生成AIを安全に利用するための社内ガイドライン

情報漏えい・著作権侵害・誤情報を防ぎながら、
業務活用を推進する実践ルール

対象：管理職／情報システム部門／法務部門／生成AI利用者

Start契hallenge契onsulting契o.,契d.

発行：2026年8月（第1版） ／ 担当：平出



Start Challenge
Consulting co., ltd.
挑む力が、世界を照らす

Confidential — 社内限り　無断転載・社外持出を禁止

はじめに：なぜ社内ガイドラインが必要なのか

生成AIの利用は一部の専門職から全社員へ拡大しており、個人判断による利用は情報漏えいと権利侵害を招く。一方で全面禁止は業務効率化の機会損失となるため、「禁止」ではなく**「安全に使える範囲」の明文化**が必要である。

利用環境の変化[事実]

01 生成AIの利用が一部の専門職から**全社員へ広がっている**

02 個人判断での利用は情報漏えいや権利侵害につながる

03 利用を全面禁止すると、業務効率化や競争力向上の機会を失う

04 「禁止」ではなく「安全に使える範囲」を明確にすることが重要

個人判断での利用に伴う主なリスク[解釈]

1. 機密情報・個人情報の入力
2. 生成内容の誤りや捏造（ハルシネーション）
3. 著作権・商標権の侵害
4. 不適切な意思決定への利用
5. 未承認ツールの利用（シャドーAI）
6. 生成物の責任所在が曖昧になること

本ガイドラインの立場[提案]：利用を禁止せず、**①入力してよい情報の範囲　②生成結果の確認手順　③責任と報告の所在**　を定義することで、リスクを抑制しながら業務活用を推進する。

事実：生成AI利用者の全社的拡大／解釈：個人判断での利用が上記6リスクを生む／提案：利用可能範囲の明文化と手順化／出典：本ガイドライン草案（社内作成）

生成AI利用に関する基本方針

7つの基本原則は**「最終的な判断と責任は人が持つ」**ことを中核に、入力情報・結果確認・利用ツール・報告の4点を統制する。適用対象は雇用形態を問わず、社内システムを利用する全関係者とする。

基本原則（7項目）

1	生成AIは**業務を支援するツール**として利用する
2	**最終的な判断と責任は人が持つ**
3	機密情報や個人情報を**無断で入力しない**
4	生成結果をそのまま利用せず、必ず確認する
5	著作権・契約・社内規程を遵守する
6	会社が承認したツールとアカウントを利用する
7	問題が発生した場合は速やかに報告する

ガイドラインの対象者

- 正社員
- 契約社員・派遣社員
- 業務委託先
- 役員・管理職
- 社内システムを利用する外部パートナー

※雇用形態・契約形態を問わず適用する。委託先・外部パートナーには契約または誓約書により遵守を求める[提案]。

原則2が本ガイドラインの中核：生成AIの出力は**判断材料**であり、意思決定の責任は**利用者と承認者**が負う。

事実：7原則および対象者範囲の定義／解釈：原則2が他6原則の前提となる／提案：委託先へは契約・誓約書で遵守を担保／出典：本ガイドライン草案（社内作成）

利用可能な生成AIと利用環境

利用は**会社承認ツールと法人アカウント**に限定し、学習利用の停止・履歴保存期間・多要素認証を設定条件とする。承認状況とその条件は管理台帳で一元管理し、情報システム部門が維持する。

利用ルール（7項目）

- 会社が**承認した生成AIサービスのみ**利用する
- 業務では**会社発行のアカウント**を使用する
- 個人アカウントとのデータ共有を**禁止**する
- 多要素認証（MFA）を設定する
- 入力データが**学習に利用されない**契約・設定を選ぶ
- チャット履歴・データ保存期間を適切に設定する
- プラグイン・外部連携・API利用は**事前承認制**とする

管理台帳の例（記載項目）

管理項目	記載内容
ツール名	ChatGPT、Microsoft Copilot など
利用目的	文書作成、要約、調査など
利用部門	営業部、管理部など
入力可能な情報	公開情報、社内一般情報
管理責任者	情報システム部門
契約・設定	法人契約、学習利用停止など

※台帳は情報システム部門が管理し、四半期ごとに棚卸しを行う［提案］。

事前承認が必要な利用：**新規ツールの追加** ／ **プラグイン** ／ **外部システム連携** ／ **API利用** — 申請先：情報システム部門・AI管理責任者

事実：利用ルール7項目と台帳項目の定義／解釈：ツール承認と設定条件の管理が漏えい防止の起点／提案：四半期棚卸しと事前承認制の運用／出典：本ガイドライン草案（社内作成）

生成AIに入力してよい情報・禁止する情報

入力可否は情報の機密性で判定する。判断に迷う場合の基準は**「その情報が外部に公開されても問題ないか」**の一点であり、否または不明であれば入力せず、匿名化（P6）または上位者へ確認する。

