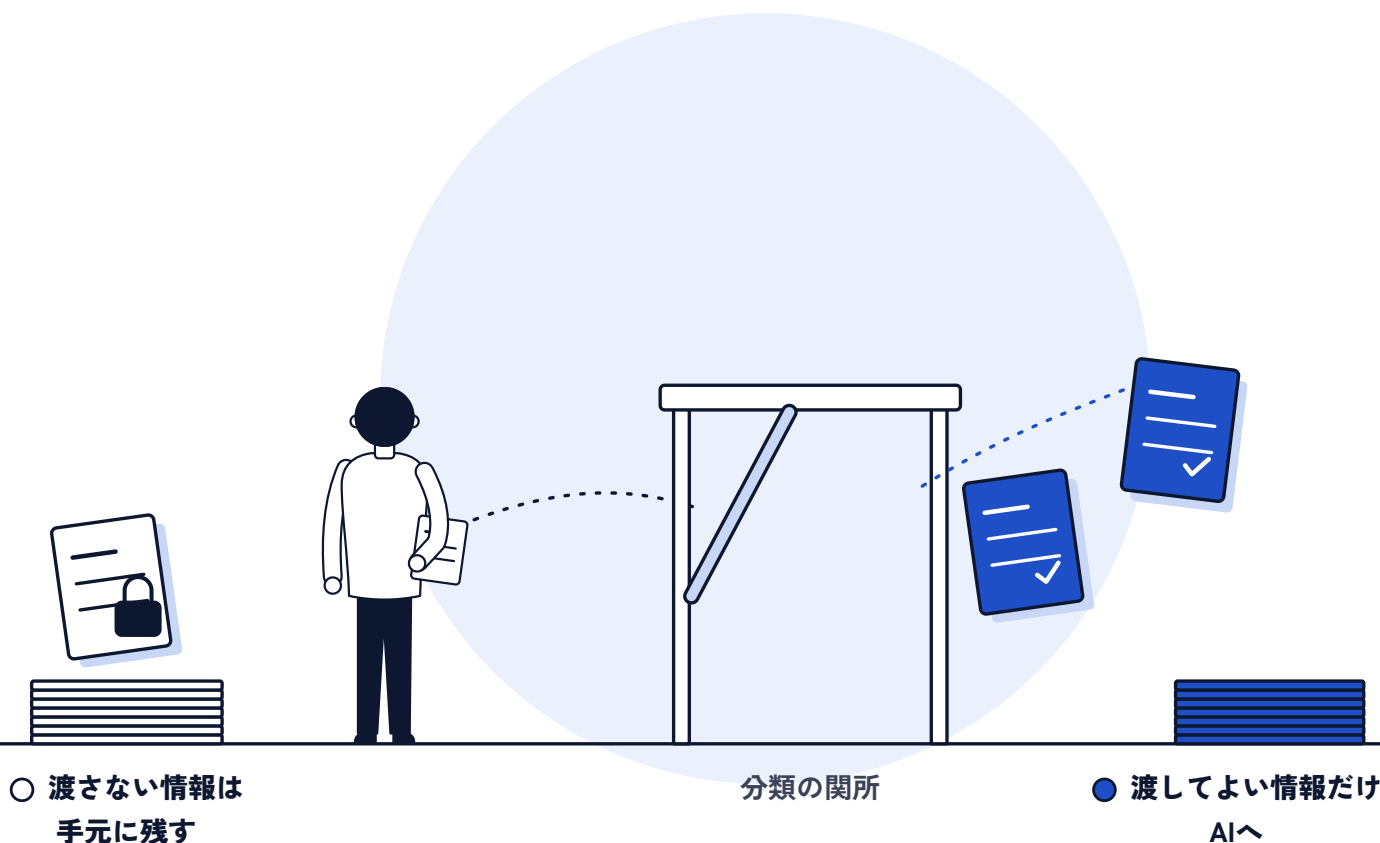


# 生成AIに入れていい情報・ だめな情報 2026

入力情報の分類表・AIサービスの確認表・利用ルールのひな形・誤入力の初動手順・  
点検表

「何を入れてよく、どのサービスなら使えて、間違えたらどう動くか」を、  
自社で決めて運用する **表とひな形** を一冊にまとめました。

**この資料の対象** 生成AIを業務で使っている、またはこれから使う会社の担当者・部門責任者・  
経営者と、情報システム・総務・法務の担当の方



## この資料に入っているもの

|   |            |                              |        |
|---|------------|------------------------------|--------|
| 1 | 入力情報の分類表   | 4区分の具体例と、自社で書き足す記入欄          | ページ 10 |
| 2 | AIサービスの確認表 | 提供会社に聞く9つの質問と、見る場所           | ページ 13 |
| 3 | プラン別の比較表   | 4社の個人・法人と3社のAPIの違いと月額（確認日つき） | ページ 16 |
| 4 | 誤入力したときの初動 | 切り取って貼れる1ページの手順              | ページ 35 |
| 5 | 利用ルールのひな形  | 条文の例。〔 〕を自社の言葉で埋める           | ページ 36 |
| 6 | 管理者向け点検表   | 頻度つきの点検項目と、確認テスト             | ページ 39 |

## 目次

|    |            |    |
|----|------------|----|
|    | この資料で分かること | 04 |
| 01 | 起きる事故      | 06 |
| 02 | 事故の経路      | 08 |
| 03 | 入力情報の分類    | 09 |
| 04 | 情報の種類と確認   | 11 |
| 05 | サービスと契約の確認 | 13 |
| 06 | 学習・保存・所在   | 16 |
| 07 | 個人で使う基準    | 21 |
| 08 | 会社全体の管理    | 23 |

|           |           |           |
|-----------|-----------|-----------|
| <b>09</b> | アカウントとログ  | <b>24</b> |
