8-09. データ利活用プロジェクトの法的論点整理（DPIA/PIA含む）

対応モデル：GPT-5.1 / Claude 4.5 Sonnet / Gemini 3

難易度・リスク：★★★★（高難易度・高リスク - 必ず法務専門家・プライバシー専門家による総合的なレビュー必須）

推定時間短縮：2 時間〜5 時間（プロジェクト規模により変動）

🎯 1. 目的

データ利活用プロジェクト（AI 活用、ビッグデータ分析、顔認証、IoT 等）における個人情報保護法上の法的論点を包括的に整理し、プライバシー影響評価（PIA）・データ保護影響評価（DPIA）を含む必要な対応策を明確化します。

2025 年の個人情報保護法改正動向（3 年ごと見直し）を踏まえ、国際的なプライバシーガバナンス基準（GDPR、ISO/IEC 29134:2023、JIS X 9251:2021）に準拠した実務的なリスク評価・対策立案を支援します。

図 1: PIA（プライバシー影響評価）実施フローチャート

2. プロンプト本体（コピペ用）

💼 プロンプト本体（このボックスをコピーして使用）

あなたはデータ利活用・プライバシー保護の専門家です。日本の個人情報保護法、GDPR、各業法を踏まえて、実務で即利用可能な形で出力してください。

【入力情報】

• プロジェクト概要：[例：顧客行動分析 AI、顔認証入退室管理、IoT センサーによる健康管理等]

• 取り扱うデータ種別：[例：氏名、顔画像、位置情報、購買履歴、健康情報等]

• データソース：[例：自社収集、第三者提供、公開データ、IoT センサー等]

• 利活用目的：[例：マーケティング分析、サービス改善、新規事業開発、学術研究等]

• 処理方法：[例：AI 機械学習、統計分析、プロファイリング、自動決定等]

• データ共有先：[例：グループ会社、業務委託先、共同研究機関、海外拠点等]

• 対象者規模：[例：1 万人、10 万人、100 万人以上等]

• 業種・分野：[例：金融、医療、小売、製造、公共等]

[不明な項目は「不明」と記載してください]

