



AIを安全に活用するための リスクマネジメント

ーAIを組織で使うために考えたいことー

那須雄介

2026.8.27



AI使っていますか？

AI使っていますか？

AI「どんなことに」使っていますか？

AIどんなことに「気をつけて」使っていますか？

AIどんなことに「組織として」気をつけて使っていますか？

個人でAIを使って事故があったら組織の問題＝組織的なガバナンスの重要性
AI利活用にあたっての注意すべき点を踏まえてAIを活用することが肝要

・・・安全に使える条件を、組織で決めていますか？

AIの代名詞「生成AI」をおさらいすることから始めてみましょう

ご留意いただきたい点

この研修は「一般的なAIとリスク」についての研修です。

財団の状況を最大限加味しますが、財団としてのルールを説明するものでも、特定のガイドラインを「これでなければダメ」と押し付けるものでもありません。

大事ななのは、経営層も現場の皆様も含めて、AIを使うとどうなるか、AIをどう扱うべきか、財団に合った形を考えるということですので、今回の研修は、それを考えるきっかけとなれば幸いです。

なにより、誰かがルールを一方的に決めても、現場に沿わないルールになり、息苦しいものになりますから。

おしながき

1. (生成) AIのおさらい
2. AIのリスク？
3. AIのリスクアセスメント
4. ちょっとワーク
5. 終わりに



1. (生成) AIのおさらい

AIの特徴

そもそもAIってなんでしょう？

「人工的につくられた人間のような知能、ないしはそれをつくる技術」（東京大学 松尾豊教授）

自律：人間の操作なく作業を実行できる

適応：知識・経験から学び、行動し、パフォーマンスを高める

} 「学習」し、「作業」、「成長」する



あらゆる情報を学習し、目的に応じた作業を行い、結果を示す

→得られた情報は（サービス・契約次第ではあるが）学習に用いられ、得られた情報を活用して成長し、可能な限り最適な結果を示す

この処理を全世界のデータセンターのどこかで行っている

生成AIでよく使われる例

質問応答	翻訳	要約	校正
〇〇について教えて	以下の文章を翻訳して 以下のページを翻訳して	以下のページを要約して 〇〇について要約して	誤字脱字を見つけて 表現を改善して
情報検索	マーケティング	プログラミング	抽出
〇〇についての論文やWeb ページを集めて	〇〇の市場規模は 〇〇が合うターゲットは？	エクセルのマクロを書いて API実行コードを書いて	レビューから要点を抽出し て
アイデア創出	ペルソナ	メール・SNS投稿文作成	企画
〇〇に関する内容案を提案 して	〇〇業で〇〇歳の男性が、 〇〇を買うメリットは	メールへの返信やSNS投稿 文を作成して	〇向けイベントを企画して
ホームページ・LP作成	チラシ作成	商品レビュー	記事作成
〇〇を基に〇〇商品のペー ジを作成して	〇〇商品の顧客と特徴を押 さえてチラシを作成して	〇〇の口コミを検索して 改善点を教えて	ブログの記事を作成して メルマガを作成して