| <b>10</b> | 外部連携と委託   | <b>27</b> |
| <b>11</b> | シャドーAI    | <b>29</b> |
| <b>12</b> | 出力の確認     | <b>31</b> |
| <b>13</b> | 誤入力の初動    | <b>33</b> |
| <b>14</b> | 利用ルールのひな形 | <b>36</b> |
| <b>15</b> | 管理者の点検表   | <b>39</b> |
| <b>16</b> | 確認テスト     | <b>41</b> |
| <b>17</b> | 次の一歩      | <b>44</b> |
|           | 参考文献と出典   | <b>45</b> |
|           | 発行情報      | <b>52</b> |

## この資料で分かること

入力の線引き・サービスの確かめ方・事故のときの動き方を、自社で決めるための道具を渡します。

生成AIを仕事で使うとき、最初に出る問いは「この情報を入れてよいか」です。次に「無料版と法人契約で何が違うのか」「間違えて入れたら誰に言うのか」が続きます。この資料は、その3つの問いに自社で答えを出し、従業員に配れる形にするための表と手順をまとめたものです。

この資料は、特定の業界に依らず、生成AIを業務で使っている、またはこれから使う会社を対象にしています。扱う範囲は、契約・設定・保存・外部連携・権限・端末・人の運用です。危険だけを並べて責任を避ける書き方はせず、取れる対策と、確かめ方をあわせて書きます。

### 読者別の読む順番

表1

| 読者           | 使う場面                    | 先に読む章                       |
|--------------|-------------------------|-----------------------------|
| 担当者（実際に使う人）  | 入力する前に、自分で判定する          | 入力情報の分類、個人で使う基準、誤入力の初動      |
| 部門責任者        | 部下の使い方と、出力の確認の担当を決める    | 出力の確認、シャドーAI、会社全体の管理        |
| 経営者          | 会社の線引きと、事故のときの動きを決める    | 起きる事故、会社全体の管理、誤入力の初動        |
| 情報システム・総務・法務 | サービスとプランを選び、ルールを作り、点検する | サービスと契約の確認、学習・保存・所在、管理者の点検表 |

