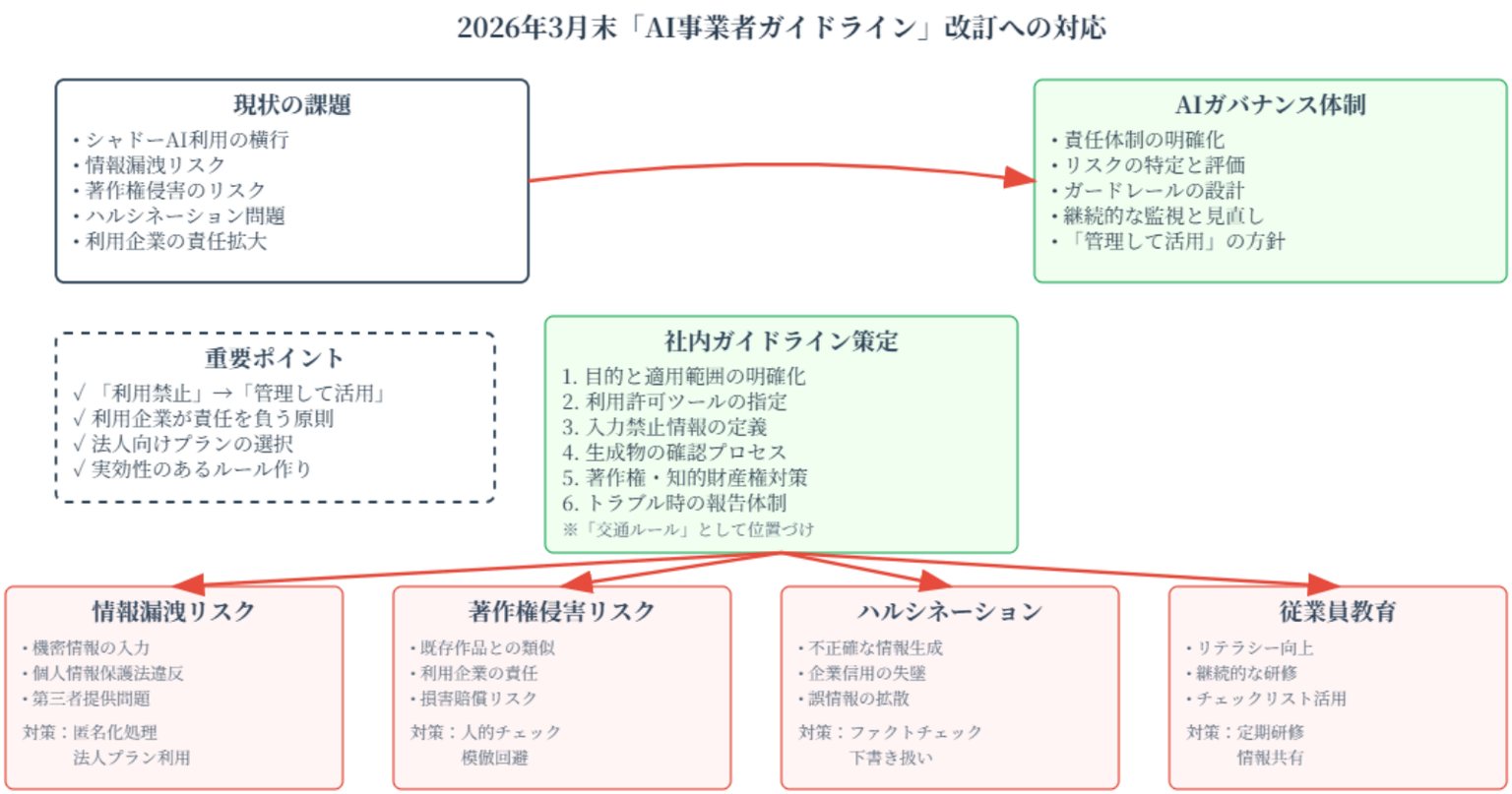
「AI事業者ガイドライン」の改訂（第1.2版）：単なる利用者（会社）でも必要な対応

