

AI 利用 セキュリティチェックリスト

会社で AI を使う前に決めておく24項目

 Tomonau株式会社

この資料の読み方

特定のサービス名を挙げて「安全」「危険」と断定する書き方は避けています。

各社の仕様は変わるためです。書いてあるのは、会社として決めておく事柄です。

この資料は誰のためのものか

従業員10名以下の会社で、業務にAIを使い始めている、または使い始めようとしている方。

- 社員が個人の判断でAIを使っていて、少し不安がある
- 顧客の情報を入れてよいのか、判断がつかない
- 「ルールを作れ」と言われても、何を書けばいいか分からない

情報システム部門がない会社を想定しています。専門知識は前提にしていません。

1. 何が起こりうるのか

AIの利用で問題になるのは、だいたい次の3つに分かれます。「AIが危ない」という話ではなく、使い方の問題です。

型1 入れた情報の行き先

入力した内容が、サービス側でどう扱われるか。設定や契約によって変わります。無料版と有料版で扱いが違ふことがあります。

型2 出てきた答えをそのまま使う

AI の出力には誤りが混ざります。事実と違う内容が、もっともらしい文体で出てきます。確認せずに社外へ出すと、そのまま自社の発信になります。

型3 アカウントと権限

誰がどのアカウントを持っているか。退職した人のアカウントが残っていないか。共有リンクが外に出ていないか。

この3つを押さえれば、実務上の大半はカバーできます。

2. チェックリストの使い方

- 「できている」に✓、「できていない」に×を付けてください
- 各項目に「なぜ必要か」「どう決めるか」を書いています
- 全部を一度に整えなくて構いません。§4に「最低限これだけ」を書いています

3. チェックリスト

A. 何を使うかを決める

A-1 業務で使ってよいAIサービスを、名前で決めている ☐

- なぜ: 決めていないと、社員ごとに違うサービスを使い、扱いを把握できなくなります
- どう決めるか: いま実際に使われているものを聞き取り、その中から選ぶ。禁止から入らない

A-2 無料版と有料版のどちらを使うか決めている ☐

- なぜ: 入力内容の扱いが版によって違うことがあります
- どう決めるか: 業務で使うなら、事業者向けの契約を検討する

A-3 新しいサービスを使いたいとき、誰に言えばよいか決まっている ☐

- なぜ: 相談先がないと、黙って使われます
- どう決めるか: 代表または担当者を1人決め、「試す前に一言」とだけ伝えておく

A-4 社員個人のアカウントで業務をしていない ☐

- なぜ: 退職時に履歴ごと持ち出される、または引き継げなくなります
 - どう決めるか: 会社のアカウントを用意する
-

B. 何を入れてよいか決める

ここが最も大事です。「機密情報を入れるな」だけでは運用できません。具体的に分けてください。

B-1 入れてはいけない情報を、具体例で書き出している ☐

- なぜ: 抽象的な指示は守られません
- どう決めるか: 自社の事例で列挙する。たとえば、顧客の氏名や連絡先、契約書の原本、未公開の財務情報、他社から預かった資料、社員の個人情報など

B-2 入れてよい情報も、具体例で書き出している ☐

- なぜ: 禁止だけを並べると、萎縮して使われなくなります
- どう決めるか: 公開済みの情報、社内で作った一般的な文章、固有名詞を伏せた相談などを例示する

B-3 迷ったときの判断基準がある ☐

- なぜ: 例示に当てはまらない場面が必ず出ます
- どう決めるか: ひとつの基準を持つ。たとえば「これが外部に出て困るか」を自問する

B-4 顧客から預かった情報を入れる場合、事前に合意している ☐

- なぜ: 契約で第三者提供が制限されていることがあります
- どう決めるか: 契約書の秘密保持条項を確認する。必要なら顧客に確認する

B-5 固有名詞を伏せて使う方法を、社内で共有している ☐

- なぜ: 実務では「相談したいが、そのままは入れられない」場面が多くあります
- どう決めるか: 社名を A 社に置き換える、金額を丸めるなど、具体的なやり方を示す

C. 設定を確認する

C-1 入力内容が学習に使われる設定になっていないか、確認している ☐

- なぜ: 既定の設定はサービスや契約によって異なります
- どう決めるか: 使うサービスの設定画面で、学習利用に関する項目を確認する。「たぶん大丈夫」で済ませない

