ChatGPT

2026年AI事業者ガイドライン改訂が生成AI利用者に与える影響

エグゼクティブサマリ

2026年の改訂（「令和7年度更新内容（案）」として公表された更新案）は、従来の生成AIを含む一般的なAI利活用の枠組みに、**AIエージェント**および**フィジカルAI**といった「自律的に行動しうるAI」を明確に取り込み、加えて**リスクベースアプローチの説明追記**や参考文献の追加を通じて、ガイドライン運用の実務適用性を高める方向性が示されています。 [1]

生成AIを「利用する側（AI利用者）」にとって最も大きい変化は、単なる“生成結果の確認”に留まらず、**自律性が高いAI（エージェント／RAG連携／マルチモーダル等）を業務フローに組み込む際の統制設計**（人間の判断の介在、最小権限、ログ・記録、注意喚起・説明、インシデント対応）を“前提”として求められやすくなる点です。 [2]

一方で、AI事業者ガイドライン自体は、基本的に**「Living　Document」としての継続更新**と、事業者による**自主的取組**を前提とするソフトローの性格が強く、明示の「施行日」「直罰」は（少なくとも第1.1版および更新案の公開情報からは）確認できません。したがって、影響は「新たな法的義務の瞬間的発生」というより、**調達・契約・監査・説明責任の“共通言語”が更新される**ことで、企業実務上の期待水準が上がる形で現れます。 [3]

実務担当者向けの結論として、短期的には（1）ユースケース棚卸しと役割区分（開発者／提供者／利用者のどれに該当するか）明確化、（2）入力データ統制（個人情報・機密情報・著作物等）と外部サービスの学習利用設定の確認、（3）人間の判断を必須化するレビュー工程の設計、（4）ログ・記録とインシデント報告導線の整備、（5）契約条項（学習利用、保持期間、監査・説明、責任分配）見直し、が優先です。これらは個人情報保護委員会の注意喚起（生成AIへ個人データを入力する場合の適法性・確認事項）とも整合します。 [4]

適用範囲と前提

対象範囲と適用開始時期

AI事業者ガイドライン（第1.1版）では、事業としてAIの開発・提供・利用を担う主体を主たる対象とし、政府・自治体等の公的機関も含みます。他方で、事業活動以外で利用する者や便益を享受／損失を被り得る者（業務外利用者）は「対象に含まない」としつつ、事業者から業務外利用者への必要な対応は記載する、という整理です。また、データ提供者も対象外とされています。 [5]

2026年更新案で追加されたAIエージェント／フィジカルAIの定義は、同ガイドラインの枠内（事業者向けのガバナンス指針）に、より自律性・物理的作用を持つAIを含める意図と整合します。 [1]

適用開始時期（施行日）は、公開情報上は**未指定**です（ガイドライン自体がLiving　Documentとして随時更新される前提であり、法令のような施行日設計ではないため）。 [6]

本レポートの分析前提

本レポートは、（a）第1.1版の本文・別添（実践）に記載された「AI利用者」向け指針、（b）2026年3月10日付の政府資料に引用された「令和7年度更新内容（案）」の抜粋、（c）個人情報・知財等の関連政府資料、（d）主要クラウド／生成AI提供者のデータ取扱い方針、（e）業界団体資料を根拠に、生成AI利用者への影響を実務観点で整理しています。 [7]
更新案は「案」であり、最終版で内容が変更される可能性があるため、更新案の全文で確認できない事項は**未指定**として扱います。 [1]

考慮すべき属性・観点

生成AI利用者が影響評価を行う際、少なくとも以下の属性を区別すると、リスクベースの優先順位付けが可能になります（組織ごとの前提により追加が必要です）。 [8]

