知らなかったでは済まされない。社員のAI利用が会社を危険にさらす。

**AIを使う社員が増える一方で、
御社のセキュリティ対策は追いついていますか？**



生成AI・AIエージェント時代の企業セキュリティ入門 ›

知らない間に進む、企業のAIセキュリティリスク



AIのリスクは“入力”だけではありません。
情報・判断・行動の3つで考える必要があります。

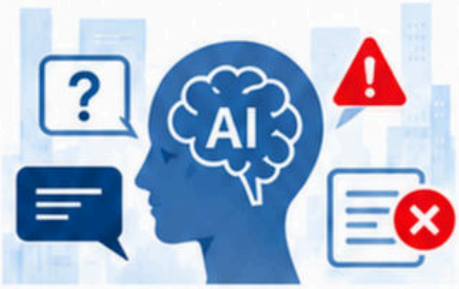
1 情報リスク



機密情報・個人情報が外部に流出するリスク

- 顧客情報・個人情報の入力
- 外部サービス連携による情報流出
- 保存先・学習利用の確認不足

2 判断リスク



誤った回答や根拠不明の提案による業務の誤り

- 誤回答・ハルシネーション
- 根拠不明の提案
- 確認不足のまま社外に共有

3 行動リスク



AIの出力や動作による不適切な行動や影響の拡大

- AIエージェントの送信・更新
- 過剰権限による誤操作
- 自律実行による影響の拡大

便利さが増すほど、管理対象も増える。

社員の何気ないAI利用に潜む4つの危険

日常業務の中にある“便利さ”が、事故の入口になることがあります。

1 顧客情報をそのまま入力

見積、契約、個人情報など、
業務で扱う機密情報を
匿名化せずに入力する。



2 AI生成文書を確認せず送信

誤回答や不正確な内容、
不適切な表現が含まれたまま、
顧客に送信してしまう。



3 個人アカウントで業務利用

会社が把握できない
個人アカウントでの利用により、
管理されない“シャドーAI”が
増える。



4 外部資料をそのまま読み込ませる

不正な指示や誤情報、機密情報が
含まれた資料を読み込ませることで、
AIの判断に悪影響を与える。



⚠ 小さな便利が、大きな事故の入口に。

シャドーAIとは？会社が知らないAI利用

会社が承認・把握していないAIの業務利用は、管理できないリスクを生みます。



よくある例

- 個人でAIを契約して業務に使う
- 未承認のAIサービスに社内データを入力する
- AIツールを独自にインストールして利用する



なぜ危険か

- 会社が実態を把握できない
- ルール・ログ・相談先が機能しない
- 情報漏洩や誤利用のリスクが見えにくい



まず取る対策

- 利用を許可するAIツールを明確にする
- 申請・相談ルートを作る
- 社員向けの周知と研修を行う



AIエージェント運用で特に注意したい4つのポイント

公的ガイドライン等を参考に整理した、実務上の重要ポイント

AIエージェントは業務の幅を広げる一方で、情報・判断・行動の管理が不十分だと様々なリスクにつながります。

1 機密情報・個人情報の漏えい

- 顧客情報、契約情報、認証情報などをそのまま入力・添付しない
- RAG（検索拡張生成）や外部SaaS（クラウドサービス）連携により、意図せぬ情報が外部に送信・記録される可能性がある



主な対策

- 入力禁止情報の定義
- マスキング・データ分類の実施
- 保存先・学習利用の確認
- 外部サービス連携設定の見直し

2 プロンプトインジェクション

（外部データ中の悪意ある指示がAIの判断に影響すること）

- Webページ、メール、PDF、外部データなどに埋め込まれた指示により、AIエージェントが誤って動作する
- 誤った判断、情報の外部送信、不正なツール実行などにつながることがある

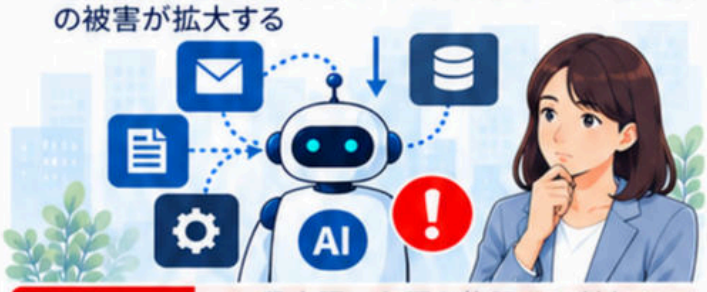


主な対策

- 信頼境界の設定
- 出力内容の検査
- 許可リスト（Allowlist）の運用
- 隔離された実行環境（サンドボックス）での実行

3 過剰権限・自律実行リスク

- メール送信、データベース更新、申請処理、API実行など、AIエージェントが実行できる範囲は影響が大きい
- 必要以上の権限が与えられると、誤操作や不正利用の被害が拡大する



主な対策

- 最小限に必要な権限のみ付与（最小権限の原則）
- 多要素認証の適用
- 人間の承認を挟む運用
- 段階的な自動化の実施

4 誤判断・監査不能

- ハルシネーション（もっともらしい誤った回答）、誤分類、根拠不明の判断により、業務や顧客対応に影響する
- 実行の経緯が記録されていないと、原因の特定、再発防止・説明責任を果たせない



