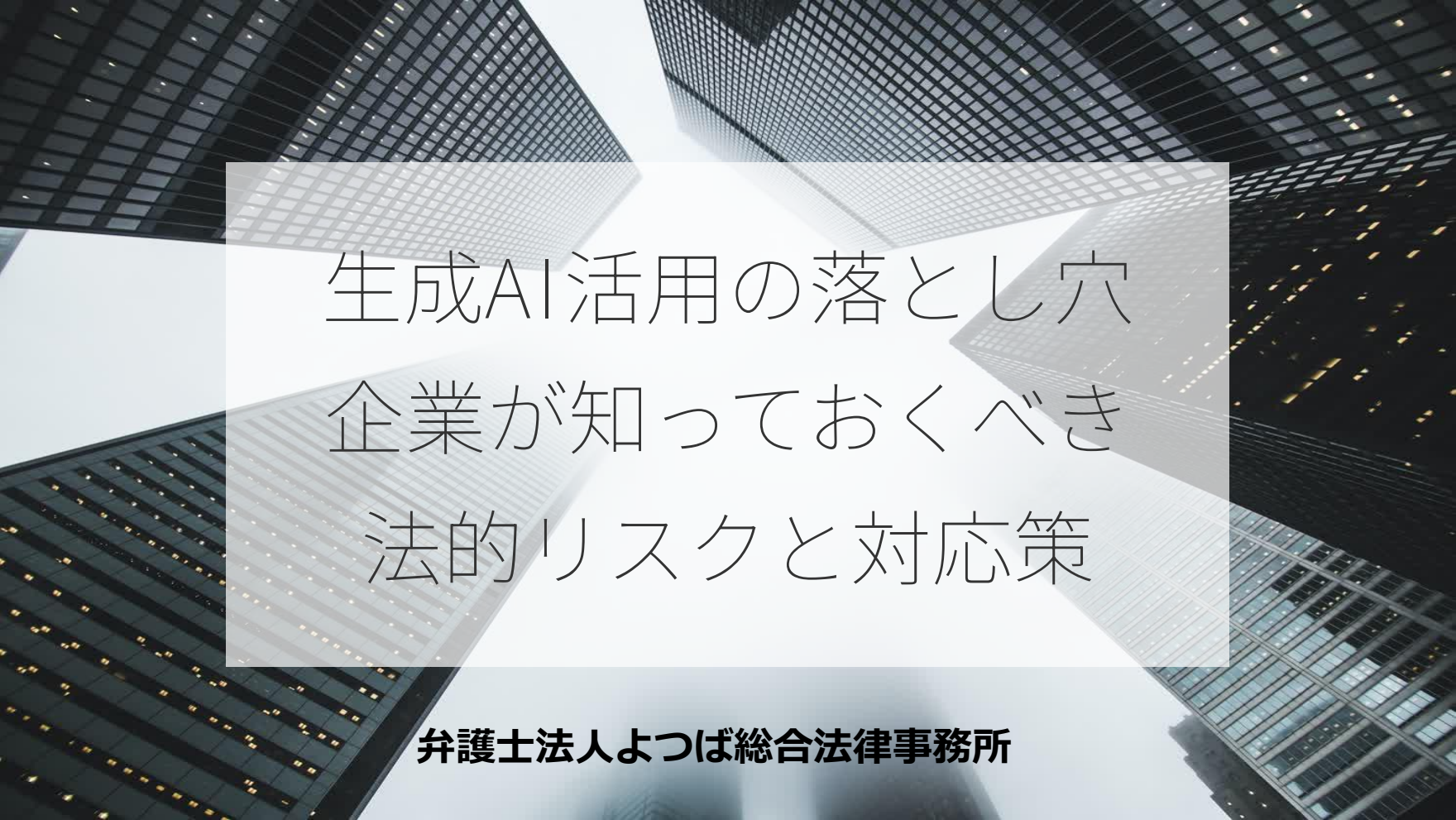

生成AI活用の落とし穴
企業が知っておくべき
法的リスクと対応策

弁護士法人よつば総合法律事務所

本日の構成

本日は4部構成で生成AIの法的リスクを説明します。

- 生成AIの特徴・種類
- 生成AIの留意点（総論）
- 生成AIの留意点（各論）
- 企業が取るべき具体的な対応策

よつば総合法律事務所のご紹介

・弁護士26名、スタッフ26名（2025年4月1日時点）が所属する法律事務所です。

・千葉３拠点（柏・千葉・船橋）、大阪、東京、名古屋の合計6拠点事務所がございます。

・企業法務（人事労務、債権回収、契約書、誹謗中傷の対応等）、交通事故、相続、不動産が中心業務です。

・約**４４０社**の企業様より顧問契約を締結いただいております。

①「できない理由」ではなく「できる方法」を考えること、②顧問会社様へのレスポンスを早くすること、③顧問会社様の経営に有益なご提案を継続することを重視しています。




担当弁護士のご紹介－弁護士 辻　悠祐

大阪弁護士会所属
よつば総合法律事務　大阪事務所所長
ファイナンシャルプランナー（AFP）
宅地建物取引士

京都府京都市市出身
立命館大学法学部卒業
中央大学法科大学院卒業
司法試験合格後、よつば総合法律事務所入所

メールアドレス（お気軽にご連絡ください）
tsuji@yotsubasougou.com

【主な取扱分野】
よつば総合法律事務大阪事務所所長。よつば総合法律事務所企業法務チームで、インターネット上の誹謗中傷の問題の対応、顧問対応、使用者側の労働問題（解雇、残業代、労災、労働審判、訴訟など）などの分野を多く扱っています。
生成AIの法的問題についても積極的に取り組んでいます。

対話型生成AIとは

対話型生成AIは、人間と話しているかのように自然な文章を生成する技術です。単なる一問一答に留まらず、会話の文脈を理解・記憶し、情報検索、要約、翻訳、アイデア出しなど、多岐にわたる作業をサポートする能力を持っています。ChatGPTやGeminiが有名です。