## この資料が扱わないこと

- 個別の事案についての法的な判断。資料の中で「専門家に確認すること」と示した点は、弁護士・社会保険労務士・所管の窓口に確かめてください。
- 特定の製品の推奨。比較表は、各社の公式資料で確認できた項目を並べたもので、順位や評価ではありません。
- 事故を完全に防ぐ保証。対策を全部入れても、すべての脅威を防げるとは書きません（会社全体の管理の章）。

## 記述の種類の見分け方

この資料では、書いてある内容の種類を4つの囲みで分けています。囲みの札を見れば、公的な資料で確かめられる事実なのか、BoostXの提案なのか、会社ごとに決めることなのかが分かります。

### 事実

公的機関の資料・法令の条文・各社の公式資料で確かめられることだけを書きます。各社のサービスの仕様と料金は、2026年10月7日に開き直した公式資料によるものです。

### BoostXの推奨

BoostXがすすめる進め方です。公的資料が求めることを、読者がそのまま使える形に並べ直したもので、理由を添えます。会社の事情に合わせて読み替えてください。

### 会社ごとに判断すること

会社ごとに決める必要があることです。決める人と、決めた日を残してください。

### 専門家に確認すること

弁護士・社会保険労務士・税理士・所管の窓口など、資格者や専門家に確かめるべきことです。資料は判断の論点を示しますが、答えは出しません。

# 生成AIの事故は7つの型で起き、入り口は日常の操作にあります

事故の型を知ると、自社でどの型が起きやすいかが見え、対策の順番が決まります。

IPAが2026年1月に公表した「情報セキュリティ10大脅威 2026」では、組織向けの脅威として「AIの利用をめぐるサイバーリスク」が3位に初めて選ばれました。生成AIの事故は、特別な攻撃を受けた会社だけに起きるのではなく、毎日の入力・確認・送信の中で起きます。

## 1-1 事故の7つの型

IPA 産業サイバーセキュリティセンターの中核人材育成プログラム9期生がまとめた手引書（2026年7月）は、AIシステムで起こり得る被害を7つに整理しています。この手引書は受講生の修了成果物で、IPAの意見を代表するものではないと明記されています。公的機関の正式な分類ではありませんが、生成AIを使う会社の立場で、何が起きて誰が困るかを見渡す型として使います。

表2 生成AIの事故の7つの型（9期生の手引書の分類による）

| 型                    | 何が起きるか                          | 誰が困るか        |
|----------------------|---------------------------------|--------------|
| 情報の漏洩                | 入力した顧客情報や社外秘が、社外に出る             | 顧客・取引先・自社    |
| 付与権限外の操作             | AIエージェントが、許した範囲を超えて操作する         | 自社のシステム担当    |
| システムや内部データの改ざん       | 設定値やRAGなどの内部データが書き換えられ、誤った出力をする | 自社の業務全体      |
| AIシステムのサービス停止        | 依存する外部サービスや基盤モデルの障害で、使えなくなる     | 現場の担当者       |
| 虚偽や低品質な出力の利用および出力の誤用 | 架空の情報・偏り・権利侵害を含む出力を、確かめずに使う     | 送った相手・権利者・自社 |

表2 生成AIの事故の7つの型（9期生の手引書の分類による）（前のページからの続き）

| 型       | 何が起きるか                             | 誰が困るか      |
|---------|------------------------------------|------------|
| 第三者への加害 | 乗っ取られたAIが権限の範囲で悪用され、連携先への攻撃や踏み台になる | 連携先・取引先・自社 |
| 過剰課金の発生 | 不正利用や処理の反復で、利用料が膨らむ                | 経理・経営者     |

## 1-2 日常の操作が入り口になる

IPAの解説書は、対話型AIが架空の情報を事実のように生成して利用者に示すことがあるとして、生成結果の精査を求めています。また、従業員が個人で使っているAIサービスを業務に使うこと（シャドーAI）を、情報漏えいにつながるリスクとして挙げています。どちらも、攻撃者がいなくても起きる事故です。