- 役割：自社が「AI利用者」に留まるか、外部提供まで行い「AI提供者」も兼ねるか（同一事業者が複数役割を兼ねる可能性を前提）。 [9]
- 自律性：チャット補助／RAG／ツール実行を伴うエージェント／物理環境へ作用するフィジカルAI。 [1]
- データ種別：個人情報（要配慮含む）・顧客データ・機密情報・著作物・社内文書・ログ等。 [10]
- 対象業務：生命・安全・権利利益に影響が大きい領域（教育、金融等）か、低リスクの事務作業か。 [11]
- 出力の利用形態：意思決定補助か、対外公表物（広告・広報・契約文書等）か、個人評価（採用・人事等）か。 [12]
- 透明性要件：AI利用の通知、生成物表示（ラベル／透かし等）、根拠提示（RAGの参照元提示等）。 [13]
- セキュリティ脅威：プロンプトインジェクション、DoS等（生成AI特有の脅威を含む）への耐性。 [14]
- 記録・監査：ログ取得可否、保存期間、説明責任に足る証跡の設計。 [15]
- 外部提供者のデータ取扱い：学習利用の有無、保持期間、オプトアウト、第三者提供、越境移転等。 [16]

主要変更点と条文要旨

主要変更点と利用者影響の対照表

以下の表は、更新案で明示された変更（確定情報）と、第1.1版における該当箇所（条文要旨＝指針・行動項目の要旨）を突き合わせ、生成AI利用者の実務影響へ翻訳したものです。更新案の全文で未確認の部分は**未指定**としています。 [17]

観点	2026年更新案の主旨（確認できた範囲）	第1.1版の条文要旨（該当箇所例）	実務上の意味（生成AI利用者）	推奨対応策（利用者側）
責任分配	AIエージェント／フィジカルAIを定義として追加。用語や主体区分の整理、（アライメントやRAG等で）どの主体が責任を担うか補足が加えられた旨が報じられている。 [1]	AI開発者・AI提供者・AI利用者を定義し、同一事業者が複数役割を兼ね得るとする。AI利用者は提供者の想定範囲内で適正利用し、業務外利用者に影響がある場合は不利益回避・便益最大化に努める。 [18]	「利用者」として使っているつもりでも、RAGで社内DBを繋ぎ外部に回答する等で実質「提供者」責任が発生しうる。責任境界が曖昧だと事故・漏えい時の説明が破綻する。 [9]	役割（利用者／提供者／開発者）をユースケース単位で再分類し、責任分界（仕様・運用・監視・インシデント対応）を契約・社内規程に落とす。
説明責任・説明可能性	リスクベースの説明追記、参考文献（EU高リスク類型等）追加。 [1]	AI利用者は、関連ステークホルダーに合理的範囲で情報提供し、問い合わせ窓口を設置し、求めに応じ説明責任を果たす。提供者から提供された文書を保管・活用し規約遵守。 [19]	「なぜその回答になったか」「誰が責任者か」を問われる頻度が増える。説明の元データ（プロンプト、参照元、ワークフロー）がないと監査・紛争対応コストが急増。 [20]	重要業務はRAG参照元や判断ログを含む“説明パッケージ”を設計。問い合わせ窓口とエスカレーションを明文化。
データ利用・学習データ	多義的な用語（学習／推論／データ）の定義明確化が進む旨が報じられている。 [21]	提供者は、学習データ収集ポリシー等の情報提供を行い、利用者に適正利用を促す注意喚起（正確性・最新性、コンテキスト内学習、個人情報入力等）を行う。 [22]	生成AI利用者は「入力が学習に使われるか」をサービスごとに確認しないと、個人情報保護法違反や機密漏えいを招く。 [23]	ベンダー評価項目に「学習利用（opt-in/opt-out）」「保持期間」「第三者提供」「越境移転」を追加し、調達チェックリスト化。 [24]
透明性表示	参考文献としてEUの高リスク類型（Annex III）等を追加。 [25]	透明性を広く「情報開示」に関する事項として整理し、AI生成物の識別（電子透かし等）も国際指針として言及。 [26]	対外向けコンテンツや顧客対応で、AI生成・AI介在の表示要請が高まる。EU等域外規制や取引先要件で“準義務化”しやすい。 [27]	「AI生成」表示基準（いつ・どこにラベル／注記するか）を業務別に標準化。出典提示（RAG参照元）をUXに組み込む。 [28]

