプライバシーに関する質問をスキップする結果となりました。1社の参加者がフィルターを通過してこれらの質問に回答し、インタビューではこれらの分野についてより詳細に議論する機会が得られました。それでもなお、知見5は本報告書の他の知見と比較して、より狭いエビデンスベースに基づいています。そのため、本プログラムの専門家グループのうち関連する専門知識を有するメンバーから、補足的な書面による意見を求める必要がありました。



注視すべき規制上のマイルストーン

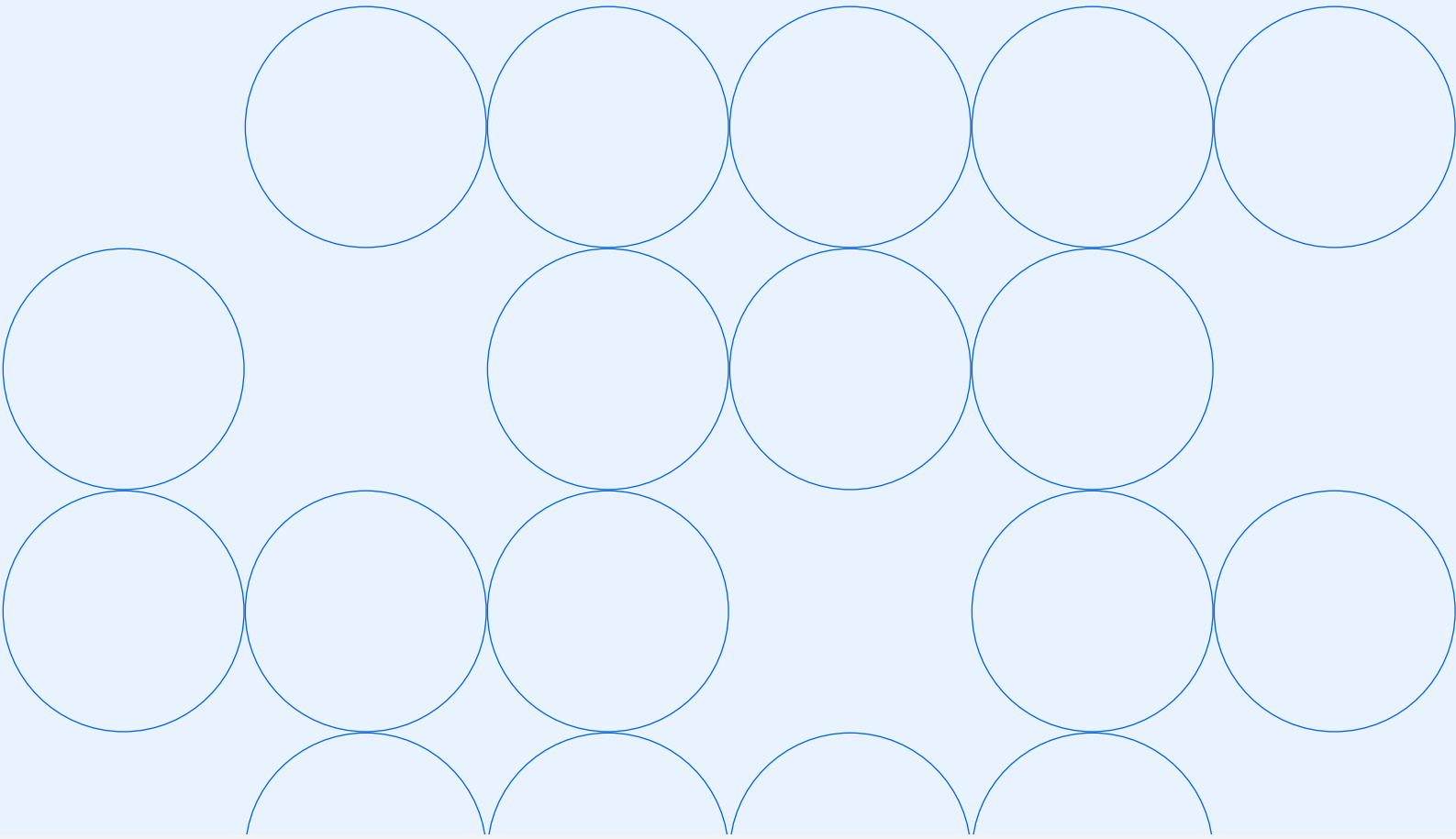
新たなAPPI規定の適用範囲を定める政令および個人情報保護委員会規則、それに伴うパブリックコメント、そして2028年7月の施行前に発出されるガイダンスがあります。これらのそれぞれが、参加者が述べた事項のどの程度が解決されるかを決定することになります。施行後に同じコホートを対象としたフォローアップ調査を実施すれば、本報告書に記録された期待が満たされたかどうかを確認できるでしょう。これは本報告書が提起できても、現時点では答えられない問いです。