### 起きやすいこと

人によって入れてよい情報の線が違う



法人契約だからと区分の判定を飛ばす



出力を誰も確かめずに社外へ送る



誤入力した人が黙ってしまう



### 先に決めること

入力情報の分類表を1枚にして配る

契約の種類に関わらず区分を先に決める

確かめる人と確かめる項目を決める

報告先と、責めない運用を決めて知らせる

### 決めること

7つの型のうち、自社で起きやすい上位2つを決めてください。次の章で、その型がどの経路で起きるかを確かめます。

# 入力から利用までの5つの経路ごとに、止める場所を決めます

情報は、入力→保存→学習・外部連携→出力→利用の順に動きます。経路ごとに止める章があります。

入力した文章はサービス側に保存され、設定によってはモデルの改善に使われ、接続した外部の仕組みにも渡ります。どこで止めるかを経路ごとに決めると、対策が重複せず、抜けも見えます。

表3 事故の経路と、止める章

| 経路      | 起きること                   | 止める章               |
|---------|-------------------------|--------------------|
| 入力      | 入れてはいけない情報を、人が入れる       | 入力情報の分類、情報の種類と確認   |
| 保存      | 会話がサービス側に残り、人が確認することがある | 学習・保存・所在、個人で使う基準   |
| 学習・外部連携 | 学習に使われる。接続先が情報を受け取る     | サービスと契約の確認、外部連携と委託 |
| 出力      | 架空の情報や、他人の著作物に似た文章が出る   | 出力の確認              |
| 利用      | 出力をそのまま送る。声や映像で本人と信じる   | 出力の確認、誤入力の初動       |

## 2-1 攻撃者が経路に入る場合

IPAの解説書は、AIが動作の途中で自ら参照したデータに不正な指示が含まれ、それを取り込んで成立する攻撃を「間接プロンプトインジェクション」と説明しています。9期生の手引書は、AIエージェントの接続先の定義を書き換え、AIに危険な操作を実行させる攻撃手法が実証された事例も挙げています。政府も2026年5月18日、AIがサイバー攻撃に悪用されることで攻撃のスピードと規模が大きく増えているとの認識を示しました。手口を全部覚える必要はなく、「AIが読む物と、つながる先は、入力と同じ扱いで確かめる」と決めておけば、起きにくくできます。残る危険は、操作ごとの人の確認で受け止めます。この章で決めることは1つです。5つの経路のうち、自社でまだ止める場所が無い経路を書き出してください。それが、先に読む章になります。

# 入れる前に4つの区分に当てはめ、扱いを決めます

公開情報・社内情報・機密情報・個人情報と預かった情報の4区分で、入力の可否を判定します。

AI事業者ガイドライン（第1.2版）は、AI利用者に対し、AIシステム・サービスに機密情報等を不適切に入力しないよう注意を払うことを求めています。IPAの中小企業の情報セキュリティ対策ガイドライン（第4.0版）のコラムも、外部に漏れると問題になるデータはAIサービスに入力しないことを挙げています。問題は、「機密」「外部に漏れると問題」の線を誰が引くかです。

## 3-1 4つの区分

4つの区分は、中核人材育成プログラム9期生の手引書が全社の利用ガイドラインの記載事項として例示する分類（公開情報・社内情報・機密情報・個人情報等）を基に、BoostXが「顧客から預かった情報」を足したものです。預かった情報は、法令より先に契約で入力できない場合があるためです。

表4 入力情報の4区分と扱い（会社で決める前の基準）

| 区分          | 具体例                                | 扱い      | 理由                         |
|-------------|------------------------------------|---------|----------------------------|
| 公開情報        | 公開済みのWebページ・製品説明・採用情報・公開した価格表      | ● 入れてよい | 社外の誰でも見られる。他人の著作物は次章の確認を通す |
| 社内情報        | 社内の手順書・会議のメモ・公開前の企画の骨子・社内連絡        | ① 条件つき  | 会社が認めたサービスとプランだけに入れる       |
| 機密情報        | 原価・取引条件・未公表の経営情報・設計図・認証情報（パスワード・鍵） | ○ 入れない  | 営業秘密として守る情報。認証情報は例外なく入れない  |
| 個人情報・預かった情報 | 氏名と連絡先・顧客名簿・履歴書・健康の情報・取引先から預かった資料  | ○ 入れない  | 法令と契約の確認が先。確認が済んだ範囲だけ条件つき  |