こんなにたくさん生成AIーカオスマップー

汎用性高し

ChatGPT

文章・要約・調査

業務全般で迷ったらこれ。対話性能や多機能さが魅力

Claude

長文・資料作成に強い

自然な日本語と高い論理的思考力が特徴

Gemini

Googleアプリとの連携○

検索結果の反映やGmail、Googleドキュメントとの相性が抜群

Microsoft Copilot

Microsoftサービスとの連携○

ExcelやWordなどの業務ソフト内での活用に強み

NotebookLM

社内データ専用AI

PDF等に基づいた資料作成や、マニュアルQAなどの作成

Notion

ワークスペースAI

ドキュメント作成・管理、データ分析、プロジェクト管理などをAIと共に行えるワークスペース

やや特化型

Perplexity

調査・検索支援

最新情報の調査・出典付き回答
市場調査や競合分析に最適

Zapier / Make/n8n

業務自動化・AIエージェント

AI同士や他のアプリを連携。人間を介さない自動フローの構築

Notta

文字起こし議事録作成の先駆け

音声の文字起こしと議事録作成
話者や業界用語も覚える

Midjourney / Canva

画像・動画生成

画像生成や資料デザインの自動化。
視覚的な訴求力を高める

Cursor / GitHub Copilot

プログラミングの自動化

コーディングやデバッグなどを自動化

Kintone AI

データベース AI

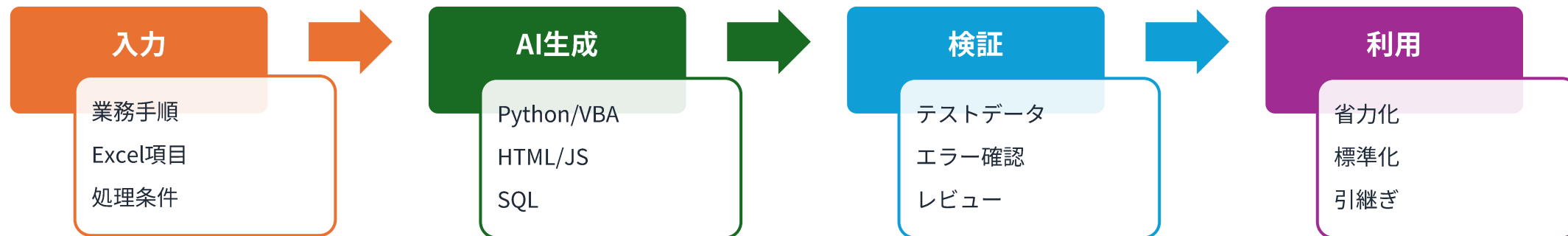
Kintone内のデータベースの情報を整理・提案

AIのちょっと進んだ利用例

AIコーディング

Codex
Claude Code

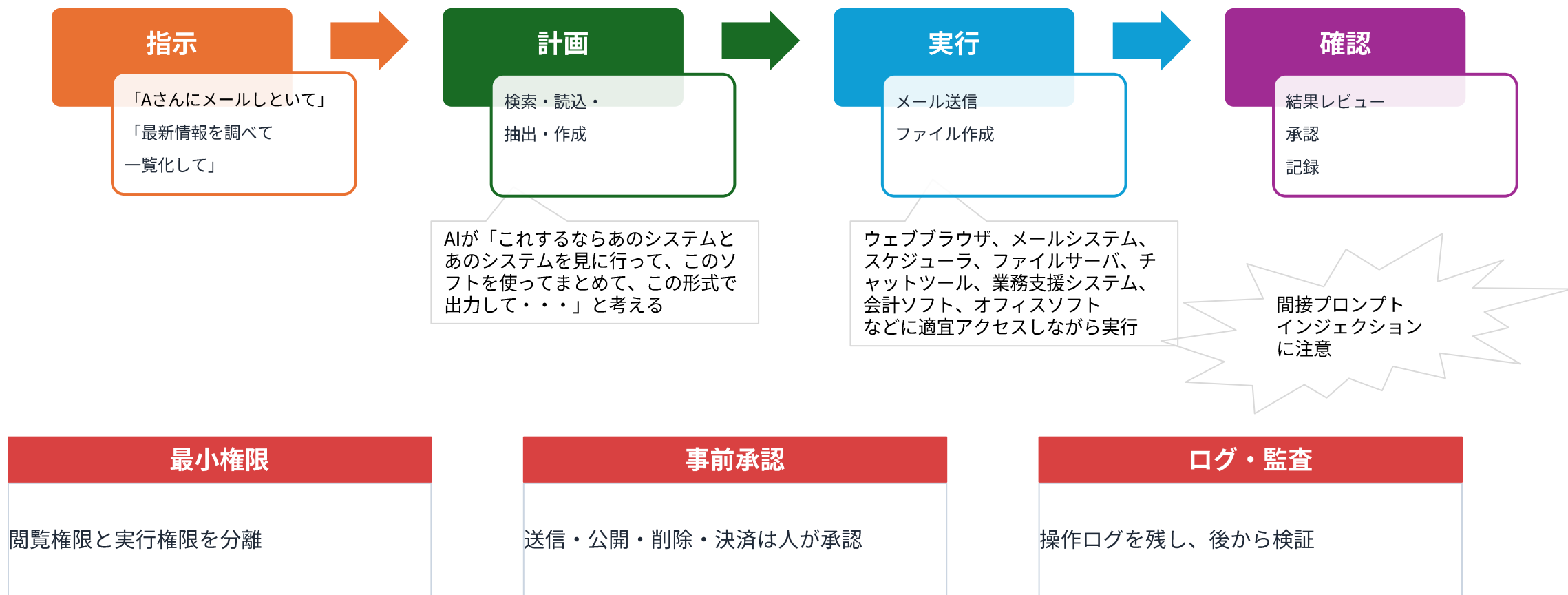
AIにプログラミングをしてもらう



特に注意：生成されたコードは、誤動作・情報流出・権限逸脱・保守不能化のリスクがあります。
「作れる」ことと「業務に使ってよい」ことは別です。

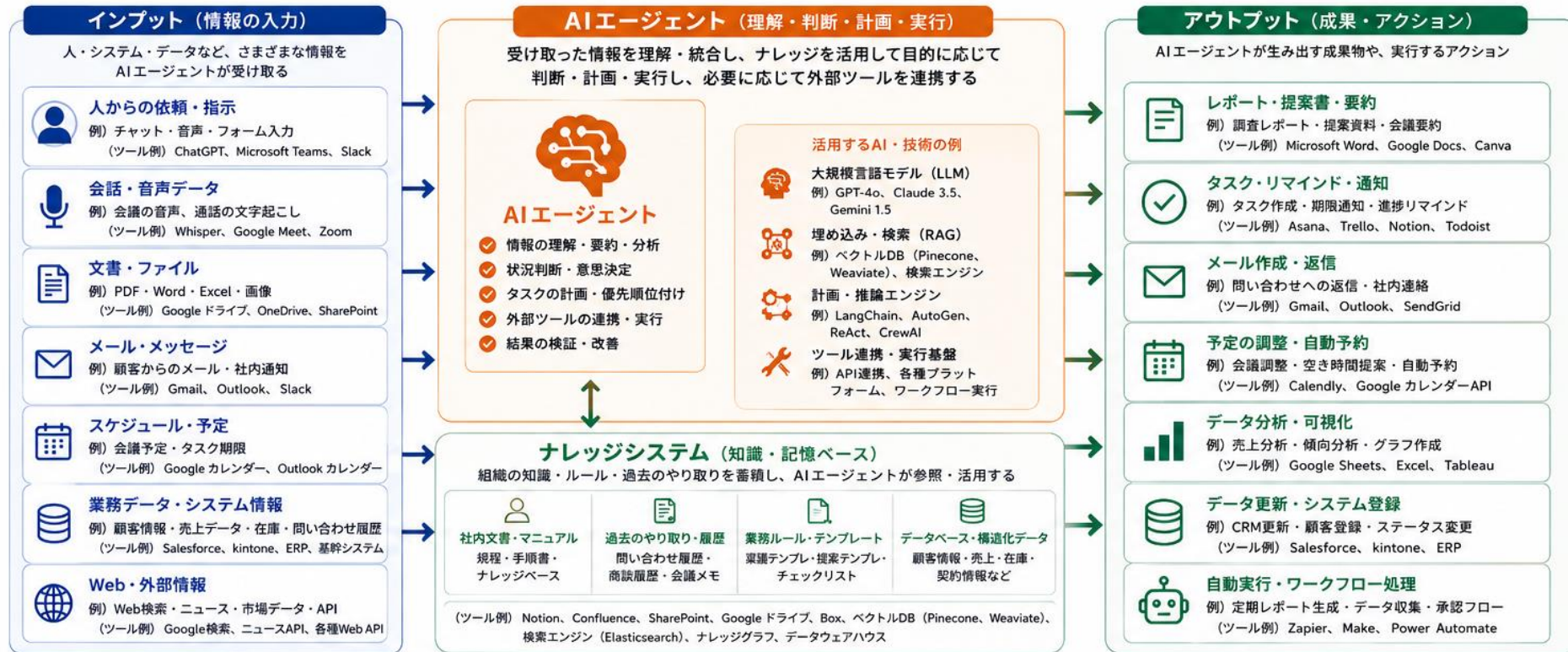
AIを手足で使う

メール・カレンダー・ファイル・Web・業務システムに接続すると、便利さUP! リスクが同時に増えます。



AIエージェントの概念図

AIエージェントは、さまざまな情報（インプット）を受け取り、ナレッジを活用して理解・計画・実行、成果やアクション（アウトプット）を生み出す



AIの使い方の変化（Before / After）

AIエージェントの登場により、AIの使い方が「人が操作する」から「AIが自律的に動き、成果を届ける」へ進化する



※記載のツールは一例です。自社の環境や目的に合わせて選定してください。

(ツール例) LLM: ChatGPT, Claude, Gemini / ナレッジ: Notion, Confluence, SharePoint / 業務: Salesforce, kintone, Microsoft 365 / 自動化: Zapier, Make, Power Automate など

AIにはリスクも・・・

IPA（情報処理推進機構）も情報セキュリティの10大脅威2026の3位に「**AIの利用をめぐるサイバーリスク**」を選出



3位 AI の利用をめぐるサイバーリスク



生成 AI の進化、普及に伴い、様々な問題、懸念が浮上している。例えば、AI に対する不十分な理解による、意図しない問題として他者の権利侵害²⁷、情報漏えい、AI が加工・生成した結果を十分に検証せず鵜呑みにすることにより生じる問題、AI の悪用によるサイバー攻撃の容易化²⁸、手口の巧妙化などがあげられる。

<脅威と影響>

人口減少と急速な高齢化、十分な雇用確保が困難な状況下において、諸外国を追いつ、AI の種別利用は国内でも進んでいる²⁹。一方、AI 活用による懸念も指摘されている。例えば、AI を利用したシステムの様々な脆弱性を狙った、外部からの攻撃リスクや AI 悪用による攻撃の容易化を招く可能性が指摘されている。また、生成 AI の業務利用においては、生成された情報の正確性を確認せず活用した結果、思わぬトラブルを引き起こされるリスクもあるため、利用者が十分に確認の必要性について指摘されている。

<リスク>

◆職場に許可なく AI を業務利用し、情報漏えいにつながる可能性

例えば職場で AI サービスの利用が無い場合など、従業員が個人的に利用している AI サービスを業務利用することがある(シャドーAI)³⁰。本来組織外への持ち出しが禁止されている業務データや資料等を AI サービスに入力すれば、情報漏えいにつながる。また、職場が従業員の個人アカウントによる AI の業務利用を認識できないこともリスクといえる。

◆実在しない情報を対話型 AI が生成する可能性(ハルシネーション)