観点	2026年更新案の主旨（確認できた範囲）	第1.1版の条文要旨（該当箇所例）	実務上の意味（生成AI利用者）	推奨対応策（利用者側）
利用者への注意喚起義務	リスク具体化（ハルシネーションや教育領域リスク、RAGプライバシー等）の記載が盛り込まれた旨が報じられている。 [21]	提供者は正確性・最新性、コンテキスト内学習、不適切な個人情報入力等を注意喚起。利用者は提供者の留意点を守り、出力の精度・リスクを理解して利用。 [22]	「注意書き」だけでは不十分になり、教育・人事・金融等では“プロセスとしての注意喚起”（同意、訓練、レビュー）が求められる。 [29]	重要領域は、①ユーザー教育、②同意取得、③レビュー（人間の判断）をセットで設計。注意喚起をUI/運用に埋め込む。
セキュリティ・安全対策	生成AI特有の脅威（プロンプトインジェクション、DoS等）と対策（ガードレール、RAG等の権限管理）を扱う技術ガイドライン（案）が政府資料で紹介。 [25]	利用者は提供者のセキュリティ留意点を遵守し、機密情報等の不適切入力を避ける。別添では侵害時の初動（ロールバック、停止、遮断、報告）等を例示。 [30]	RAGやエージェント導入は“新しい攻撃面”を増やす。従来の情報セキュリティ統制だけでは不足し、生成AI向けガードレール・権限設計・監視が必要。 [31]	最小権限、外部参照データ検証、プロンプト注入対策、キルスイッチ、インシデント報告導線を設計。
個人情報保護	RAGやマルチモーダル活用時のプライバシーリスクが盛り込まれた旨が報じられている。 [21]	利用者は個人情報の不適切入力を避け、プライバシー侵害情報を収集し防止を検討。 [12]	個人情報を含むプロンプト入力は、利用目的逸脱・同意欠如・学習利用等で法令違反となり得る。提供者側の取扱い確認が必須。 [32]	個人データ入力が必要な業務は、(1)目的内/最小限の確認、(2)学習利用しない設定・契約確認、(3)匿名化・仮名化・DLP導入を標準化。 [33]
著作権・知財	知財・透明性に関するプリンシプル・コード（案）の動向が政府資料で紹介（生成AI事業者を対象、comply-or-explain）。 [34]	第1.1版は、データ類型に応じ個人情報・知的財産権等の法令適合が必要とする。 [35]	利用者側は「出力が侵害しないか」を目視確認するだけでは限界があるため、プロンプト設計・用途制限・素材管理・出典管理等のプロセス設計へ重心が移る。 [36]	生成物の利用ルール（素材の出所、似せる指示の禁止、公開前チェック、権利処理）を業務別に整備。ベンダーには透明性・権利侵害対応窓口を要求。 [37]
監査・報告義務	（更新案自体の“義務化”は未確認＝未指定）ただし、参照文献やツール整備（活用ガイド、チャットボット等）の検討が報じられている。 [1]	本編・別添でログ記録・保存や、インシデントの文書化・報告、ステークホルダーへの情報共有が推奨される。 [38]	監査対応は法的義務でなくても、取引先監査・内部監査・事故対応で必要になる。ベンダー側のログ保持が短い場合、利用者側で補完が必要。 [39]	監査証跡の最小セット（プロンプト、参照元、権限、実行ログ、レビュー記録、版管理）を定義し、保存設計（未指定の場合は方針策定）を行う。

観点	2026年更新案の主旨（確認できた範囲）	第1.1版の条文要旨（該当箇所例）	実務上の意味（生成AI利用者）	推奨対応策（利用者側）
罰則・行政指導	ガイドライン自体の罰則は未指定（ソフトローとしての運用が前提）。[40]	ガイドラインは自主的取組の参考。社会から不適切と評価されれば機会損失等のリスクがある旨を明記。[40]	直罰はなくても、個人情報保護法等の既存法令で行政対応が起こり得る。実際に個人情報保護委員会は生成AI提供者に注意喚起を実施。[32]	“ガイドライン不遵守＝違法”ではない前提を社内共有しつつ、既存法令でのリスク（個人情報、著作権、秘密情報等）を中心にコンプラ統制を組む。[41]

