社外秘

生成AI利活用ガイドライン

Generative AI Usage Guidelines

版数	第1.0版
制定・改定日	YYYY年M月D日
次回改定	次回改定時期
適用範囲	全社（グループ会社・業務委託先を含む）
管理部門	情報システム部 / DX推進室
利用スタンス	標準運用

作 成	確 認	承 認
情報システム部 / DX推進室	AI管理委員会	代表取締役

本ガイドラインは、総務省・経済産業省「AI事業者ガイドライン（第1.2版）」、内閣府「人工知能関連技術の研究開発及び活用の推進に関する法律（AI推進法）」「人工知能基本計画」、デジタル庁「行政の進化と革新のための生成AIの調達・利活用に係るガイドライン（第2.0版）」、EU AI Act 等を参照して策定している。

このテンプレートの使い方

本書は、どの企業でも下敷きにできる生成AI利活用ガイドラインの雛形です。次の3つの手順で自社の文書に仕上げてください。仕上げたら、このページは削除します。

1. **色の付いた記入欄を埋める。**会社名、日付、部門名、問い合わせ先など、この色で示した箇所へ自社の情報を入れます。
2. **編集メモに従って直す。**本文中の「編集メモ」は差し替えの指示です。反映したら、その行を削除します。
3. **関係のない章と行を削る。**業種別の留意事項、海外規制、調達、コストの章などは、章ごと削除して構いません。ジェネレーター（指針工房）で章を外すと、目次と章番号と章どうしの参照は自動で振り直されます。手作業で削る場合は番号を振り直してください。

> **法令と数値の扱い**
>
> 第1章の参考法令や、ログの保存期間、報告の期限などの数値は、本書を作った時点の一般的な目安です。配布する前に、自社の規程と最新の法令を確かめて調整してください。

目次

1. はじめに
2. 生成AIの基礎知識
3. 適用範囲と対象者
4. 用語の定義
5. 基本原則
6. 利用ルール
7. データ取扱いルール
8. 生成物の品質管理
9. 著作権・知的財産権
10. AIエージェント利用ルール
11. セキュリティ
12. プライバシー保護
13. リスク管理
14. 業種別の追加留意事項
15. 海外規制・グローバル対応
16. 調達・契約・ベンダー管理
17. AIを組み込んだシステムの開発
18. 組織体制・ガバナンス
19. 教育・リテラシー
20. インシデント対応
21. 違反時の措置
22. コストと環境への配慮
23. 定期見直し・改定サイクル
24. 参考法令・ガイドライン一覧
25. よくある質問（FAQ）
26. 付録（記入式テンプレート集）

1. はじめに

改定履歴

編集メモ：自社の制定・改定の経緯に置き換えてください。初版制定なら不要な行を削除します。

版数	日付	主な改定内容
第1.0版	初版制定日	初版制定
第1.0版	改定日	全面改定（業種別留意・海外規制・調達管理・記入式テンプレート集を追加）

1.1 本ガイドラインの目的

生成AIは業務の生産性を大きく高める一方で、機密情報の漏洩、著作権侵害、ハルシネーション（事実と異なる出力）、差別的出力といったリスクを抱える。2025年以降はAIエージェントやフィジカルAIの実用化が進み、AIが自律的に判断・行動する場面が増えた。

本ガイドラインは、会社名および関連会社の全従業員が生成AIを安全かつ効果的に活用するための行動基準を定める。目指すのは「禁止による萎縮」ではなく「ルールに基づく積極活用」である。

> **当社の利用スタンス（標準運用）**
>
> リスクの大きさに応じて対策を変える。低リスクは自由、限定リスクは承認、高リスクは厳格管理とし、活用と統制のバランスを取る。

1.2 位置づけと法的根拠

本ガイドラインは、以下の法令・公的指針に準拠して策定している。

法令・指針	策定主体	位置づけ
AI事業者ガイドライン（第1.2版）	総務省・経済産業省	2026年3月公表。フィジカルAI・AIエージェント対応
人工知能関連技術の研究開発及び活用の推進に関する法律（AI推進法）	内閣府	2025年6月公布・9月全面施行。理念・推進を定める（罰則なし）
人工知能基本計画	内閣府	2025年12月閣議決定。AI推進法に基づく法定計画

行政の進化と革新のための生成AIの調達・利活用に係るガイドライン（第2.0版・DS-920）	デジタル庁	2025年5月策定、2026年6月12日に第2.0版へ改定。行政機関向けだが、調達審査の観点は民間でも参照できる
人工知能関連技術の研究開発及び活用の適正性確保に関する指針	内閣府	AI推進法に基づく指針。開発者と利用者が守る適正性の考え方を示す
EU AI Act（Regulation 2024/1689）	EU	2024年8月発効。透明性義務は2026年8月適用。高リスク義務はDigital Omnibus（Regulation (EU) 2026/1744、2026年7月27日発効）により2027年12月以降へ延期。域外適用あり
個人情報保護法	個人情報保護委員会	2026年7月10日成立、7月17日公布（令和8年法律第56号）。AI開発・統計目的の同意例外と課徴金制度を導入。罰則関連の規定は2027年1月17日に先行施行、主要部分は2028年7月16日までの政令で定める日
不正競争防止法	経済産業省	営業秘密の保護。AIへの入力による秘密管理性の喪失に注意
著作権法（第30条の4 等）	文化庁	AI学習・生成に関する考え方を整理（2024年3月）
ISO/IEC 42001:2023	ISO/IEC	AIマネジメントシステム国際規格

1.3 改定方針

AI技術と規制は速く変化する。半期に一度の定期改定を原則とし、重大な法改正や技術的転換が生じた場合は臨時改定を行う。改定履歴は記録し、全従業員へ通知する。

2. 生成AIの基礎知識

2.1 生成AIのしくみ（要点）

大規模言語モデル(LLM)は、大量のテキストから「次に来る語の確率」を学習している。質問の意味を理解しているのではなく、もっともらしい続きを統計的に生成している。だからこそ、流暢でも誤る（ハルシネーション）。この性質を理解することが安全利用の出発点になる。

2.2 種類とできること

種類	主な用途	代表例
テキスト生成	文章作成・要約・翻訳・調査補助	ChatGPT, Claude, Gemini
コード生成	実装・レビュー・デバッグ補助	GitHub Copilot, Cursor, Claude Code
画像・動画・音声生成	素材作成・デザイン補助	Firefly, DALL-E, 各種動画/音声AI
AIエージェント	複数手順の自律実行・業務自動化	各種エージェント基盤

2.3 苦手なこと（過信しない）

- 最新情報や社内固有の事実は知らない（学習時点・与えた情報の範囲でしか答えられない）。
- 計算・厳密な事実確認・出典提示は誤りやすい。数値・固有名詞・URLは必ず裏取りする。
- 「根拠」を聞いても、内部の判断過程ではなく、もっともらしい理由を後付けで出力しているにすぎない。

3. 適用範囲と対象者

区分	対象	適用レベル
正社員・契約社員	全部門・全職位	全条項を適用
派遣社員	当社業務に従事する者	全条項を適用（派遣元にも通知）
業務委託先	当社データを扱う委託業務	データ・セキュリティ関連条項を契約条件として適用
グループ会社	連結子会社・関連会社	本ガイドラインを基に各社版を策定
役員	取締役・執行役員・監査役	全条項を適用（ガバナンス章の責務あり）