対話型 AI は時に、架空の情報をあたかも事実として生成し、利用者に提示することがある。問いに対する答えが容易に得られ、利便性の高さ、手軽さから過剰依存し、誤った生成結果を鵜呑みにしてしまうことも考えられる。利用者は生成結果の精査を行うことが求められる。

◆AI を助力に得たサイバー脅威の増長

AI による翻訳機能・能力の向上により、攻撃者が Web ページの翻訳やフィッシングの文面を標的の母国語で違和感なく表現することを可能にし、言語の壁を実質的に乗り越えた多言語での攻撃を格段に容易にする。また、生成 AI をサイバー攻撃のアシスタントとして利用することで、様々な攻撃が容易に展開できるようになり、対処しなければならないインシデントの頻度・数量が増えたり、平均的な攻撃の技術水準が高まったりしている。

<事例または傾向>

◆生成 AI の業務利用による情報漏えい

米国の AI 企業の調査³¹によれば、業務において、生成 AI にデータをコピー＆ペーストしてプロンプト(指示文)として入力している利用者が 77%おり、そのうち 82%が組織に管理されていないアカウントによるものであったという。こうした行為により、組織が把握できない形で情報漏えいが発生するリスクが高まる。

◆生成 AI を使い作成した資料に、実在しない判例が含まれていた事例

2025 年 1 月、米国テキサス州の裁判所で公聴会が開催された。前年に同州の弁護士が提出した意見書に実在しない判例が引用されていることが判明し、生成 AI を用いて作成していたことが明らかになった。当該弁護士は、生成 AI を用いて作成したデータにハルシネーションが起こりうることを知らなかったという³²。

◆生成 AI を悪用したプログラムの作成

2025 年 2 月、不正に入手した ID とパスワードを機械的に入力して携帯電話の回線契約まで行うプログラムを用いて携帯電話の回線を契約したとして、中高生 3 人が不正アクセス禁止法違反と電子計算機使用詐欺の疑いで逮捕された。生成 AI を補助的に使いプログラムを自作したという³³。

◆AI の脆弱性

2025 年 6 月、Microsoft 365 Copilot の脆弱性「EchoLeak」の存在が報道された。この脆弱性を悪用する不正プロンプトが外部から注入されると、不適切な AI の動作が誘発され、Microsoft 365 Copilot にアクセスを許可した社内の秘密データ等が流出する可能性があったという³⁴(詳細はコラムを参照のこと)。

<対策と対応>

※以下では「AI 事業者ガイドライン³⁵」に言う AI 利用者における対策を想定している。

経営者層

- シャドーAI 回避のため、AI サービス利用の検討
 - ・未許可・未承認の AI サービス利用(シャドーIT)の禁止
- AI ガバナンスおよびサービス利用規定の整備
 - ・AI 事業者ガイドライン等の参照・準拠
 - ・個人アカウントにおける業務利用の制限
 - ・規程違反時の対応(ペナルティ)の明確化

出展：(独法)情報処理推進機構『情報セキュリティ10大脅威2026 解説書 [組織編]』
https://www.ipa.go.jp/security/10threats/omgdg50000008fi8-att/kaisetsu_2026_soshiki.pdf



2. AIのリスク？

AI利用の主要リスク

AIのリスクってなんでしょう？



個人情報・顧客情報の漏えい



営業秘密・機密情報の流出



誤情報・もっともらしい誤答



権利侵害・著作権／知的財産権の問題



なりすまし・詐欺・ディープフェイク



シャドーAIによる統制不全



データのントリーリスク

便利さとリスクは同時に増える

リスク1



個人情報・顧客情報の漏えい



営業秘密・機密情報の流出

- ・顧客名、担当者名、連絡先、顧客リスト
- ・クレーム内容、相談履歴、面談記録、会議記録
- ・従業員の評価、給与、勤怠、健康情報
- ・16歳未満者の情報、顔特徴データ、音声・画像・動画
- ・見積単価、原価、利益率
- ・設計図、仕様書、新製品計画
- ・契約条件、取引条件、未公開の財務情報
- ・補助金申請書、事業計画書、提案書の原文

令和8年改正個人情報保護法：2026年7月17日公布
主要部分の施行日は今後政令で定められる

迷ったときの基準

その情報を、
社外の第三者に送ってよいか。

送ってよくない情報なら、
外部AIにも入力しない。

個人情報・企業情報は「預かりもの」
その情報は「誰かのもの」であることを自覚する

リスク2



誤情報・もっともらしい誤答

- 存在しない制度・補助金・法令を案内する
- 古い情報を最新情報として扱う
- 実在しない出典・統計・判例を示す
- 間違ったExcel関数・計算式を使う
- 技術仕様や契約内容を誤って説明する
- 顧客向け資料に誤った内容を掲載する

[ハルシネーション]

生成AIが事実とは異なる情報や架空の事実を、あたかも正しいかのように自信満々に出力する現象

= 「AIが教えてくれた回答」は正しくない、と思うことが大事

公式サイト・法令原文・一次資料・契約書・計算過程・引用元を確認

他のAIによるレビューは補助策。最終確認と責任は人が担う

AIの回答は完成品ではなく「下書き」

**数値・法令・制度・契約・技術・引用元・・・
必ず人が「正しいか」確認する**

AI利用が逆に負担を増やしている・・・？

実はAIを使うことで「ムダ」が増えるという報告も・・・

その内容本当に正しいですか？ → 修正 / そもそも書いている内容分かってる？ → 解説作成・・・

AIが生成する「手抜き仕事」で同僚の仕事を増やしていないか

実は生産性と信頼性を低下させている

by ケイト・ニーダーホフファー、ガブリエラ・ローゼン・ケラーマン、アンジェラ・リー、アレックス・リーブシャー、クリスティーナ・ラプアノ、ジェフリー T. ハンコック

翻訳 石原 薫

2025.11.18



HBR Staff/AI

ケイト・ニーダーホフファー、ガブリエラ・ローゼン・ケラーマン、アンジェラ・リー、アレックス・リーブシャー、クリスティーナ・ラプアノ、ジェフリー T. ハンコック「AIが生成する「手抜き仕事」で同僚の仕事を増やしていないか」

<https://dhbr.diamond.jp/articles/-/12882> (2026.7.23閲覧)

【AIを使うほど“ムダ”が増える】ChatGPT・Geminiの落とし穴
「ワークスロップ」とは／修正コストで年14億円の損失／スタンフォード大学教授「“パイロット思考”でAIを強い味方に」

【1on1】



2026.03.26 12:00



TBS CROSS DIG with Bloomberg

【AIを使うほど“ムダ”が増える】ChatGPT・Geminiの落とし穴
「ワークスロップ」とは／修正コストで年14億円の損失／スタンフォード大学教授「“パイロット思考”でAIを強い味方に」 【1on1】

<https://newsdig.tbs.co.jp/articles/withbloomberg/2554965?display=1> (2026.7.26閲覧)

リスク3



権利侵害・著作権／知的財産権の問題



なりすまし・詐欺・ディープフェイク

権利侵害・著作権／知的財産

- 【入力時】他社資料や著作物をAIへ送信する権限があるか
- 【出力利用時】既存作品との類似性・権利侵害がないか
- 【知財】AIそのものは発明者になれない。
人が実質的に関与したAI支援発明は特許対象になり得る