C-2 履歴の保存期間を把握している ☐

- なぜ: 消したつもりが残っていることがあります
- どう決めるか: 設定画面で確認する

C-3 共有リンクを作った場合、公開範囲を確認している ☐

- なぜ: 会話の共有リンクが、誰でも見られる状態になることがあります
- どう決めるか: 共有機能を使ったら、範囲と期限を確認する

C-4 設定を確認した日を記録している ☐

- なぜ: 仕様は変わります。いつ時点の確認かが分らないと、確認した意味が薄れます
- どう決めるか: 確認日をメモしておく。年に1度は見直す

D. 出てきた答えの扱い

D-1 社外に出すものは、必ず人が確認している ☐

- なぜ: AI の出力には誤りが混ざります
- どう決めるか: 誰が最終確認するかを決める。ひとりの会社なら「送る前にもう一度読む」を習慣にする

D-2 事実・数値・固有名詞は、出典を確かめている ☐

- なぜ: AI はもっともらしい嘘を出します。実在しない法令や統計を作ることがあります
- どう決めるか: 数値や条文が出てきたら、必ず一次情報で照合する

D-3 法務・税務・労務の判断を、AI の答えだけで決めていない ☐

- なぜ: 責任を負えません

- どう決めるか: 下調べには使い、判断は専門家に確認する

D-4 AI を使って作ったことを、必要な場面で伝えられる ☐

- なぜ: 取引先によっては、生成物の扱いに条件を付けていることがあります
 - どう決めるか: 契約や仕様書に生成AIに関する条項がないか確認する
-

E. アカウントと退職者

E-1 誰がどのアカウントを持っているか、一覧がある ☐

- どう決めるか: 表を1枚作る。サービス名・利用者・作成日でよい

E-2 退職・異動のときに止める手順がある ☐

- なぜ: 止め忘れが最も多い抜けです
- どう決めるか: 退職時のチェック項目に AI のアカウントを加える

E-3 二段階認証を有効にしている ☐

- なぜ: パスワードだけでは、業務の履歴ごと乗っ取られます
 - どう決めるか: 使うサービスの設定で有効にする
-

F. 決めたことを残す

F-1 ここまでの内容を、1枚の文書にまとめている ☐

- なぜ: 口頭の取り決めは引き継げません
- どう決めるか: A4で1〜2枚。長い規程は読まれません

F-2 新しく入った人に渡している ☐

- どう決めるか: 入社時の書類に加える

F-3 問題が起きたときの連絡先を決めている ☐

- なぜ: 入れてはいけない情報を入れてしまったとき、隠されるのが最も困ります

- どう決めるか: 「気づいたらすぐ言う。責めない」と明示する。誰に言うかを決める

F-4 年に1度、見直す日を決めている ☐

- なぜ: サービスの仕様も、自社の業務も変わります
- どう決めるか: 決算期など、思い出せる時期に紐づける

4. 最低限これだけ

24項目のうち、**まずこの3つ**から始めてください。他が未着手でも、この3つで多くを防げます。

項目		理由
1	B-1 入ってはいけない情報を具体例で書き出す	事故の入口をふさぎます
2	C-1 学習に使われる設定を確認する	一度確認すれば済みます
3	D-1 社外に出すものは人が確認する	誤りが外に出るのを止めます

この3つは、費用をかけずに今日から始められます。

5. よくある誤解

「機密情報を入れなければ安全」 入力だけが論点ではありません。出力をそのまま使うこと（型2）と、アカウントの管理（型3）も同じくらい起きています。

「有料版なら安全」 版によって扱いが違うのは事実ですが、有料であれば自動的に安全になるわけではありません。設定は別途確認が必要です。

「ルールを厳しくすれば安心」 禁止だけを増やすと、隠れて使われます。そのほうが危険です。**使ってよい範囲を明示するほうが安全**です。

「小さい会社だから狙われない」狙われるかどうかとは別に、うっかり社外に出してしまう事故は規模に関係なく起きます。

「一度決めれば終わり」サービスの仕様は変わります。F-4 のとおり、見直す日を決めてください。

6. 次の一步

チェックした結果、次のような状態であれば、ご相談ください。

- × が多く、どこから手をつけるか決められない
- B の線引きを、自社の業務に合わせて具体化したい
- C の設定確認を、使っているサービスごとに見てほしい
- F の文書を1枚にまとめたい

Tomonau では、この24項目を一緒に確認するところから始めています。オンラインで30～45分、無料です。強引な営業はしません。2営業日以内にご返信します。

参考: Tomonau の進め方

私たち自身が、お客様の情報を扱うときに守っていることです。

- | | |
|---|---------------------|
| 1 | AI に学習させない設定で利用します |
| 2 | 機密情報は、入力前にお客様と合意します |
| 3 | 最終確認は人が行います |
-
-

会社情報

社名	Tomonau株式会社（Tomonau Inc.）
代表者	代表取締役 西田 忠
設立	令和8年8月8日
所在地	〒550-0003 大阪市西区京町堀1-17-16 京町堀センタービルディング301
事業内容	AI/DXコンサルティング、デザイン・Web制作、システム開発、AIスクール、マーケティング

本資料は一般的な考え方を整理したものであり、法的な助言ではありません。個別の判断は専門家にご確認ください。内容は作成時点で確認できる範囲に基づいています。