編集メモ：業務委託先の適用レベルは、契約実務に合わせて調整してください。全条項を課すか、データ・セキュリティ条項に絞るかで、契約書の書きぶりが変わります。

3.1 対象となるAI

提供形態を問わず、次のいずれかに当たるものを対象とする。ツール名を限定列挙すると新しいサービスが漏れるため、機能で定義する。

種別	対象
テキスト生成	対話型AIサービス、文章の作成・要約・翻訳を行う機能。業務システムに組み込まれた同種の機能を含む
画像・音声・動画生成	画像生成、音声合成、動画生成、および既存素材の生成的な加工
コード生成	開発環境に組み込まれる補完・生成機能、コードレビュー支援
AIエージェント	AIが自ら判断して外部システムを操作する形態（第10章）
社内開発のAI	自社で構築したAIシステム、社内文書を参照させる仕組み（RAG）を含む
既存製品への搭載機能	日常的に使う業務ソフトへ後から追加されたAI機能。追加された時点で本ガイドラインの対象となる

対象は増えていく前提で運用する

使い慣れた業務ソフトにAI機能が追加され、意識しないまま使い始める場面が増えている。新しいツールを導入したときだけでなく、既存ツールに機能が追加されたときも第6章の審査の対象となる。

4. 用語の定義

主要用語は、AI事業者ガイドライン（第1.2版）の定義に準拠する。

用語	定義
生成AI	LLM等を基盤とし、テキスト・画像・音声・動画・コード等を生成するAIシステムの総称。
AIエージェント	目標達成のため環境を感知し自律的に行動するAIシステム。複数システムと連携して調整・分析・実行を行う。
エージェンティックAI	複数のAIエージェントが自律的に連携し、意思決定と行動を行うシステム。
フィジカルAI	センサで物理環境を取り込み、AI処理を経てアクチュエータ等で物理行動につなげるシステム。
プロンプト	生成AIへの入力指示文。システムプロンプトとユーザープロンプトを区別する。
ハルシネーション	事実と異なる情報をもっともらしく出力する現象。
RAG（検索拡張生成）	外部データから関連情報を検索し、その結果をLLMに渡して回答精度を高める手法。
ファインチューニング	学習済みモデルに特定タスク向けの追加学習を行うこと。
Human-in-the-Loop	AIの判断・行動に人間の介在を組み込むしくみ。
プロンプトインジェクション	悪意ある入力で制御を迂回し意図しない動作を引き起こす攻撃。間接型も含む。

5. 基本原則

5.1 10の共通原則

AI事業者ガイドライン（第1.2版）の10原則を、自社の事業文脈に即して解釈・適用する。

No.	原則	解釈と適用
1	人間中心	AIの出力は参考情報であり、最終判断は人間が行う。意思決定の操作や感情の搾取を行わない。
2	安全性	危害の発生を避けるため利用方針を定める。モデルの真正性を確認する。
3	公平性	バイアスに配慮し、差別的出力が業務判断に反映されないよう検証する。
4	プライバシー保護	個人情報・プライバシーに関わるデータのAI入力を厳格に制限する。
5	セキュリティ確保	インジェクション、データ汚染等に技術的・組織的対策を講じる。外部連携は最小権限で行う。
6	透明性	AIで作成したコンテンツはその旨を明示する。顧客対応でのAI利用は事前に説明する。
7	アカウンタビリティ	利活用の結果について組織として説明責任を果たす。利用ログを保全する。
8	教育・リテラシー	全従業員に教育を実施する。過度な依存を防ぎ批判的思考を保つ。
9	公正競争確保	不当な市場支配やデータ独占を行わない。
10	イノベーション	過度な規制による萎縮を避け、リスクに応じたグラデーション管理を行う。

5.2 リスクベースアプローチ

すべてのAI利用を一律に規制せず、リスクの大きさと発生可能性に応じて対策の優先順位を決める。

禁止	高リスク	限定リスク	最小リスク
許容不可	厳格管理	透明性義務	自由利用

レベル	判断基準	対応例
禁止	人権侵害・違法行為に直結	ソーシャルスコアリング、従業員監視・感情操作、なりすまし

高リスク	人事・与信・法務・医療/安全の判断	人間が最終判断、リスクアセスメント、定期監査、ログ保全
限定リスク	顧客向けコンテンツ、社外公開資料	AI利用を明示、ファクトチェック、上長承認
最小リスク	社内下書き、要約、検索、翻訳、コード補完	機密データ入力禁止のみ遵守、自由に活用可

6. 利用ルール

6.1 利用許可ツール（ホワイトリスト方式）

業務利用が認められる生成AIツールは、情報システム部 / DX推進室が審査・承認したものに限る。未承認ツールの業務利用は禁止する。

編集メモ：自社で実際に契約・承認しているツールに置き換えてください。製品名は改称されることがあるため、改定のたびに現行名を確認してください。

承認済みツール（例）

- ChatGPT Business / ChatGPT Enterprise（テキスト生成）
- Claude Team / Claude Enterprise、Claude Code（テキスト・コード生成）
- Microsoft 365 Copilot（社内データ連携あり） / Microsoft 365 Copilot Chat（Web情報ベース）
- Gemini（Google Workspace 上位プランに搭載） / Gemini Enterprise
- GitHub Copilot Business / GitHub Copilot Enterprise（コード生成）
- Adobe Firefly（法人向け Teams / Enterprise プラン、画像生成）
- 社内専用LLM基盤（機密データ可・条件付き）

区分	利用条件
テキスト生成（法人契約）	入力データが学習に使われない契約であることを確認したうえで、機密度B以下を入力できる（第7章）
コード生成	生成コードはレビュー・テスト・ライセンス確認を経て採用する。顧客資産は契約条件を優先する
画像・音声・動画生成	商用利用可能なライセンスの範囲で使う。実在の人物・既存著作物に似た出力は公開前に確認する
AIエージェント基盤	第10章を全面的に適用する。承認対象操作は人の承認を経る
社内専用LLM基盤	機密度Aまで入力できる。アクセス権と利用ログの管理を前提とする

新規ツールの審査には通常2週間程度を要する。急ぐ場合も審査を省略しない。

個人アカウントでの業務利用は禁止し、会社が契約したEnterprise版のみを使う。

ツール追加申請

新たなAIツールの導入を希望する場合は「AI利用申請書」（付録B）を提出する。セキュリティ審査・データ保護方針確認・利用規約の法務レビューを経て承認する。

6.2 利用が認められる業務範囲

- 社内文書・報告書・メールの下書き作成
- 会議の議事録要約・アクションアイテム抽出
- 市場調査・情報収集の補助
- プログラムコードの生成・レビュー・デバッグ支援
- 社内FAQ・ナレッジベースの構築支援
- 翻訳・多言語コンテンツの作成補助
- データ分析・可視化の補助、アイデア出し
- 業務プロセスの自動化（承認済みエージェント基盤上）

