ChatGPT・Claude 法人利用の落とし穴

生成AIは危険なのか？

法人契約だけでは、守れない。



4つのリスクと、導入前にやる10項目

合同会社REN

2026年10月時点の公式情報をもとに作成

基本の考え方

AIはクラウドサービスの一つ

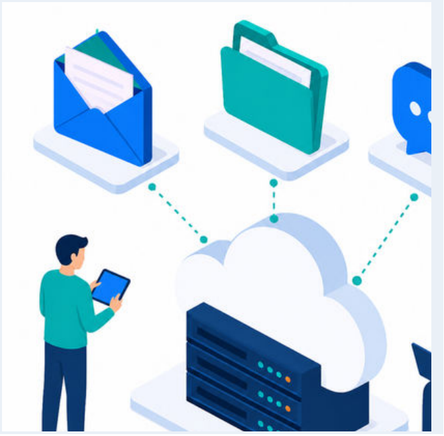
メールやファイル共有と同じく、データを社外に預けるサービスです。
判断の物差しは「すでに受け入れているクラウドと同じ水準か」。
その上で、AIにだけある「振る舞い」のリスクを足して考えます。



既存のSaaS

- メール・ファイル・CRM
- 利用者と共有範囲の管理
- 契約とログの確認

→ すでに受け入れている水準



生成AIサービス

- 同じクラウド管理が必要
- ＋外部情報からの指示混入
- ＋自動操作の権限管理

→ 同じ管理＋AI特有の確認



出典：OpenAI Business data／Enterprise privacy、Anthropic公式ヘルプをもとに合同会社REN整理（確認日 2026年10月29日）

AIで増える4つのリスク



リスク01

入力

機密情報を
そのまま渡してしまう

対策：匿名化と入力ルール



リスク02

共有

回答やリンクを
広く公開してしまう

対策：共有範囲と
公開前の確認



リスク03

指示混入

Webやメールに潜む
指示に従ってしまう
（プロンプト注入）

対策：外部データと
指示を分離



リスク04

誤操作

送信・削除・更新を
誤って実行する

対策：操作権限と
実行前の承認

出典：OpenAI「Agent builder safety」、OWASP Top 10 for LLM Applications を参考に合同会社REN整理（確認日 2026年10月29日）

安全性の構造

安全性は「製品×設定×運用」

どれか一つがゼロなら、全体もゼロ。

製品：学習条件・認証・監査・保持の機能
設定：SSO・共有範囲・接続先・権限の有効化
運用：入力ルール・承認・退職処理・事故対応

高機能なプランでも、
過剰な共有や権限は運用で減らす。



出典：OpenAI 法人料金ページ、Anthropic Enterprise、OpenAI Agent builder safety をもとに合同会社REN整理（確認日 2026年10月29日）

AIセキュリティの4分類



分類01

学習への不使用

入力・出力を
モデル改善に使うか

確認：契約上の既定
フィードバック時の扱い



分類02

不正アクセス防止

本人確認と権限を
どう管理するか

確認：MFA・SSO・SCIM
RBAC・IP制限



分類03

情報漏えい防止

外への流出経路を
どう抑えるか

確認：入力・共有
コネクター・エージェント



分類04

監査・統制

利用を追跡し
問題時に止められるか

確認：監査ログ
Compliance API・保持

「学習に使われない」一項目だけで安全性全体を判断しない。出典：OpenAI Business data、Anthropic「Is my data used for model training」、Anthropic Enterprise（確認日 2026年10月29日）

データの扱い

学習不使用 ≠ 非保存

「モデル改善に使うか」と「どこに、いつまで残るか」は別の条件です。
学習・保持・外部転送の3つを分けて確認します。

学習しない
≠
保存しない



学習
モデル改善

法人プラン・APIは既定で
学習に使わない。
例外：別途の同意・契約
（Claudeは明示的な
フィードバックを利用する場合あり）



保持
残る場所・期間

会話履歴・ファイル・監視ログは
一定期間残る。
OpenAI APIの不正利用監視ログは
既定で最大30日。
保持の設定はChatGPTはBusinessから、
ClaudeはEnterpriseのみ



外部転送
第三者アプリ

コネクターや第三者アプリへ
渡したデータは、
その先の規約・保持に従う。
接続先と権限を管理者が管理する

出典：OpenAI「Business data」「Enterprise privacy」「Your data」、Anthropic「Is my data used for model training」（確認日 2026年10月29日）

不正アクセス防止

入口を5つの仕組みで守る

- MFA：追加の本人確認。IdP側も含めて適用を確認
- SSO：社内IDで一元認証。個人アカウントとの混在を防ぐ
- SCIM：入退社を自動反映。退職時の削除漏れを減らす
- RBAC：役割に応じた権限。管理者と一般利用者を分ける
- IP制限：許可したネットワークからだけ接続させる