自分ではその意識は無くても、
AIが勝手に侵害していることも

なりすまし・詐欺（悪用されたAI）

- 社長・役員を装った音声やメール
- 取引先を装う振込先変更依頼
- 自然な日本語のフィッシングメール
- 偽請求書・偽契約書・偽動画

重要な依頼は、メール・チャット・音声だ
けで判断せず、別の連絡経路で確認する

リスク4



データのカントリーリスク

- 保存国・処理国／適用法令／再委託先／暗号化／アクセス権限
- 保存期間／削除方法／ログ／障害・終了時対応／契約上の保証

保存・処理される国と適用される法制度のリスク

データセンターや処理用サーバがある国の**政治状況でデータが損失する可能性**やその国のルールで**強制的に開示される**可能性

そのAIのデータセンター
どこにあるか分かりますか？

処理全体と契約を確認
※契約・設定・機能により異なる

リスク5



シャドーAIによる統制不全

会社が把握しないまま、AIが業務に使われている状態
= シャドーAI

無料AI・個人アカウント
利用履歴や入力内容を会社が把握しにくい

私物端末・私的利用との混在
業務情報が管理外に出る可能性

「禁止」だけの対応
水面下で利用・更に管理できない可能性

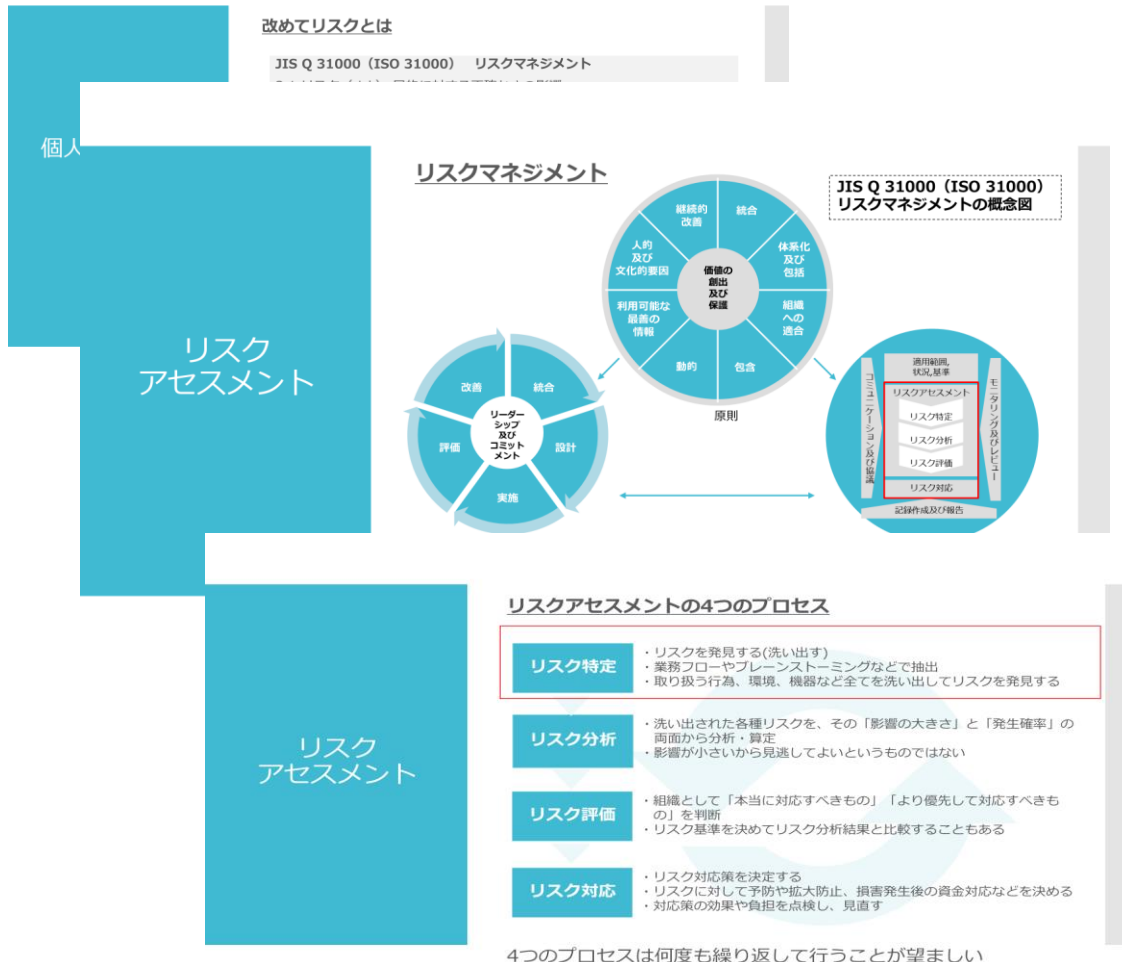
リスクを踏まえないAIの個人利用がリスクを現実化することに
会社未承認のAIも同様のリスクがある
→組織でAIをどう使うかルールを決めたうえで、組織の責任下での利用が必要



3 . AIのリスクアセスメント

リスクアセスメントってなんだ？

2023年度個人情報保護研修（全体研修）より



【リスク】
目的に対する不確実性

【リスクマネジメント】
組織的にリスクを管理する活動

【リスクアセスメント】
リスクを認識して、分析して、対策を行うこと
(個人情報保護規程3.3.3にも規定)

「それするとこんなことになるんじゃない？」ということを見つけて、そうならないように対策を打つこと

リスクを承知で使うことも、リスク回避することも、リスクを金で解決することも全てリスク対策

(大前提) なんでAIを使いたいなの？

一般的な企業活動ではこんなことに使われています（よく相談されます） 

業務効率化・生産性向上

- ・ 定型業務の自動化(データ入力、書類作成、問い合わせ対応など)
- ・ 従業員がより付加価値の高い業務に集中できる時間の創出
- ・ 処理速度の向上とヒューマンエラーの削減

コスト削減

- ・ 人件費や運用コストの最適化
- ・ 少人数でも業務が回る体制の構築(特に人手不足に悩む中小企業で顕著)

意思決定の質の向上

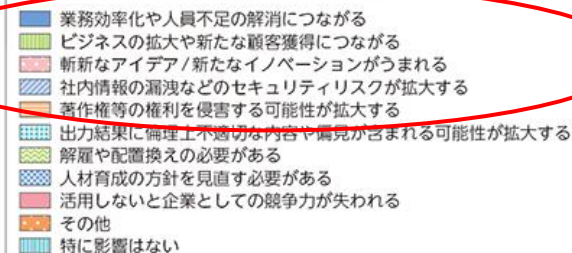
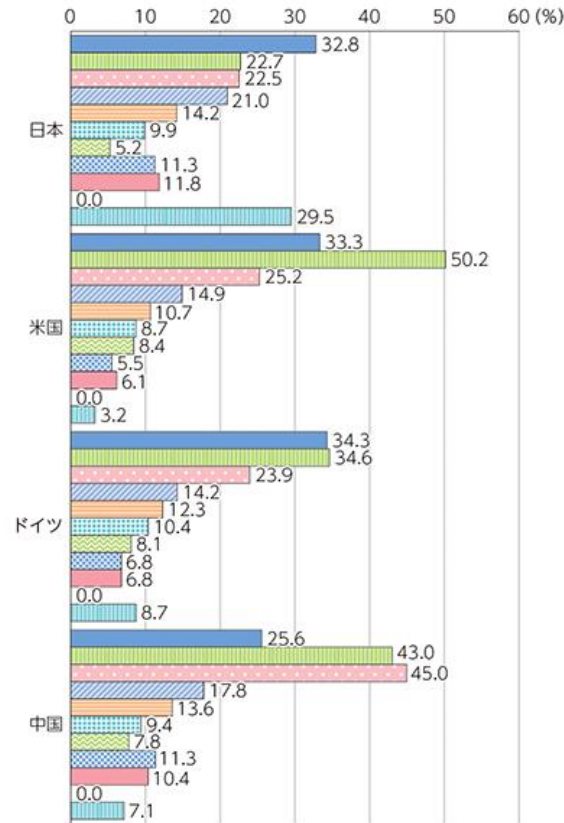
- ・ データ分析による市場動向・顧客ニーズの把握
- ・ 需要予測や在庫管理の精度向上
- ・ 経営判断のスピードアップ