【処理手順】

1) 法的基盤の確認（個人情報該当性、要配慮個人情報、仮名・匿名加工情報の検討）

2) 取得・利用の適法性評価（利用目的、同意取得、通知公表の要否）

3) プライバシー影響評価（PIA/DPIA）の実施判断と評価項目の特定

4) データガバナンス体制の評価（責任者設置、管理体制、監査体制）

5) 安全管理措置の検証（組織的・人的・物理的・技術的措置）

6) 第三者提供・委託・共同利用スキームの法的整理

7) 越境データ移転の適法性確認（十分性認定、基準適合体制）

8) 個人の権利対応体制の構築（開示、訂正、削除、利用停止）

9) インシデント対応計画の策定（漏えい時の報告・通知体制）

10) リスク評価と対策優先順位の決定

【出力形式】

• エグゼクティブサマリー：プロジェクトの法的リスク評価結果の要約

• 法的論点整理表：個人情報保護法の各要件に対する適合性評価

• PIA/DPIA 評価結果：プライバシーリスクの影響度×発生可能性マトリクス

• データフロー図：個人データの収集→保管→利用→提供→廃棄の流れ

• リスク対策計画：優先順位付けした対策項目と実施スケジュール

• 必要文書リスト：プライバシーポリシー、同意書、契約書等の整備項目

• コンプライアンスチェックリスト：法令要件の充足状況一覧

【重点観点】

以下の点を必ず検討してください：

• プロファイリング・自動決定を行う場合の GDPR 型規制への対応

• 顔認証・生体情報を扱う場合の要配慮個人情報としての取扱い

• AI の学習データとしての利用における著作権・肖像権の整理

• 公益目的でのデータ利活用における例外規定の適用可能性

• 仮名加工情報・匿名加工情報への加工による規制緩和の検討

• データマッピングによる個人データの可視化と管理

• 個人情報保護法の 3 年ごと見直し（2025 年）への対応準備

• 業界特有の規制（金融：FISC、医療：次世代医療基盤法等）

• ISO/IEC 29134:2023、JIS X 9251:2021 準拠の PIA 実施

【チェックリスト】

出力前に以下を確認してください：

☐ 実名・機微情報は含めていないか

☐ 条文根拠（個人情報保護法、GDPR 等）は明示されているか

☐ PIA/DPIA の実施要否判断は適切か

☐ リスク評価は定量的・客観的か

☐ 対策の優先順位は明確か

☐ 業界特有の規制は考慮されているか

☐ 国際標準（ISO/JIS）への準拠は確認されているか

【注意事項】

• 本出力は法的判断の代行ではなく、検討材料の提供です

• 必ず人が検証し、組織の承認フローに従ってください

• 高リスクプロジェクトは弁護士・プライバシー専門家への相談を推奨

• PIA/DPIA は継続的な見直しが必要です

