WHITE PAPER

非エンジニアのためのClaude実践ガイド

生成AI 社内利用ガイドライン＆セキュリティ策定ガイド

情報漏洩不安を解く ― ガイドライン雛形＆チェックリスト付き（2026年6月最新）

発行：2026年6月　／　対象：経営者・管理職・情シス兼務

Claude Works（クロードワークス）

非エンジニアのためのClaude実践メディア　claudelab.jp

生成AI 社内利用ガイドライン＆セキュリティ策定ガイド

中小企業の社長・役員の方、そして情シスを兼務しながらバックオフィスを回している管理職の方へ。このガイドは、あなたのためのものです。

生成AIを使ってみたい。でも「うちの顧客名簿や見積もりを入れて、それが外に漏れたらどうするのか」という不安が消えず、結局「当面は禁止」で止まっている。あるいは、禁止と言いながら現場が勝手に使い始めていて、実態がつかめない。私が経営者の方とお話ししていて、最も多く出会うのがこの状態です。

このガイドは、その不安を**禁止ではなく『見える化＋ルール』で解く**ための実務書です。読み終えたら、そのまま社内に配れるガイドライン雛形と、稟議に添付できるチェックリストが手元に残ります。一人称は「私」、専門用語は1行で訳しながら進めます。

このガイドが解く問題

不安だから禁止 → 統制不能なシャドーAIが増える + **塞ぐべきリスクは「学習への入力」と「シャドーAI」の2つだけ** + **オプトアウト・管理コンソール・入力禁止リストの3点で大半を防げる**

---

1. なぜ『不安だから禁止』が一番の損失なのか

2026年1月、管理職1,008名を対象にした調査（コーレ社、commercepick経由・2026年6月時点）で、生成AIが社内で定着しない理由の最多は**セキュリティ懸念で33.5%**でした。次いで活用アイデア不足26.0%、情報システム部門の非協力22.4%。つまり、現場が使えないのではなく、**「漠然とした不安」が一番のブレーキ**になっているのです。

さらに同じ調査では、使いこなせていない層が課長・リーダー職29.3%、経営層26.8%、一般職25.6%。現場よりも、むしろ**意思決定する側の習熟が遅れている**という結果でした。決める人が不安なまま「禁止」を選ぶと、組織全体が止まります。

ここで起きるのが逆説です。会社が禁止すると、業務効率を上げたい社員は**個人のスマホやアカウントでこっそり使い始めます**。これを「シャドーAI」（会社が把握・許可していないAIツールの利用）と呼びます。禁止は表向きの安心と引き換えに、**会社が一切ログを取れない・設定もできない無許可利用**を増やし、かえって統制不能な状態をつくってしまうのです。

だからゴールを置き換えます。目指すのは「リスクをゼロにする」ことではありません。リスクをゼロにできる道具は世の中に存在しないからです。目指すべきは、**『管理された状態で、安全に使えるようにする』**こと。これがこのガイドの基本姿勢です。

> **この章のまとめ**：不安は禁止ではなく『見える化＋ルール』で解く。禁止はシャドーAIを増やすだけ。

---

2. 非エンジニアが知るべき2大リスクを1行で

セキュリティと聞くと、無数の技術用語が押し寄せてくる気がします。でも、非エンジニアの経営者・管理職がまず塞ぐべきリスクは、たった2つです。

リスク	1行で言うと	まず取る対策
リスク1：学習への入力	入力した社内情報がAIの学習に使われる可能性	法人プランの設定で回避できる（第3章）
リスク2：シャドーAI	社員が会社の許可なく無許可ツールを使う	正規ツールを用意し、ガイドラインで誘導する

「学習への入力」は、たとえば顧客リストや未公開の決算数字を無料ツールに貼り付けたとき、それが**将来モデルの学習に使われる可能性がある**、というリスクです。**法人向けプランを正しく設定すれば、この入力は学習に使われないようにできます**（NTT、2026年6月時点）。

「シャドーAI」は、人の問題です。便利だから使う。でも会社が知らない。だから設定もログも効かない。これは禁止では消えず、**正規の選択肢を渡して初めて減ります**。

細かい技術リスク（プロンプトインジェクション等）は確かに存在しますが、**まずこの2点を塞いでから考えれば十分**です。順番を守ることが、非エンジニアが息切れしないコツです。