代表的な生成AI①：ChatGPT

ChatGPTは最も有名な対話型AI

ChatGPTの概要	OpenAIが開発したChatGPTは、高度な言語モデルを搭載しており、特にその自然な対話能力で知られています。
多様なプラン	ChatGPTには個人向け（無料版、有料版）と法人向け（Team, Enterprise）のプランがあり、ニーズごとにプランを使い分けることが可能。
成長スピード	GPT-1（2018年）から始まり、2025年4月時点で、GPT-4.5まで登場。年に何度も新しいモデルを発表することも珍しくない。

代表的な生成AI②：Google Gemini

Googleの生成AI-Gemini

Gemini の概要	GeminiはGoogleが提供する対話型の生成AIサービス。Google Workspace製品との連携が強み。
多様なプラン	ChatGPTには個人向け（無料版、有料版）と法人向け（Gemini for Google Workspace）のプランがあり、ニーズごとにプランを使い分けることが可能。
成長スピード	2023年12月にGemini 1.0が発表されて以降、Gemini 1.5（2024年2月発表）、Gemini 2.0（2024年12月発表）、Gemini 2.5（2025年3月発表）と進化を続けています。

代表的な生成AI③：Perplexity

Perplexityは情報収集に特化したAI技術

Perplexityの特徴	Perplexityは、出典を明記した回答を提供することで、信頼性の高い情報収集や調査をサポートするAIです。
AIモデルの選択	自らAIモデルを開発することはなく、他社のモデルを選択して利用するため、最適な情報を提供することができます。
利用シーン	Perplexityは主に情報の正確性を確認する場面や、信頼性のあるデータを引用したい場合に活用できます