3. 入力例

• プロジェクト概要：小売店舗における顔認証を活用した来店客の行動分析システム

• 取り扱うデータ種別：顔画像、性別・年代推定情報、店内動線、滞在時間、購買履歴

• データソース：店舗内カメラ（50 台）、POS システム、会員カード情報

• 利活用目的：店舗レイアウト最適化、マーケティング施策立案、防犯対策

• 処理方法：AI 顔認証エンジンによる属性推定、動線分析、購買行動予測モデル構築

• データ共有先：システム開発ベンダー（国内）、クラウドサービス（AWS 東京リージョン）

• 対象者規模：月間来店客約 10 万人（全国 50 店舗）

• 業種・分野：小売業（アパレル）

4. 出力例

【データ利活用プロジェクト法的論点整理】

■ エグゼクティブサマリー

リスクレベル：高（要配慮個人情報＋大規模処理＋プロファイリング）

PIA 実施：必須（JIS X 9251:2021 準拠の詳細評価が必要）

主要課題：顔画像の要配慮個人情報該当性、本人同意取得の実務的困難性

■ 法的論点整理（抜粋）

1. 顔認証データ：要配慮個人情報として原則本人同意が必要

2. カメラ告知：店舗入口での明確な掲示義務（個人情報保護法 21 条）

3. 統計情報化：個人識別性を完全に排除すれば規制対象外

■ リスク対策優先順位

【緊急】顔画像を即座に特徴量変換し、元画像は破棄する仕組みの実装

【重要】オプトアウト手段の提供（顔認証を望まない来店客への対応）

【推奨】プライバシーバイデザインに基づくシステム設計見直し

**※本分析は法的助言ではありません。最終判断は、弁護士・プライバシー専門家にご相談くださ*

い。*

🔧 5. カスタマイズのポイント

自社向けに調整する場合

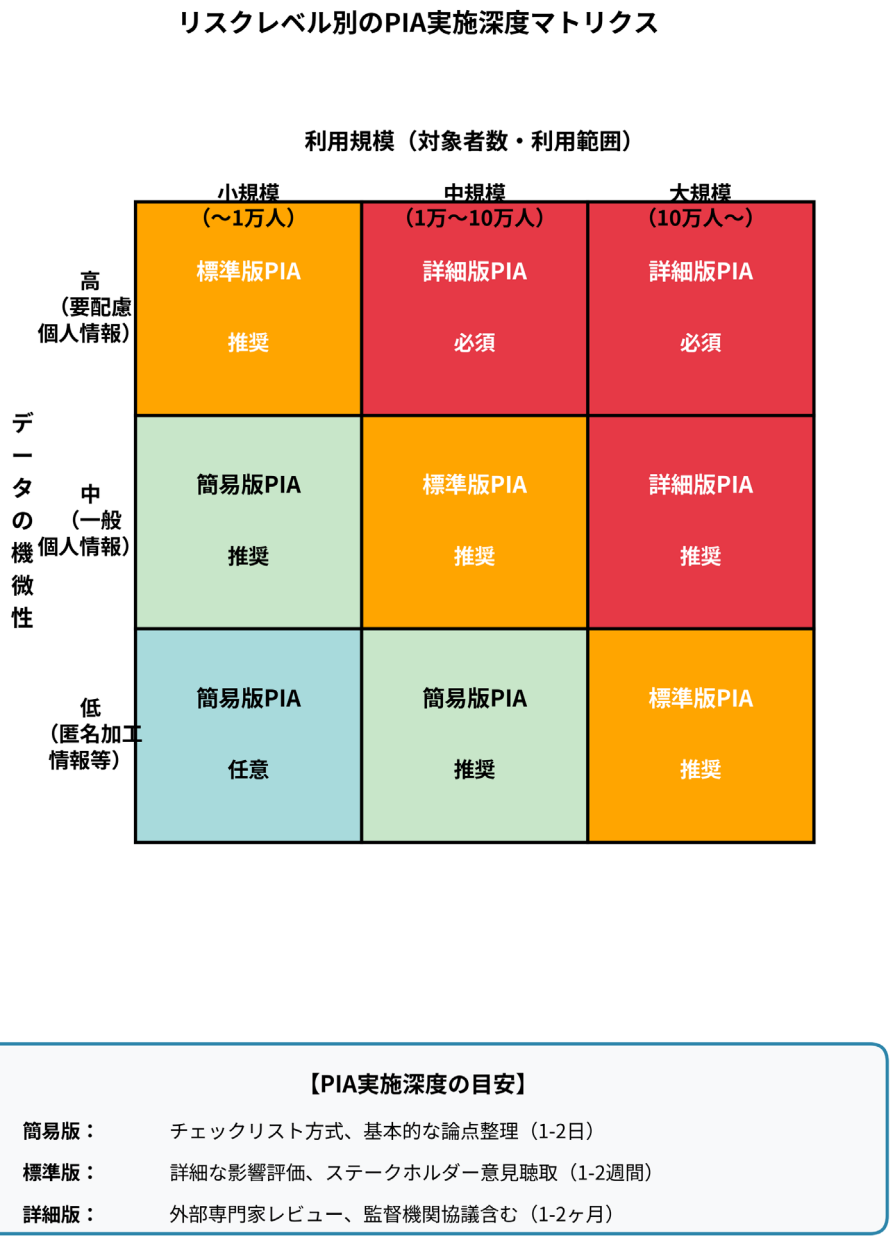

図 3: リスクレベル別の PIA 実施深度マトリクス

- データ利活用の成熟度に応じて、PIA 実施の深度を調整（簡易版／標準版／詳細版）

• 業界ガイドライン（認定個人情報保護団体の指針等）を参照基準に追加

• 自社のプライバシーガバナンス体制（CPO、プライバシー委員会等）に合わせた承認フロー設計

業種別の注意点

業種	特記事項
金融・保険	FISC 安全対策基準、信用情報機関との連携、マネロン対策での個人データ活用。AI による与信判断は説明責任が重要。
医療・ヘルスケア	次世代医療基盤法の活用検討、医学研究倫理指針への準拠、医療 AI 開発での学習データ利用の同意取得。
小売・EC	購買履歴・行動履歴の分析における透明性確保、レコメンドエンジンでのプロファイリング規制対応、カメラ画像利用の告知。
製造・IoT	産業 IoT での従業員モニタリング、労働安全衛生法との調整、スマートファクトリーでのデータ共有スキーム構築。