## 3-2 判定の流れ

- 1 情報を4区分のどれかに当てはめる。迷ったら、より厳しい区分に入れる。
- 2 サービスとプランが会社の一覧にあるかを確認する。無ければ入れない。
- 3 条件つきなら、条件（消す項目・使うプラン）を満たしてから入れる。
- 4 迷ったら入れずに、分類表の相談先へ聞く。

区分の判定は契約の種類より先に行います。法人契約でも、預かった資料は守秘条項で入力できないことがあり、個人情報利用目的の確認が要ります。「条件つき」の条件は会社が決めます（例: 会議のメモは氏名と取引先名を消してから入れる）。

## 3-3 自社の分類表を作る

次の表を印刷し、自社で扱う情報を、業務で実際に使う書類名・システム名で書き足してください（足りなければ行を足す）。この章で決めることは、4区分それぞれの自社の情報、「条件つき」の条件、迷ったときの相談先の3つです。

### 入力情報の分類表（自社で書き足す）

印刷して、線で囲んだ欄に書き込んで使います。

| 区分          | 自社の情報の例 | 扱い      | 条件・消す項目 | 決めた人 |
|-------------|---------|---------|---------|------|
| 公開情報        |         | ● 入れてよい |         |      |
|             |         |         |         |      |
| 社内情報        |         | ○ 条件つき  |         |      |
|             |         |         |         |      |
| 機密情報        |         | ○ 入れない  |         |      |
|             |         |         |         |      |
| 個人情報・預かった情報 |         | ○ 入れない  |         |      |
|             |         |         |         |      |
| 迷ったときの相談先   |         |         |         |      |

# 個人情報・営業秘密・預かった情報・著作物は確認の相手が違います

法令・指針・契約のどれで確かめるかが、情報の種類によって変わります。

法令や指針が個別に扱う情報の種類ごとに、何を確かめるかを整理します。2026年10月時点の条文と指針に基づきます。個人情報は法令、営業秘密は指針、預かった情報は契約、著作物は文化庁の考え方で確かめます。

## 4-1 個人情報

個人情報保護委員会は2023年6月の注意喚起で、事業者が生成AIサービスに個人情報を含む指示文を入力する場合、特定された利用目的の達成に必要な範囲内であることを十分に確認するよう求め、本人の同意なく個人データを含む指示文を入力し、応答結果の出力以外の目的で取り扱われる場合は法違反となる可能性があるとして、提供事業者が個人データを機械学習に利用しないこと等を十分に確認するよう求めています。

個人情報保護法第27条は、法令に基づく場合などを除き、あらかじめ本人の同意を得ないで個人データを第三者に提供してはならないと定めています。第28条は、外国にある第三者に提供する場合、同条が定める除外に当たらない限り、あらかじめ外国にある第三者への提供を認める旨の本人の同意を得なければならないと定めています。個人情報保護委員会のQ&Aは、外国にある事業者のサーバーに保存しても、契約条項で事業者が保存された個人データを取り扱わない旨が定められ、適切にアクセス制御を行っている場合等は、外国にある第三者への提供に当たらず、その場合も外国の制度を把握した上で安全管理措置が要るとしています。これはサーバーへの保存についての整理です。生成AIサービスは入力进行处理して応答を返すため、提供会社が入力を「取り扱わない」と言えるかは別の判断になります。この当てはめはBoostXの解釈であり、次の囲みの専門家確認の対象です。

### 専門家に確認すること

生成AIサービスへの個人データの入力が、第三者提供・委託・外国にある第三者への提供のどれに当たるかは、契約と実際の取り扱いで変わります。持参するもの: 契約書とDPA等の契約書類、学習利用の設定、保存と処理の国、再委託先の一覧、入力するデータの種類。これらを示して弁護士に確かめてください。