顧客体験の向上

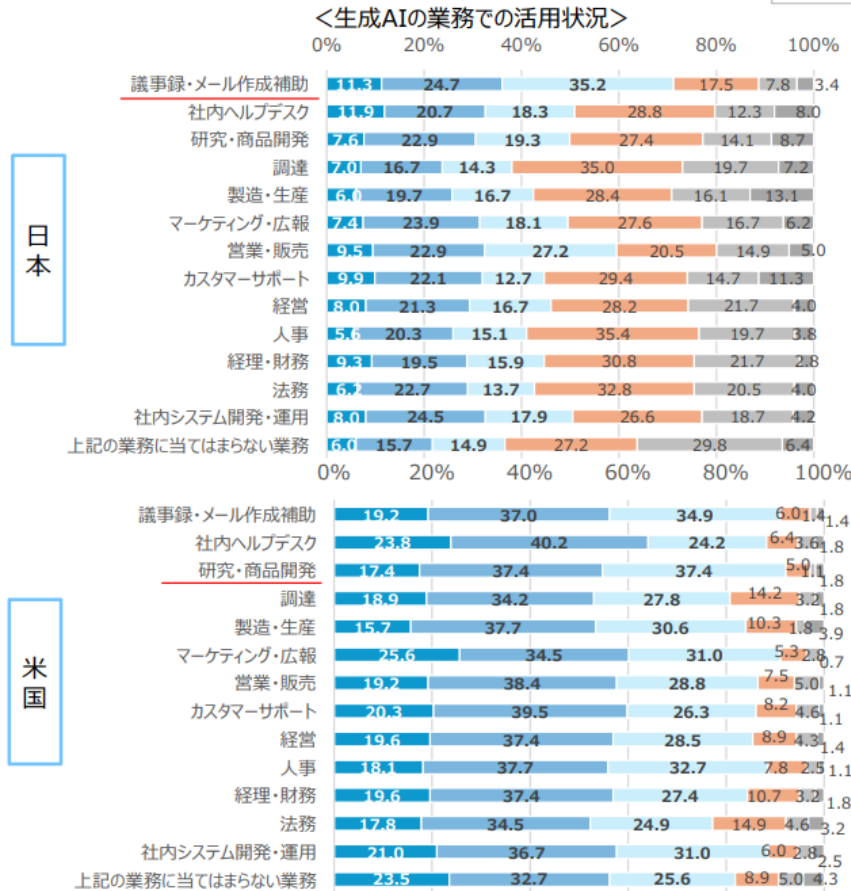
- ・ チャットボットによる24時間対応
- ・ 個人に最適化したマーケティング・提案
- ・ 顧客満足度／リピート率の改善

(大前提) なんでAIを使いたいのか？

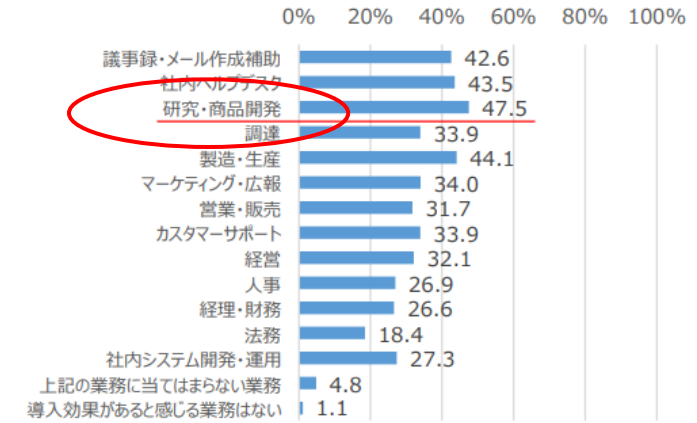
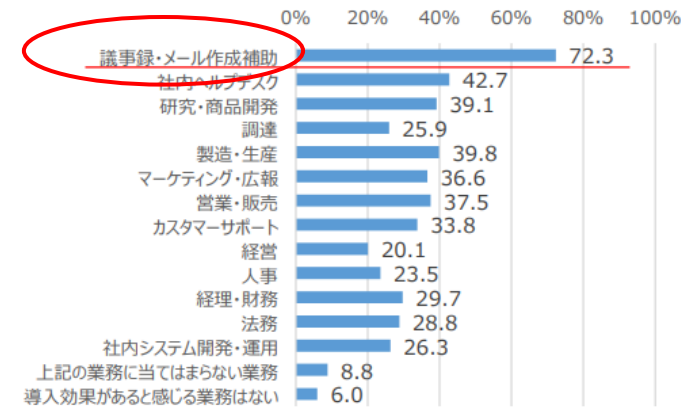
図表 I-1-2-16 生成AIの活用による効果・影響(国別)



業務類型ごとの生成AI活用状況と効果の実感(日本、米国)



＜生成AIの活用効果を感じる割合＞



出展：情報通信白書令和8年版

<https://www.soumu.go.jp/johotsusintokei/whitepaper/r08.html>

(大前提) なんでAIを使いたいのか？

大別すると以下のようなこと 📌

①業務の効率化・生産性の向上

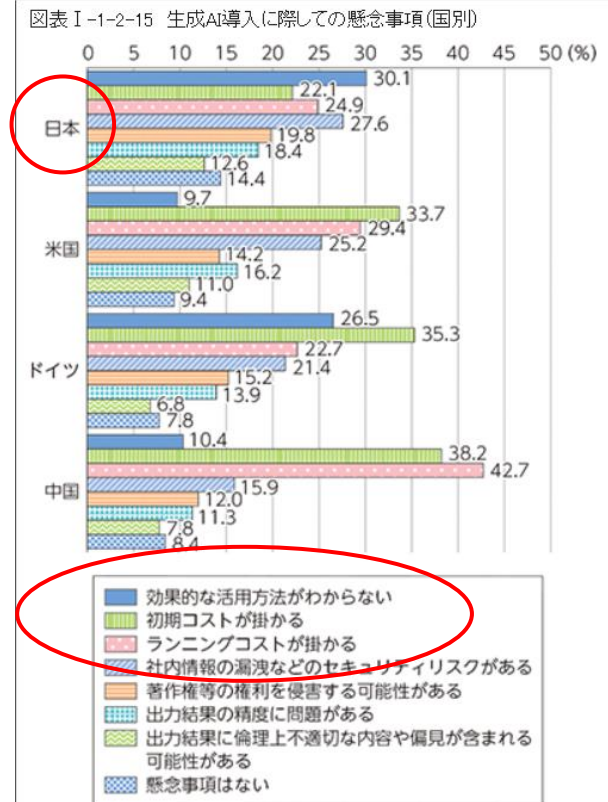
何の業務のどこにAIを使うと何がいいのか
なんとなく「楽にならないかな」から解像度を上げていく