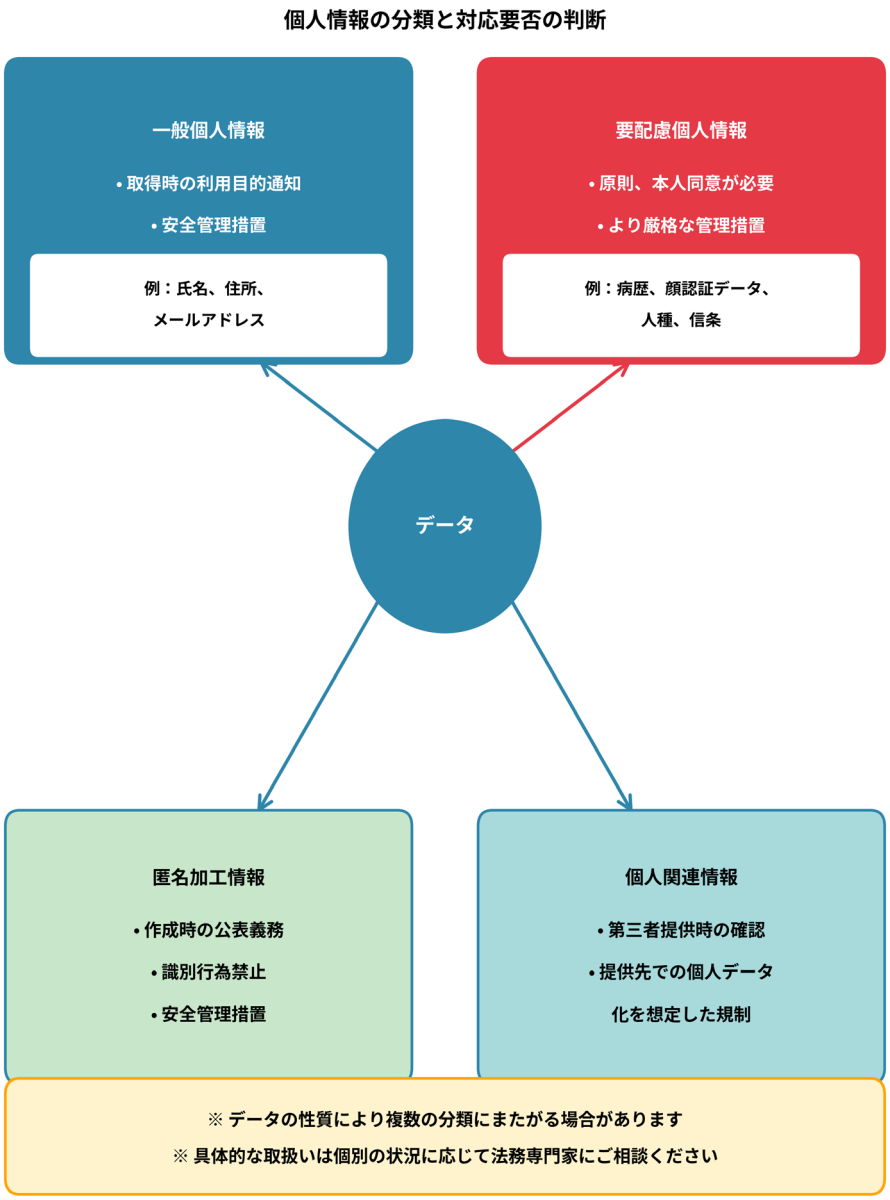

図 2: 個人情報の分類と対応要否の判断

❓ 6. よくある質問

Q1: PIA（プライバシー影響評価）は法的義務ですか？

A: 日本の個人情報保護法では現時点（2025 年）で民間企業への義務化はされていませんが、個人情報保護委員会が推奨しており、3 年ごと見直しで検討対象となっています。

ただし、GDPR では高リスク処理について DPIA 実施が義務化されており、グローバル企業では事実上必須となっています。

Q2: 匿名加工情報にすれば、PIA 不要で自由にデータ利活用できますか？

A: 匿名加工情報は個人情報保護法の多くの規制が緩和されますが、完全に自由ではありません。

作成時の公表義務、識別行為禁止、安全管理措置等の義務は残ります。また、プライバシー侵害リスクは残るため、PIA 実施が推奨されます。

Q3: 顔認証システムは必ず要配慮個人情報になりますか？

A: 顔認証データ（生体情報）は原則として要配慮個人情報に該当します（個人情報保護法 2 条 3 項、令 2 条 2 号）。

ただし、防犯カメラで本人特定せずに属性推定のみ行う場合等、個人識別性がない処理であれば個人情報に該当しない可能性があります。具体的な実装方法により判断が分かれるため、専門家相談を推奨します。

🔗 7. 関連プロンプト

このプロンプトと併せて使うと効果的：

• 8-06. 個人情報の越境移転適法性チェック - クラウド利用・海外データセンター活用時の検討

• 8-03/8-04. 利用規約の作成 - プライバシーポリシーへの PIA 結果反映

• 2-06. コンプライアンスプログラム作成 - データガバナンス体制の構築

• 1-02. 業務委託契約書作成支援 - データ処理委託における責任分界の明確化

⚠ 8. 重要な注意事項

🚨 必ずお読みください

【法的位置づけ】

• AI 出力は「分析の材料」「検討の視点」を提供するものです

• AI 出力をそのまま法的判断として使用しないでください

• データ利活用プロジェクトは複雑な法的論点を含むため、必ず弁護士・プライバシー専門家による最終確認が必要です

• 最終的な法的判断・リスク判断は、必ず人（法務責任者・専門家）が行ってください

【情報セキュリティ】

• 機密情報・個人情報は匿名化・マスキングを前提に入力してください

• 実名、具体的な技術仕様、固有名詞は伏せ字または架空の例に置き換えてください

• プロジェクトの詳細情報を入力する場合は、AI への入力自体が情報漏洩にならないか確認してください

• 各 AI のセキュリティ設定と利用規約を必ず確認してください

【PIA/DPIA 実施の留意点】

• PIA は一回限りの評価ではなく、継続的な見直しが必要です（PDCA サイクル）

• リスク評価は主観的になりやすいため、複数の視点での検証を推奨します

• 国際標準（ISO/IEC 29134:2023）は定期的に更新されるため、最新版の確認が必要です

• 消費者・利用者の視点を含めたマルチステークホルダーでの評価を検討してください

【弁護士法第 72 条との関係】

本プロンプトは「法律事務の代行」を行うものではありません。データ利活用の適法性判断、リスク評価は専門的法律事務に該当する可能性があるため、最終的な判断・意思決定は、必ず人（適切な権限を持つ者・専門家）が行います。

【技術進化への対応】

• AI 技術・データ分析手法は急速に進化しており、新たな法的論点が随時発生します

• 生成 AI、合成データ、連合学習等の新技術には既存の法的枠組みが追いついていない場合があります

• 個人情報保護委員会のガイドライン、Q&A 等の最新情報を定期的に確認してください

• グローバルなデータ規制動向（EU AI Act、米国州法等）にも注意が必要です