COLUMN | AI活用 | 2026.07.22

生成AIの情報漏洩リスクと安全な活用ルール

株式会社DnD — Distill n Develop

SUMMARY

この資料の要点

3つのポイント

- 無料・個人向けAIツールへの業務情報入力は、利用規約によっては学習データとして活用される場合がある。
- 「入れてよい情報・入れてはいけない情報」の線引きを社内で明文化するだけで、リスクを大幅に下げられる。
- 企業向けプランへの切り替えと、管理者によるアクセス制御の整備が、組織的な安全対策の2本柱になる。

生成AIへのデータ入力に潜む2つのリスク

生成AIのセキュリティリスクは、大きく2種類あります。

- **学習への利用リスク**：入力したデータがモデルの改善・学習に使われ、他のユーザーへの回答に間接的に反映される可能性がある。
- **データ保管リスク**：クラウドサービス上にやり取りの履歴が保存され、不正アクセスや事業者のインシデントによって情報が漏れるリスクがある。

どちらも「使うツールの種類」と「利用規約の設定」によって大きく変わります。

無料プランと企業向けプランの違い

無料・個人向けプランはデフォルト設定のまま使うと学習に活用される場合があります。企業・チーム向けプランでは以下が契約上保証されます。

- 入力データはモデルの学習に使用しない。
- データは契約企業の管理下に置かれ、第三者に共有されない。
- 管理者が利用状況を監査ログで確認できる。

> *「何となく使っている」状態から「管理された環境で使っている」状態への移行が、組織的なリスク管理の第一歩です。*

GUIDELINES

「入れてよいデータ」「入れてはいけないデータ」の判断基準

判断の基準はシンプルです。**「その情報が外部に出たとき、問題になるか」**という一点に尽きます。

入れてよい情報（例）

- 公開資料の要約・一般的な文書のリライト
- 汎用的な調査・情報収集
- 社内の非機密ドキュメントの文章整理
- 一般的な質問・アイデア出し

原則入れてはいけない情報（例）

- 顧客の氏名・連絡先・契約内容などの個人情報
- 未発表の事業計画・財務データ
- 取引先との秘密保持契約（NDA）対象情報
- 採用候補者の個人情報

ツール選定のセキュリティ視点 3つのチェックポイント

- **① 利用規約のデータ学習条項**：入力データが学習に使われないことが契約上明記されているか。「オプトアウトできる」と「契約上使わない」は意味が異なります。
- **② 管理者機能の有無**：組織のアカウントを一元管理でき、社員の利用状況を把握・監査できるか。
- **③ データ保管場所と暗号化**：データが契約したリージョンに保管され、転送・保管ともに暗号化されるか。

ACTION STEPS

社内ルール整備の3ステップ

ステップ1：現状把握

社員がどのAIツールをどのような業務に使っているかを確認します。簡単なアンケートや1on1の場でも把握できます。現状を知ることがすべての起点です。

ステップ2：入力可否の基準を決める

「入れてよい情報・入れてはいけない情報」の区分を自社の業種・業務に合わせて文書化します。完璧なルールより、まず基準を明文化することが重要です。

ステップ3：推奨ツールを指定して切り替える

個人アカウントの利用から企業向けプランへ移行し、管理者を設置します。ChatGPT Team、Claude for Work（Team）、Google Workspace のGemini機能などが選択肢になります。

> *ルールは運用しながら改善できます。基準がないまま使い続けることがリスクを積み上げます。*

まとめ

生成AIの情報漏洩リスクは「使ってはいけない」という話ではなく、「どのツールで」「何を入れるか」を決めることで管理できます。無料プランから企業向けプランへの切り替えと、入力情報の社内基準の明文化——この2つを実践することで、リスクを抑えつつAIの恩恵を最大限に活用できる環境が整います。

相談・見積り無料 → https://dnd-inc.jp/contact.html