> **この章のまとめ**：覚えるリスクは『学習への入力』と『シャドーAI』の2つだけ。

---

3. 最も即効性のある3つの技術的対策

リスクが2つに整理できたら、対策も明快です。情報漏洩リスクへの即効性ある対策は、以下の3点に集約されます（NTT、2026年6月時点）。

漏洩リスクを塞ぐ3ステップ

1. ① 学習オプトアウト：入力を学習に使わせない設定をON
2. ② 管理コンソール：IT管理者が全社の設定を一括統一
3. ③ 入力禁止リスト：何を入れてはいけないかを具体名で配布

① 学習オプトアウト（学習拒否）設定。「オプトアウト」とは、自分のデータを学習対象から外す設定のことです。ここで朗報があります。**ClaudeのTeamプランは、デフォルト（初期設定）でユーザーデータをモデルの学習に使いません**（claude.com/pricing、2026年6月時点）。上位のEnterpriseプランもこのTeam機能を含みます。つまり法人プランを選ぶだけで、リスク1の大部分が初期状態で塞がれている、ということです。

② 管理コンソールで全社統一。個々の社員に「設定してね」と任せると、必ず抜けが出ます。IT管理者が**一括で全社の設定を適用できる管理画面**を使い、誰がどう触っても同じ安全設定になる状態をつくります。

③ 入力禁止情報リスト＋利用ガイドライン。技術設定だけでは人の判断を縛れません。**「これは入れてはいけない」を具体名で**書き出します。顧客の個人情報、未公開の財務数字、パスワード、取引先との守秘契約に関わる情報。抽象的な「機密情報」ではなく、自社の言葉で列挙するのがコツです。

> **この章のまとめ**：『オプトアウト・管理コンソール・入力禁止リスト』の3点で、漏洩リスクの大半を塞げる（万能ではありませんが、優先度は最も高い）。

---

4. そのまま使える 社内ガイドライン雛形（章構成つき）

ここからが、持ち帰っていただく実物です。以下の章構成を、自社の言葉で埋めれば社内ガイドラインが完成します。重要なのは、**禁止だけで終わらせないこと**。ガイドラインは禁止事項に加えて、推奨する業務や効果的なプロンプト例も書くと定着が進みます（aibrainpartners、2026年6月時点）。

【ガイドライン雛形・章構成】

1. **目的・適用範囲**：なぜ作るか、誰に適用するか（全社員／業務委託含む等）
2. **使ってよいツールと禁止ツール**：会社が契約した正規ツールを明記。それ以外は禁止＝シャドーAI対策
3. **入力禁止情報リスト**：顧客個人情報／未公開の財務・人事情報／パスワード・認証情報／取引先の守秘情報
4. **推奨する業務と効果的なプロンプト例**：（下表）禁止だけにしないのが定着の鍵
5. **違反時の対応**：誰に・どう報告し、どう是正するか
6. **問い合わせ窓口・改訂ルール**：迷ったときの相談先と、見直し頻度

【推奨業務とプロンプト例（雛形の中身サンプル）】

業務	効果的なプロンプト例	注意
議事録の要約	「この議事録を3つの決定事項と担当者付きで箇条書きにして」	個人名は社内限定なら可、社外共有時は伏せる
メール下書き	「取引先への納期遅延のお詫びメールを丁寧な敬語で」	金額・契約番号は入れない
文章チェック	「この文章の誤字脱字と分かりにくい箇所を指摘して」	未公開資料は社内設定のツールでのみ

なお、現行のClaudeには **Opus 4.8（最上位）／Sonnet 4.6（標準）／Haiku 4.5（高速・低コスト）** があり、迷ったらまずOpus 4.8で問題ありません（公式、2026年6月時点）。ターミナル（黒い画面のコマンド操作）が苦手な非エンジニアの方には、**Coworkという、ターミナル不要でPC上のファイル作業を任せられるデスクトップ型のAIエージェント**（2026年4月提供開始、非技術職向け）も選択肢になります。

> **この章のまとめ**：ガイドラインは『禁止＋推奨＋プロンプト例』の3点セットで初めて使われる。

---

5. 導入前セキュリティ確認チェックリスト＆シャドーAI点検リスト

稟議に出す前の最終確認です。上から潰していけば、**安全水準を満たしたと社内で説明できる**状態に届きます。

【導入前セキュリティ確認チェックリスト】

- ☐ 学習オプトアウト（学習拒否）設定が有効になっているか確認した
- ☐ 管理コンソールで全社の設定を統一した（個人任せにしていない）
- ☐ 入力禁止情報リストを作成し、全社員に周知した
- ☐ 正規ツールを社員に案内し、申請・付与の流れを決めた
- ☐ 違反時の報告窓口と担当者を決めた