入力可能な情報［原則○］

- ○ 一般に公開されている情報
- ○ 自社Webサイトで公開済みの内容
- ○ 個人や取引先を特定できない情報
- ○ 匿名化・抽象化した業務情報
- ○ 会社が入力を許可した社内情報

入力禁止情報［×｜全面禁止］

- × 顧客・取引先の個人情報
- × 氏名、住所、電話番号、メールアドレス
- × **ID、パスワード、APIキー**
- × 未公開の経営情報・財務情報
- × 契約書、見積書、顧客名簿
- × ソースコードやシステム構成などの機密情報
- × 医療・健康・人事評価などの要配慮情報
- × 秘密保持契約（NDA）の対象となる情報

判断基準：**「その情報が外部に公開されても問題ないか」**を入力前に確認する。判断できない場合は入力せず、上司または情報システム部門へ照会する。

事実：入力可能5類型／禁止8類型の定義／解釈：機密性の有無が入力可否を決定する／提案：判断不能時は入力停止と照会を義務化／出典：本ガイドライン草案（社内作成）

情報の匿名化・加工方法

入力禁止情報も**固有名詞の一般化と数値の丸め**で入力可能な形に加工できる。ただし単独では特定できない情報も**組み合わせにより個人が特定される**ため、属性・所属・地域の粒度まで確認する。

安全に入力するための加工例

加工前（入力不可）	加工後（入力可能）
株式会社〇〇からの問い合わせ	製造業A社からの問い合わせ
山田太郎、営業部長	顧客担当者
売上高8億4,000万円	売上高約8億円
東京都新宿区〇丁目	東京都内
実際の契約書全文	契約条項を抽象化した文章
社員番号・メールアドレス	削除または仮の記号に置換

匿名化時の注意点

- 氏名だけでなく、**所属・役職・住所**なども確認する
- 複数情報の**組み合わせによる個人特定**を防ぐ
- ファイルの作成者情報やコメントも削除する
- PDFや画像に残る情報にも注意する

加工の考え方：**「誰が・どこの・いくら」を業務判断に必要な粒度まで落とす。**ファイル添付時はメタデータ（作成者・変更履歴・コメント）の削除を必須とする。

事実：加工例6類型と注意点4項目／解釈：単独では非特定の情報も組合せで特定に至る／提案：添付前のメタデータ削除を必須化／出典：本ガイドライン草案（社内作成）

生成結果の確認ルール

生成AIの回答は**「完成品」ではなく「確認が必要な下書き」**である。事実・数値・固有名詞・鮮度・表現の5観点を確認し、社外に出る成果物は一次情報照合と第三者レビューを経る。

必ず確認する項目（7点）

1. 事実関係は正しいか
2. 数字、日付、固有名詞に誤りがないか
3. **存在しない法律、文献、事例を作っていないか**
4. 情報が古くなっていないか
5. 差別的・偏見を含む表現がないか
6. 社内ルールやブランド表現に合っているか
7. 読み手に誤解を与えないか

重要な原則

生成AIの回答は「完成品」ではなく「確認が必要な下書き」として扱う。

確認方法（4手段）

- 公式Webサイトや**一次情報**との照合
- 社内データとの照合
- 別担当者によるレビュー
- 法務・情報システム・専門部署への確認

社外提出物・公開物は、**一次情報照合＋別担当者レビュー＋責任者承認**の3段階を必須とする[提案]。

事実：確認7項目と確認手段4種の定義／解釈：誤り・捏造は出力の性質上必ず生じ得る／提案：社外公開物は3段階確認を必須化／出典：本ガイドライン草案（社内作成）

著作権・商標・知的財産への対応

権利侵害リスクは**既存作品の入力・模倣・商用公開**の場面で顕在化する。社外公開物は担当者審査を経ることを条件とし、指示内容と確認結果を記録して説明可能性を確保する。

注意が必要な利用例[リスク事象]

- ! 記事や書籍を丸ごと入力して要約する
- ! 他社サイトの文章を模倣させる
- ! 特定の作家やデザイナーの作品に酷似させる
- ! 他社ロゴやキャラクターを生成物に使用する
- ! **生成されたプログラムコードを無確認で商用利用する**

社内ルール[対応策]

- 出典や利用条件を確認する
- 既存作品との**類似性**を確認する
- 他社の文章をそのまま転用しない
- 商用公開する画像や文章は担当者が審査する
- 重要な制作物は**法務・知財担当**へ確認する
- 生成に利用した指示や確認結果を**記録する**