社外公開・送付するコンテンツにAIを用いた場合は、ファクトチェックの上で上長の承認を得る。

6.3 禁止事項

以下の行為は理由を問わず禁止する

1. 顧客・取引先の個人情報、機密情報をAIに入力する行為
2. AI出力をファクトチェックなしに社外へ公開・送付する行為
3. AIで他者の著作物を模倣・複製する行為
4. ディープフェイク（音声・画像・動画の偽造）の作成
5. AIによる従業員の心理的操作・感情搾取
6. 採用選考・人事評価をAI出力のみで決定する行為
7. 未承認のAIツールを業務に使用する行為
8. 安全機能・ガードレールを意図的に回避する行為（ジェイルブレイク）
9. 悪意あるコード・マルウェア・攻撃ツールの生成
10. 承認なくエージェントへ外部書き込み・データ削除等の権限を付与する行為

6.4 未承認ツールの利用（シャドーAI）への対応

禁止を掲げるだけでは未承認ツールの利用はなくならない。**当社**は、検知の仕組みと、申告しやすい窓口の両方を用意する。

手段	内容
通信ログの点検	プロキシ・CASB等で生成AIサービスへのアクセスを可視化し、未承認サービスの利用を検知する
定期棚卸し	半期に一度、部門ごとに利用中のAIツールを申告してもらい、付録Eの棚卸し表を更新する
経費・購買の突合	AIサービスの個人課金・部門課金が経費精算に現れていないか確認する
申告の受付	すでに使ってしまっている場合、申告期間内に自己申告すれば処分の対象としない。隠したまま事故に至った場合との差を明確にする

編集メモ：検知手段は自社で実施できるものだけ残してください。実施しない手段を書くと、運用されないルールになります。申告の免責を設けるかは経営判断です。

6.5 業務別の使い方とやってはいけない例

編集メモ：現場が迷う場面を具体的に書くほど守られます。自社で実際に多い業務へ差し替えてください。

業務	進め方	やってはいけない例
議事録の要約	録音・文字起こしから氏名等を伏せて入力し、要約後に担当者が事実確認する	顧客名や未公開の取引条件を含んだまま個人版へ貼り付ける
資料・提案書の作成	構成案とたたき台をAIに作らせ、数値・固有名詞は原典で裏を取る	AIが挙げた市場規模や他社事例を未確認のまま提案書へ載せる
翻訳	公開情報・社内文書は承認済みツールで翻訳し、契約書等は専門家の確認を経る	契約書・法的文書をAI訳のまま相手方へ送付する
コードの生成・レビュー	承認済みのコード生成ツールを使い、生成コードはレビュー・テスト・ライセンス確認を経て採用する	顧客から預かった資産や認証情報を含むコードを外部ツールへ入力する
メール・問い合わせ対応	下書きをAIに作らせ、送信前に担当者が内容と宛先を確認する	AIの下書きを読まずに顧客へ送信する
調査・情報収集	出典URLを併せて出力させ、一次情報にあたって確認する	出典を確認せず、AIの回答を根拠として意思決定する

6.6 部門固有ルール・私物端末・社外発信

- **部門固有の上乗せ** — 人事・経理・法務・広報など、取り扱う情報の機微性が高い部門は、部門長が本ガイドラインに上乗せするルールを定める。上乗せは本書の付属文書としてAI管理委員会へ届け出る
- **私物端末・個人契約のAI（BYOAI）** — 私物端末および個人契約のAIサービスを業務に使用しない。個人アカウントでの利用は個人アカウントでの業務利用は禁止し、会社が契約したEnterprise版のみを使う。
- **社外発信での利用** — SNS・ブログ・登壇資料などで社外へ発信する内容にAIを用いる場合、公開前に上長の確認を得る。自社の見解として発信する内容は、AI出力をそのまま用いない
- **採用・人事・評価** — 応募者情報や人事評価の材料をAIへ入力しない。選考・評価の判断は人が行う

7. データ取扱いルール

7.1 機密度分類

編集メモ：自社の情報資産管理規程の分類に合わせて調整してください。

レベル	分類	具体例	AI入力
S	極秘	経営戦略、M&A、未公開決算、顧客DB全件、認証情報・暗号鍵	× 不可
A	秘密	顧客個人情報、契約書、技術仕様、人事評価、非公開ソースコード	△ 条件付き可（社内専用LLMのみ）
B	社内限定	社内マニュアル、議事録、業務報告、一般的な社内メール	○ 可（Enterprise版）
C	公開	プレスリリース、公開Web情報、製品カタログ	○ 可

7.2 入力可否マトリクス

編集メモ：ヒアリング結果を反映しています。運用に合わせて微調整してください。

データ種別	社内専用LLM	Enterprise版外部	個人版外部
公開情報（C）	○ 可	○ 可	○ 可
社内文書（B）	○ 可	○ 可（匿名化後）	× 不可
顧客情報（A）	△ 条件付き可	× 不可	× 不可
極秘情報（S）	× 不可	× 不可	× 不可
個人情報（氏名・住所等）	△ 匿名化後のみ可	× 不可	× 不可
ソースコード（非公開）	○ 可	△ 承認済みツールのみ	× 不可

7.3 個人情報の取扱い

個人情報保護法に基づき、個人情報をAIに入力する場合は以下をすべて満たす。

- 利用目的の範囲内であること
- 必要最小限のデータに限定すること（データ最小化）

- 不要な属性情報を付与しないこと
- 匿名加工または仮名加工を施すこと
- 社内専用LLM以外への入力は原則禁止

> **マルチモーダル入力への注意**
> 画像・音声・動画にも個人情報は含まれる。カメラ・音声認識を使うシステムでは対象者への通知・同意取得が必要。フィジカルAIではデバイス上の残存データ削除も考慮する。

7.4 社内データとの連携（RAG・社内文書検索）

社内文書をAIに検索・参照させる仕組み（RAG）は、元の文書のアクセス権を引き継がないと、本来閲覧できない情報が回答に混ざる。構築時と運用中の双方で次を守る。

論点	守ること
アクセス権の継承	利用者ごとの閲覧権限を検索対象に反映し、権限のない文書が回答や出典に現れないようにする。全社共有の索引に人事・経理等の限定文書を混ぜない
対象データの選定	索引に含める範囲を事前に定義し、機密度Sの文書は含めない。含める文書は第7章の分類に沿って棚卸しする
鮮度と出典	回答には出典文書と更新日を併せて表示する。古い規程が現行として引用される事故を防ぐため、更新・削除を索引へ反映する運用を定める
退職者・異動者	権限変更を検索側にも反映する。索引だけ旧権限で残らないようにする
構築側の責任	社内でRAGを構築・提供する部門は、単なる利用者ではなくAIを提供する立場として、第18章の管理下で品質・安全性に責任を負う

編集メモ：社内文書検索やRAGを導入していない場合は、この節を削除してください。導入予定がある場合は残し、構築部門を明記してください。

7.5 入力・出力ログの保存と閲覧

項目	取り決め
保存対象	利用者、日時、使用ツール、入力の概要、出力の利用先。エージェント利用時は実行した操作と承認者（第10章）
保存期間	90日（高リスク業務は1年）
閲覧できる人	情報システム部 / DX推進室の指定担当者と、インシデント調査時の調査担当者に限る