【シャドーAI点検リスト】

- ☐ 現在、無許可で使われているAIツールの実態を棚卸しした
- ☐ 棚卸し結果を責めるためでなく、正規ツールへ誘導するために使うと決めた
- ☐ 「禁止」ではなく「正規の選択肢を渡す」方針を社内に明言した

【プラン要件の線引き（2026年6月時点）】

TeamとEnterpriseの線引き

Before → **After**

要件	適したプラン
社員5〜150名で、まず安全に使い始めたい	**Team**（デフォルトで学習に不使用、一元管理）
SSO（社内IDで一括ログイン）・監査ログ・データ保持の指定が必須	**Enterprise**（要問い合わせ）

ここが、雛形だけでは埋まらない論点です。**自社がTeamで足りるのか、Enterpriseが必要なのか**は、既存の社内規程や監査要件によって変わります。判断に迷う場合は、巻末のご相談先で一緒に整理できます。

> **この章のまとめ**：チェックリストを上から潰すだけで、稟議に出せる安全水準に届く。

---

6. 運用フェーズ：ログ・権限・費用をどう回すか

ガイドラインは「作って終わり」ではありません。安全は**運用で守られます**。

ガバナンス（統制）のゲート条件として、常に見ておくべきは**機密・権限・ログ・費用の4点**です（exawizards、2026年6月時点）。

- **機密**：入力禁止リストが守られているか
- **権限**：誰がどのツール・データにアクセスできるか
- **ログ**：いつ誰が何に使ったかを追えるか（Enterpriseの監査ログ等）
- **費用**：想定外のコストが出ていないか

そして大切なのは、この**ガバナンスと、効果のKPI（時間・品質・満足度）を同じ会議で見る**ことです（exawizards、2026年6月時点）。安全だけを見ると現場が萎縮し、効果だけを見ると統制が緩む。両方を一枚で見て、**安全と効果を両輪で回す**のが、定着している会社の共通点です。

最後に、**最低でも年1回はガイドラインを改訂**してください。加えて、新しいモデルや新機能が出たタイミングでは、その都度**入力禁止リストとプラン設定を見直す**ようにします。AIは新しいモデルや新機能が継続的に出るため、古い前提のまま運用すると、せっかくの設定が形骸化します。この「年1回＋新ツール登場時」の見直し習慣が、長期の安全を支えます。

> **この章のまとめ**：安全は『作って終わり』ではなく『年1回＋新ツール登場時に見直す運用』で守られる。

雛形は渡せます。でも『自社固有の3つ』は残ります

ここまでで、ガイドライン雛形とチェックリストはお渡しできました。これをそのまま使えば、最初の一歩は確実に踏み出せます。

ただ、雛形だけでは埋まらない論点が3つ残ります。これは御社の事情を知らないと、誰にも代わりに決められない部分です。

1. **入力禁止リストの確定**：御社の業種・既存規程・扱う情報に合わせて「何を入れてはいけないか」を具体名で固める
2. **Team / Enterpriseの判断**：監査ログやデータ保持の要件を、どちらのプランで満たすか
3. **既存規程との接続**：すでにある情報セキュリティ規程やNDAと矛盾しない形に仕上げる

私は、ここを御社と一緒に詰める伴走をしています。**御社の規程に合わせてガイドラインを仕上げ、プラン選定とセキュリティ設定まで**、非エンジニアの言葉で並走します。「情報漏洩が不安で踏み出せない」――その入口を、安全に踏み出せる状態に変えるところまでが私の仕事です。

まずは現状をお聞かせください。30分で、御社が次に何をすべきか（次の1アクション）が明確になります。

無料30分オンライン相談はこちら → 予約フォーム（ご連絡：support@lexor.jp）

※本資料の制度・料金・仕様は2026年6月時点の情報です。プラン仕様やセキュリティ設定は変更される場合があるため、導入前に各サービスの最新の公式情報をご確認ください。

無料30分オンライン相談を受け付けています

「自社の場合どう進めればいいか」を、御社の状況に合わせて具体的にご提案します。売り込みはいたしません。

📅 ご予約：**https://app.spirinc.com/patterns/availability-sharing/evuvVnwxGC-HC8t6imBtr/confirm**

✉️ support@lexor.jp ／ 🌐 https://claudelab.jp