

社内 生成AI利用ルール（ひな形・1枚）

研修1「シャドーAIの制御」持ち帰り資料 ※受講企業が社名を入れてそのまま使える形で提供します

株式会社（ ）は、生成AIを業務で安全に活用するため、次のとおり定めます。 制定日： 年 月 日

1 生成AIに入れてはいけない情報（3つだけ覚える）

- (1) 顧客の個人情報 …… 氏名・住所・電話・メール・購入履歴など
- (2) 取引先との機密 …… 見積・契約条件・図面・先方から預かった資料
- (3) 非公開の社内数字 …… 売上・原価・給与・未公表の計画

※迷ったら「社外の人に見せられるか」で判断する。見せられないものは入れない。

2 会社が認める使い方（禁止ではなく、公式に使う）

- ・会社が指定したサービス・アカウントを使う（個人アカウントでの業務利用はしない）
- ・「入力データを学習に使わない」設定（法人プラン・履歴オフ等）を必ず有効にする
- ・AIの出力は必ず人が確認してから使う（誤りが含まれる前提で扱う）

3 相談窓口（責めないルール）

- ・「入れてしまったかも」と思ったら、すぐ下記へ。報告した人を責めません。
- ・相談窓口：（ 役職・氏名 ） 連絡先：（ ）

※発見が早いほど打てる手が増えます。「隠す」ことだけが最大の損失です。

4 このルールの適用範囲

- ・役員を含む全従業員に適用します（経営陣も同じルールに従います）。
- ・年1回、利用サービスと設定を見直します。 見直し担当：（ ）

情報セキュリティ 自社診断シート（10項目）

研修1 持ち帰り資料 ※IPA「5分でできる！情報セキュリティ自社診断」の考え方を参考に当社編集

項目	できている	一部	まだ
1. メール・クラウド会計・ネットバンキングに多要素認証を設定している	☐	☐	☐
2. バックアップを取り、業務ネットワークから切り離して保管している	☐	☐	☐
3. OS・ソフトの更新を自動更新にしている	☐	☐	☐
4. パスワードを使い回していない（管理ツール等を使っている）	☐	☐	☐
5. データへのアクセス権限を「必要な人だけ」に絞っている	☐	☐	☐
6. 振込先変更などの依頼は、メール以外の手段で本人確認するルールがある	☐	☐	☐
7. 「ファイルが開けない」等の異常時に、最初に連絡する人が決まっている	☐	☐	☐
8. 退職者のアカウント・共有パスワードをすぐ止める手順がある	☐	☐	☐
9. 生成AIの業務利用ルール（入れてはいけない情報の線引き）がある	☐	☐	☐
10. 困ったときの外部相談先（IPA・警察）を全員が知っている	☐	☐	☐

「まだ」が付いた項目のうち、今週やるものを1つ決める：

やること：	担当：	期限：	月	日
-------	-----	-----	---	---

インシデント初動カード — 被害に気づいた最初の1時間

研修2 持ち帰り資料 ※印刷して事務所・レジ横に貼っておく想定のア4カード

1

切り離す

その端末のLANケーブルを抜く／Wi-Fiを切る。電源は切らない（証拠が消える）

2

報告する

決めておいた報告先1人に連絡（下欄）。全員への一斉連絡はしない

3

記録する

時刻・画面・やったことをスマホで撮る／メモする（時刻つき）

4

パスワード変更

感染していない別の端末から、重要サービスのパスワードを変える

5

外部に相談

IPA安心相談窓口・警察サイバー窓口へ。早いほど打てる手が増える

6

身代金は保留

その場で判断しない。払っても復旧しない事例がある。まず相談

自社の連絡先（研修の場で記入して持ち帰る）

社内の報告先：（ 役職・氏名 ） 携帯：（ ）

IT対応を頼める先（保守業者等）：（ ） 電話：（ ）

IPA 情報セキュリティ安心相談窓口／警察 サイバー犯罪相談窓口（＃9110）