## 4-2 営業秘密

経済産業省の営業秘密管理指針（令和7年3月31日最終改訂）は、秘密管理している情報を生成AIに利用し、その後に同じ管理単位でAI生成物として出力されたことだけでは、秘密管理性は否定されないと考えられるとしています。一方で、その情報が自社以外の第三者（例として生成AI提供事業者等）に提供される場合は、秘密管理性が否定される場合もあり得るとしています。

IPAの啓発資料（2026年4月）は、最低限の対策の一つとして「クラウドAIに営業秘密は教えない」を挙げています。原価・取引条件・設計図・未公表の経営情報は機密情報の区分に入れ、クラウド型の生成AIには入れないことを基本にします。

### 専門家に確認すること

入力した情報が不正競争防止法の営業秘密として引き続き保護されるかは、自社の秘密管理の実態とサービスの契約内容で変わります。自社の管理の状況を示して弁護士に確かめてください。

## 4-3 顧客から預かった情報

顧客や取引先から預かった資料は、個人情報を含まなくても、契約の秘密保持条項で第三者への開示が禁じられていることがあります。生成AIサービスへの入力が「開示」や「再委託」に当たるかは、契約の文言で決まります。法令の確認より先に、契約書の該当する条項を読み、不明なら契約先に確かめます。

## 4-4 他人の著作物

文化庁の小委員会の「考え方」（令和6年3月）は、AI生成物の生成・利用の段階で既存の著作物との類似性と依拠性が認められれば、著作権侵害として差止請求や損害賠償請求を受け得るとの考え方を示しています（法的な拘束力は持ちません）。文化庁のチェックリストは、まず既存の著作物と類似していないかを確認することが重要だとしています。社外に出す文章・画像・コードは、出力の確認の章の3つの確認を通します。この章で決めることは、4種類の情報それぞれの確かめる担当（法務・契約担当・現場責任者）と専門家に聞く窓口です。預かった情報は、業務ごとに契約を読んだ結果を「入力できる・できない・確認中」で分類表に書きます。

# 契約の前に提供会社へ聞く9つの質問と、見る場所

同じ会社のサービスでも、プランと版で扱いが違います。確認はサービスとプランの単位で行います。

IPAの中小企業の情報セキュリティ対策ガイドライン（第4.0版）のコラムは、生成AIを使う前に利用規約とプライバシーポリシーを確認し、データの取り扱い方針を把握することを挙げています。IPAの解説書は、経営者層の対策として、契約時の約款確認と、入力データを学習対象から除外する設定（オプトアウト）の徹底を挙げています。確認の中身を9項目に分けます。

## 5-1 提供会社に聞く9つの質問

表5 AIサービス・契約の確認表（聞く質問と見る場所）

| 項目        | 提供会社に聞く質問                            | 公式資料のどこを見るか                              |
|-----------|--------------------------------------|------------------------------------------|
| 学習利用の既定   | 入力と出力は、既定でモデルの学習に使われますか              | プライバシーの説明ページ。個人向けと法人向けで別のページになっている       |
| 学習を止める設定  | 利用者または管理者が止められますか。止めた後の扱いは           | データ管理・データコントロールの設定の説明                    |
| 保存期間と削除   | 会話はどれだけ保存され、削除すると何日で消えますか            | データ保持の項。削除後の猶予（例: 30日）と例外（法令・違反対応）       |
| データの所在    | 保存と処理はどの国で行われますか。選べますか               | サーバーの所在・データレジデンシーの項。契約書類（DPA等）に書かれることもある |
| 人による確認    | 提供会社の担当者や委託先が入力内容を見ることがありますか。どの場合ですか | プライバシーの説明の「人によるレビュー」の項。個人向けでは確認することがある   |
| 管理者機能     | 管理者は、利用者の会話を閲覧・書き出し・削除できますか          | 管理者向けヘルプ。プランごとの機能表                       |
| SSOと多要素認証 | 自社のID管理とつなげますか。多要素認証を必須にできますか        | SSOの設定手順。多要素認証は自社のID管理側の説明もあわせて見る        |