Felo AI



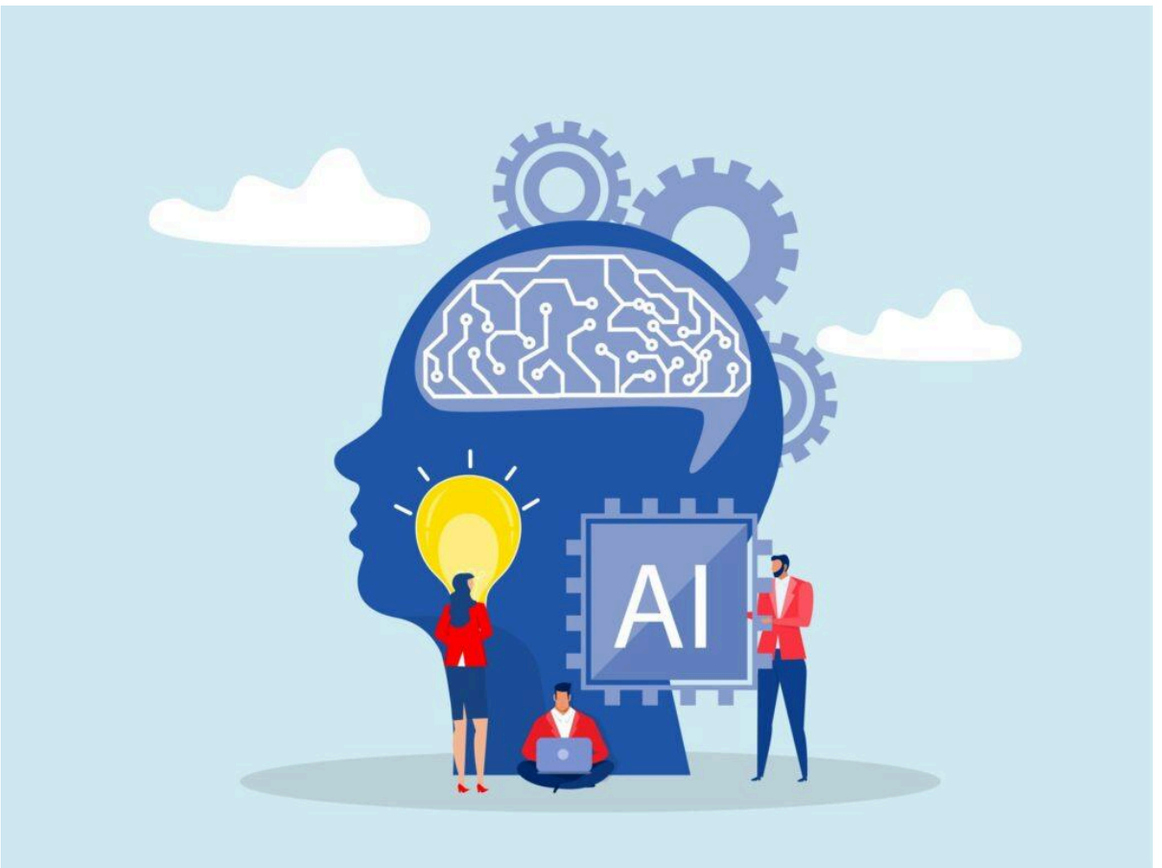
Overview

2026年3月末に予定されている「AI事業者ガイドライン」の改訂は、AIを開発・提供する事業者だけでなく、業務で生成AIを「利用」する企業にも重大な影響を及ぼします。今回の改訂は、生成AIや自律的にタスクを遂行する「AIエージェント」の急速な普及と、それに伴う情報漏洩、著作権侵害、ハルシネーション（誤情報生成）といった新たなリスクの顕在化に対応するものです[6] [12]。

単なるAI利用企業であっても、従業員の個人的な利用（シャドーIT）を含め、組織としての管理責任が問われる時代に突入しています[34] 。万が一、著作権侵害や情報漏洩が発生した場合、その責任はAI開発会社ではなく、AIを利用した企業自身が負うのが原則です[10] 。
このため、利用企業には、法的・倫理的リスクを管理し、AIを安全かつ効果的に活用するための「AIガバナンス」体制の構築が急務となります[6] [13] 。その中核となるのが、実効性のある「社内ガイドライン」の策定と運用です[18] [24] 。これは単なる「禁止リスト」ではなく、従業員が安心してAIの恩恵を享受するための「交通ルール」と位置づけ、利用目的の明確化、許諾ツールの指定、入力禁止情報の定義、生成物の確認プロセスなどを具体的に定める必要があります[20] [48] 。