機能があるかと「強制できる範囲」は別。プラン別の対応は11枚目で確認

出典：OpenAI 法人料金ページ、Anthropic「Set up SSO」「Set up JIT or SCIM provisioning」（確認日 2026年10月29日）

情報漏えいの4経路



経路01

入力

顧客情報や認証情報を
AIに送る

対策：分類・匿名化
入力禁止項目



経路02

共有

回答や成果物を
外へ公開する

対策：共有範囲
リンク・宛先の確認



経路03

コネクター

外部サービスへ
データが渡る

対策：接続先・OAuth権限
転送先の確認



経路04

エージェント

AIが送信・更新・削除する

対策：最小権限・承認
停止機構

共有先の権限が広すぎると、AIに接続する前から流出範囲が広い。出典：OpenAI「Agent builder safety」「Enterprise privacy」、Anthropic Enterprise（確認日 2026年10月29日）

監査・統制

監査・統制は「追える・消せる・止められる」



利用統計、監査ログ、会話本文の取得は別の機能です。
Claudeの監査ログには会話本文が含まれません。
本文を取得する手段と権限は、別に確認します。

追える
誰がいつ何をしたか

監査ログとCompliance API
取得対象・保存先・閲覧権限を確認
ClaudeはEnterpriseで直近180日分

消せる
どの情報をいつまで

会話・ファイル・ログを分けて管理
削除後や例外保存の扱いを確認
保持の組織設定は主にEnterprise

止められる
事故時に制限できるか

アカウント・接続・自動操作を停止
証拠を保全し影響範囲を調査
連絡と復旧の手順を事前に試す

出典：OpenAI 法人料金ページ、Anthropic「Access audit logs」「Access the Compliance API」「Custom data retention controls」（確認日 2026年10月29日）

プラン構造

利用枠と統制は、別の軸で選ぶ

席・契約	ChatGPT Business	Claude Team
Standard席	年払 $20／月払 $25	年払 $20／月払 $25
Premium席	$100／$125 利用枠5倍	$100／$125 利用枠5倍
Enterprise	個別見積もり	1席$20＋利用料 （最低20席）
主な差	席＝利用量 Enterprise＝統制	席＝利用量 Enterprise＝統制

選び方の目安



利用量が足りない → Premium席を検討

統制が足りない → Enterpriseを検討

価格はUSDの公式表示例。

税・契約・利用量で変動

出典：OpenAI 法人料金ページ・Premium seats、Anthropic「Pricing」「Purchase and manage seats on Team plans」（確認日 2026年10月29日）。ChatGPT Businessは最低2席（2〜200名）、Claude Teamは2〜150名

4プラン比較：学習・認証・管理

確認項目	ChatGPT Business ／ Enterprise	Claude Team ／ Enterprise	注意点
業務データを学習に使わない（既定）	対応 ／ 対応	対応 ／ 対応	両社とも商用プランの既定
フィードバック送信時	学習しない（別契約時のみ）	条件付き（最長5年保存・学習あり）	両社とも管理者が 送信を無効化できる
SAML SSO	対応 ／ 対応	対応 ／ 対応	ドメイン検証も全プランで可
SCIM（入退社の自動反映）	非対応 ／ 対応	非対応 ／ 対応	Claude Teamは JITプロビジョニングのみ
RBAC／カスタムロール	非対応 ／ 対応	非対応 ／ 対応	Business／Teamは 基本ロールのみ
IP許可リスト	非対応 ／ 対応	非対応 ／ 条件付き	Claudeは Anthropicへの申請で設定
MFAの強制	非対応 ／ 非対応	公式に記載なし	SSOを使い IdP側でMFAを強制する
コネクター・アプリの管理	対応 ／ 対応	対応 ／ 対応	両社とも管理者が 連携先を管理できる
GPTs／MCPの管理	条件付き ／ 対応	対応 ／ 対応	BusinessはGPTの 細かい権限制御なし

出典：OpenAI 法人料金ページ・Enterprise privacy・MFAヘルプ、Anthropic「Pricing」「Set up SSO」「JIT or SCIM provisioning」「Is my data used for model training」（確認日 2026年10月29日）