②思考のパートナー 考えること・分析をお願いする

どんな時に相談するのか
個人的な相談と組織・業務の相談を分ける

どんなことが課題で、どう解決したら期待した効果が得られるか

漠然と「使いたい」は導入のコスト（金銭的・時間的・マンパワー的）に見合う効果は得られない
統制にパワーがかかります ある意味AIリスク



(出典)総務省(2025)「国内外における最新の情報通信技術の研究開発及びデジタル活用の動向に関する調査研究」

組織におけるAI活用の2つのアプローチ

AIを使いたい、リスクもどうにかしたい・・・2つのアプローチ

アプローチ① 業務起点 (リスク評価・本格活用タイプ)

- ・業務におけるAI利用のリスクを踏まえて、利用可能と判断したAIを利用
- ・業務 → リスク洗い出し → 分析・対策 → 利用判断
- ・AIなら何でも使える、ということではないが、一度利用条件を決めれば、同じ条件の範囲では都度の個別判断は不要。（年1回・必要に応じた見直しは必要）
- ・手間はかかるが、利用範囲を広げやすい

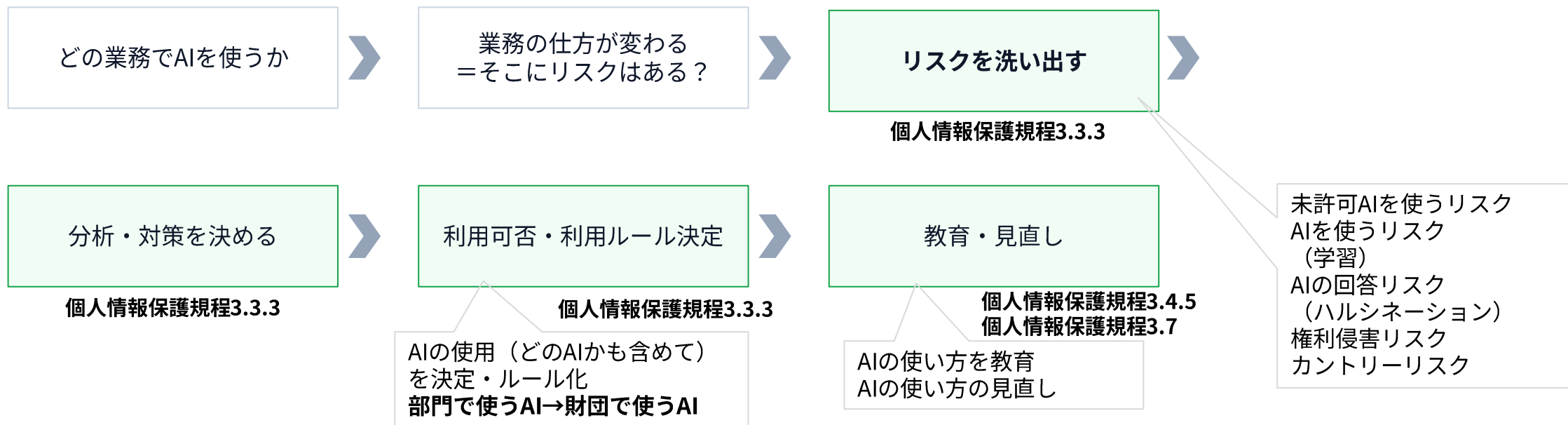
アプローチ② AI先行 (リスク回避・クイック利用タイプ)

- ・とにかくAIを使う。そのために、リスクを徹底的に避けながら利用
- ・リスク回避、入力情報区分、回答の使い方の管理
- ・始めやすく、使うAIの限定も少ないが、都度AI利用のリスク判定を行う必要あり
- ・シャドーAIを回避しきれない可能性があるため、その点のリスクは受容（何にどう使っているか把握できないかもしれません）
- ・利用範囲は比較的限定

どちらか一方が正解ではなく、どこまで組織として必要と考えるか

アプローチ① PMSによるリスクマネジメントの対象とする

業務からのアプローチ＝「この業務をどう進めるか」からAI利用を考える



実は個人情報・企業情報の取り扱いにおいて、財団の個人情報保護規程にて求められていることで対応可能

個別具体的な業務での検討から始めて、他部門でも活用していく、という方が進めやすいかもしれません。

AI利用でよくある一般的なリスク・リスク分析・対策例一覧

リスク	リスク分析の観点	対策例
個人情報・機密情報の漏えい	どの情報を入力するか／保存・学習・再利用されるか／誰が閲覧できるか／漏えい時の影響は大きい	入力情報の制限、匿名化、承認済みAI利用、アクセス権限制御、守秘義務・契約確認
誤情報・ハルシネーション	誤答をそのまま使う可能性はあるか／対外説明・判断への影響は大きい	AI回答を下書き扱い、公的情報・原資料による確認、レビュー・承認ルール
権利侵害・著作権	入力資料をAIへ渡す権限があるか／出力物が既存作品と類似しない	入力可否ルール、引用元確認、対外利用前のチェック、社内法務確認
カントリーリスク	保存国・処理国・再委託先はどこか／適用法令や削除対応を説明できるか	契約・プライバシー情報確認、国内・管理可能環境優先、削除・終了時対応確認
シャドーAI・統制不全	未承認AIや個人アカウント利用の余地はあるか／ログや管理が効く	承認済みAIの明確化、会社アカウント利用、教育、相談窓口、定期見直し
AIエージェントの自動実行リスク	AIが閲覧・送信・削除まで行うか／誤実行時の影響は大きい	最小権限、閲覧権限と実行権限の分離、人の承認、操作ログ、緊急停止手順

まずは「リスクを特定 → 影響を考える → 対策を決める」の型をつくると、業務ごとのAI利用判断がしやすくなる。

アプローチ② とにかくAIを使う 4つの質問でリスク回避

業務に寄らずAIを使いたい、リスクアセスメントなんて難しい・・・

Chat GPTもGeminiもClaudeも使いたいし・・・
せめて、リスクを回避するようにしましょう

1

それ入力していい情報？

個人情報・顧客情報の漏えい

営業秘密・機密情報の流出

心配ならば入力しない

2

そのAI使っていいの？

データのコントリブリスク

シャドーAIによる統制不全

分からないならば
入力しない

3

出力結果どう使う？

誤情報・もっともらしい誤答

権利侵害・著作権／知的財産権の問題

回答が確かか自信がない
ならば使わない

4

誰かの権利、侵害していない？

権利侵害・著作権／知的財産権の問題

入力や回答が誰かの
権利を侵害して
いるか自信が無い
ならば使わない

⇒得られた回答を個人以外に使う時は（組織内）リスクチェック
組織のリスクヘッジができないならば、利用用途を制限する

どの情報を、どのAIに、どの目的で使うか、AI任せにしていないか

迷ったら入力前に相談

どんな情報ならばAI使っていいの？（あくまで例示です）

とにかくAIを使うにしても、せめて、AIを使ってはいけない情報と回答の使い方は決めておきましょう

情報区分	主な例	外部AIへの入力	回答の使い方
公開情報	公開済みWeb情報、公開済み資料	原則利用可	参考情報程度 社内外問わず回答を使わない
社内一般情報	一般手順書、非機密の業務メモ	条件付き利用	参考情報程度 社内外問わず回答を使わない
機密情報	見積、原価、設計、案件情報、取引条件	原則利用不可	参考情報程度 社内外問わず回答を使わない
個人情報	顧客名簿、応募者情報、人事情報、相談記録	原則利用不可	
要配慮個人情報等	健康情報、病歴、障害、労務相談等	原則利用不可	