生成AI利用者への影響分析

法的リスク

個人情報については、個人情報取扱事業者が生成AIに個人情報を含むプロンプトを入力する場合、**利用目的の達成に必要な範囲内か**を十分確認すべきであり、本人同意なく個人データを入力し、それが「応答出力以外の目的」で取り扱われる場合には**個人情報保護法違反となる可能性**があるため、提供者が機械学習に利用しないこと等を十分確認するよう注意喚起されています。[42]
この整理は、生成AI利用者にとって「データ入力可否の社内ルール」は、単に“機密だから禁止”ではなく、**目的・同意・提供者の取扱い（学習利用／保持）を含む要件定義**に移行することを示唆します。[43]

著作権・知財では、文化庁の「AIと著作権に関する考え方について」が、現行著作権法の解釈整理として公表されており（法的拘束力は持たない旨も明記）、判例の蓄積等に応じて見直し予定とされています。[44]
実務としては、生成物の個別確認には限界があるため、JDLAが指摘するように「使い方（プロセス／プロンプト設計／社内ルール）の整理」で侵害リスクを低減する方向が合理的になり得ます。[45]

運用負担

第1.1版のAI利用者向け指針では、提供者の留意点を守って想定範囲内で利用し、入力データの正確性・必要な場合の最新性を担保し、出力の精度とリスクを理解して利用すること、個人情報や機密情報の不適切入力を避けること等が明確に列挙されています。[30]
更新案はAIエージェント／フィジカルAIのような自律性の高いAIを想定に入れるため、運用負担は「利用者教育と注意書き」だけでなく、**権限・レビュー・監視・復旧**の工程を含む運用設計へ拡大する可能性が高いです。[1]

コスト影響

工数・コストの公的な統一見積は**未指定**です（組織規模、ユースケース、既存統制、外部委託範囲で大きく変動）。[46]
ただし、コストが増えやすい要素として、（a）RAGやエージェント導入に伴う権限管理・ガードレール・監視、（b）ログ・証跡基盤、（c）社内教育、（d）契約・審査体制（法務・セキュリティ・監査）の常設化、が挙げられます。[31]

サービス設計・利用フロー変更

AI利用者は、出力を事業判断に活用した際に合理的範囲で情報提供を行うこと、個人評価に利用する場合にはAI利用を通知し、求めに応じ説明責任を果たすことが求められています。[12]

この指針は、生成AIのUI/UX上、少なくとも「AIが関与していることの通知」「参照元と制約の提示」「人間の最終確認」「問い合わせ窓口」が一体として設計されるべきことを意味します。[47]

また、RAGはハルシネーション抑制や根拠の透明性向上、コスト低減が期待される一方、間接プロンプトインジェクション等の悪用リスクがあり、参照データの適切取扱いや管理・監査の必要性も指摘されています。[48]
このため、RAGやエージェントを採用する場合は「検索・参照データの検証」「権限管理」「外部参照データのガードレール」が設計要件になります。[49]

契約・利用規約の改定

外部の生成AIサービスに依存するほど、契約と設定確認がリスク低減の実体になります。個人情報保護委員会は、同意なく個人データを入力する場合に、提供者が当該個人データを機械学習に利用しないこと等を十分確認するよう求めています。[42]
さらに、JDLAは生成AI開発の外部委託において、ユーザ・ベンダ間の契約締結を円滑化するための契約ガイドライン（ひな形を含む）を公開しています。[50]
利用者としては「学習利用（オプトイン／アウト）」「保持期間」「監査・説明」「侵害申立て対応」「責任制限」「再委託（サブプロセッサ）」等を条項・SLA・運用で詰める必要があります。[51]

コンプライアンス体制・ユーザー教育・同意取得

更新案は用語定義や主体区分の整理を含むとされ、実務担当者が使える形（活用ガイドやチャットボット検討）に寄せる方向性が示唆されています。[52]
これは、生成AIの利用統制を「現場任せ」にせず、**標準実務（説明、権限、記録、教育）**として運用に落とす必要が高まっていることを意味します。[53]

ログ・記録保存要件

第1.1版別添では、検証可能性確保のためのログ記録・保存（目的、精度、頻度、保存期間、保護等の考慮事項）が具体例として提示されています。[54]
加えて、生成AIサービス側のログ保持が短い場合、利用者側の規程や監査要件に合わせるには自社での補完が必要になります。例えば、OpenAI[55]のAPIでは「APIデータは学習に使わない（明示的オプトイン除く）」一方で、乱用監視ログが既定で最大30日保持される旨が明記されています。[56]
同様に、Amazon Web Services[57]の生成AI関連サービスでは、サービスによって「学習等に利用され得るため組織単位でオプトアウト可能」とする設計があり、オプトアウト時に過去の関連コンテンツが削除される（機能提供に必要なものを除く）旨も説明されています。[58]
したがって「どのログを、どこで、どの期間」保持するかは、利用者側の統制設計（未指定の場合は方針策定）が不可欠です。[59]

