8-07. 生成 AI 調達時のベンダーDD チェックリスト

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

難易度・リスク：★★★（高リスク：法的リスク・データプライバシー・セキュリティの専門的評価が必要）

推定時間短縮：2 時間〜4 時間（チェックリスト作成・初期評価を大幅に効率化）

🎯 目的

生成 AI サービス導入時のベンダー選定において、技術的・法的・セキュリティの観点から包括的にチェックすべき項目を整理し、リスクを最小化しながら最適なベンダーを選定するためのデューデリジェンスチェックリストを作成します。

図 1: ベンダーDD 実施の全体フロー

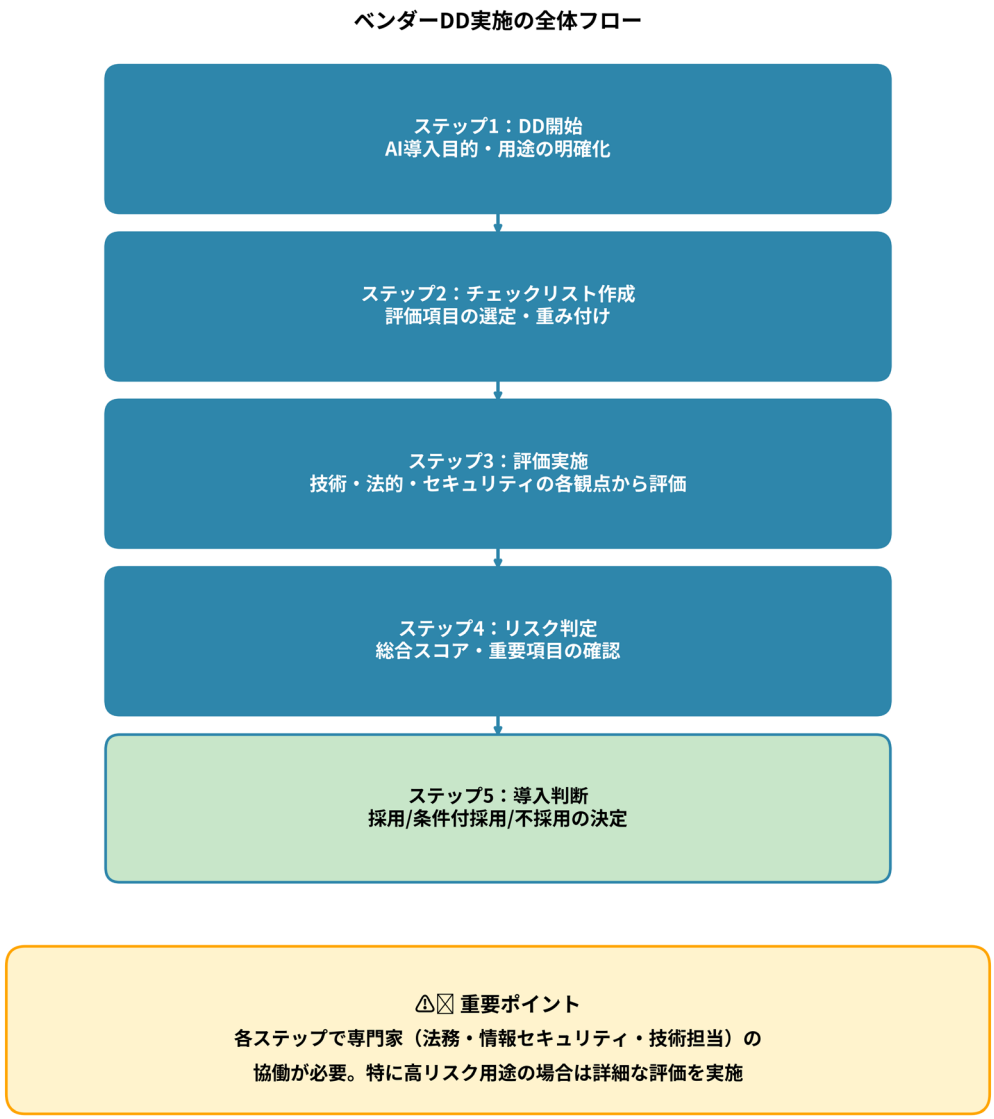
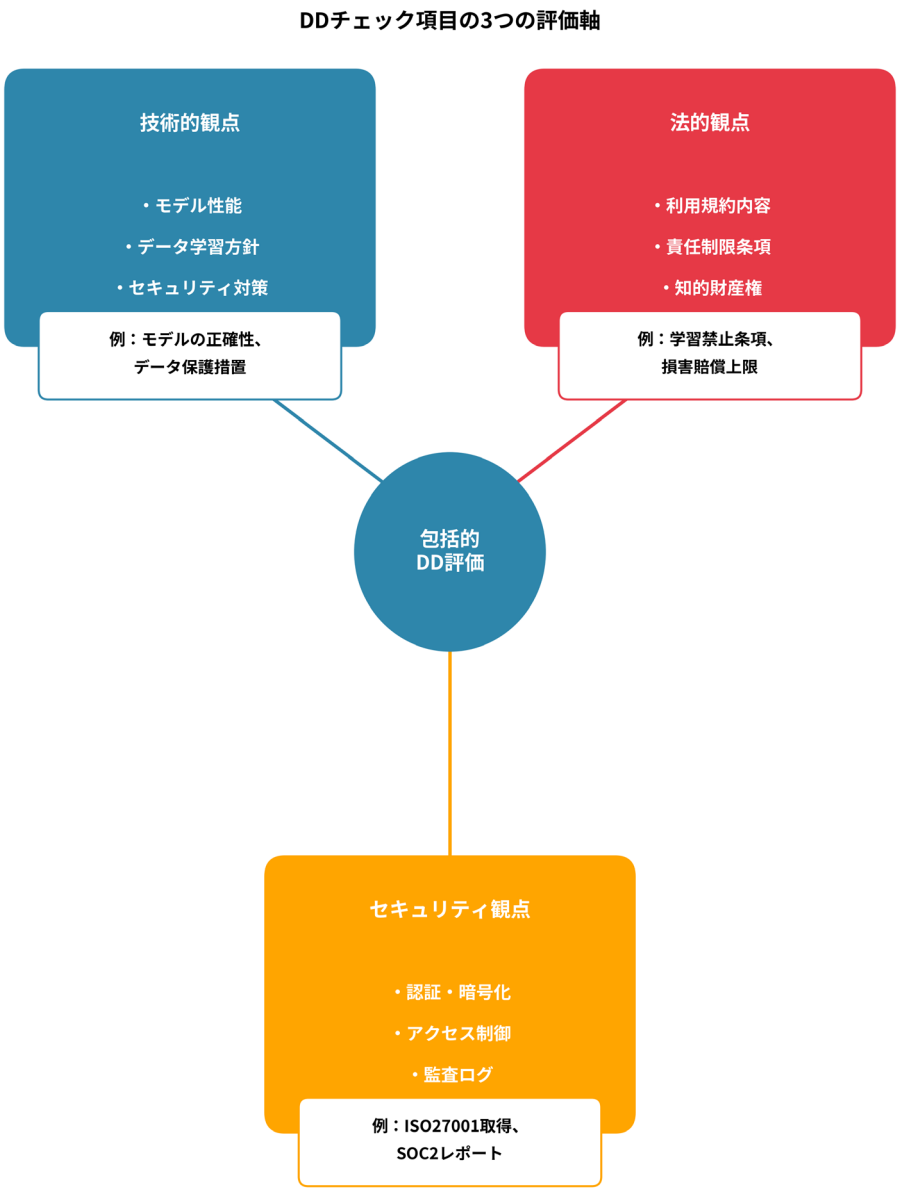