閲覧の目的	インシデント調査、監査対応、利用状況の集計に限る。人事評価や個人の監視の目的では用いない
利用者への周知	ログを取得している事実と目的を、利用開始時に利用者へ知らせる

編集メモ：ログの取得は従業員のモニタリングに当たるため、目的外利用をしないことを明記しています。労働組合・従業員代表への説明が必要かは自社で確認してください。

8. 生成物の品質管理

8.1 ファクトチェックプロセス

リスクレベル	検証要件	検証者
高リスク	一次情報源で全項目を裏付け。法務・専門部門レビュー必須	専門部門担当 + 上長
限定リスク	数値・固有名詞・法的記述を信頼できる情報源と照合	担当者 + 上長
最小リスク	明らかな事実誤認がないか通読確認	担当者本人

8.2 出力の利用承認フロー

1. AI出力の取得
2. ファクトチェック
3. リスクレベル判定
4. 必要に応じ承認
5. 利用・公開

8.3 ハルシネーション対策

- 出力中の数値・日付・人名・法令名・URLは必ず原典で確認する
- RAGで社内の信頼できるデータソースに基づく回答を促す
- 自信の度合いを示すプロンプト設計を推奨する
- 複数モデルでのクロスチェックも有効
- 業務損害につながった場合はインシデント報告する（第20章）

9. 著作権・知的財産権

9.1 生成物の著作権

現行著作権法上、AIが自律生成したコンテンツに著作権は発生しない。ただし人間の創作的関与があれば、その度合いに応じて著作物性が認められうる。業務での生成物は原則として自社の職務著作とする。

9.2 他者の著作権への配慮

- 特定の著作物・アーティスト・ブランドの「スタイル」を意図的に模倣するプロンプトは使わない
- 生成物が既存著作物と類似していないか公開前に確認する
- 商用利用する画像・音声・動画は商用ライセンス条件を確認する
- 生成素材を商標・意匠登録する場合は法務に事前相談する

9.3 学習データとしての自社コンテンツ

外部AIへ入力したデータがモデル学習に使われる可能性がある。Enterprise契約ではオプトアウトが保証される場合が多いが、利用規約を確認する。

9.4 コード生成AIの知的財産

- 生成コードにOSSライセンス条件が混入しうる。ライセンス互換性を確認する
- 生成コードをそのまま採用せず、レビューとテストを経る
- 特許出願を検討するコードにAI生成部分があれば知財部と協議する

10. AIエージェント利用ルール

本章の根拠

AI事業者ガイドライン（第1.2版）で、AIエージェント・フィジカルAIの定義・リスク・留意事項が追加された。Human-in-the-Loop、最小権限、操作ログ記録が事実上の必須になっている。

10.1 AIエージェントの分類

区分	自律度	例	承認レベル
タスク実行型	低	メール下書き、定型レポート	部門長承認
ワークフロー型	中	収集→分析→レポート生成の自動化	部門長＋情シス
自律判断型	高	顧客対応自動化、発注判断、運用自動化	AI管理委員会
マルチエージェント型	最高	エージェンティックAI、複合業務自動化	AI管理委員会＋経営層

10.2 Human-in-the-Loop（事前承認が必要な操作）

クリティカル操作	承認方式
メール・メッセージの外部送信	送信前ドラフト確認＋承認
ファイル・データの削除	対象一覧表示＋明示的承認
金銭に関わる操作（発注・送金・購入）	金額と取引先表示＋二段階承認
本番環境への変更適用	diff表示＋承認＋自動ロールバック
外部API・サービスへのデータ送信	送信先・データの事前確認＋承認
アクセス権限の変更	変更内容の表示＋管理者承認

10.3 権限設計と緊急停止

- 付与する権限は業務遂行に必要な最小限に限定する
- 連携ツール・システムをホワイトリストで制限する
- 読み取り専用と書き込み権限を分離する
- すべてのエージェントに即時停止機能を実装し、停止後の状態復元手順を整備する
- 想定外の連続実行、大量アクセス、想定しない宛先への通信を検知した場合に自動で停止する仕組みを設ける
- 停止の操作権限は運用担当者以上に付与し、誰が停止できるかを事前に周知する

- 権限の棚卸しを四半期ごとに実施する

10.4 トレーサビリティ要件

記録項目	内容
いつ	操作のタイムスタンプ（ISO 8601 / UTC）
誰が	実行ユーザーID + エージェントID
何を	操作対象・入力内容（構造化ログ）
結果	成功/失敗/エラー内容
根拠	適用ポリシー・ルール（ポリシーID参照）

ログの保存期間は 90日（高リスク業務は1年） とする。

11. セキュリティ

11.1 アクセス管理

- AIサービスのアカウントはSSOまたは多要素認証で管理する
- 退職者・異動者のアカウントは即時無効化する
- APIキーはシークレットマネージャで管理し、コードに直接記載しない
- 利用ログを一元管理し、不審なアクセスを監視する

11.2 プロンプトインジェクション対策

- ユーザー入力とシステムプロンプトを明確に分離する
- RAGで外部文書を取り込む際、埋め込まれた悪意ある指示を検出するフィルタを置く
- エージェントが受け付ける操作をホワイトリストで限定する
- 出力のサニタイズ（コード実行・SQLへの直接反映を防止）を行う
- 定期的にレッドチーム演習を実施する

11.3 外部連携時の安全基準

連携先	セキュリティ要件
外部API	TLS 1.2以上、APIキーのローテーション90日以内、送信データ暗号化
クラウドストレージ	ACL設定、暗号化保存、監査ログ有効化
社内システム	VPN/プライベートネットワーク経由、最小権限でのAPI連携
オープンソースモデル	開発元の信頼性確認、取得経路検証、改ざん検知

AIエージェント特有のセキュリティリスク

エージェントは外部システムへ自ら接続し、操作を実行する。不正な指示を受けて社内データを外部へ送り出す経路になりうるため、連携先を必要最小限に絞り、新たな連携の追加は事前承認とする。想定外の通信・大量アクセスを検知する仕組みを設け、異常時は自動で停止する（第10章）。

11.4 モデル・提供元の確認

- 導入時にモデルカード・システムカード等の技術文書を確認し、想定用途、既知の限界、評価結果を把握する
- 提供元、学習データの来歴、再委託・サプライチェーンの透明性を確認する
- 公開モデルを自社で動かす場合は、取得元の正当性と改ざんの有無を検証する
- モデルの更新・切り替えが自動で行われるサービスでは、挙動が変わりうる前提で運用と検証を設計する

12. プライバシー保護

- 個人情報保護法、GDPR（EU域内処理時）その他適用法令を遵守する
- AIへの入力は必要最小限に限定する（データ最小化）
- 個人を特定可能な情報は匿名化・仮名化してから入力する
- 出力に個人情報が含まれた場合も適切に取り扱い、関係者のプライバシーを尊重する
- カメラ・音声認識を使うシステムでは利用目的の通知・同意取得を行う
- フィジカルAIではデバイス上の残存データを定期削除する
- 高リスクなAI利用開始前にプライバシー影響評価（PIA）を実施する