生成AI利用における4つのリスク視点

入力情報のリスク

01

プロンプトとして入力する情報には、他人の著作物や個人情報が含まれる場合があり、著作権侵害や個人情報保護法違反に注意が必要です。

出力情報の利用リスク

02

AIが生成する出力には、他者の権利を侵害する可能性があります。既存の著作物と類似した内容を無意識に使用することのリスクを考えましょう。

利用規約違反のリスク

03

利用規約を遵守すること、内容を理解することは重要です。有料版と無料版、個人向けサービスと法人向けサービスで利用規約の内容が異なるケースもあります。

内部統制の違反リスク

04

従業員が個人のアカウントを使用して企業情報の入力を行うことはリスクがあります。社内ルールと社内体制の整備及び周知することが重要です。

利用規約を確認する5つのポイント

利用プランに応じた規約

各プランによって利用規約が異なるため、選択したプランに適した規約を必ず確認する必要があります。

入力データの取り扱い

AIに入力したデータが学習に利用されるか否かを確認することが重要です。

出力データの権利

出力されたデータの権利が誰に帰属するのかを明確に理解しておくことが大切です。

禁止事項の確認

利用規約に含まれる禁止事項を理解しておくことは重要です。特に入力していはいけない内容を事前に把握しておきましょう。

データ管理の確認

データの保管場所や管理方針についても事前に確認し、企業としてのリスクマネジメントを行いましょう。

視点① 入力情報のリスク - 著作権

他人の著作物の入力

他人の著作物（文章、画像等）を無断でAIに入力する行為は、著作権法上の「複製権」や「公衆送信権」を侵害する可能性があります。社外の著作物を扱う際は、権利関係の確認が不可欠です。安易なコピー＆ペーストは避けましょう。

視点① 入力情報のリスク （著作権）ー例外規定「30条の4」

CHECK POINT

30条の4の内容

著作権法30条の4は、情報解析などで著作権者の利益を不当に害さない範囲での利用を認めています。「非享受目的」など要件があり、通常の業務利用が常に許されるわけではない点に注意が必要です

（著作物に表現された思想又は感情の享受を目的としない利用）
第３０条の４　著作物は、次に掲げる場合その他の当該著作物に表現された思想又は感情を自ら享受し又は他人に享受させることを目的としない場合には、その必要と認められる限度において、いずれの方法によるかを問わず、利用することができる。ただし、当該著作物の種類及び用途並びに当該利用の態様に照らし著作権者の利益を不当に害することとなる場合は、この限りでない。
一　著作物の録音、録画その他の利用に係る技術の開発又は実用化のための試験の用に供する場合
二　情報解析（多数の著作物その他の大量の情報から、当該情報を構成する言語、音、影像その他の要素に係る情報を抽出し、比較、分類その他の解析を行うことをいう。第四十七条の五第一項第二号において同じ。）の用に供する場合
三　前二号に掲げる場合のほか、著作物の表現についての人の知覚による認識を伴うことなく当該著作物を電子計算機による情報処理の過程における利用その他の利用（プログラムの著作物にあつては、当該著作物の電子計算機における実行を除く。）に供する場合

視点①入力情報のリスク - 個人情報保護法（利用目的との関係）

01

個人情報の目的外利用の禁止

氏名や住所などの個人情報をAIに入力する際は、個人情報保護法が問題となります。本人の同意なく、取得時の利用目的を超えてAIに入力・処理することは原則として違法です。

02

注意点

個人情報を取得したときの目的は何か、生成AIへのプロンプトは個人情報取得との関係で目的外の利用となっていないのかを慎重に検討すること。取得時に様々な利用目的が想定されるケースではプライバシーポリシーに記載しておく。

（利用目的の特定）
第１７条　個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」という。）をできる限り特定しなければならない。
２　個人情報取扱事業者は、利用目的を変更する場合には、変更前の利用目的と関連性を有すると合理的に認められる範囲を超えて行ってはならない。

（利用目的による制限）第１８条　個人情報取扱事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。

（取得に際しての利用目的の通知等）第２１条　個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。

視点①：入力情報のリスク – 個人情報保護法（第三者提供）

個人データとは	個人情報のうち、体系的に整理されて検索可能な状態になっているもの（例：顧客管理システムに登録されている情報）
第三者への提供	個人データをAIに入力する行為は、「第三者」へのデータ提供と見なされることがあります。
本人の同意が必要	個人データを第三者に提供するには、原則として本人の同意を得る必要があります。同意を得ることなく第三者提供すると違法となるリスクがあります