さらなる調査が最も有益となる分野

APPIの定義における学習済みモデルの位置づけ、およびそれに伴う開示、訂正、利用停止の権利への影響は、参加者が最も確定的な見解に達することができず、また最もガイダンスが不足している問題です。撮影と事後的な認識処理の関係、すなわち録画に関して行われた通知が当該録画への認識技術の適用にまで及ぶかどうかという問題は、現在すでに通常の商用展開において生じており、新たなカテゴリーが発効すればより先鋭化することになります。また、データの取得を容易に認識できるかという基準の下での、デバイスの利用者本人の位置づけは、当該カテゴリーの実務上の適用範囲を最も左右する問題です。

附録



I. Open Loop Japanについて

i.i プログラムの趣旨

Open Loop Japan 2026は、日本における効果的なAIおよびデータガバナンスの枠組みの構築を支援するエビデンスに基づく知見を創出するために設計された、マルチステークホルダー型の政策プロトタイピングプログラムです。本プログラムは2026年6月から9月まで実施され、企業、政策立案者、学識経験者、および市民社会を招集し、新たな規制の枠組みが実務上どのように実施できるかを協働で検討しました。

日本はAIガバナンスへのアプローチにおいて重要な岐路に立っています。2025年5月のAI推進法の制定によりAI政策の戦略的方向性が確立され、一方で進行中の個人情報保護法（APPI）の3年ごとの見直しは、急速な技術変化を踏まえてデータ保護規則を現代化する機会を提供しています。特にG7広島AIプロセスを通じた国際的なAIガバナンスのリーダーとして、イノベーションと保護のバランスをとる日本のアプローチは、アジア太平洋地域およびその他の地域において大きな影響力を有しています。

Open Loop Japanは、この規制上の重要な時期に本プログラムの確立された「政策プロトタイピング」手法を適用し、企業が自社のAIシステムおよびデータ慣行において新たなガバナンス要件をどのように運用できるかを検証することで、政策意図と実務上の実施との間のギャップを埋めています。

i.ii パートナー

本プログラムは以下のパートナーシップを通じて実施されました：

Meta

プログラム主催者

MetaのOpen Loopイニシアチブは、本プログラムのグローバルインフラ、手法、および招集プラットフォームを提供しました。

FUTURE OF PRIVACY FORUM

主任調査パートナー

FPFは、本プログラムの調査設計、データ収集、専門家グループのファシリテーション、および最終報告書の起草を主導しました。

accenture

現地デリバリーパートナー

Accentureは、参加企業の募集、リサーチプランの策定、アンケート調査、東京でのイベント運営、および翻訳を支援しました。

i.iii 参加企業（コホート）

参加者の選定方法

Open Loop Japanは、日本においてAIシステムの開発、導入、または利用を行う企業を募集しました。参加者は、Meta、Future of Privacy Forum、およびAccentureのネットワーク、ならびに本プロジェクトの専門家グループのメンバーを通じて選定されました。選定基準は以下のとおりです。

- **日本における事業活動：**各参加者は、日本企業として、または国際企業グループの日本での事業拠点として、日本法の適用を受けるAI関連活動を日本国内で行っています。
- **調査対象となる論点に関する直接的な経験：**各参加者は、APPI、AI推進法、および／または自主的なAIガイダンスを、抽象的な検討としてではなく、実際のAI関連活動に適用しています。