業種別影響と具体例

業種別影響サマリ表

業種	典型ユースケース	主要リスク（改訂で顕在化しやすい点）	実務上の要点（利用者側）
教育	教職員の校務支援（教材・文書たたき台）、学習支援	誤情報（ハルシネーション）、偏り、思考力への影響、著作権・セキュリティ等の幅広い論点	文科省ガイドラインに沿った場面別ルール・チェック項目整備。児童生徒向けは特に「目的・禁止事項・指導」をプロセス化。[60]

業種	典型ユースケース	主要リスク（改訂で顕在化しやすい点）	実務上の要点（利用者側）
医療	文書作成補助、院内QA、問い合わせ一次対応	要配慮情報の取扱い、学習利用・再出力、誤回答による安全リスク	個人情報取扱いの厳格化（目的内・最小限・学習利用しない確認）。人間の最終確認を必須化し、院内での権限分離とログを整備。 [4]
金融	顧客対応、文書作成、リスク分析補助	ディープフェイク等で詐欺が容易化、既存対策を超える脅威、AIガバナンス構築の必要性	金融庁資料が示すように、生成AI導入ルールを整備し既存フレームへ接続。高リスク用途は評価基準・監督・記録を強化。 [61]
クリエイティブ	画像・文章生成、広告素材、企画案	侵害判断の難しさ、透明性要求、権利者からの開示要求	文化庁の考え方（非拘束）を踏まえた注意事項整備。個別確認依存からプロセス統制へ。プリンシプル・コード（案）の動向も取引要件化し得る。 [62]
カスタマーサポート	RAGでFAQ・ナレッジ連携、エージェントで手続自動化	プロンプトインジェクション、参照データ漏えい、誤回答の拡散	外部参照データの検証・権限管理・ガードレールを実装し、回答の根拠提示を設計。インシデント対応（停止・遮断・報告）を準備。 [31]

具体例（実務で起きやすい“変更点の効き方”）

教育領域では、文科省ガイドラインが「利活用は一律に禁止／義務付けではない」としつつ、学校現場が混乱しないための実務ポイント（チェック項目、リスク例等）を提示しています。更新案が示す「教育領域で思考力発展を妨げる可能性」といった観点は、まさに“授業・評価・校務”の区分や指導計画に落とすべき論点です。 [60]

金融領域では、金融庁の資料が、ディープフェイク等により本人確認等がすり抜けられるリスクや、既存対策だけでは対応しきれない規模の脅威になり得る点を挙げています。更新案がセキュリティ／リスクの具体化へ進むほど、金融機関は監督・監査の観点から、ログ・評価・権限管理の“基準化”を求められやすくなります。 [63]

クリエイティブ領域では、権利侵害リスクに対して「生成物の目視確認」に依存する運用は限界があるというJDLAの整理が、利用者側の現実的な統制設計（プロンプト／素材／公開前レビュー／権利者対応窓口）へ直結します。 [64]

移行計画と推奨対応策

対応優先度の考え方

ガイドラインはLiving　Documentとして更新され、社会から不十分と評価される場合に機会損失等を招き得ることが明記されています。したがって、優先順位は「法令違反の回避」だけでなく、「説明責任・取引要件・事故対応」を含む実務コスト最小化の観点で付けるのが合理的です。 [65]