12.1 影響評価（PIA / DPIA）の実施

次のいずれかに当てはまる場合、利用開始前に影響評価を実施し、結果をAI管理委員会へ提出する。

- 個人情報を含むデータをAIで継続的に処理する
- 顧客・従業員の評価、選別、スコアリングにAIを用いる
- カメラ・音声・位置情報など、本人が気づきにくい形でデータを取得する
- 要配慮個人情報を扱う、またはEU域内の個人データを処理する（GDPR上のDPIAが必要となりうる）

手順	内容
1. 対象の特定	処理する個人データの種類、取得元、利用目的、保存期間、関係者を洗い出す
2. 必要性の検討	その目的にその個人データが本当に必要か、より影響の小さい方法がないかを検討する
3. リスクの評価	本人に生じうる不利益（誤判定、差別、漏洩、想定外の利用）と、その大きさ・起こりやすさを評価する
4. 対策の決定	匿名化、アクセス制限、保存期間の短縮、人による確認など、残るリスクに応じた対策を決める
5. 記録と見直し	評価結果を記録し、処理内容が変わったとき、および年1回見直す

編集メモ：評価の記録は付録Dのリスクアセスメントシートを流用できます。様式を分ける場合は、この節に自社の様式名を記載してください。

13. リスク管理

13.1 リスク分類体系

大分類	中分類	リスク例
技術的リスク	学習・入力段階	データ汚染攻撃、学習データへの不正混入
	出力段階	バイアス・差別的出力、一貫性のない出力、ハルシネーション
	事後対応段階	ブラックボックス化、判断の説明不足
社会的リスク	倫理・法	個人情報の不適切取扱い、事故、差別、過度な依存、悪用
	経済活動	知財侵害、金銭的損失、機密流出、雇用への影響
	情報空間	偽・誤情報の流通、フィルターバブル、多様性の喪失
	環境	エネルギー使用量・環境負荷

13.2 リスクアセスメント手順

1. 目的・範囲特定
2. リスク洗い出し
3. 影響度×発生可能性
4. 対策の設計・実装
5. モニタリング

> **攻めのガバナンスの考え方**
>
> 過度なリスク対策はコスト増とAI活用の萎縮を招く。リスクの性質・蓋然性に照らし、限られた資源を効果的に配分する。

13.3 リスク低減策

リスク領域	低減策
ハルシネーション	RAG、ファクトチェック（第8章）、温度パラメータ調整
機密情報漏洩	データ分類の徹底（第7章）、DLP導入、入力フィルタ
バイアス・差別	出力の多様性テスト、クロスチェック、定期バイアス監査
プロンプトインジェクション	入出力サニタイズ、レッドチーム演習（第11章）

過度な依存	教育（第19章）、人間が最終確認する文化
著作権侵害	商用ライセンス確認、類似性チェック（第9章）
エージェントの暴走・誤操作	権限の最小化、承認対象操作の限定、異常検知による自動停止、操作ログの記録（第10章）
生成コードの欠陥	レビュー必須化、静的解析、テストカバレッジの確保、依存ライブラリとライセンスの検査
未承認ツールの利用	通信ログの点検、定期棚卸し、申告窓口の設置（第6章）

14. 業種別の追加留意事項

編集メモ：全業種を載せています。自社に当てはまる業種だけ残し、他は削除してください。

14.1 業種ごとの留意点

全業種共通

観点	留意事項
自社の中核情報	競争力の源泉となる情報（戦略・顧客・ノウハウ）は外部AIへ入力しない。社内専用基盤に限定する。
顧客・取引先データ	預かったデータを自社AI活用へ転用しない。契約上の利用目的の範囲内で扱う。
取引先との合意	顧客・取引先との契約や秘密保持契約に、AIへの入力を制限する条項がないか確認する。
業界の自主規制	所属する業界団体のガイドラインがある場合は、本ガイドラインに優先して適用する。

製造業

観点	留意事項
設計・製造データ	図面・CADデータ・製造ノウハウは営業秘密に該当しうる。外部AIサービスへの入力は原則禁止し、社内専用基盤に限定する。
フィジカルAI・産業用ロボット	AIを組み込んだ装置・ロボットは人身安全に直結する。機能安全（ISO 12100 / IEC 61508）と整合させ、緊急停止と人手介在を必須とする。
品質・トレーサビリティ	AIを検査・品質判定に用いる場合、判定根拠と入出力を記録し、最終判定は有資格者が行う。

金融・保険業

観点	留意事項
与信・引受・不正検知	信用スコアリングや保険引受へのAI利用はEU AI Actの高リスク領域に該当しうる。説明可能性の確保と人間による最終判断を必須とする。

顧客資産・取引情報	口座・取引・資産情報は最高機密として扱い、外部AIへの入力を全面禁止する。
金融規制対応	金融庁の監督指針、システムリスク管理態勢、外部委託管理と整合させる。AIの誤りが顧客被害に直結する点を踏まえ保守的に運用する。

医療・ヘルスケア

観点	留意事項
診断・治療支援	診断・治療方針へのAI関与は医師法・薬機法の規律下にある。AIは補助に留め、医療判断は必ず有資格者が行う。
要配慮個人情報	病歴・検査結果等は要配慮個人情報。外部AIへの入力を全面禁止し、院内基盤でも匿名化・アクセス制限を徹底する。
プログラム医療機器(SaMD)	AIを医療機器として用いる場合は薬機法の承認・認証と市販後の性能監視が必要。

公共・自治体

観点	留意事項
行政情報・住民情報	デジタル庁「行政の進化と革新のための生成AIの調達・利活用に係るガイドライン」に準拠する。住民の個人情報は外部AIへ入力しない。
公平性・説明責任	行政判断へのAI利用は不利益処分の根拠としない。判断過程の説明可能性と記録保全を徹底する。
調達・委託管理	AI調達では学習データの来歴、再委託、データ越境を契約で明確化する。

小売・サービス業

観点	留意事項
顧客対応・接客自動化	チャットボット等で顧客対応する場合はAI利用を明示し、人へのエスカレーション経路を用意する。
購買・需要予測	発注・価格決定をAI出力のみで自動確定しない。Human-in-the-Loopを組み込む。
顧客データ・購買履歴	会員情報・購買履歴は秘密情報として扱い、外部AIへの入力前に匿名化する。

IT・ソフトウェア業

観点	留意事項
ソースコード・設計情報	非公開リポジトリのコードは承認済みコード生成ツールに限り入力可。顧客の受託開発資産は契約条件を優先する。
生成コードの品質・ライセンス	AI生成コードはレビュー・テスト・OSSライセンス検査（SBOM）を経て採用する。
顧客データの取扱い	SaaS等で預かる顧客データを自社AI活用の入力に転用しない。データ処理契約(DPA)の範囲を遵守する。

建設・不動産業

観点	留意事項
設計図面・積算データ	図面・積算根拠・協力会社の見積は営業秘密に当たりうる。外部AIへの入力は承認済みツールに限る。
現場の安全管理	AIによる危険検知は補助であり、安全確認の責任は現場管理者にある。検知漏れを前提とした運用にする。
公共工事・入札	入札関連情報の取扱いは発注者の定めに従う。積算・応札価格に関する情報を外部AIへ入力しない。