私たちは、業種、組織規模、およびAIバリューチェーンにおける位置づけの多様性を考慮して募集を行いました。統計的な代表性を目的とした募集は行っておらず、本調査の参加者群は日本産業界の標本として解釈されるべきではありません。

参加者群

16社が、AIの利用方法、関連する個人情報、活動の段階、ガバナンス体制、参照する枠組み、直面する不確実性、およびその不確実性が意思決定に与える影響に関する25問の日英バイリンガルアンケートに回答しました。そのうち8組織は、フォローアップインタビューにも参加しました。調査およびインタビューの詳細については、下記の**調査方法**をご参照ください。

各参加者は、AIガバナンス、プライバシー、法務、またはデジタルトランスフォーメーションを担当し、組織全体を代表して回答できる回答者を指名しました。

帰属表示

調査結果は集計形式で報告されます。本報告書では、いかなる発言、数値、または見解も特定の組織名や個人名に帰属させておらず、また個々の参加者が特定され得るような業種の記述も使用していません。

i.iv 調査方法

調査アプローチ

本調査は、構造化アンケート、半構造化インタビュー、専門家からの書面による情報提供、および関連する日本の法令・ガイダンスの分析を組み合わせた混合研究法を採用しています。

データ収集

アンケート調査：アンケートは、2026年6月18日から8月25日の間に、日本語と英語でオンライン形式により実施されました。各参加者は、組織を代表して回答するよう指名された担当者が1件の回答を提出しました。

アンケートは25問で構成され、AIバリューチェーンにおける組織の役割、取り扱う個人情報とそのAI関連活動における段階、ガバナンス体制、参照する枠組み、直面する不確実性、その不確実性が意思決定に与える影響、および優先すべき政策変更について調査しました。設問形式は、単一選択、複数選択、順位付け、およびリッカート尺度と自由記述欄を組み合わせたものでした。

- **複数選択式設問**
  ほとんどの設問において参加者は複数の選択肢を選ぶことができたため、これらの設問で報告される数値の合計は100%を超えます。
- **ウェアラブル技術に関するフィルター設問**
  参加者は、日本市場向けに先進的なウェアラブルデバイスを開発または導入しているかどうかを尋ねられました。この設問は、その後のウェアラブル関連の設問ブロックへの回答対象者を絞り込むものでした。フィルター設問に肯定的に回答した参加者は1組織のみであったため、その後の設問に回答したのはその参加者のみでした。したがって、知見5の根拠は、アンケート回答よりも、主にインタビュー、専門家からの情報提供（後述）、および法的分析に基づいています。**§3.4**では、これが今後の研究に与え得る影響について論じています。

インタビュー：2026年8月から9月にかけて、参加組織8社に対して半構造化インタビューを実施しました。インタビューはビデオ会議形式で約60分間行われ、日本語で実施し、通訳および文字起こしの支援を受けました。

インタビューで提示された質問は、各参加者のアンケート回答に基づいてカスタマイズされました。インタビューは3つの目的を追求しました：アンケート回答の背景にある理由を明らかにすること、暫定的な知見を参加者自身の経験に照らして検証すること、そして参加者がアンケート回答で提起した疑問や課題の解決に資する日本の政策変更（もしあれば）について尋ねることです。

2026年7月17日のAPPI改正法案公布後に実施されたインタビューでは、改正に関する参加者の事前の期待を改めて確認することも可能となりました。

専門家グループ：本調査は、20名で構成される専門家グループの支援を受けました。同グループは、学界、産業界、法曹界、および非政府組織から選出された、日本およびアジア太平洋地域の技術ガバナンスと規制に関する専門家で構成されています。

専門家グループは、プロジェクト期間中に3回のオンライン会合を開催しました。すべての専門家がすべての会合に出席したわけではありません。会合では、Open Loopチームが研究の方向性および予備的な調査結果に関する情報を共有し、専門家は提示された情報について質問し、コメントを述べました。数名の専門家からは追加の書面によるフィードバックが提供されました。本報告書に記載のとおり、Open Loopチームは、知見5で提起されたウェアラブル技術およびAPPIの新カテゴリーである特定生体個人情報に関する問題について、数名の専門家にさらなる書面での意見提供を依頼し、4名の専門家から回答がありました。