詳細レポート

AIガバナンス体制の構築：単なる「利用禁止」から「管理して活用」へ



生成AIの導入において、リスクを恐れて全面的な「利用禁止」を選択することは、もはや競争戦略上の悪手と見なされています[34]。重要なのは、リスクを正確に理解し、それを管理・統制（ガバナンス）する体制を構築した上で、AIがもたらす生産性向上の恩恵を最大化することです[6] [13]。

AIガバナンスとは、企業がAI技術を法規制、倫理、社会的責任に則って適切に管理・運用するための枠組みを指します[6]。改訂されるAI事業者ガイドラインも、このリスクベースアプローチに基づく自主的なガバナンス構築を企業に求めています[12] [13]。
求められる主な取り組み:

- 責任体制の明確化: AIの利用に関する責任部署や担当者を明確に定めます[8]。
- リスクの特定と評価: 自社の業務内容に即して、情報漏洩、著作権侵害、ハルシネーションなどのリスクを洗い出し、その影響度を評価します[29] [43]。
- ガードレールの設計: 特定したリスクを低減するための具体的なルールや技術的制限（ガードレール）を設けます[6] [13]。
- 継続的な監視と見直し: AI技術の進化や新たなリスクの出現に対応するため、ガバナンス体制を定期的に見直し、改善していくプロセスを構築します[51]。

社内ガイドラインの策定と見直し：最も実践的な第一歩

AIガバナンスの中核をなし、企業が直ちに着手すべき最も重要な対策が、社内向け「生成AI利用ガイドライン」の策定です[18] [20] [24]。ガイドラインがない状態では、従業員が個人アカウントで機密情報を入力してしまうなど、管理不能な「シャドーAI」利用が横行し、リスクが野放しになります[20] [34]。
ガイドラインは、従業員が安全にAIを活用するための具体的な「ルールブック」として機能します[4]。策定にあたっては、以下の項目を網羅することが推奨されます[10] [20] [48]。

項目	内容とポイント
1. 目的と適用範囲	「禁止」ではなく「安全な活用」が目的であることを明記し、ポジティブなトーンで策定する。正社員、業務委託など、対象となる従業員の範囲を明確にする[20]。
2. 利用を許可するツール	会社として利用を許可するAIサービス（例：

項目	内容とポイント
	ChatGPT Enterprise, Microsoft Copilot）を具体的に指定する。セキュリティや契約内容が不透明なサービスは禁止リストに入れる20 32 。
3. 入力してはならない情報	個人情報（顧客・従業員）、取引先の機密情報、未公開の決算情報など、具体的な禁止事項をリストアップする。原則として、機密情報は匿名化・加工しない限り入力しないことを徹底させる16 26 47 。
4. 生成物の取り扱いと確認	AIの生成物は「下書き」または「参考資料」と位置づけ、必ず人間がファクトチェックや内容の検証を行うことを義務付ける8 54 。特に、著作権侵害のリスクを避けるため、生成物が他者のコンテンツと酷似していないか確認するプロセスを設ける10 。
5. 著作権・知的財産権	生成物が他者の著作権を侵害するリスク（依拠性・類似性）と、その場合の責任は利用者にあることを明記する。特定の作家風の画像を生成させるなどの行為はリスクが高いことを周知する10 11 。
6. トラブル発生時の報告体制	情報漏洩や権利侵害が疑われる事態が発生した場合の報告先（例：情報システム部、法務部）と報告フローを定めておく8 20 。

富士通などの企業も従業員向けのガイドラインを公開しており、これらを参考に自社の状況に合わせてカスタマイズすることが有効です28 57 。

利用するAIサービスの選定と契約内容の確認

従業員が利用する生成AIサービスを企業が管理することは、リスクコントロールの基本です。特に、無料プランや個人向けプランは、入力データがAIの学習に利用されたり（オプトアウト不可）、情報漏洩時の責任分界点が曖昧であったりするケースが多く、ビジネス利用には推奨されません16 。