運輸・物流業

観点	留意事項
配送先・顧客情報	配送先住所・受取人名は個人情報。ルート最適化等に用いる場合も外部AIへ生データを入力しない。
運行・安全	運行管理や車両制御に関わる判断をAI出力のみで確定しない。法定の管理者の判断を経る。
需要予測と在庫	予測結果を発注へ自動反映する場合、上限と例外時の停止条件を定める。

教育

観点	留意事項
学習者の情報	成績・出欠・相談内容は機微性が高い。外部AIへの入力を禁止し、学内基盤でもアクセスを限定する。

評価への利用	成績評価・合否判定をAI出力のみで決定しない。EU AI Actでは教育分野の一部が高リスクに位置づけられる。
学習者による利用	課題等での生成AI利用の可否と引用ルールを明示し、指導する。

14.2 共通の上乗せ管理

- 規制業種では、業法・監督指針・業界自主規制を本ガイドラインに優先して適用する
- 顧客から預かったデータを自社のAI活用に転用しない
- 高リスク用途は導入前にリスクアセスメント（第13章）と必要な承認を経る

15. 海外規制・グローバル対応

編集メモ：海外拠点・海外顧客・EU向け製品がない場合は、この章ごと削除して構いません。

15.1 EU AI Act（欧州AI規則）

リスクに応じて4区分（許容できないリスク・高リスク・限定リスク・最小リスク）で規律する。EU域内の利用者・市場に影響する場合は域外の企業にも適用されうるため、EU向けに製品・サービスを提供する場合は自社の該当区分を確認する。高リスクAI（採用・与信・教育・重要インフラ等）にはリスク管理体制、データガバナンス、人間による監督、技術文書と記録保持、適合性評価の義務が課される。

義務	適用時期	内容
禁止AI慣行	適用済み（2025年2月）	サブリミナル操作、社会的スコアリング、無差別な顔画像収集などの禁止
汎用AIモデル（GPAI）の義務	適用済み（2025年8月）	技術文書、学習データの概要公開、著作権方針
透明性義務（第50条）	2026年8月2日	AIとの対話であることの通知、AI生成コンテンツの明示、感情認識・生体分類の告知
生成物の機械可読マーキング	2026年12月2日	生成AI出力への電子透かし等の付与
高リスク（附属書III型）	2027年12月2日	雇用・教育・基本的サービス等の単独型システム。当初2026年8月から延期
高リスク（附属書I型）	2028年8月2日	製品に組み込まれる型。当初2027年8月から延期

高リスク義務の適用が延期された点に注意

2026年7月に成立したDigital Omnibus（デジタル・オムニバス。Regulation (EU) 2026/1744、2026年7月24日官報公表・7月27日発効）により、高リスクAIの適合期限が上記のとおり後ろ倒しされた。ただし透明性義務の2026年8月2日は据え置かれている。延期は準備期間の猶予であって免除ではないため、対象となる企業は適合性評価の準備を継続する。最新の適用時期は配布前に確認すること。

15.2 主要国の動向

地域	概要

米国	連邦レベルの包括規制はなく、政権の方針転換により推進・規制緩和寄りへ動いている。実務上はNIST AI RMF等の任意フレームワークと、州法（カリフォルニア州・コロラド州等）が先行する。州ごとに義務が異なる点に注意する。
EU	AI Actによる包括的・横断的規制。域外適用あり。本章の冒頭のとおり段階適用。
中国	生成AIサービス管理暫行弁法等により、アルゴリズム届出、生成物の識別表示、コンテンツ規制が課される。中国国内でのサービス提供時は現地要件を個別に確認する。
英国	包括法を置かず、既存の規制当局が分野別に原則を適用するアプローチ。
その他	韓国・カナダ等でAI法制の整備が進む。国際的な相互運用性と、広島AIプロセス等の国際規範との整合が論点。

15.3 越境データ移転

- 海外のAIサービス利用はデータの越境移転に当たりうる。移転先国の保護水準と、個人情報保護法上の同意・体制整備の要否を確認する
- GDPR対象データは適法な移転根拠（標準契約条項（SCC）等）を確保する
- データの保存国・処理国、サブプロセッサの所在を契約で明確化する
- 国内保存が求められるデータ（業法・契約上の制約があるもの）は、リージョン指定が可能なサービスを選定する

15.4 海外拠点・グループ会社への適用

- 本ガイドラインをグループ共通の最低基準とし、各国拠点は現地法令がより厳しい場合に上乗せする
- 現地法令と本ガイドラインが矛盾する場合は現地法令を優先し、第18章の管理部門へ報告する
- 拠点ごとの上乗せルールは、本書の付属文書として管理する

16. 調達・契約・ベンダー管理

編集メモ：AIツール・サービスの導入審査基準です。情シス・調達・法務の運用に合わせて調整してください。

16.1 導入審査チェック項目

観点	確認内容
データの取扱い	入力データの学習利用有無、オプトアウト可否、保存場所・期間、削除手順
セキュリティ	第三者認証（ISO 27001 / SOC 2 等）、暗号化、アクセス制御、脆弱性対応
コンプライアンス	準拠法令、個人情報・越境移転の扱い、利用規約の法務レビュー
事業継続性	SLA、サポート体制、ベンダーロックイン、撤退時のデータ移行
モデルの真正性	提供元・モデルの来歴、再委託・サプライチェーンの透明性

16.2 契約で明確化する事項

- 入力・出力データの権利帰属と二次利用の可否
- 学習へのデータ利用の可否（オプトアウト）
- 秘密保持、データ保存国、再委託の制限
- セキュリティ事故時の通知義務と責任分担
- サービス終了・解約時のデータ返却・削除

17. AIを組み込んだシステムの開発

編集メモ：社内でAIを使ったシステム・機能を作る部門がない場合は、この章ごと削除してください。外部委託で開発する場合も、委託先に同等の内容を求める前提で残す価値があります。

ここまでの章は生成AIを「使う」立場のルールである。本章は、自社の製品・社内システムにAIを組み込んで「提供する」場合に、追加で守ることを定める。提供する立場になると、利用者に対する責任が生じる。

17.1 企画・設計

- AIに何を任せ、何を人が決めるかを設計段階で切り分ける。人の判断を挟む箇所を仕様として明記する
- 誤った出力が出たときに利用者にどのような不利益が生じるかを洗い出し、影響が大きい用途はリスクアセスメント（第13章）を経る
- 個人データを扱う場合は影響評価（第12章）を設計と並行して実施する
- 採用・与信・評価など人に不利益を与えうる用途は、説明可能性と異議申立ての手段を設計に含める

17.2 実装

- システムプロンプトと利用者入力を分離し、外部から取り込む文書に埋め込まれた指示に従わないようにする（第11章）
- AIに与える権限は最小限とし、外部システムへの書き込み・削除・送信は承認または明示的な操作を経る
- 入力・出力・使用モデル・バージョンを記録し、後から挙動を追跡できるようにする
- APIキー・認証情報はシークレット管理の仕組みで扱い、プロンプトやコードに直接書かない

17.3 評価とリリース

観点	確認すること
正確性	想定する業務データで出力品質を評価し、許容できる誤り率を事前に決めておく
安全性	不適切な出力、機密情報の漏出、指示の乗っ取りを試す試験を行う
公平性	属性による出力の偏りがないか、代表的なケースで確認する
回帰	モデルやプロンプトを変更したとき、既存の品質が落ちていないか同じ試験で確認する
利用者への説明	AIを使っている旨、限界、問い合わせ先を利用者が分かる形で示す