個人情報でなくても特定個人への働きかけが可能な情報や顔特徴データ等の取り扱いは避けた方が良いでしょう。

組織として選ぶAI利用の3段階

利用目的・回答の使い方に応じて、運用レベルを選ぶ

積極活用
↑
↓
限定活用

アプローチ	運用レベル	回答の活用範囲	取りうる方法	使える幅・難しさ
業務起点	レベル3 積極活用	社内外に活用	リスクアセスメントにより、リスク分析・対策を踏まえて利用できるAIを決定して活用	難しいが 利用幅大
業務起点 AI利用先行	レベル2 限定活用	社内中心 一部社外利用	選択的にAIを使えるようにするが、リスク回避を前提とし、組織的な確認ができない場合は対外的な利用や資料転記は不可	比較的容易 利用幅は中
AI利用先行	レベル1 個人補助	個人で活用 対外利用不可	選択的にAIを使ってよいが、対外的な利用や資料への転記は認めない	始めやすいが 利用幅は狭い

AIサービス利用前の確認項目

いよいよAIを導入するか・・・そのAI本当に大丈夫？
以下は確認した方がいいかもです。　ここまでしたら「より安心」

分類	確認項目	確認する内容	主な確認ポイント
データ処理	回答生成のための処理	入力情報が回答生成の過程でどのように処理されるか	処理場所、外部機能への送信、回答生成後の取扱い
	一定期間の保存	入力、ファイル、回答、会話履歴が保存されるか	保存対象、保存期間、履歴オフ時の取扱い、バックアップ
	モデル改善への利用	入力情報や生成結果がAIの改善に利用されるか	無料版・法人版の違い、利用停止設定、管理者による一括設定
	人による内容確認	提供者や委託先の担当者が内容を閲覧する可能性	閲覧目的、閲覧者の範囲、守秘義務、アクセス記録
委託・移転	再委託先での処理	他の事業者が保存、処理、監視等を担当するか	再委託先、処理内容、所在国、監督方法、変更時の通知
	国外への移転	データが日本国外で保存・処理・閲覧されるか	保存国、処理国、アクセス国、適用法令、開示請求への対応
セキュリティ	アクセス権限	誰がサービスやデータを利用・閲覧・変更できるか	会社管理アカウント、権限設定、退職・異動時の停止、最小権限
	暗号化	通信中・保存中のデータが保護されているか	通信・保存時の暗号化、暗号鍵の管理、バックアップの暗号化
	利用ログ	AIの利用・操作履歴を会社が確認できるか	ログイン、入力、出力、ファイル操作、設定変更、重要操作の記録
データ管理	削除方法	入力情報やファイル等を削除できるか	利用者・管理者による削除、完全削除までの期間、削除証明
組織管理	管理者設定	会社が利用方法を一括して統制できるか	モデル改善の停止、共有制限、機能制限、連携先制限、監視機能
契約管理	契約上の保証	安全性やデータの取扱いが契約に明記されているか	秘密保持、データの権利、事故通知、再委託、国外移転、責任分担
事業継続	障害発生時の対応	障害、誤動作、情報漏えい時の対応が定められているか	通知期限、窓口、原因調査、復旧、緊急停止、代替手段
	サービス終了時の対応	契約終了やサービス停止時にデータを移行・削除できるか	データ出力、移行期間、返却・削除、設定の移行、仕様・料金変更

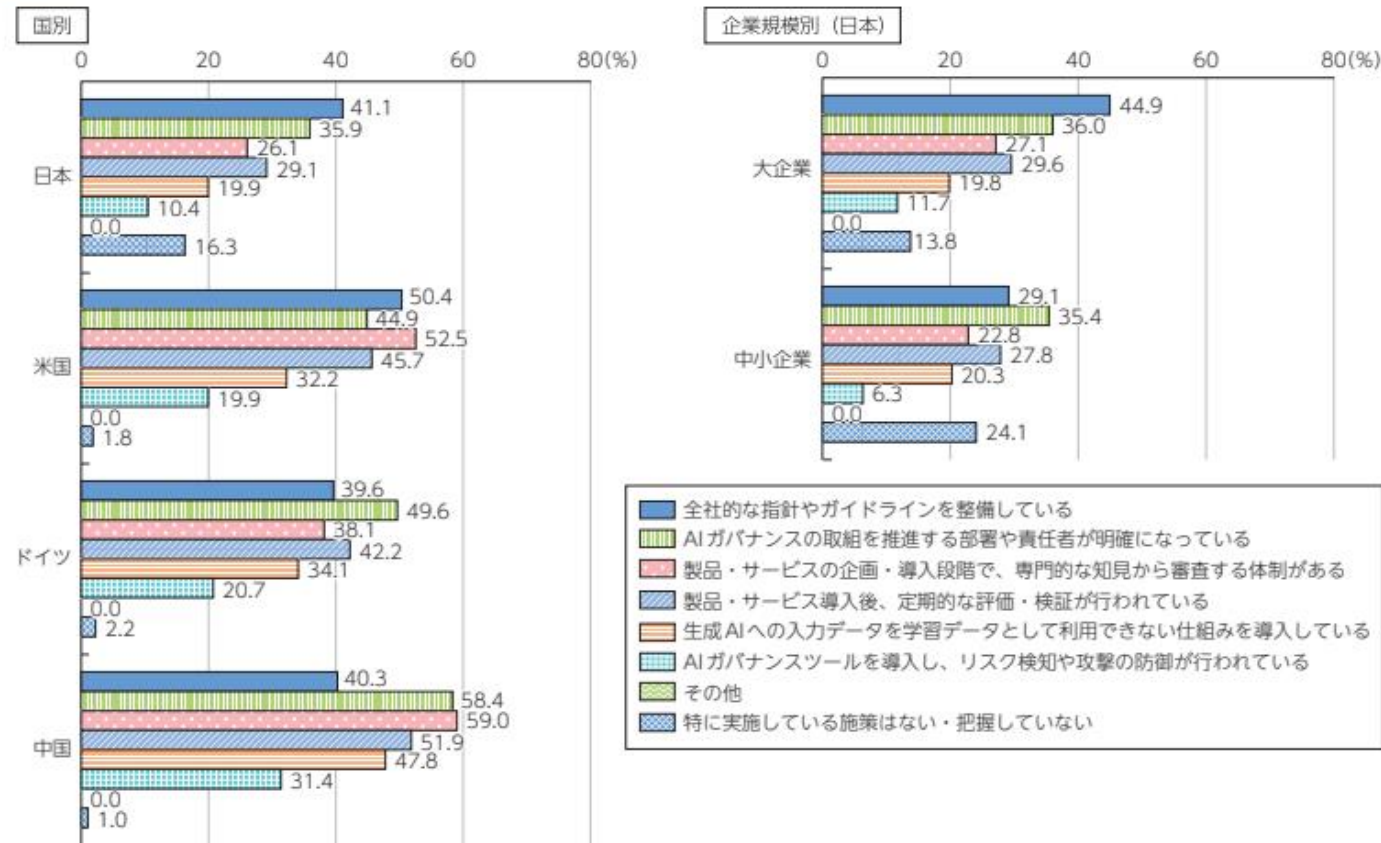


判定区分	考え方
利用可能	会社が安全性を確認し、通常業務での利用を認めたもの
条件付き利用	情報区分、用途、機能等に条件を付けて認めるもの
個別承認	利用前に個別に承認が必要なもの
利用禁止	リスクを会社が管理できないもの