表5 AIサービス・契約の確認表（聞く質問と見る場所）（前のページからの続き）

| 項目    | 提供会社に聞く質問                              | 公式資料のどこを見るか              |
|-------|----------------------------------------|--------------------------|
| 監査ログ  | 誰が・いつ・何をしたかの記録を、どのプランで、何日分取れますか        | 監査ログの項。対象プランと書き出しの期間     |
| 契約と通知 | 契約書類（DPA等）、再委託先、事故のときの通知、削除を頼む窓口はどこですか | 利用規約・DPA。法人向けの説明ページの契約の項 |

9項目を契約前に公式資料で確かめ、確認日と確認したページを記録します。理由は2つです。同じ会社でも個人向けと法人向けで学習利用の既定が違うこと、名称とプランが変わり、一度見た資料が古くなることです。

## 5-2 自社の確認記録

### AIサービスの確認記録（サービス・プランごとに1枚）

印刷して、線で囲んだ欄に書き込んで使います。

| 項目        | 確認した結果 | 確認したページ | 確認日 | 確認者 |
|-----------|--------|---------|-----|-----|
| 学習利用の既定   |        |         |     |     |
| 学習を止める設定  |        |         |     |     |
| 保存期間と削除   |        |         |     |     |
| データの所在    |        |         |     |     |
| 人による確認    |        |         |     |     |
| 管理者機能     |        |         |     |     |
| SSOと多要素認証 |        |         |     |     |
| 監査ログ      |        |         |     |     |
| 契約と通知     |        |         |     |     |

### 5-3 名称とプランは変わる

Microsoftの2026年9月30日更新の公式ページは、Microsoft 365 Copilot が Microsoft Copilot に、Microsoft 365 Copilot Chat が Microsoft Copilot Chat に名称が変わったとしています（変更の日付はページに無く、更新日で時点を示します）。OpenAIの個人向けデータ利用の説明ページは法人向けを「ChatGPTチーム」と書き、別の公式ページは ChatGPT Business と書いており、表記がそろっていません。

記録には、確認日・確認したページの題名・プラン名（旧名称があれば併記）を残します。デジタル庁のガイドライン（2026年6月12日改定）は、政府機関が、不特定多数の利用者に提供され、かつ定型約款や規約等への同意のみで利用できるクラウドサービス型の生成AIを業務で使う場合、原則として要機密情報を取り扱えないとしています。民間企業に直接適用される規則ではありませんが、線引きの参考になります。

### 5-4 使ってよいサービスとプランの一覧

確認記録が済んだサービスとプランだけを、次の一覧に載せます。この一覧が、利用ルールのひな形の別表、点検表、確認テストの前提になります。

#### 使ってよいサービスとプランの一覧

印刷して、線で囲んだ欄に書き込んで使います。

| サービス名とプラン | 使ってよい用途 | 入れてよい区分 | 確認日 | 承認者 |
|-----------|---------|---------|-----|-----|
|           |         |         |     |     |
|           |         |         |     |     |
|           |         |         |     |     |
|           |         |         |     |     |
|           |         |         |     |     |

#### 決めること

会社として使ってよいサービスとプランの一覧を作る担当と、記録を見直す周期（この資料では四半期ごとをすすめます）を決めてください。

## 「学習に使わない」と「保存されない」は別の話です

4社の公式資料で確認できた項目だけを、個人・法人・APIの区分で並べます。2026年10月7日時点です。

「学習を止める設定にした」で確認を終えると、次の3つが抜けます。保存されないこと、人が確認しないこと、国内に置かれることは、学習に使われないこととは別の項目です。比較表は、この4つを分けて読みます。