17.4 運用と変更管理

- 提供元によるモデルの更新で挙動が変わりうるため、変更を検知して再評価する手順を定める

- 利用者からの誤り報告を受け付ける窓口を設け、第20章の報告経路につなぐ
- 停止の判断基準と停止手順を定め、重大な誤りが判明した場合は速やかに提供を止められるようにする
- 外部のツール・データソースと接続する場合、接続先の追加は事前承認とし、接続の一覧を維持する

18. 組織体制・ガバナンス

18.1 推進体制

編集メモ：自社の実体制に合わせて部門名・役職名を置き換えてください。

役割	担当	責務
最高責任者（CAIO）	代表取締役	AI戦略策定、ガイドライン承認、リスク判断の最終権限
AI管理委員会	情シス・法務・人事・DX・各事業部代表	運用・改定、リスクアセスメント審査、インシデント対応方針
AI推進担当	各部門1名以上	部門内の活用推進、遵守の啓発、利用状況の報告
情報システム部 / DX推進室	情シス	ツール審査・導入、セキュリティ管理、ログ監視、技術サポート
法務部	法務	法的リスク評価、規約レビュー、インシデント時の法的対応
内部監査部	監査	遵守状況の定期監査、改善勧告

18.2 経営層の責務

- AIガバナンス方針を策定し全社に明示する
- AI管理委員会の活動を監督し、四半期ごとに報告を受ける
- インシデントについて迅速な判断と対応指示を行う
- 活用推進とリスク管理のバランスを取る経営判断を行う
- AI活用に必要な投資（ツール、基盤、人材育成）の意思決定を行う

18.3 AI管理委員会の運営

- 開催頻度: 月1回の定例 + 必要に応じた臨時開催
- 審議: 新規利用の審査、アセスメント結果の確認、インシデント報告、改定案審議
- 議事録を作成し経営層へ報告する

18.4 利用申請から承認までの流れ

1. 申請（付録B）
2. 部門長の確認
3. 情シスの技術・セキュリティ審査
4. 法務の規約レビュー
5. AI管理委員会の承認
6. 棚卸し表へ登録

項目	取り決め
標準の審査期間	申請受付から通常2週間程度
高リスク用途の扱い	リスクアセスメント（第13章）と影響評価の結果を添付し、AI管理委員会が個別に審議する
却下されたとき	理由を申請者へ書面で伝える。条件を満たせば再申請できる
承認後	付録Eの棚卸し表へ登録し、契約更新時に再確認する

18.5 利用状況の把握

AI管理委員会は、次の指標を四半期ごとに集計して経営層へ報告する。数値は、活用が進んでいるかと、決めたルールが守られているかの両方を確かめるために用いる。

指標	見るもの
ライセンスの利用率	契約数に対して実際に使われている割合。低い場合は教育か用途開拓の不足
部門別の利用者数・利用頻度	活用が一部部門に偏っていないか
新規ツールの申請件数・承認率	現場のニーズと審査の詰まり具合
インシデント・ヒヤリハット件数	統制の実効性。報告が極端に少ない場合は報告しにくい状態を疑う
教育の受講率・理解度テストの結果	第19章の実施状況
未承認ツールの検知件数	シャドーAIの広がり（第6章）

編集メモ：最初から全部を測る必要はありません。取れる指標から始めて、報告の場を先に決めるほうが続きます。

18.6 監査

- 内部監査部は年1回以上、本ガイドラインの遵守状況を監査する

- 監査の観点は、承認済みツール以外の利用の有無、機密情報の入力実態、ログの保存状況、申請・承認の記録、教育の受講状況とする
- 監査に備え、次を証跡として保管する — 利用申請書と承認記録、リスクアセスメント結果、棚卸し表、インシデント報告書、教育受講記録（いずれも付録の様式）
- 指摘事項は是正計画を作成し、AI管理委員会が是正の完了を確認する
- 外部認証（ISO/IEC 42001 等）を取得する場合は、本ガイドラインと認証要求事項の対応関係を整理する

18.7 退職者・異動者・委託先の管理

対象	取り決め
異動者	異動と同時にアクセス権を見直す。旧部門の機密文書が検索・参照できる状態を残さない（第7章）
退職者	退職日にアカウントを無効化する。退職時にAIへ入力・保存した業務データの取扱いを確認し、持ち出しを禁止する旨を誓約書で確認する
業務委託先	本ガイドラインの遵守を契約条件とする。特に第6章の禁止事項、第7章のデータ取扱い、第20章の報告義務を明記する
再委託	事前承認制とし、再委託先にも同等の義務を課す
監査権	委託先の遵守状況について、報告を求め、必要に応じて確認できることを契約に定める
契約終了時	貸与アカウントの停止、預けたデータの返却または削除、削除証明の取得

19. 教育・リテラシー

対象	内容	頻度	形式
全従業員	AIリテラシー基礎、リスク認識、禁止事項	入社時 + 年1回	eラーニング + 理解度テスト
部門別	業務特化の活用スキル、プロンプト設計	半期1回	ワークショップ
管理職	ガバナンス、リスク判断、初動対応	年1回	集合研修
技術者	セキュア開発、エージェント設計、RAG構築	四半期1回	ハンズオン
AI管理委員会委員	法規制動向、海外規制、先進事例	四半期1回	勉強会

過度な依存の防止

AIへの心理的依存・過度な信頼のリスクも扱う。人間が最終判断する文化を維持し、出力を無批判に受容しない批判的思考力を養う。

20. インシデント対応

20.1 インシデントの定義

- 機密情報・個人情報がAIサービスに入力された（データ漏洩）
- AI出力に基づく判断・行動で損害が生じた
- AI生成物が著作権侵害として指摘された
- エージェントが意図しない操作を実行した（誤発注・誤送信・データ削除等）
- AIシステムへの攻撃が検知された
- 生成物が差別的・有害な内容を含んでいた

20.2 対応フロー

1	2	3	4	5
発見・検知	初動対応	報告	原因分析	再発防止
即時	1時間以内	4時間以内	24時間以内	1週間以内

ステップ	担当	アクション
発見・検知	発見者	当該利用を即時停止。エージェントは緊急停止。上長と情シスに一報
初動対応	情シス + 発見者	被害範囲の特定、証拠保全、被害拡大の阻止
報告	上長 → AI管理委員会	報告書（付録C）を作成。重大時は経営層へ即時報告
原因分析	AI管理委員会	根本原因の特定、影響範囲の確定、通知判断
再発防止	AI管理委員会 + 関連部門	運用改善、教育追加、必要に応じ外部報告・公表

21. 違反時の措置

違反レベル	例	措置
軽微	未承認ツールの一時利用（機密入力なし）、手順省略（実害なし）	口頭注意、再教育
中程度	社内限定データの未承認ツール入力、禁止事項抵触（軽微な実害）	書面注意、利用権限一時停止、再教育・テスト合格義務
重大	機密・個人情報の外部AI入力、故意のジェイルブレイク、ディープフェイク、重大損害	就業規則に基づく懲戒、法的措置の検討