図 2: DD チェック項目の 3 つの評価軸



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）

あなたは生成 AI 導入・調達の専門知識を持つ企業法務担当者です。日本法（個人情報保護法、AI 事業者ガイドライン等）に基づき、実務で即利用可能な形で出力してください。

【入力情報】

- 導入予定の AI サービスの種類：[例：ChatGPT Enterprise / Claude for Work / Gemini Advanced / 自社開発 AI 基盤]
- 主な用途：[例：契約書レビュー / カスタマーサポート / マーケティングコンテンツ生成 / 社内業務効率化]
- 想定入力データの機密レベル：[例：公開情報のみ / 社外秘 / 個人情報含む / 機密情報含む]
- 利用部門：[例：法務部 / カスタマーサポート / 全社展開]
- 予算規模：[例：年間 500 万円 / 月額 50 万円]

[不明な項目は「不明」または「調査中」と記載してください]

【処理手順】

1) 入力情報から、特に重要なリスク領域を特定

2) 以下の 8 カテゴリについて、具体的なチェック項目をリスト化

- データプライバシー・個人情報保護
- セキュリティ・インシデント対応
- AI 倫理・透明性・説明可能性
- 知的財産権・著作権
- サービス継続性・SLA
- ベンダーの信頼性・財務健全性
- 契約条件・責任範囲
- コンプライアンス・法規制対応

3) 各チェック項目について、確認方法と評価基準を明示

4) 高リスク項目を特定し、優先的に確認すべき事項を強調

【出力形式】

■ デューデリジェンス実施方針（1 パラグラフで要約）

■ カテゴリ別チェックリスト（表形式）

- カテゴリ名
- チェック項目（具体的な確認事項）
- 確認方法（ベンダーへの質問／資料請求／デモ確認 等）
- 重要度（高／中／低）

- 評価基準（合格ライン）

■ 高リスク項目（特に重点的に確認すべき項目）

■ ベンダーへの確認質問リスト（5-10 項目）

【重点観点】

以下の点を必ず検討してください：

- 個人情報保護委員会「AI 事業者ガイドライン」（2024 年 4 月公表）への準拠状況
- 学習データに自社データが使用されないことの契約上の保証
- データの越境移転の有無と安全管理措置（GDPR・個人情報保護法 27 条対応）
- AI 出力の著作権・知的財産権の帰属先
- ハルシネーション（誤情報生成）のリスクと免責条項の範囲
- セキュリティ認証取得状況（ISO27001、SOC2 Type2 等）
- インシデント発生時の通知義務と対応体制
- サービス終了・事業撤退時のデータ返却・削除プロセス
- AI 倫理原則（公平性・透明性・説明可能性）への取り組み
- 法規制変更時のサービスアップデート対応方針

【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
- ☐ 最新の AI 事業者ガイドライン（2024 年 4 月版）を反映しているか
- ☐ 高リスク項目は明確にマーク済みか
- ☐ データの越境移転リスクを適切に評価しているか
- ☐ 知的財産権の帰属について明確な確認項目があるか

【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
- ● ベンダー選定の最終判断は、技術部門・法務部門・情報セキュリティ部門の合議で行ってください
- ● 高リスク AI システム（EU AI Act 対象等）の場合は、より詳細なデューデリジェンスが必要です

入力例

【入力情報】

- 導入予定の AI サービスの種類：ChatGPT Enterprise（OpenAI 社）
- 主な用途：契約書レビュー、法務相談対応の補助、社内規程のドラフト作成
- 想定入力データの機密レベル：社外秘情報を含む（契約書本文、取引先名、金額等）、個人情報は含まない
- 利用部門：法務部（10 名）
- 予算規模：年間 360 万円（月額 30 万円×12 ヶ月）

出力例

■ デューデリジェンス実施方針

ChatGPT Enterprise の導入に際し、契約書等の機密情報を入力するため、データプライバシー、セキュリティ、知的財産権の 3 領域を最重点項目として評価します。特に、学習データへの利用禁止の契約上の保証、データの越境移転における安全管理措置（米国への送信）、AI 出力の著作権帰属について、OpenAI 社から書面による明確な回答を得ることを必須とします。