入力情報のリスク – 個人情報保護法（第三者の同意が不要となるケース）
→自動学習がオフとされていることが前提です

01

クラウド例外のケース

クラウドでデータを取り扱う場合、特定の条件を満たすと第三者の同意が不要になることがあります。

02

委託のケース

利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部を委託していると評価できる場合は第三者の同意は不要となります

（第三者提供の制限）
第２７条
１　個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。
①法令に基づく場合
②人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。・・・

５　次に掲げる場合において、当該個人データの提供を受ける者は、前各項の規定の適用については、第三者に該当しないものとする。
①個人情報取扱事業者が利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部を委託することに伴って当該個人データが提供される場合

視点①：入力情報のリスク – 個人情報保護法（要配慮個人情報との関係）
→要配慮個人情報は特に慎重な取り扱いが求められます。

要配慮個人情報の定義	人種、信条、病歴、犯罪歴などの情報は「要配慮個人情報」として、特に慎重に取り扱う必要があります。
通常の個人情報よりも厳格な扱い	これらの情報は、取得自体に本人の同意が原則必要など個人情報保護法の取り扱いも厳格です。
入力の禁止	要配慮個人情報を求めるプロンプトや要配慮個人情報を記載したプロンプトは入力しないようにすることが重要です。

視点①：入力情報のリスク – 個人情報保護法（海外移転規制との関係）
→海外への個人情報移転には特別な規制があります。

海外移転のリスク	個人データを海外に移転する場合、特定の条件を満たさない限り、原則として本人の同意が必要となります。
規制除外のケース	海外移転規制の対象外となるケースが存在します。具体的には、相手が日本の個人情報保護法の趣旨に沿った適切な措置の実施を確保している場合などがあります。
総合的な判断が必要	各状況を個別に判断する必要があり、一概にOKとは言えません。そのため、専門的な知識が求められます。

（外国にある第三者への提供の制限）
第28条
1　個人情報取扱事業者は、外国（本邦の域外にある国又は地域をいう。以下この条及び第三十一条第一項第二号において同じ。）（個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国として個人情報保護委員会規則で定めるものを除く。以下この条及び同号において同じ。）にある第三者（個人データの取扱いについてこの節の規定により個人情報取扱事業者が講ずべきこととされている措置に相当する措置（第三項において「相当措置」という。）を継続的に講ずるために必要なものとして個人情報保護委員会規則で定める基準に適合する体制を整備している者を除く。以下この項及び次項並びに同号において同じ。）に個人データを提供する場合には、前条第一項各号に掲げる場合を除くほか、あらかじめ外国にある第三者への提供を認める旨の本人の同意を得なければならない。この場合においては、同条の規定は、適用しない。

