中小企業のための「AI利用リスク判定チェックリスト（全10項目）」＆安全活用スタートアップガイド

中小企業のための「AI利用リスク判定チェックリスト（全10項目）」＆安全活用スタートアップガイド

現場の業務効率化を目的に生成AIの利用が急速に広がる一方、会社が把握していないところで従業員が個人アカウントのAIを無断利用する **「シャドーAI」や、AIの出力結果を無検証のまま実務に流用することによる情報漏洩・システム障害・法的トラブル** が急増しています。

自社の現場に「見えない爆弾」が潜んでいないか、以下の10項目で現在の管理状況を判定してください。

PART 1：自社の危険度を可視化する「AI利用リスク判定チェックリスト（全10項目）」

現在の社内の状況に当てはまる項目にチェック（✓）を入れてください。

【A. 情報漏洩・シャドーAIリスク（入力の管理）】

- ☐ **1. 誰がどのAIツールを業務に使っているか、会社として正確に把握していない**
  （会社が許可していない無料ツールや個人アカウントを、従業員が独断で業務利用している可能性がある）
- ☐ **2. AIの「学習機能（オプトアウト設定）」のオフ手順を、利用者に徹底していない**
  （初期設定のまま業務データを入力し、自社の機密情報がAI開発企業の学習データとして吸い上げられているリスクがある）
- ☐ **3. 「入力してはいけない情報（個人情報・取引先機密）」の明確な基準がない**
  （議事録の要約やメール作成のため、顧客の実名・メールアドレス・未公開の契約条件などをそのまま貼り付けている恐れがある）

【B. 品質事故・ブラックボックス化リスク（出力の検証）】

- ☐ **4. AIが生成したプログラムコードやExcelマクロを、構造を理解しないまま本番業務に組み込んでいる**
  （「動くから問題ない」と過信し、セキュリティの脆弱性やバグが潜んだまま運用されている危険性がある）
- ☐ **5. AIが出力した調査数値や事実関係を、一次情報（公的統計や公式文書）で裏付け確認していない**
  （AI特有の「もっともらしい嘘＝ハルシネーション」に気づかず、誤ったデータで経営判断や営業提案を行うリスクがある）

- [ ] **6. AIが作成した記事・画像・デザインを、著作権や商標権の確認なしにWebサイトや広告へ公開している**
（既存の他社著作物と酷似した生成物をそのまま公開し、著作権侵害等の法的トラブルに発展する恐れがある）
- [ ] **7. 業務フローの自動化を従業員個人のアカウントやノウハウに依存しており、社内で仕組みが共有されていない**
（作成した本人しか中身がわからない「ブラックボックス」となり、エラー発生時や退職時に業務が完全停止するリスクがある）

【C. 組織統治・教育体制リスク（ガバナンス）】

- [ ] **8. 社内に「AI利用ガイドライン（利用規定）」が存在しない、または形骸化している**
（善悪や安全の判断基準が従業員個人のリテラシーに丸投げされており、事故が起きた際の責任所在が曖昧になっている）
- [ ] **9. 現場で「この使い方は安全か？」「なぜエラーが出るのか？」と迷った際、すぐに相談できる専門家がいない**
（疑問を解消できないまま自己流で危険な運用を続けるか、あるいは怖くなってAI利用そのものをやめてしまう）
- [ ] **10. 体系的なAIの基礎研修を実施しておらず、「使い方は各自で覚える（OJT・独学任せ）」になっている**
（指導側の時間不足により教育が行き届かず、安全に使いこなせる人と危険な使い方をする人の二極化が進んでいる）

【判定結果】チェックがついた数でわかる自社のリスクレベル

- **チェック 0個：【安全（統治状態）】**
AIを安全に統治し、生産性を高める土台が整っています。最新ツールの実践活用へステップアップしましょう。
- **チェック 1〜3個：【要注意（予備軍）】**
一部の現場で「シャドーAI」や確認漏れが発生し始めています。早急に利用ルールの明文化と基礎教育が必要です。
- **チェック 4個以上：【危険（事故発生リスク大）】**
いつ情報漏洩やシステムトラブル、対外的な信用失墜が起きてもおかしくない状態です。直ちに利用実態の把握と、正しいAI教育の導入を開始してください。

PART 2：今日から社内で共有できる「AI安全活用・3つの鉄則テンプレート」

リスクを防ぐためにAIを「全面禁止」すれば、企業の競争力は失われます。重要なのは「禁止」ではなく **「正しいルールと知識による統治」** です。まずは以下の3原則を社内チャットや朝礼で周知してください。

鉄則①：入力のルール（機密と個人情報は絶対に入れない）

1. 会社が許可したアカウント（学習オフ設定済み）以外を業務で使用しないこと。

2. **顧客の氏名・連絡先・マイナンバー等の個人情報**、および**社外秘の取引データ・認証パスワード**は、いかなる場合もプロンプトに入力しないこと（匿名化・マスキング処理を徹底する）。

鉄則②：検証のルール（AIの出力は「下書き」として扱う）

1. AIが生成した文章・数値・コードは「完成品」ではなく「精度の高いタタキ台」と定義する。
2. 外部へ提出・公開する資料や、本番システムへ実装するコードは、**必ず人間が根拠（一次情報）と安全性を確認（レビュー）し、最終責任を持つ**こと。

鉄則③：共有のルール（疑問やエラーを1人で抱え込まない）

1. 挙動が理解できないコードやツールを独断で業務に組み込まないこと。
2. 判断に迷うケースや便利な活用法を見つけた際は、必ず管理者・推進チームへ共有し、組織の共通資産として安全性を検証すること。

PART 3：現場の摩擦ゼロで「安全なAI自走組織」をつくるには？

ルールを定めても、現場に「正しい知識」と「すぐに質問できる環境」がなければ、安全かつ効果的なAI活用は定着しません。

実践型AI学習プラットフォーム **「オルタナファンカレッジ（Alterna.fun College）」** は、長時間の座学で現場を疲弊させることなく、安全なAI統治と業務効率化を同時に実現します。

1. **1回約10分の実務画面動画で「セキュリティと実践」を効率習得**
   「セキュリティ上のリスクと対策」「検索エンジンとの使い分け」「失敗事例から学ぶ対策」から、ChatGPT・Gemini・Copilotの実務操作まで426講座以上を提供。スキマ時間で正しい知識が身につきます。
2. **実務家・エンジニアへの「直接深掘り質問」でブラックボックス化を防止**
   「自社の業務にどう組み込めば安全か」「出力されたコードのどこを確認すべきか」といった疑問を、現場目線の実務家が直接解説・サポートします。
3. **国の助成金活用で「実質月額2,800円（税抜）/ 1ID」からスモールスタート**
   厚生労働省「人材開発支援助成金（定額制訓練）」に対応。まずは経営陣やリーダー層3名（最小単位）から、最小限のコストとリスクで安全なAI教育をテスト導入いただけます。

▼ 無料トライアル・自社向けカリキュラム診断のお申し込み

自社の課題に合わせた「推奨カリキュラム（10時間分）の無料設計」および、実際の講座・管理画面をお試しいただける「無料トライアル」を受け付けております。

- **オルタナファンカレッジ 公式LP：** https://alternativecomputers.org/lp9/
- **助成金活用・申請ステップ解説：** https://alternativecomputers.org/alternafun-hojo/
- **運営：** 有限会社野田収一事務所（オルタナティブ・コンピュータ）