■ カテゴリ別チェックリスト

【1. データプライバシー・個人情報保護】

1. 学習データへの利用：入力データが AI モデルの学習に使用されないことが契約で保証されているか【重要度：高】

　確認方法：利用規約・DPA（Data Processing Addendum）の該当条項確認

　評価基準：「学習に使用しない」旨の明文規定があること

2. データの保存場所・越境移転：データがどの国・地域で処理・保存されるか【重要度：高】

　確認方法：ベンダーへの質問票、データセンター所在地の開示

　評価基準：個人情報保護法 27 条の基準（GDPR 十分性認定国または標準契約条項締結）を満たすこと

3. データ削除・返却：契約終了時にデータが確実に削除されるか【重要度：高】

確認方法：契約書の該当条項、削除プロセスの説明資料

評価基準：30 日以内の削除完了、削除証明書の発行があること

【2. セキュリティ・インシデント対応】

4. セキュリティ認証：ISO27001、SOC2 Type2 等の取得状況【重要度：高】

確認方法：認証書のコピー提出要求、有効期限確認

評価基準：ISO27001 または SOC2 Type2 のいずれかを取得済みであること

5. インシデント通知：セキュリティ侵害時の通知義務と期限【重要度：高】

確認方法：契約書・インシデント対応規程の確認

評価基準：48 時間以内の通知義務が明記されていること

6. 脆弱性対応：既知の脆弱性への対応プロセスと実績【重要度：中】

確認方法：過去のセキュリティインシデント開示状況、対応履歴

評価基準：重大脆弱性を 7 日以内に修正する体制があること

【3. AI 倫理・透明性・説明可能性】

7. AI 倫理原則：公平性・透明性・説明可能性への取り組み【重要度：中】

確認方法：AI 倫理ポリシーの開示、バイアス対策の説明

評価基準：成文化された AI 倫理ポリシーがあること

8. ハルシネーション対策：誤情報生成のリスクと対策【重要度：高】

確認方法：技術資料、免責条項の範囲確認

評価基準：ハルシネーションのリスクが明示され、利用者側の検証責任が契約で明確化されていること

【4. 知的財産権・著作権】

9. AI 出力の権利帰属：生成物の著作権・知財権の帰属先【重要度：高】

確認方法：利用規約の該当条項、ベンダーへの質問

評価基準：利用者に権利が帰属する、またはベンダーが権利を主張しない旨の明文規定があること

10. 第三者権利侵害リスク：AI 出力が第三者の著作権等を侵害した場合の責任【重要度：高】

確認方法：利用規約の免責条項、補償条項の確認

評価基準：ベンダーが一定の補償責任を負うか、利用者が最終検証責任を負うことが明確であること

（以下、カテゴリ 5〜8 は紙面の都合により省略）

■ 高リスク項目（特に重点的に確認すべき項目）

1. 学習データへの利用禁止の契約上の保証（最重要）
2. データの越境移転（米国送信）における安全管理措置と GDPR 対応
3. AI 出力の著作権帰属と第三者権利侵害時の責任分担
4. セキュリティインシデント発生時の 48 時間以内通知義務
5. ハルシネーション（誤情報生成）のリスク開示と免責範囲