視点①：入力情報のリスク - 機密情報の入力禁止

01

機密情報とは

自社の開発情報や戦略、計画などの機密情報をAIに入力する際には、特に慎重になる必要があります。

02

データの流出リスク

学習利用される可能性がゼロではありません。仮に、学習利用の設定をオフにしていても慎重に対応するべきです

03

学習利用のオフにしておく重要性

自動学習はオフにしておくのが基本ですが、最も安全なのは機密情報をAIに入力しないことです。社内ルールを強化しましょう。

視点② 出力情報のリスク - 著作権は誰のもの？

01 AIによる創作物

日本の現行法では、AIが自律的に生成した著作物に著作権は発生しないと考えられています。

02 人間の創作性

AIを用いてプロンプトの工夫や大幅な修正を経て創作的表現を行った場合、著作権が認められる可能性があります。

03 権利の扱い

著作権を確実に取得したい場合は、AI任せにするのは適切ではありません。自ら作成に関与したという要素が重要となってきます。

視点② 出力情報のリスク ー生成物による権利侵害リスク

01 / 学習データの影響

AIは学習データに基づいてコンテンツを生成します。そのため、生成物が既存の著作物に酷似するリスクがあります。

02 / 意図しない侵害

自社の生成物が他者の著作権を侵害する場合、意図せずに法的なトラブルを引き起こす可能性があります。

03 / リスク軽減措置

生成物をそのまま利用するのは極力控えましょう。自分の著作物を前提にプロンプトを入力する、生成物から大幅に加筆修正することで権利侵害リスクを減らせます。

視点③　利用規約違反のリスク

利用規約の確認は極めて重要です。利用規約は１つではない可能性もあります。基本規約をベースに追加規約でルールが修正されている例も珍しくはないです。基本の利用規約のみではなく、追加規約まで確認することで、生成AI利用のリスク等を適切に把握しましょう。

無料ユーザーは入力情報が自動学習に利用される可能性があります
（無料ユーザーのリスク）

無料プランの落とし穴

無料プランでは、ユーザーの入力情報が自動で学習に用いられるため、注意が必要です。安易に利用しないことが望ましいです。

機密情報の漏洩リスク

企業の機密情報を無断で学習させてしまうと、有害な結果を招きかねません。機密情報は入力しないなど自社の情報管理を徹底しましょう。

統制の重要性

各ユーザーが無統制に生成AIを利用することは、企業全体の情報資産を危険に晒す行為です。ガイドラインを作成すべきです。

ChatGPTのプラン構成ーChatGPTのプランには様々な選択肢があります。

プランのバリエーション	ChatGPTには個人向け無料版・有料版（Plus、Pro）や法人向けプラン（Team、Enterprise）があります。
ビジネス利用に向けて	法人向けプランでは、セキュリティや管理機能が強化されており、企業が安心して利用できるよう設計されています。
プラン選択のポイント	ビジネスで利用する場合、セキュリティや管理機能が強化され、入力データが学習に利用されない法人向けプランの契約がおすすめです。

ChatGPT：適用される利用規約はプランによって異なります。

個人向けプランの規約	個人向けプランには通常の「利用規約」が適用されており、ユーザーはそれに従って利用することが求められます。 参考https://openai.com/ja-JP/policies/row-terms-of-use/
法人向けプランの違い	法人向けプラン（Team, Enterprise）には「OpenAIサービス契約」が適用されており、より厳格なデータ保護や秘密保持義務が定められており、企業のコンプライアンスを重視しています。 参考https://openai.com/policies/services-agreement/

ChatGPT：入力データの学習利用

個人向けプラン	個人向けプランでは、デフォルト設定では入力データが学習に利用されますが、ユーザーの設定で変更が可能です。
法人向けプラン	法人向けプランでは、Team、Enterprise、API経由の利用で、入力データが学習に利用されないことが保証されています。
学習利用がされているかの意識	利用者は入力データがどのように扱われているのかを理解し、適宜設定を確認した上で利用する必要があります。

ChatGPT：学習利用の停止（オプトアウト）ー利用者は学習利用の停止を選択することが可能です。

オプトアウトの方法

個人向けプランでは、設定画面から設定変更することで入力データの学習利用を停止することができます（法人プランでは各自このような設定変更をする必要はありません）。

リスク管理の必要性

個人向けプランだと、自動学習の有無はユーザー個々の設定に依存します。組織的な管理は法人プランが必要となります。

ChatGPT：禁止事項とデータ管理

禁止事項	規約には他者の権利侵害や違法行為が禁止されているため、利用者はこれに従わなければなりません。
個人情報の取扱い	個人向けサービスでは個人情報の入力は向いていないです。 法人向けサービスでも個人情報を処理する場合は、DPA（OpenAIデータ処理補足契約）を締結することが前提とされています。
データ移転の確認	データは米国のサーバー等に保存される可能性があり、国外移転のリスクを認識する必要があります。チャット履歴はユーザーが削除するまで保存されますが、一時的なチャットは最大30日間保持されます