本報告書に記載された見解は、必ずしも専門家の見解を反映するものではありません。

分析の枠組み

調査への回答：参加者16社からの回答を分析しました。パーセンテージは、参加者が特定の質問に回答しなかった場合も含め、全体を通じて16を分母として最も近い整数で報告しています。参加者に対し、自社のAI事業に最も有益な政策変更を順位付けするよう求めた質問については、上位の順位により大きな重みを与える加重順位付けを適用しました。これにより、少数の参加者が1位に選んだ選択肢が、多数の参加者が最下位に選んだ選択肢によって順位を下げられることがないようにしています。§2.0では、本章が「順位付けされた政策要望」と枠組みの優先順位に関する別の質問との間に設けた区別について説明しています。

インタビュー資料：調査から浮かび上がったテーマおよび検討対象の枠組みに基づいて、インタビューの書き起こしをコード化しました。インタビューにおいて調査が想定していなかったテーマが提起された場合は、調査データに立ち返り、そのテーマがどの程度広く当てはまるかを検証しました。参加者の説明が調査データと矛盾する場合は、解決を試みるのではなく、その矛盾を報告しています。

専門家の意見：専門家からの書面による回答は、日本法における未解決の問題に対する専門家の見解として扱い、コンセンサスとしては扱っていません。専門家間で意見が分かれた場合、本報告書はその相違を記録しています。専門家が一次資料を指摘した場合は、その資料に基づいて検討を行いました。**§2.5**における特定生体個人情報を定義する基準に関する議論は、2026年7月17日および8月26日に個人情報保護委員会が公表した資料に基づいています。

法的分析：改正後のAPPI、AI推進法、AI事業者ガイドライン（バージョン1.2）、および関連する個人情報保護委員会のガイドライン、Q&A、公表資料を分析しました。義務の内容が政令、委員会規則、またはガイドラインの制定を待っている場合は、その旨を明示しています。

対象範囲：プロジェクトの焦点に沿って、本分析はAPPI、AI推進法、および日本の任意のAIガバナンス枠組みが交差する領域、ならびにその交差領域がAIシステムおよびウェアラブル技術にどのように関係するかを扱っています。参加者から提起された事項のうち、この交差領域の範囲外のものは、知見として扱っていません。

i.v 制約事項

本報告書は有益な知見を提供していますが、その調査結果は一定の方法論上の制約の範囲内で解釈される必要があります。

サンプルサイズと代表性

本調査は16社からの回答を反映しており、方向性を示す知見は得られるものの、一般化には限界があります。有意抽出法は、AIバリューチェーンにおけるセクターおよび役割の多様性を確保することを目的としていましたが、結果が日本のAIエコシステム全体を代表するものではない可能性があります。

自己申告データ

すべての調査結果は、自己申告によるアンケートおよびインタビュー回答に基づいています。これらは、独立して検証されたデータではなく、参加者が申告した実務および認識を反映したものです。

横断的調査設計

本調査は、特定の時点（2026年半ば）における組織の実務および認識を捉えたものです。AIガバナンスおよびコンプライアンスの状況は変化するため、調査結果の一部は変わる可能性があります。

組織規模別の分類なし

本報告書では、組織規模（スタートアップ、中小企業、大企業など）による回答の区分を行っていません。これにより、コンプライアンス成熟度やリソース制約における差異が回答に影響を与えている可能性が見えにくくなっている場合があります。複数の参加者がリソース制約について直接言及しており、**§2.2**ではそれらの報告を記載していますが、本調査では、コホートの回答が組織規模とどの程度相関しているかを検証することはできません。

社会的望ましさバイアスの可能性

本テーマの規制上の機微性を考慮すると、一部の回答は評判やコンプライアンス関連の考慮に影響されている可能性があります。なお、複数の参加者が自社の事業に影響を与える未解決の問題について率直に語っており、この影響がコホート全体に均一に及んでいたわけではないことが示唆されます。