短期・中期・長期の推奨タスク一覧

工数・コストは、公式な統一見積がないため**未指定**とし、相対的な難易度（小/中/大）のみを付しています。

期間	推奨タスク（利用者側）	目的	工数	コスト
短期	ユースケース棚卸し（どの業務で、どのデータを、どのAIで扱うか）	適用役割・規制論点の確定	中	未指定
短期	役割区分の明確化（利用者／提供者の兼務有無）と責任分界の文書化	事故時の説明可能性	中	未指定
短期	入力データ統制（個人情報・機密情報・著作物）とDLP/アクセス制御	漏えい・違反予防	中〜大	未指定
短期	外部サービスの「学習利用・保持期間・ログ」確認（設定＋契約）	個人情報・秘密情報リスク低減	小〜中	未指定
短期	人間の判断を必須化するレビュー工程（高リスク領域から）	誤回答・不利益の抑止	中	未指定
中期	RAG/エージェント導入時の最小権限・ガードレール・参照データ検証	生成AI特有脅威への対応	大	未指定
中期	ログ・証跡設計（プロンプト、参照元、権限、実行、レビュー、版管理）	監査・紛争・品質改善	中〜大	未指定
中期	インシデント対応計画（停止・遮断・復旧・通知・報告）訓練	被害最小化	中	未指定
中期	契約・利用規約改定（学習利用、透明性、権利侵害対応、責任制限等）	取引条件の安定化	中	未指定
長期	継続的モニタリングと定期レビュー（更新への追随）	Living Document対応	中	未指定
長期	組織体制の高度化（CAIO相当機能、教育、人材、調達統合）	ROI最大化とリスク低減の両立	大	未指定

上記は、AI利用者に対して「提供者の留意点を守り、出力リスクを理解し、個人情報・機密情報の入力を避け、説明責任を果たす」などを求める第1.1版の要請を、実装タスクへ落とし込んだものです。[66]
外部サービスのデータ取扱い確認については、例えば以下のように主要提供者が「学習に使わない」または「企業向けは域外学習しない」旨を明示している一方、ログ保持やオプトアウトの仕組みがサービスにより異なるため、調達・設定の標準化が実務上の要になります。[67]

- OpenAI[55]：企業向けは既定で学習に使わない、APIの乱用監視ログは既定で最大30日保持等。[68]
- Microsoft[69]：商用のCopilotではデータが基盤モデル学習に使われない旨等。[70]
- Google[71]：WorkspaceのGeminiはドメイン外の学習利用をしない旨と、無ライセンス利用時の注意点を明示。[72]
- Amazon Web Services[57]：Bedrockはプロンプト／補完を学習に使わない旨。サービスによっては組織単位のAIオプトアウト政策を提供。[73]

対応優先度タイムライン（例）

下図は「正式版公表をT0」とする相対タイムライン例です。正式版公表日・移行期間が公式に示されていないため、日付は便宜的な目安であり、**適用開始時期は未指定**です。[46]

```
gantt
    title 生成AI利用者の対応優先度タイムライン（例：T0=正式版公表）
    dateFormat  YYYY-MM-DD
    axisFormat  %Y-%m

    section 短期（T0〜2か月）
    ユースケース棚卸し・役割区分・暫定ルール策定 :a1, 2026-04-01, 30d
    外部サービスの学習利用/保持/ログ確認（設定・契約） :a2, 2026-04-01, 30d
    高リスク業務の人間レビュー必須化（暫定） :a3, 2026-04-15, 45d

    section 中期（T0+3〜6か月）
    RAG/エージェントの最小権限・ガードレール実装 :b1, 2026-06-01, 90d
    ログ・証跡基盤（保存・検索・権限制御）整備 :b2, 2026-06-01, 90d
    インシデント対応訓練（停止・遮断・報告） :b3, 2026-07-01, 60d

    section 長期（T0+6〜12か月）
    監査・定期レビュー（運用KPI/教育/契約更新） :c1, 2026-09-01, 180d
    体制高度化（CAIO相当機能/調達統合/継続改善） :c2, 2026-09-01, 180d
```

推奨フローチャート（リスクベース運用）

更新案が明示するリスクベースアプローチの追記と、第1.1版の「適正利用・説明・記録・セキュリティ」要求を、実装フローに落とすと以下の形になります。 [74]

```
flowchart TD
    A[ユースケース棚卸し] --> B[役割区分の確定: 利用者/提供者/開発者]
    B --> C[リスク分類: データ種別×自律性×影響領域]
    C --> D[統制設計]
    D --> D1[入力データ統制: 個人/機密/著作物]
    D --> D2[権限設計: 最小権限・分離]
    D --> D3[人間レビュー: 高リスク必須]
    D --> D4[ログ/証跡: プロンプト・参照元・実行]
    D --> D5[透明性: 通知/表示/根拠提示]
    D --> E[導入・運用]
    E --> F[監視・品質評価]
    F --> G[インシデント対応: 停止・遮断・報告・再発防止]
    G --> H[定期レビュー/ルール更新]
    H --> C
```