Geminiのプラン構成ーGeminiも法人向けプランが充実しています。

01 利用可能なプラン

Geminiには個人向けサービス（無料版・有料版）と法人向けサービスの「Gemini for Google Workspace」があります。

---

02 セキュリティ基盤

ビジネス向けのWorkspace版は、Googleの強固なセキュリティ基盤上で運用されており、管理機能が充実しています。

Gemini：適用される利用規約ーGeminiにも様々な適用規約があります。

Google全体の規約

GeminiにはGoogle全体の利用規約に加え、プランに応じたプライバシーポリシーが適用されます。

個人向けサービスのプライバシーポリシー

「Geminiアプリのプライバシーハブ」を参照してください。
＜参考＞https://support.google.com/gemini/answer/13594961?hl=ja

法人向けけサービスのプライバシーポリシー

「Google Workspace の生成 AI に関するプライバシー ハブ」を参照してください。
＜参考＞https://support.google.com/a/answer/15706919?sjid=4863130603879577308-NC

Gemini：入力データの学習利用ーGeminiにおける入力データの学習利用の状況を理解しましょう。

01 個人向けプランの特性

原則として、個人向けプランでは入力データがAIの学習に利用されます。
機密情報の入力も禁止されています。自動学習をオフにする場合は個別設定が必要です。

02 法人向けプランの安心感

法人向けWorkspace版では、入力データがAIの学習に利用されることは一切なく、人間によるレビューも行われないことが保証されています。そのため、安心して利用することができます。

Gemini：禁止事項とデータ管理

禁止事項（個人向けプラン）

- 個人向けプランでは、「会話には機密情報を入力しないでください。また、レビュアーに見られたくないデータや、Google のプロダクト、サービス、機械学習技術の向上に使用されたくないデータも入力しないでください。」と記載されています。個人情報や機密情報の入力は控えるべきです。

データの保存と管理

- 法人向けのWorkspace版では、プロンプトや回答はセッション終了後に破棄され、保存されません。明確なデータ管理が大きな利点です。
- 個人向けプランでは、保存期間も最大3年です

視点④内部統制の違反リスクー社内ルールを作成して、従業員各自がルールに違反しないよう運用することが重要

POINT

従業員が個人アカウントでAIを利用してしまうと、情報漏洩のリスクが高まります。たとえば、無料版の生成AIに会社の機密情報を入力してそれが自動学習で利用されてしまうケースです。これを防ぐには、社内のルール作りと社内研修が重要。