サービス選定のポイント:

- 法人向けプランの選択: 多くの法人向け有料プランでは、入力データをAIの学習から除外する設定（オプトアウト）がデフォルトであり、秘密保持契約（NDA）やデータ処理契約（DPA）が締結されるため、情報管理と責任所在が明確になります16 。
- 利用規約の確認: AI生成物の著作権の帰属、商用利用の可否、学習データへの利用の有無など、利用規約を法務部門が精査することが不可欠です18 。
- ベンダーの信頼性: 第三者によるセキュリティ監査を受けているかなど、サービス提供者のガバナンス体制も選定の重要な基準となります27 。

主要リスクと具体的な対策

AI利用企業は、ガイドライン改訂で指摘される主要なリスクを理解し、具体的な対策を講じる必要があります。

1. 情報漏洩リスク

- リスク: 従業員がプロンプトに顧客の個人情報や社外秘の情報を入力し、それがAIの学習データとして取り込まれたり、外部サーバーから漏洩したりする2 25 。個人データの入力は個人情報保護法上の「第三者提供」に該当し、原則として本人の同意が必要となる可能性があります1 25 。
- 対策:
  - 社内ガイドラインで機密情報の入力を原則禁止する26 。
  - 入力が必要な場合は、個人名や企業名を仮名に置き換えるなどの「匿名化処理」を徹底する16 17 。
  - 入力データが学習に使われない法人向けプランを利用する16 27 。
  - 機密情報を自動で検知・マスキングするデータフィルタリング技術の導入を検討する27 。

2. 著作権・知的財産権侵害リスク

- リスク: AIが生成した文章や画像が、学習元となった既存の著作物と酷似しており、著作権者から権利侵害を主張される2 10 。この場合の法的責任は、AI開発者ではなく生成物を利用した企業が負うことになります10 。
- 対策:
  - 生成物は必ず人の目でチェックし、既存の作品と類似していないか確認する10 。
  - 特定のクリエイターの作風を模倣するようなプロンプトの使用を避ける11 。
  - 利用者が著作権侵害で訴えられた場合に法的責任を補償するプログラムを提供するAIサービス（例：一部の大手AI企業）の利用を検討する11 。
  - 生成物がAIによって作成されたことを明記するよう義務付ける18 。

3. 不正確な情報（ハルシネーション）のリスク

- リスク: 生成AIは、事実に基づかないもっともらしい嘘の情報を生成することがあります（ハルシネーション）8 。これを検証せずに顧客への提案書や公式な報告書に利用した場合、企業の信用を大きく損なう可能性があります8 40 。
- 対策:
  - AIの生成内容は必ず裏付けを取り、正確性を人間が担保する40 54 。

    - 社内ガイドラインで、AI生成物を「下書き」と位置づけ、最終的な責任は利用者が負うことを明確にする54 。
    - 正確性が求められる業務では、参照元を示す機能を持つAIサービスの利用を検討する。

従業員への教育と啓発

どれだけ優れたガイドラインやシステムを導入しても、それを使う従業員のリテラシーが低ければ形骸化してしまいます24 。全従業員を対象に、AI利用に伴うリスクや社内ルールに関する継続的な教育を実施することが不可欠です26 。

- 研修の実施: 生成AIの仕組み、具体的なリスク事例、社内ガイドラインの内容について、定期的に研修会を開催する31 。
- チェックリストの活用: AIを利用する前に確認すべき事項をまとめたチェックリストを作成し、従業員が自己点検できるようにする26 。
- 情報共有の徹底: 法改正やガイドラインの更新、新たな脅威に関する情報を社内で迅速に共有する体制を整える24 。