審査を必須とする範囲：**社外公開する文章・画像・動画／商用利用するプログラムコード／ブランド表現を含む制作物** ―記録項目：指示文・生成日・確認者・確認結果

事実：注意すべき利用例5件と社内ルール6項目／解釈：入力・模倣・商用公開の3場面にリスクが集中／提案：社外公開物の担当者審査と記録の義務化／出典：本ガイドライン草案（社内作成）

業務別の利用可否

利用可否は業務ごとに3区分で定める。**個人情報の取扱い・人の処遇に関わる判断・認証情報の入力**は原則禁止であり、条件付き（△）は必ず責任者または専門部署の最終確認を伴う。

○ 利用可　△ 条件付き（確認・承認が必要）　× 原則禁止

業務	利用可否	条件
メール文章の下書き	○	顧客情報を匿名化する
会議アジェンダ作成	○	機密情報を入力しない
公開情報の要約	○	出典を確認する
アイデア出し	○	人が評価・選定する
社内議事録の要約	△	承認環境・匿名化が必要
契約書のレビュー	△	法務担当者が最終確認する
採用候補者の評価	△	AIだけで判断しない
顧客への正式回答	△	責任者が内容を確認する
個人情報を含むデータ分析	×	原則禁止。承認環境のみ検討
人事処分・与信判断	×	AI単独で決定しない
パスワードやAPIキーの入力	×	**全面的に禁止する**

△の業務は「承認された環境で行うこと」と「人による最終確認者を明示すること」の2条件を同時に満たす場合のみ実施できる。判断が難しい業務はAI管理責任者へ照会する。

事実：業務11区分の可否と条件の定義／解釈：人の処遇・認証情報・個人情報が禁止領域を形成／提案：△業務は承認環境と最終確認者の明示を条件化／出典：本ガイドライン草案（社内作成）

高リスク業務における利用制限

人の権利・資産・安全に影響する業務は、**生成AIのみで結論を出すことを禁止**する。専門資格者または責任者の確認、判断根拠の記録、対象者への説明可能性の確保を利用条件とする。

高リスクとなる業務（8領域）

- 採用・評価・昇進・解雇
- 融資・保険・与信判断
- 法務・税務・会計判断
- 医療・健康に関する判断
- 顧客との契約条件の決定
- 経営計画や投資判断
- セキュリティ設定や本番環境の変更
- 社外向けの公式見解の作成

利用条件（5要件・すべて充足が必要）

1. **生成AIだけで結論を出さない**
2. 専門資格者や責任者が確認する
3. 判断根拠と確認者を記録する
4. 必要に応じて複数名で承認する
5. 顧客や対象者への**説明可能性**を確保する

高リスク業務での生成AIは**「案の作成と論点整理」**までに限定し、**決定行為には用いない。**

事実：高リスク8領域と利用条件5要件の定義／解釈：人の権利・資産・安全への影響度が制限根拠／提案：用途を案作成と論点整理に限定／出典：本ガイドライン草案（社内作成）

安全なプロンプト作成と利用例

安全な指示は**「役割・目的・条件・禁止事項・確認事項」の5要素**で構成する。個人情報を含む依頼は、集計・抽象化した設問へ言い換えることで、目的を維持したまま入力リスクを除去できる。

安全な指示の基本形（5要素）

役割	何の専門家として回答するか
目的	何を作成するか
条件	文字数、形式、対象者
禁止事項	推測しない、個人情報を出さない
確認事項	不明点を明示する、根拠を示す

プロンプト例（推奨形）

以下の公開情報をもとに、営業メールの下書きを300文字以内で作成してください。個人名や実在企業名は使用せず、不明な情報を推測しないでください。事実確認が必要な箇所には「要確認」と記載してください。

悪い例（入力禁止情報を含む）

この顧客名簿を分析して、契約しそうな顧客を特定してください。

改善例（抽象化して目的を維持）

個人を特定できない業種別・規模別の集計データをもとに、反応率が高い顧客層の傾向を整理してください。

プロンプト設計の要点：**「個票を渡さず、集計で問う」**。加えて「推測の禁止」と「要確認の明示」を指示に含めることで、誤情報の混入を検知しやすくする。

事実：指示の5要素と例文3種の定義／解釈：個票を集計へ言い換えることで目的を保持しリスクを除去できる／提案：推測禁止と要確認明示の定型化／出典：本ガイドライン草案（社内作成）

事故・問題が発生した場合の対応

被害拡大の主因は発見の遅れである。事象を認識した時点で**直ちに利用を停止し、当日中に上司と情報セキュリティ窓口へ報告**する。自己解決・履歴削除・翌日以降への先送りは禁止する。

報告が必要な事象

- 個人情報や機密情報を入力してしまった
- 誤った生成内容を社外へ送信した
- 著作権侵害の可能性が判明した
- 未承認ツールを業務で利用した
- アカウントの不正利用が疑われる
- 不適切な回答や有害な生成結果が出た