■ ベンダーへの確認質問リスト

Q1. 弊社が入力したデータ（契約書等）は、OpenAI のモデル学習に一切使用されないことを契約で保証いただけますか？

Q2. データはどの国・地域のデータセンターで処理・保存されますか？日本国内での処理は可能ですか？

Q3. 契約終了時、弊社データはどのように削除されますか？削除完了の証明書は発行されますか？

Q4. セキュリティ侵害（情報漏洩等）が発生した場合、何時間以内に弊社に通知する義務がありますか？

Q5. AI 出力の著作権は弊社に帰属しますか？OpenAI 社が権利を主張することはありますか？

Q6. AI 出力が第三者の著作権を侵害した場合、OpenAI 社は補償責任を負いますか？

Q7. AI が誤った法的助言（ハルシネーション）を生成し、弊社が損害を受けた場合、OpenAI 社の責任範囲はどこまでですか？

Q8. ISO27001 または SOC2 Type2 の認証を取得していますか？認証書のコピーを提供いただけますか？

※実際の AI 出力ではより詳細なチェックリストが生成されます

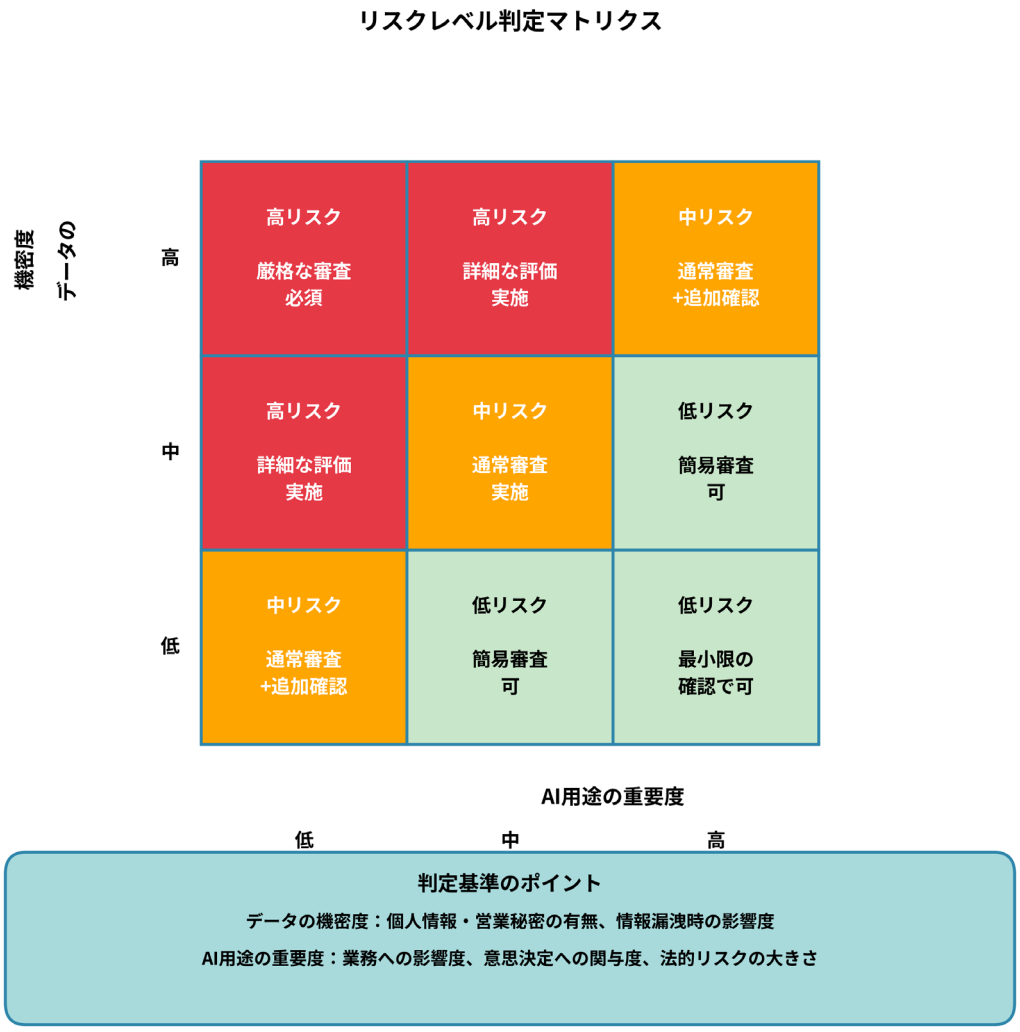
🔧 カスタマイズのポイント

自社向けに調整する場合

- 導入する AI の用途（高リスク業務か低リスク業務か）に応じて、チェック項目の重要度を調整
- 自社の情報セキュリティポリシー・データガバナンス基準に合わせて、評価基準をカスタマイズ
- 海外展開企業の場合は、GDPR・CCPA 等の各国法令への準拠状況も追加確認
- 公共調達・金融機関等の規制業種は、業界ガイドラインへの準拠確認を追加