主な対策

- 高リスク業務は最終判断を人間が行う
- 監査ログ・操作履歴の保存
- 定期的な評価・レビューの実施
- 判断基準や利用ルールの明確化

AIエージェントは「文章を作るAI」ではなく、「権限を持って行動するソフトウェア」として管理することが重要です。

参考資料：経済産業省・総務省『AI事業者ガイドライン（第1.2版）』（2026年3月）／IPA『生成AIおよびAIエージェントを安全に活用するための手引書』（2026年7月）／OWASP『Top 10 for LLM Applications 2025』

※本ページは、上記資料の考え方を参考に、実務上の注意点を整理したものです。

AIエージェントは、なぜ従来のAIより注意が必要なのか

“答えるAI”から“実行するAI”へ。管理の考え方も変わります。

従来の生成AI

質問 → 回答

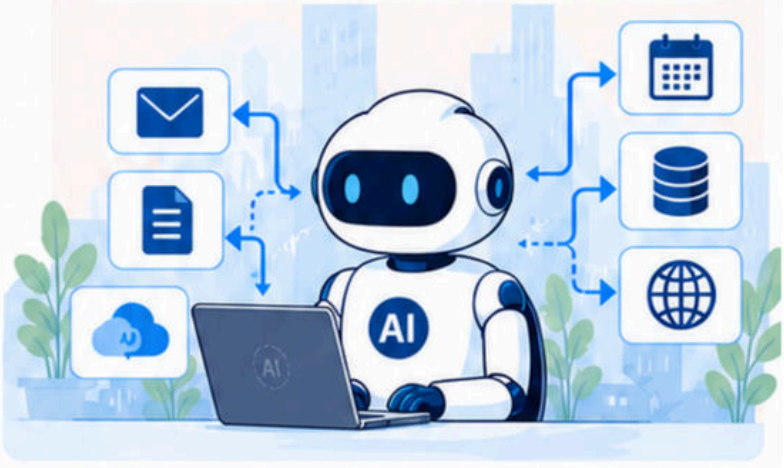
- 文章作成
- 要約
- アイデア出し
- 回答は人が使う



AIエージェント

情報収集 → 判断 → 実行

- メール送信
- ファイル更新
- 外部ツール連携
- 複数の作業を自律的に進める



権限を持って動くAIは、管理の考え方が変わる。

用語解説

AIエージェント＝
複数の作業をAIが自律的に進める仕組み

AIサービスを選ぶときに確認したい5つのポイント

安全性は、無料か有料かだけでなく、契約・設定・運用体制でも変わります。

	個人利用中心のサービス	法人利用を想定したサービス
	 手軽に試せるが制限がある場合も	 業務利用を前提とした管理・統制機能が備わることが多い
データの取り扱い	**サービスにより異なる** 入力データが学習に使われる場合がある。	**学習利用を制御できる** 学習利用のオプトアウトやデータの取り扱い設定が用意されていることが多い。
アカウント管理	**個別に確認が必要** 個人アカウントでの管理が前提で、管理機能は限定的。	**組織での一元管理が可能** 所属・権限管理など、組織単位での管理機能が用意されていることが多い。
操作履歴・監査	**提供されない場合が多い** 利用履歴の確認などができないことが多い。	**操作履歴の確認や監査が可能** 管理者による利用状況の確認や、監査・エクスポート機能が用意されていることが多い。
外部連携	**限定的な場合が多い** 外部サービスとの連携は個人向けの簡易的なものに限られる。	**外部サービスとの連携が可能** 業務システムやSSO、データ制御など、組織向けの連携機能が用意されていることが多い。
契約・サポート	**個別に確認が必要** 利用規約の内容やサポートの範囲はサービスにより異なる。	**法人向けの契約・サポートが充実** 専用の契約形態やサポート窓口が用意されていることが多い。



“有料なら安全”ではありません。

契約・設定・社内ルール・教育をあわせて確認しましょう。



※一般的な傾向であり、サービス・プラン・契約内容により異なります。

御社は大丈夫？10項目セルフチェック

自社のAI利用ルールや運用体制に、抜け漏れがないか確認しましょう。

1. ☐ **利用を許可するAIを決めている**
   業務で使用できるAIを選定し、利用範囲を明確にしている。
2. ☐ **入力禁止情報を定義している**
   機密情報や個人情報など入力してはいけない情報を定義している。
3. ☐ **個人契約AIの扱いを決めている**
   従業員による個人契約AIの利用ルールを定め、業務での扱いを明確にしている。
4. ☐ **AI出力の最終確認者が決まっている**
   AIの回答や生成物の内容を確認する責任者・担当者が決まっている。
5. ☐ **AIエージェントの権限を管理している**
   AIエージェントに付与する権限を最小限にし、適切に管理している。
6. ☐ **承認フローとログ保存がある**
   AI利用の承認手順を定め、利用ログを保存している。
7. ☐ **シャドーAIの把握方法がある**
   従業員による未承認AIの利用を把握する仕組みがある。
8. ☐ **相談窓口がある**
   AI利用に関する疑問や問題を相談できる窓口を設置している。
9. ☐ **社員向けAI研修を実施している**
   全社または対象者向けに、AIの安全な利用に関する研修を行っている。
10. ☐ **定期見直しの計画がある**
    AI利用ルールや運用体制を定期的に見直す計画を立てている。