初動対応フロー（発見から再発防止まで）

1. **利用・送信を直ちに停止する**
2. 入力・出力・送信先を確認する
3. **上司と情報セキュリティ窓口へ報告する（当日中）**
4. 履歴や画面、日時を記録する
5. データ削除やアカウント停止を実施する
6. 影響範囲を調査する
7. **再発防止策を決定する**

禁止事項［発生時］

① 自分だけで解決しようとする　② 履歴を隠す・削除する　③ 報告を翌日以降に先送りする

事実：報告対象6事象・初動7手順・禁止3行為の定義／解釈：被害拡大の主因は発見・報告の遅延／提案：当日中の報告を義務化し記録を必須とする／出典：本ガイドライン草案（社内作成）

管理体制・教育・定期見直し

ガイドラインは策定で完結しない。**役割分担の明確化・必須研修・半年〜年1回の見直し**を運用サイクルとして定着させ、法令やサービス仕様の変更に追随する。

推奨する管理体制（役割と責任）

役割	責任範囲
経営責任者	生成AI活用方針の承認
AI管理責任者	全社ルールと活用状況の管理
情報システム	ツール、アカウント、ログの管理
法務・知財	契約・著作権・法的リスクの確認
部門責任者	利用目的と業務上の妥当性を判断
利用者	ルール遵守と生成結果の確認

運用施策（PDCA）

- 利用開始時の**必須研修**
- 年1〜2回の再教育
- 承認ツール一覧の更新
- 利用状況・インシデントの定期確認
- 法令・サービス仕様変更への対応
- 半年または年1回の見直し

教育テーマ（5項目）

情報の分類 / 安全なプロンプト作成 / ハルシネーションへの対応 / 著作権・個人情報 / 事故発生時の報告方法

運用サイクル

研修（利用開始時） ▶ 利用状況・インシデントの定期確認 ▶ 承認ツール一覧の更新 ▶ ガイドライン改定（半年〜年1回） ▶ 再教育

事実：役割6区分・運用施策6項目・教育5テーマの定義／解釈：策定のみでは陳腐化しリスクが再発する／提案：研修〜改定〜再教育を年次サイクルとして固定／出典：本ガイドライン草案（社内作成）

利用前チェックリスト・まとめ

利用前の10項目を全て満たしたときのみ生成AIを業務利用できる。**目的の明確化・入力情報の管理・人による確認・責任者の関与・継続的な教育更新**の5点が本ガイドラインの要旨である。

生成AI利用前チェックリスト（10項目）

- ☐ 会社が承認した生成AIを使用している
- ☐ 会社の業務用アカウントでログインしている
- ☐ **個人情報や機密情報を含んでいない**
- ☐ 必要な情報は匿名化・抽象化している
- ☐ 入力データが学習に利用されない設定を確認した
- ☐ **生成結果の事実確認を行った**
- ☐ 著作権や商標権の問題がない
- ☐ 社外公開前に責任者の承認を受けた
- ☐ **AIだけで重要な判断を行っていない**
- ☐ 問題発生時の報告窓口を把握している

まとめ（5要旨）

1. 生成AIの利用目的と許容範囲を明確にする
2. 入力情報を管理し、機密情報の漏えいを防ぐ
3. 生成結果は必ず人が確認する
4. 高リスク業務では責任者と専門部署が関与する
5. 作成して終わりではなく、教育と定期更新を続ける

巻末案内（問い合わせ窓口）

- ・生成AI利用申請窓口
- ・情報セキュリティ相談窓口
- ・インシデント報告先
- ・社内研修／改定履歴

意思決定事項

① 本ガイドラインの承認　② 承認ツールと利用環境の確定　③ 必須研修の開始時期　④ 見直し頻度（半年／年1回）の決定

事実：チェック10項目・要旨5点・窓口4種の定義／解釈：10項目は本文P3～P13の要件を実務手順に落としたもの／提案：全項目充足を利用条件とする／出典：本ガイドライン草案（社内作成）

お問い合わせ先

本ガイドラインの解釈、利用申請、インシデント報告は下記窓口が一元的に受け付ける。**緊急時（情報漏えい・誤送信）は判断を待たず即時連絡**のうえ、P12の初動対応フローに従うこと。

お問い合わせ窓口

会社名	Start Challenge Consulting
メールアドレス	info@startchg.com
担当	平出

受付内容

- 生成AI利用申請・ツール追加申請
- 社内研修・改定履歴の照会
- 入力可否・匿名化の判断照会
- **インシデント報告（即時）**

Start Challenge
Consulting co., ltd.

挑む力が、世界を照らす

本ガイドラインは半年または年1回見直しを行い、
最新版を社内ポータルで公開する。

Confidential — 社内限り　無断転載・社外持出を禁止　／　発行：2026年8月（第1版）　Start Challenge Consulting co., ltd.