業種別の注意点

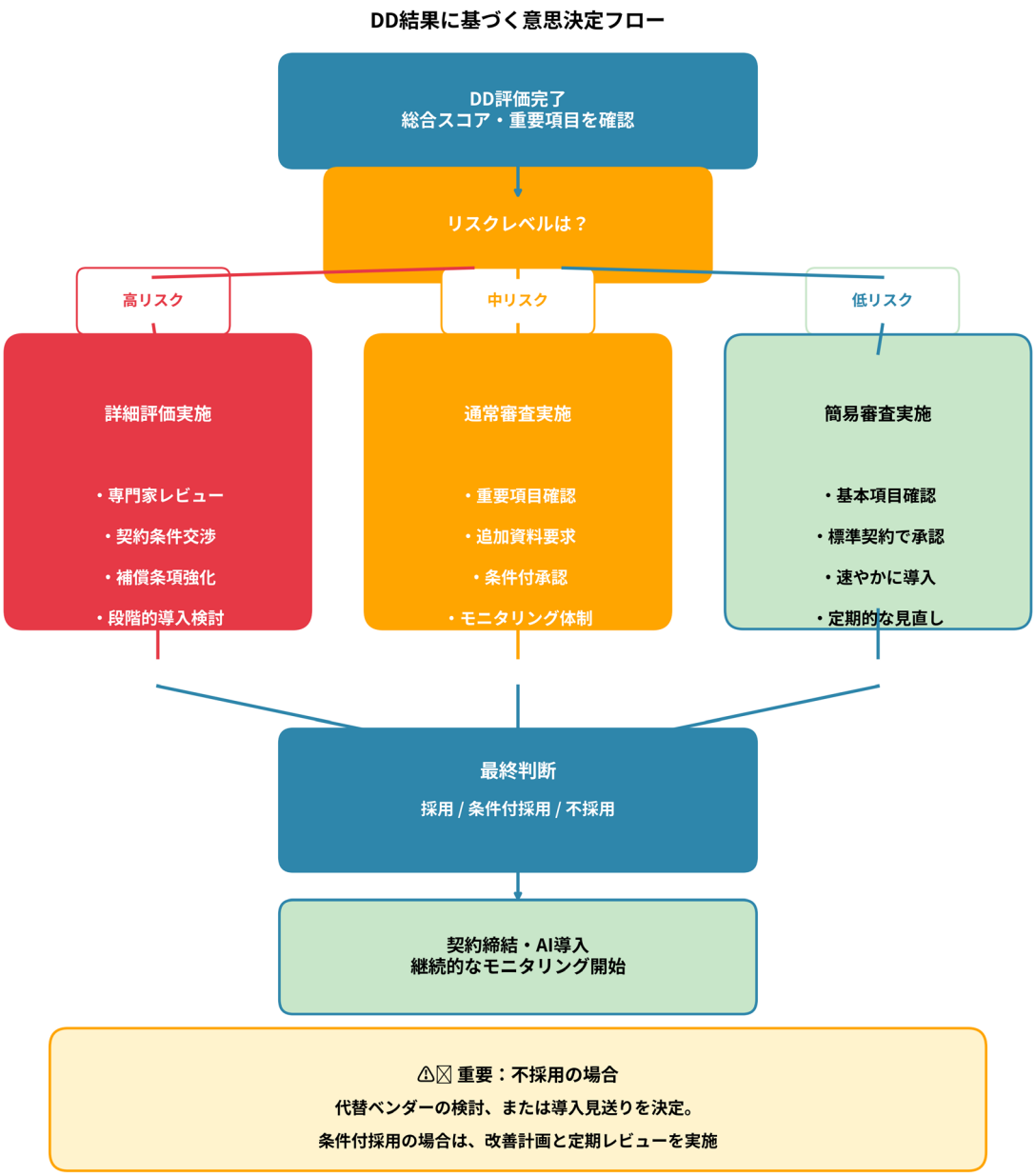
図 3: リスクレベル判定マトリクス



業種	特記事項
金融・保険	金融庁「金融分野における AI 活用ガイドブック」への準拠確

	認、マネロン対策での個人情報利用の適法性、AI 与信判断の説明可能性（貸金業法 13 条の 2）
医療・ヘルスケア	医療機器プログラム該当性（薬機法）、要配慮個人情報の取扱い、医療 AI 開発ガイドラインへの準拠、診断補助 AI の法的責任
製造業	産業 IoT での機密技術情報の保護、設計図・ノウハウの学習利用禁止、AI 不良品検知の精度保証と PL 法責任
IT・ソフトウェア	AI コーディングアシスタント利用時の OSS License 違反リスク、コード生成物の著作権、脆弱性のあるコード生成時の責任

図 4: DD 結果に基づく意思決定フロー



❓ よくある質問

Q1: AI 事業者ガイドラインは法的拘束力がありますか？

A: 個人情報保護委員会「AI 事業者ガイドライン」（2024 年 4 月公表）は法的拘束力のあるガイドラインではありませんが、個人情報保護法の解釈・運用基準として極めて重要です。ガイドラインに従わない場合、個人情報保護法違反として行政指導・命令の対象となる可能性があります。また、民事訴訟で過失認定の判断材料とされるリスクもあります。

Q2: ChatGPT Enterprise なら学習に使われないので安全ですか？

A: ChatGPT Enterprise は入力データをモデル学習に使用しない契約になっていますが、それだけで「完全に安全」とは言えません。データの越境移転（米国送信）、セキュリティ侵害リスク、ハルシネーション、第三者権利侵害等の別のリスクが存在します。包括的なリスク評価が必要です。

Q3: ベンダーDD の結果、リスクが高いと判定された場合はどうすべきですか？

A: 以下の選択肢があります：（1）ベンダーに契約条件の改善を交渉（学習禁止条項の追加、補償条項の強化等）、（2）導入範囲を限定（機密情報を入力しない用途に限る）、（3）代替ベンダーの検討、（4）自社 AI 基盤の構築検討。特に高リスク項目（学習利用、越境移転）は妥協せず、書面での明確な保証を求めることが重要です。