先進的ウェアラブルデバイスに関するコホートの経験の限定性

日本市場向けに先進的ウェアラブルデバイスを開発または展開している参加者は1社のみでした。そのため、ウェアラブルデバイスに特化した調査項目からは十分なデータが得られず、知見5の分析はインタビュー、専門家グループメンバーからの書面による意見、および法的文書自体に基づいています。**§3.4**では、この分野における今後の研究への示唆を示しています。

翻訳

アンケートは日本語と英語で実施され、インタビューは通訳および文字起こしの支援を受けて日本語で実施されました。分析は英語で行われました。参加者の表現に技術的または法的な区別が含まれる場合は、日本語の用語に基づいて作業を行い、その区別が重要な箇所では本文中に日本語を記載しています。

下位法令が未確定

改正APPIがAIおよびウェアラブル技術を扱う組織に求める事項の多くは、本報告書執筆時点で確定していなかった政令、委員会規則、およびガイドラインに委ねられています。本報告書では、これらの法令が解決する論点およびそれに関連する考慮事項を特定していますが、それらがどのように解決されるかを述べることはできません。

II. 主要概念と定義

エージェント型AI
人間の介入を最小限に抑えながら、特定の目標を達成するために自律的な計画、意思決定、および行動を行う能力を持つ人工知能（AI）システムです。

集計
個人レベルのデータを、より広範な統計形式（合計、平均、範囲など）に編集・要約し、特定の個人に関する情報を分離または識別できないようにする処理です。

匿名化／匿名加工情報（Anonymously processed information）
特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であって、当該個人情報を復元することができないようにしたものです。（参照：個人情報の保護に関する法律（個人情報保護法）第2条第6項）。

生体力学データ
人体の力学に関するデータ（関節角度、筋力、動作パターンなど）であり、多くの場合、ウェアラブルデバイスやセンサーを通じて、複雑な物理的測定値の連続的なストリームとして収集されます。

生体データ
個人の身体的、生理的、または行動的特徴に関する特定の技術的処理から得られるデータであり、当該個人を一意に識別することを可能にするものです。APPIにおいては、これは「個人識別符号」（Individual Identification Code）のカテゴリーに該当し、コンピュータによる認識のために身体的特徴から変換されたデータ（顔認識データ、指紋など）を含みます。（参照：APPI第2条および関連政令）。

生体推論
AIアルゴリズムを使用して身体的、生理的、または行動的データ（声のピッチ、表情、眼球運動など）を分析し、個人を識別するのではなく、二次的な状態や特性（感情状態、ストレスレベル、健康状態など）を推論する手法です。

周囲の非利用者のプライバシー
機器の主要なユーザーではないものの、公共空間や共有空間において、機器の外向きセンサー（カメラ、マイクなど）によって個人情報（顔、声、歩行パターンなど）が偶発的に捕捉される可能性のある個人に関するプライバシー上の考慮事項です。

仮名化／仮名加工情報（Pseudonymously processed information）
他の情報と照合しない限り特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報です。

（参照：個人情報保護法第2条第5項）

要配慮個人情報
（Sensitive Personal Information）

本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実、その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報。

（参照：APPI 第2条）

特定生体個人情報
（Specific Biometric Personal Information）

特定生体個人識別符号を含む個人情報です。この符号には、身体の一部の特徴に関する情報で、特別の技術や多額の費用を要しない方法で取得でき、かつ本人がその取得を容易に認識できないものを変換して得られる符号が含まれます。

（参照：2026年改正個人情報保護法 第16条第5項

ウェアラブルデバイス（Wearables）

ユーザーの身体に装着するか、衣類に組み込むことを目的として設計された電子機器（例：スマートグラス、AR/VRヘッドセット、スマートウォッチ、健康トラッカー）。これらのデバイスには、高度なセンサー（カメラ、マイク、加速度計など）およびエッジコンピューティング機能が搭載されていることが多く、利用者に固有の身体由来データと周囲の環境データの両方を継続的に収集・処理することが可能です。

III. 注釈

[本文中で参照される番号付き注釈]

IV. 参考文献

[学術形式の参考文献一覧]