違反の判定はAI管理委員会が行い、懲戒は人事と協議の上、就業規則に基づき決定する。意図的でなくても繰り返す場合は上位措置を適用する。

22. コストと環境への配慮

編集メモ：環境負荷の記述はサステナビリティ報告と整合させてください。コスト管理だけ残す形でも構いません。

22.1 コストの管理

項目	取り決め
費用の可視化	ライセンス費とAPI従量課金を部門別に集計し、四半期ごとに第18章の報告に含める
従量課金の管理	API利用は上限額または上限リクエスト数を設定し、超過時に通知が届くようにする。エージェントによる連続実行は特に予算を超えやすい
モデルの選び方	用途に対して過剰な性能のモデルを常用しない。要約・分類などは軽量なモデルで足りることが多い
遊休ライセンス	3か月以上利用のないライセンスは棚卸しで洗い出し、再配分または解約する
費用対効果	削減できた時間や作業量を部門ごとに把握し、次年度の投資判断に用いる

22.2 環境への配慮

- 大規模な学習・推論は電力消費が大きい。必要のない大量実行を避け、試行はサンプルデータで行う
- 同じ処理を繰り返す用途では、結果の再利用やキャッシュによって実行回数を減らす
- 自社のサステナビリティ方針に環境負荷の報告義務がある場合、AI利用分の扱いを所管部門と整理する

23. 定期見直し・改定サイクル

区分	頻度	トリガー
定期改定	半期	スケジュールに基づく定期レビュー
臨時改定	随時	重大な法改正、新リスクの顕在化、技術的転換、経営環境の重大変化

改定案はAI管理委員会が作成し、経営層の承認を経て全社に通知する。改定履歴はバージョン管理し、過去版を参照できる状態を維持する。

24. 参考法令・ガイドライン一覧

編集メモ：法令・指針は改定が続いています。本表の年月は本書作成時点のものです。配布前に最新版を確認してください。

名称	発行元	備考
AI事業者ガイドライン（第1.2版）	総務省・経済産業省	2026年3月。フィジカルAI・AIエージェント対応
人工知能関連技術の研究開発及び活用の推進に関する法律（AI推進法）	内閣府	2025年公布・全面施行。理念・推進法
人工知能基本計画	内閣府	2025年12月閣議決定
行政の進化と革新のための生成AIの調達・利活用に係るガイドライン（第2.0版・DS-920）	デジタル庁	2026年6月12日に第2.0版へ改定
人工知能関連技術の研究開発及び活用の適正性確保に関する指針	内閣府	AI推進法に基づく指針
AI時代の経営意思決定とガバナンス 戦略レポート	AIガバナンス協会(AIGA)	攻めのガバナンス
EU AI Act（Regulation 2024/1689）	EU	2024年8月発効。透明性義務は2026年8月、高リスク義務は2027年12月以降へ延期
個人情報保護法	個人情報保護委員会	2026年7月17日公布（令和8年法律第56号）。罰則関連は2027年1月17日先行施行
不正競争防止法	経済産業省	営業秘密の保護。AIへの入力と秘密管理性
著作権法	文化庁	第30条の4 等。AIと著作権に関する考え方（2024年3月）
AI・データの利用に関する契約ガイドライン	経済産業省	データ提供・利用契約の実務
ISO/IEC 42001:2023	ISO/IEC	AIマネジメントシステム
NIST AI Risk Management Framework 1.0	NIST(米国)	2023年。生成AI追補2024年
広島AIプロセス国際行動規範	G7	高度AI開発組織向け

25. よくある質問（FAQ）

編集メモ：自社で実際に多い質問に差し替えると、現場での参照率が上がります。

質問	回答
個人のChatGPT無料版を業務で少しだけ使ってもよいですか。	承認済みのEnterprise/Team版に限ります。個人版は入力データが学習に使われる可能性があり、機密漏洩のリスクがあります。
社内会議の議事録を要約させたい。入力してよいですか。	社内限定（Bランク）であれば承認済みEnterprise版に入力できます。氏名等の個人情報は匿名化してください。
AIが出した数字をそのまま資料に使ってよいですか。	いけません。数値・日付・固有名詞・URLは必ず原典で確認してください。
お客様対応のチャットをAIに任せたいです。	AI利用であることを明示し、人へエスカレーションできる経路を用意してください。高リスク判断は人が行います。
生成した画像を販売物に使えますか。	利用するツールの商用ライセンス条件を確認し、既存著作物との類似がないか公開前に確認してください。
新しいAIツールを使いたい場合は。	付録Bの利用申請書を提出してください。審査を経て承認されます。

26. 付録（記入式テンプレート集）

付録A: セルフチェックリスト

A-1. AI利用前

- ☐ 使用するツールは社内承認リスト（第6章）に含まれている
- ☐ 入力データの機密度分類（第7章）を確認した
- ☐ 個人情報・機密は入力しない、または匿名化済みである
- ☐ 利用目的は認められた業務範囲に含まれる
- ☐ Enterpriseアカウントでログインしている

A-2. AI出力利用時

- ☐ ファクトチェックを実施した（第8章）
- ☐ 数値・日付・人名・法令名・URLを原典で確認した
- ☐ 社外公開はリスクに応じた承認を得た
- ☐ AI生成の明示が必要な場合は記載した
- ☐ 著作権侵害の懸念がないことを確認した（第9章）

A-3. AIエージェント利用時

- ☐ 自律度に応じた承認を得ている（第10章）
- ☐ クリティカル操作にHuman-in-the-Loopを実装した
- ☐ 最小権限の設計を行った
- ☐ 緊急停止が実装されている
- ☐ トレーサビリティ5項目を記録している
- ☐ 外部システムとの連携先を必要最小限に制限した

付録B: AI利用申請書

項目	記入欄
申請日	
申請者（氏名・部門）	
利用予定ツール名	
提供元・契約形態	

利用目的	
入力データの機密度分類	
利用部門・利用者数	
リスクレベル（自己評価）	
リスク低減策	
承認欄（情シス）	
承認欄（法務）	
承認欄（AI管理委員会）	

付録C: インシデント報告書

項目	記入欄
報告日時	
報告者（氏名・部門）	
発生日時	
インシデント種別	データ漏洩 / 誤出力 / 著作権 / エージェント誤動作 / 攻撃検知 / その他
使用ツール・システム	
概要	
影響範囲	
初動対応	
原因（判明範囲）	
再発防止策（案）	
対応ステータス	初動完了 / 調査中 / 対策実施済 / クローズ

付録D: AIリスクアセスメントシート

項目	記入欄
対象のAI利用・システム	
利用目的・業務範囲	
入力データの種別・機密度	
想定されるリスク	
影響度（大/中/小）	
発生可能性（高/中/低）	
総合リスクレベル	禁止 / 高 / 限定 / 最小
低減策	
判定（承認/条件付/不承認）	
判定者・日付	

付録E: 承認済みAIツール棚卸し表

ツール名	用途	契約形態	許可データ範囲	承認日

付録F: 教育受講記録

対象者・部門	研修名	受講日	理解度テスト

本ガイドラインに関する質問は、AI管理委員会事務局（情報システム部）（**メールアドレス**）まで。
生成AI利活用ガイドライン 第1.0版 / **制定日** / 次回改定: **次回改定時期**