🔗 関連プロンプト

このプロンプトと併せて使うと効果的：

- 8-03/8-04. 利用規約の作成 - AI 導入後の社内利用規約・ガイドライン作成
- 8-06. 個人情報の越境移転適法性チェック - データの海外送信の法的評価
- 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） - AI 導入プロジェクトのプライバシー影響評価
- 1-02. 業務委託契約書作成支援 - ベンダー契約書のドラフト作成
- 6-06. 営業秘密侵害リスクの事前調査 - AI 学習データに営業秘密が含まれるリスク評価

⚠ 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
- ベンダー選定の最終判断は、必ず人（法務担当者・弁護士・情報セキュリティ担当者）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

- ベンダー名、具体的な金額、固有の技術情報は伏せ字または架空の例に置き換えてください
- 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

【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。最終的な法的判断・意思決定は、必ず人（適切な権限を持つ者）が行います。

【ベンダーDD の限界】

- デューデリジェンスは「リスクの発見」であり、「リスクの完全な除去」ではありません
- 高リスク AI システム（EU AI Act 対象等）の場合は、本チェックリストに加え、専門家による詳細な評価が必要です
- ベンダーの回答は書面で受領し、契約条件に反映させることが重要です（口頭説明のみでは不十分）
- AI 技術・法規制は急速に変化しています。定期的な再評価（年 1 回以上）を推奨します