1. 生成AIと個人情報―法的論点と実務上の対策の概説
2. 生成AIを安全に使うには？ビジネスで注意すべきリスクと具体 ...
3. 生成AIのセキュリティリスクとは？具体的な対策方法をわかり ...
4. 生成AIガイドラインの作り方とは？リスク対策やひな形まで ...
5. 「生成 AI・AI エージェントの業務利用とリスク管理」に関する実態 ...
6. AIガバナンスとは？生成AI導入に必要な企業向け実務フレーム ...
7. AI活用における倫理問題とは？ 企業は何に留意すべきか
8. 法務担当者がおさえておくべき生成AI（Generative AI）の基礎
9. 生成AIサービスの利用に関する注意喚起等について
10. 生成AI利用で企業が負う著作権リスクと5つの実践対策
11. 生成AIのリスクを整理する｜3つの観点でリスクと対策を解説
12. 【2026年最新】AI事業者ガイドライン改訂の要点｜生成AI利用 ...
13. 生成AI活用のためのリスクマネジメント
14. 【業種別】生成AIの活用事例10選！導入時のポイントや注意点 ...
15. 生成AIに求められる倫理とは
16. 事業者が生成AIを利用する際の注意点と法的リスクを考察！
17. 生成AIと個人情報保護：安全な利用のための必須ガイド
18. 生成AIサービスの利用者が注意すべき法的ポイント
19. 生成AIのセキュリティリスクとは？企業が安全に利用するため ...
20. 生成AI利用のルールがまだない会社へ｜そのまま使える社内 ...
21. 生成AI、企業の76%が法務で活用 リスク管理が課題
22. 中小企業は生成AIをどう使う？ 課題と事例、おすすめツールを ...
23. 【専門家監修】生成AIの倫理的課題とガードレール
24. 【2026年最新】生成AIの法律問題とは？著作権やビジネス利用 ...

25. 生成AI利用時の個人情報漏洩を防ぐ方法｜企業が実施すべき ...
26. 生成AIを社内に導入するための「社内ポリシー」と運用ルール作り
27. 生成AI活用におけるセキュリティリスク対策の勘所
28. Fujitsu 生成AI利活用 ガイドライン
29. AIのリスクとは？ 企業が実施すべきリスク管理とガイドライン ...
30. 生成AI活用の第一歩：企業が策定すべきガイドラインとは？
31. 生成AIにおけるリスクと対策｜社会的な懸念や対処法について ...
32. “AIと法務” 生成AIの社内利用に関するルール作りのポイント
33. 生成AI活用時代のデータプライバシー完全ガイド
34. 生成AI活用の注意点/企業が直面する7つのリスクとガバナンス ...
35. 生成AI活用のリスクをどう防ぐか｜AIセキュリティの基礎
36. 会社の業務で使用するための生成AIの利用規定を作りたいです ...
37. 生成AI導入のリスク管理｜情報漏洩・ハルシネーション対策 ...
38. 生成AIの法規制とは？日本・海外の動向と安全に活用するため ...
39. 生成AIを利用する企業のセキュリティリスクと対策
40. 生成AIのビジネス活用におけるリスクと企業がとるべき対策を紹介
41. 生成AIに対するセキュリティ脅威と対策 第2回
42. 生成AIガイドライン策定ガイド！国・企業の実例10選や注意点 ...
43. AIリスク管理: AIシステムのセキュリティを確保するための総合 ...
44. 【中小企業向け】生成AI利用は著作権侵害になる？重要な法 ...
45. プライバシー保護と生成AIについて～セキュリティ ...
46. 生成AIの問題点とは？企業が直面するリスクと対策を徹底解説
47. 企業に広がる生成AI ～その導入、AIガバナンスとセキュリティは ...
48. 企業のAI利用ガイドライン策定ガイド｜社内ルールの作り方と ...
49. 国内外の規制動向を踏まえた生成AIの企業活用の留意点 ...
50. 生成AIはユーザーのデータをどう扱っているか－－主要9サービス ...
51. なぜ生成 AI は企業でうまく使えないのか？その原因と解決策 ...
52. 【2026年版】生成AIのセキュリティリスク対策ガイド
53. 【企業向け】生成AI社内ガイドライン策定の進め方と注意点
54. 小さな会社のための「生成AI利用ポリシー」のつくりかた【社内 ...
55. 生成AIの社内活用事例まとめ｜導入メリットや注意点まで ...
56. 情報漏えいだけじゃない！生成AIのセキュリティ課題と社内 ...
57. 生成AI利用ルールとは？ 安全な運用に役立つガイドラインの ...
58. 【中小企業必見】生成AI利用時の個人情報保護ガイド

59. 情報漏洩？企業における生成AI活用の落とし穴 ｜ DATA INSIGHT