チェックが付かなかった項目は、対策の見直しが必要な可能性があります。
特に、重要情報の取り扱いとAIの実行権限に関わる項目から優先的に確認しましょう。

セルフチェック結果をもとに無料30分相談

現在のAI利用状況と課題を一緒に整理します。

※技術的なセキュリティ監査や安全性の保証を行うサービスではありません。



詳しくは最終ページへ ›

企業が整備したい5つの防衛ライン

ツール導入だけでは守れません。ルール・技術・運用・教育を組み合わせる必要があります。



1 利用ルール

許可するAI・禁止情報・相談先を明確にする。

2 権限管理

最小権限・承認者・アクセス範囲を設計する。

3 技術設定

データ設定・外部連携・入出力の検査を確認する。

4 監査ログ

いつ・誰が・何をしたか追跡できる状態にする。

5 社員教育

現場が迷わない判断基準を共有する。

ルール × 技術 × 運用 × 教育 の組み合わせが必要です。

※具体的な技術対策は、導入環境に応じた専門的な検討が必要です。

企業・自治体の現場で培った AI研修・活用支援の実績

安全なAI活用を実現するには、ルールや技術対策に加え、現場で使う人の理解が欠かせません。



1 会社・講師実績

実務に即したAI研修と活用支援を、現場目線で提供しています。

AI講座開催



100回以上

延べ受講者数



1000名以上

公的機関・企業向け研修実績



自治体・中小企業・各種団体など

多数

講師：上田良江



AI活用・業務改善をテーマに、企業・自治体での研修を多数担当。実務に寄り添った、わかりやすい解説に定評があります。

2 主な研修・登壇実績

AI活用研修・講演に関する主な実績です。

北海道庁
（北海道経済部労働政策局 産業人材課）



北広島市



由仁町



北海道産業資源循環協会



江別まちなか仕事プラザ



北海道土地改良事業団体連合会



※上記はAI活用研修・講演に関する実績です。セキュリティ監査実績を示すものではありません。

安全なAI活用に向けて、まず整えたいこと

事故を防ぐには、社内での整理・周知・確認・見直しが重要です。

企業が整理したい4つの視点

1 社内ルールの整理

入力禁止情報・承認フロー・利用範囲を明確にする。

- ☑ 入力禁止情報
- ☑ 承認フロー
- ☑ 利用範囲



2 社員への周知・教育

正しい使い方・禁止事項・相談先を共有する。

- ☑ 正しい使い方
- ☑ 禁止事項
- ☑ 相談先



3 導入前の確認

権限設計・ログ・外部連携・最終承認を確認する。

- ☑ 権限設計
- ☑ ログ
- ☑ 外部連携
- ☑ 最終承認



4 導入後の見直し

運用状況を確認し、改善と定着につなげる。



安全なAI活用を定着させる3つの実践ポイント

1 ルールの共有

- ☑ 利用可能なAI
- ☑ 入力禁止情報
- ☑ 承認手順
- ☑ 相談窓口



2 実務に即した教育

- ☑ 情報の取り扱い
- ☑ AI出力の確認
- ☑ 業務での注意点
- ☑ 具体例で学ぶ



3 定期的な見直し

- ☑ 利用状況の確認
- ☑ 新たなリスクの把握
- ☑ ルール更新
- ☑ 教育内容の改善



※運用状況に応じて、ルール・教育内容を定期的に見直すことが重要です。

単発の注意喚起ではなく、現場で安全に使うための定着づくりが重要です。



セルフチェックで気になる項目があれば、まず**無料30分相談**へ



セルフチェック結果をもとに、現在のAI利用状況と課題を一緒に整理し、貴社の状況に合わせた進め方を一緒に検討します。

1 無料30分相談でできること

貴社の状況に合わせて、以下のような内容をお伺いし、具体的なアドバイスを行います。

1 現状のヒアリング



- AIの利用状況
- 現在の課題・お悩み
- 社内のルール・体制
- 今後の活用予定

2 リスク・課題の整理



- 想定されるリスクの洗い出し
- 優先的に対応すべき課題の整理
- 対策の方向性のご提案

3 今後の進め方のご提案



- 貴社に合った進め方
- 必要な支援内容のご提案
- 概算スケジュールのご案内
- ご質問・ご相談への回答

2 こんな方におすすめです

- AIの利用が広がり始めたが、ルール整備に不安がある
- 社内のリテラシーにばらつきがあり、教育方法を知りたい
- 導入前にリスクチェックを行い、安心して進めたい
- 自社に合った具体的な進め方を相談したい

3 お問い合わせ

ハッピーステート株式会社

URL https://happystate.co.jp/

メール info@happystate.co.jp

LINE

LINEでのご相談はこちら

Webフォームはこちら

無料30分相談はこちら