視点④内部統制の違反リスクー企業が今すぐとるべき３つの対応策

01

法人向けプランの利用

利用するサービスを、セキュリティが担保された法人向けプランに限定することが第一歩です。無用なリスクを減らすことができます。

02

社内規程の整備

生成AI利用に関する明確な社内規程やガイドラインを整備し、全社員に周知することが重要です。

03

従業員への教育

ガイドラインを基に従業員に生成AIの利用方法について社内研修を行うなどしてリスクと適切な利用方法について理解してもらうことが重要です。

対応策① なぜ法人向けプランが必須なのか

01 学習利用の排除

法人向けプランでは入力データが学習に利用されることがなく、企業情報の保護に繋がります。

02 管理機能の充実

法人向けプランはセキュリティや管理機能が充実しており、社内での情報管理がしやすくなります。

03 秘密保持の保障

秘密保持やデータ保護が保証されており、安心して業務に取り組むことができます。

対応策② 生成AI利用ガイドラインの策定及び社内体制の整備

1 ガイドラインの必要性

ガイドラインは従業員を法令や規約の違反から守り、安全な活用を促進するための重要なルールとなります。

2 活用方針の明確化

禁止事項だけでなく、企業としての活用方針を明確にし、従業員が安心して使える環境を整えることが重要です。

3 専門担当者の設置

ガイドラインの作成には生成AIに詳しい人材を担当者として、他の従業員からの相談や定期的な更新に対応できる体制を整える必要があります。

ガイドラインの基本構成ー参考例

目的の明示

ガイドラインの目的を明示し、なぜこのルールが必要か従業員に理解してもらうことから始めます。

利用方針の設定

生成AIの利用に関する方針として、許可制や特定のサービスの利用に限定することを列挙します。

生成AI利用上の注意点及びリスク説明

生成AI利用上の注意点及びリスク説明を盛り込み、従業員に具体的なリスクを理解してもらいましょう。

入力情報と出力情報のルール

入力情報や出力情報の利用ルールを具体的に定め、実務に沿ったガイドラインとすることが重要です。

禁止事項の明示

利用規約等で禁止されている行為も参考にしつつ、ガイドラインでも禁止事項を明示します。

相談窓口の整備

従業員がガイドラインに疑問を持った際の相談窓口と担当部署を明記し、適切なサポートを提供できる体制を作りましょう。

対応策③　ガイドラインの運用と教育ーガイドライン作成後も運用と教育が非常に大切です。

研修会の実施	ガイドラインを策定するだけでは効果がありませんので、全従業員を対象にした研修会を実施し、内容を周知します。
定期的な見直し	AI技術やサービス規約は常に変化しますので、定期的な見直しを行い新しい情報を従業員に提供することが重要です。
情報提供の継続	従業員に対して継続的な情報提供を行うことで、生成AI活用において求められる知識を常に更新し続けることが求められます。

まとめ

法的リスクを理解し、適切に対応する

生成AIはビジネスを加速させる強力なツールですが、一定の法的リスクも伴います。リスクを正しく理解し、「法人プランの導入」、「生成AI利用ガイドラインの策定及び社内体制の整備」、「ガイドラインの運用と教育」という体制を構築することで、AIを安全かつ効果的な武器とすることができます。

よつば総合法律事務所が支援できること

「課題は理解しているが担当できる人材がいない」「専門家のサポートがほしい」という方は当事務所で継続サポートが可能です

利用規約のチェック

生成AIの複雑な利用規約について弁護士が貴社の代わりにチェックを行い、リスク判定を行います

業務効率化のサポート

貴社の事業内容を踏まえて業務効率化のための生成AIの活用方法についてご相談に乗ります。

生成AIガイドライン作成

社内向けの生成AIガイドラインの作成サポートを行います。貴社の状況を踏まえて個別に作成します。

チャットで相談可

手軽に相談できるように、チャットワークやLINEなどのチャットサービスでのご相談も可能です。

社内向け研修

社内向け研修の講師も担当します。リアル研修以外にオンライン研修動画として納品させていただくことも可能です。

定期的な情報発信

生成AIは日々刻々と進化しています。利用規約も定期的に変更・修正されています。定期的な情報発信・ガイドラインのアップデートをサポートします

よつば総合法律事務所が支援できること（料金プラン）

	通常の顧問プラン		
プラン	月50,000円 （税込55,000円）	月100,000円 （税込110,000円）	月150,000円 （税込165,000円）
プランの選び方	困ったときにすぐに相談したい	契約書等の書類作成・チェックを日常的に任せたい	自社に法務部が欲しい
基本業務の対応時間の目安 （相談／契約書その他書類作成・チェック）	2時間まで／月	4時間まで／月	8時間まで／月
個別の案件費用の割引	10%	20%	30%

ご清聴ありがとうございました

生成AIに関してのご相談をご希望の方は、ぜひ一度弁護士にご相談ください。

01

アンケートのご協力のお願い

本日はご清聴いただき、ありがとうございました。セミナー時間内にてアンケートの時間を確保しておりますので、ご協力お願いいたします。

02

継続的なサポートをご希望の場合

生成AIの利用規約の確認や、自社に最適なガイドラインの作成には専門的な知見が不可欠です。「適切な担当者がいない」「継続的にサポートしてほしい」とのご希望がある場合は顧問プランにてサポートをさせていただきます。継続的なサポートに興味ある場合は、その旨をアンケートにご記載いただけると幸いです。