4プラン比較：監査・保持・データ管理

確認項目	ChatGPT Business ／ Enterprise	Claude Team ／ Enterprise	注意点
監査ログ	非対応 ／ 対応（Compliance API）	非対応 ／ 対応	Claudeは直近180日分 （本文なし・IDのみ）
Compliance API	非対応 ／ 対応	非対応 ／ 対応	会話・ファイルを 利用者や期間で取得
保持期間の管理者設定	対応 ／ 対応	非対応 ／ 対応	Claude Enterpriseは最短30日
既定の保持期間	定めなし（削除まで）／ 未設定なら削除まで	定めなし ／ 未設定なら無期限	削除した会話は 30日以内に削除
ZDR（保存しない設定）	非対応 ／ 非対応	非対応 ／ 条件付き	ZDRは両社とも主にAPI向け チャットは対象外
保存時・通信時の暗号化	対応 ／ 対応	対応 ／ 対応	方式名はOpenAIのみ明記 （AES-256・TLS1.2以上）
顧客管理の暗号鍵（EKM／CMEK）	非対応 ／ 対応	非対応 ／ 条件付き	対象組織・契約の条件あり
データ保存地域（日本）	原則なし ／ 条件付き	米国 ／ 米国	ChatGPT Ent.は新規顧客で 日本保存可（推論は対象外）
第三者認証	SOC 2のみ ／ SOC 2・ISO	対応 ／ 対応	Business欄のISOは「No」 Claudeは全商用製品で取得

出典：OpenAI 法人料金ページ・Enterprise privacy・Business data・Data residency・EKM、Anthropic「Pricing」「Access audit logs」「Compliance API」「Custom data retention」「CMEK」「Data residency」（確認日 2026年10月29日）

ChatGPT：Business と Enterprise

主な違い

項目	Business	Enterprise
SCIM・カスタムロール	なし	あり
監査ログ Compliance API	なし	あり
データの日本保存	原則なし	新規顧客は可
暗号鍵の自社管理（EKM）	なし	条件付き

選び方の目安



Business
少人数で、SSOと業務アプリ連携があれば足りる会社

Enterprise
入退社が多い、監査が必要、保存先を指定したい会社

出典：OpenAI 法人料金ページ・Enterprise privacy・Data residency（確認日 2026年10月29日）

Claude：Team と Enterprise

主な違い

項目	Team	Enterprise
SCIM 入退社の自動反映	なし（JITのみ）	あり
監査ログ Compliance API	なし	あり
保持期間の設定	なし	30日以上
IP許可リスト カスタムロール	なし	あり

選び方の目安



Team

少人数で、SSOで入口を締めれば始められる会社

Enterprise

人数が多く、監査や保持期間を自社で決めたい会社

出典：Anthropic「Pricing」「JIT or SCIM provisioning」「Access audit logs」「Custom data retention」（確認日 2026年10月29日）

情報分類ポリシー

● 4つの区分

区分	例	AIへの入力
公開	Webサイト 公開資料	可
内部	社内マニュアル 議事録	法人プランなら可
機密	顧客名簿 見積・契約	仮名化して可
高機密	個人番号 健康情報 パスワード	入力しない

● 迷ったときのルール



迷ったら、一段上の区分として扱う

パスワードやAPIキーは、どの区分でも入力しない

※区分と例は一般的な目安。自社の情報管理規程に合わせて調整する

AIエージェントの安全設計



01 必要なデータだけに接続

02 まず読み取りだけで始める

03 送信・削除は人が承認

04 操作ログを必ず残す

05 異常時はすぐ止める

06 元に戻す手順を用意



導入前チェックリスト10項目

● 契約と設定

- □ 01 法人プランで契約し、学習不使用を確認
- □ 02 SSOで入口を一本化（MFAはIdP側）
- □ 03 退職時のアカウント停止手順を決める
- □ 04 保持期間と削除の設定を確認
- □ 05 外部連携は管理者の許可制にする

● ルールと運用

- □ 06 情報分類と入力ルールを周知
- □ 07 入力禁止の情報を具体例で示す
- □ 08 エージェントは読み取りから始める
- □ 09 利用状況とログを月1回確認
- □ 10 事故時の連絡先と停止手順を決める

10項目がそろえば、メールやクラウドストレージと同じ水準でAIを使える





まとめ

禁止より統制。
プランより運用。

AIは「新しい種類のクラウドサービス」の一つ。

情報を分け、入口を締め、記録を残せば、安心して使える。



ご相談

導入前チェック、10項目を一緒に確かめませんか

自社でできている所と足りない所を、30分で整理します。契約プランの選び方、社内のAI利用ルールづくり、最初の設定までご相談いただけます。

合同会社REN　代表社員 原田 敬介
拠点：愛媛（全国どこでもオンラインで対応）
事業：業務構造診断・AI戦略策定／AI実装・定着支援／組織育成・研修
info@ren-llc.jp　／　https://ren-llc.jp/

30分・オンライン・無料

https://ren-llc.jp/contact/

QRコードからお申し込みください。
ご相談の種類は自動で選ばれます。