結局Chat GPTやGeminiだった
それでも良いんです
検証したかしないかが違うのです

(参考) 他社はどんな取り組みが多い？

図表 I-2-1-9 リスク対策のための取組状況 (国別、企業規模別 (日本))



(出典) 総務省 (2026) 「国内外における最新の情報通信技術の研究開発及びデジタル活用の動向に関する調査研究」

ガイドライン策定
AIガバナンスの統制部門・責任者明確化
サービス導入時・導入後の評価検証
学習不可の仕組み導入
などなど

👉 は、AI導入の大先輩が行っていること

AIっていいね！本格的に使おう！という時には更にもう一歩進んだガバナンスを考えてください

4. ちょっとワーク

業務のリスクを考えてみましょう

ケースA：事業計画をレビューする

担当者がお客様の事業計画をブラッシュアップすべく、有料利用しているAIに事業計画の内容を読み込ませて、レビューをしてもらっています。

どんなリスクがありますか？

ケースB： 会議録の要約

担当者が、部門会議の録音データを無料AIにアップロードし、議事録を自動作成しようとしています

どんなリスクがありますか？

ケースC： AIエージェントにメール作成・送信まで任せる

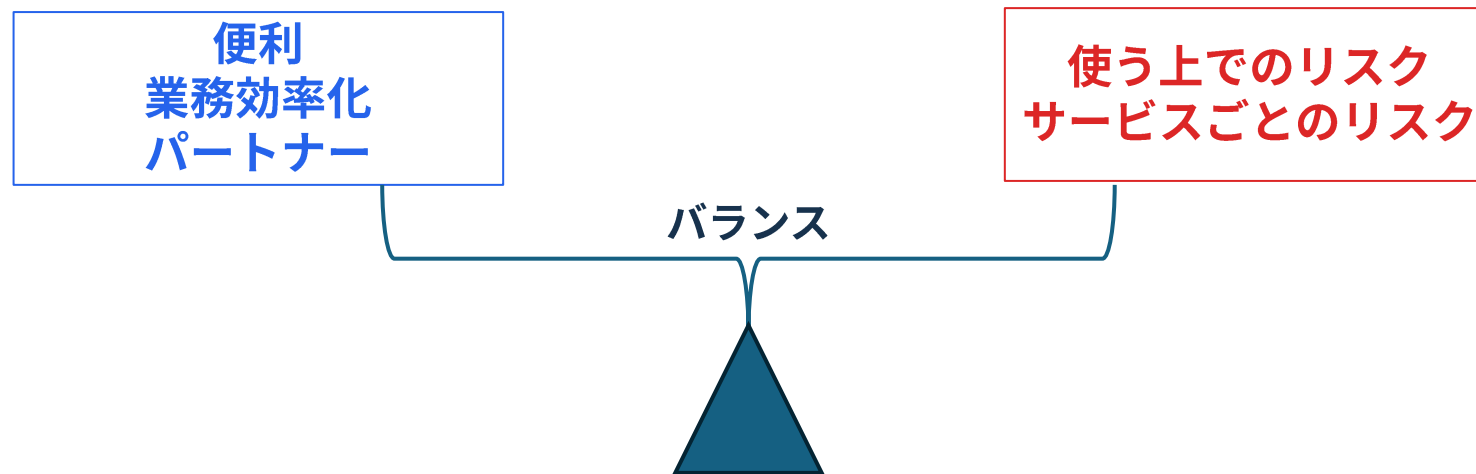
担当者が、顧客から来たメールをAIに読ませたうえで、返信メールをAIに作成させて、更にAIに送信までさせます。

どんなリスクがありますか？



5. 終わりに

AI時代のリスクマネジメント



リスクを知り、対策すれば最高のパートナー
大事なのは組織としてのリスクの考え方・対策の仕方・リスクの取り方

極論を言えば、組織がリスクを受容するか、利用できる場面を絞れば、無料の個人アカウントでも・・・

重要なのは無料・有料という区分だけではなく、情報・用途・契約・設定・管理方法を含めて組織が判断すること

**AIを使わないことが安全なのではありません。
ルールを決めずに使うことが危険です。**

適切なルールを整えれば、AIは情報漏えいのリスクではなく、業務の質と生産性を高める力になります。

参考情報

Googleの利用規約改訂（2026.7.30）

- ・ [検索サービス履歴] がオンになっているとメディアを保存する
- ・ 保存されたメディア（検索サービスを利用した際の画像、ファイル、音声、動画など）は、ユーザーの利便性につながります
- ・ 検索サービス履歴と保存されたメディアは、AIモデルや安全対策など、Googleのサービスの技術の開発と改善に使用されます

・・・???

例えば、

- ・ Googleレンズを使って翻訳した、何かを調べた、という履歴とGoogleレンズで撮影した画像がAI学習に使われる可能性があります

便利だと思って自然に使っている機能がAI学習に使われているかもしれません・・・

検索サービスの新しいプライバシー設定 [変更ドレミ](#)

Google <google-noreply@google.com>
To 自分 ▼

5月28日(木) 4:58

Google

さん

Google は、検索、マップ、ショッピング、ホテル、フライト、翻訳、ニュースなど、Google 検索サービス全体で、保存された履歴やパーソナライズされたおすすめ表示をさらに細かく管理できるよう、設定を更新しています。この変更は、数日以内に Google アカウントに反映されます。

変更点

これまで、履歴の保存とパーソナライズは、ウェブとアプリのアクティビティで管理されていました。今後は、より自分に合ったサービスを利用できるよう、2つの新しい設定（**検索サービス履歴とパーソナライズされたおすすめ表示**）で個別に管理できるようになります。これらの設定では、過去の検索内容を再確認したり、エクスペリエンスをカスタマイズするかどうかを決めたりできます。これらの設定の有効と無効はいつでも切り替えることができます。Google レンズで写真を検索するなど、新しい方法で検索するユーザーが増えているため、検索サービス履歴に、ユーザーが操作した際のメディアが含まれるようになりました。メディアの保存はいつでも停止できます。

この変更によるアカウントへの影響

- ・ **履歴とパーソナライズに関する新しい設定**: これらの新しい設定は、ウェブとアプリのアクティビティ設定および検索のパーソナライズ設定に関する直近の選択内容に基づきます。これらの設定が有効になっている場合は、新しい設定も有効になります。無効になっている場合は、新しい設定も無効になります。移行後は、ウェブとアプリのアクティビティと検索サービスの設定が分かれ、一方の変更がもう一方に影響することはありません。

- ・ **[検索サービス履歴] がオンになっている場合、メディアが保存されるようになります**: 保存されたメディア（検索サービスを利用した際の画像、ファイル、音声、動画など）は、ユーザー エクスペリエンスの向上に役立てられます。たとえば、過去にレンズで行った画像検索を再確認したり、聞いた曲についての検索 Live の会話を続けたりできます。このようなインタラクティブなサービス エクスペリエンスをサポートするため、Google はユーザーのメディアを検索サービス履歴に保存し、堅牢なプライバシーとセキュリティの保護を適用します。保存されたメディアも、検索サービス履歴と同様に、AI モデルや安全対策など、Google のサービスや技術の開発と改善に使用されます。今回の移行に伴い、[ウェブとアプリのアクティビティ] 設定が現在オンになっている場合、この新しい [メディアを保存] サブ設定も [検索サービス履歴] とあわせてオンになります。[[メディアを保存](#)] サブ設定はいつでもオフにできます。また、履歴から個々のメディアを削除することもできます。