主要根拠URL

```
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/80174015-
f73b-4d98-811e-c601c26c0ba5/c0a1cfcc/20260310_meeting_ai-advisory_%20outline_02.pdf
https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20250328_1.pdf
https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20250328_3.pdf
https://www.ppc.go.jp/files/pdf/230602_alert_generative_AI_service.pdf
https://www.ppc.go.jp/files/pdf/230602_alert_AI_utilize.pdf
https://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kousou/2026/dai2/shiryo1.pdf
```

```
https://openai.com/enterprise-privacy/
https://developers.openai.com/api/docs/guides/your-data/
https://learn.microsoft.com/en-us/copilot/microsoft-365/enterprise-data-protection
https://knowledge.workspace.google.com/admin/gemini/gemini-for-google-workspace-faq
https://docs.aws.amazon.com/bedrock/latest/userguide/data-protection.html
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_ai-opt-out.html
https://www.mext.go.jp/content/20241226-mxt_shuukyo02-000030823_001.pdf
https://www.fsa.go.jp/news/r6/sonota/20250304/aidp_summary.pdf
https://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/pdf/94037901_01.pdf
https://www.jdla.org/news/20260203001/
https://www.jdla.org/news/20250919001-2/
https://it-trend.jp/news/01-009
```

---

1 8 14 17 25 27 31 34 46 49 69 74 https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/80174015-f73b-4d98-811e-c601c26c0ba5/c0a1cfcc/20260310_meeting_ai-advisory_%20outline_02.pdf
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/80174015-f73b-4d98-811e-c601c26c0ba5/c0a1cfcc/20260310_meeting_ai-advisory_%20outline_02.pdf

2 21 52 https://it-trend.jp/news/01-009
https://it-trend.jp/news/01-009

3 5 6 7 9 10 12 13 18 19 20 22 26 30 35 40 47 53 57 65 66 https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20250328_1.pdf
https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20250328_1.pdf

4 23 32 33 41 42 43 https://www.ppc.go.jp/files/pdf/230602_alert_generative_AI_service.pdf
https://www.ppc.go.jp/files/pdf/230602_alert_generative_AI_service.pdf

11 61 63 https://www.fsa.go.jp/news/r6/sonota/20250304/aidp_summary.pdf
https://www.fsa.go.jp/news/r6/sonota/20250304/aidp_summary.pdf

15 16 24 39 55 56 https://developers.openai.com/api/docs/guides/your-data/
https://developers.openai.com/api/docs/guides/your-data/

28 38 48 54 59 https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20250328_3.pdf
https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20250328_3.pdf

29 60 https://www.mext.go.jp/content/20241226-mxt_shuukyo02-000030823_001.pdf
https://www.mext.go.jp/content/20241226-mxt_shuukyo02-000030823_001.pdf

36 45 64 71 https://www.jdla.org/news/20260203001/
https://www.jdla.org/news/20260203001/

37 https://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kousou/2026/dai2/shiryo1.pdf
https://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kousou/2026/dai2/shiryo1.pdf

44 62 https://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/pdf/94037901_01.pdf
https://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/pdf/94037901_01.pdf

50 51 https://www.jdla.org/news/20250919001-2/
https://www.jdla.org/news/20250919001-2/

58 https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_ai-opt-out.html
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_ai-opt-out.html

67 68 https://openai.com/enterprise-privacy/
https://openai.com/enterprise-privacy/

70 https://learn.microsoft.com/en-us/copilot/microsoft-365/enterprise-data-protection
https://learn.microsoft.com/en-us/copilot/microsoft-365/enterprise-data-protection

72 https://support.google.com/a?hl=en&p=gemini_terms
https://support.google.com/a?hl=en&p=gemini_terms

73 https://docs.aws.amazon.com/bedrock/latest/userguide/data-protection.html
https://docs.aws.amazon.com/bedrock/latest/userguide/data-protection.html