### 6-1 学習を止める設定と、保存されないは別

表6 「学習を止める」と「保存されない」の違い

| 項目      | 意味                | 確かめ方                          |
|---------|-------------------|-------------------------------|
| 学習に使わない | 入力と出力をモデルの改善に使わない | 学習利用の既定と、止める設定                |
| 保存されない  | 会話がサービス側に残らない     | 保存期間と削除。一時チャットでも短期間保持される場合がある |
| 人が確認しない | 提供会社の担当者が内容を見ない   | 人のレビューの項。個人向けでは確認することがある      |
| 国内に置かれる | 保存と処理が日本で行われる     | データの所在。選べるプランは限られる            |

学習を止めても保存はゼロになりません。Geminiの個人向けアプリは保存をオフにしても72時間、ChatGPTの一時チャットは最大30日保持される場合があります（表7）。

### 6-2 プラン別の比較表

次の3つの表は、2026年10月7日に各社の公式資料を開き直して確認できた項目だけを書いています。「記載なし」は、その日の確認で公式資料に記載を見つけられなかった欄で、契約前に営業窓口で確かめてください。プラン名は公式ページの表記に合わせています。

表7 学習利用・止める設定・保存と削除（2026年10月7日時点）

| サービス（区分）                    | 学習利用の既定                        | 利用者が止める設定                        | 保存期間・削除                               | 確認日        |
|-----------------------------|--------------------------------|----------------------------------|---------------------------------------|------------|
| ChatGPT 個人（無料版・Go・Plus・Pro） | 設定で止めない限り、学習に使うことがある           | 設定「すべての人のためにモデルを改善する」をオフ         | 削除は30日以内に消去（例外あり）。一時チャットは最大30日        | 2026-10-07 |
| ChatGPT Business・Enterprise | 既定では学習に使わない                    | 既定で使わない。評価を送ると、その会話が学習に使われることがある | 管理者が保持期間を決める。削除は30日以内に消去（法的義務などの例外あり） | 2026-10-07 |
| OpenAI API                  | 明示的に共有しない限り学習に使わない             | —                                | 監視ログを既定で最長30日保持                       | 2026-10-07 |
| Claude 個人（Free・Pro・Max）     | 利用者が許可を選んだ場合などに使う              | 設定で許可しない                         | 削除した会話は30日以内に消去。許可した場合は識別できない形で最長5年   | 2026-10-07 |
| Claude Team・Enterprise      | 既定では学習に使わない                    | 管理者が評価の送信を無効にできる                 | 削除した会話は30日以内に消去                       | 2026-10-07 |
| Anthropic API               | 既定では学習に使わない                    | —                                | 30日以内に自動で削除（例外あり）                     | 2026-10-07 |
| Gemini 個人                   | 保存がオンなら改良（学習を含む）に使う。人のレビューあり   | アクティビティの保存をオフ、一時チャット             | 既定18か月。オフでも72時間保持。レビュー済みは削除しても最長3年    | 2026-10-07 |
| Google Workspace の Gemini   | 許可なくドメインの外の学習に使わない             | —                                | 既定18か月。3・18・36か月から管理者が決める             | 2026-10-07 |
| Gemini API                  | 無料枠は改良に使い、人のレビューあり。有料枠は改善に使わない | 有料枠を使う                           | 違反の検出のため55日保持                         | 2026-10-07 |

表7 学習利用・止める設定・保存と削除（2026年10月7日時点）（前のページからの続き）

| サービス（区分）                                         | 学習利用の既定                    | 利用者が止める設定           | 保存期間・削除                           | 確認日        |
|--------------------------------------------------|----------------------------|---------------------|-----------------------------------|------------|
| Copilot 個人（2026年8月18日からの新版）                      | 基盤モデルの学習に使わない              | 既定で使わない（止める設定の案内なし） | 期間の記載なし。チャットは1件ずつ削除できる            | 2026-10-07 |
| Copilot 個人（旧版）                                   | サインインした利用者の会話を学習に使う（対象外あり） | いつでも止められる           | 既定で18か月保存                         | 2026-10-07 |
| Microsoft Copilot 法人向け（旧称 Microsoft 365 Copilot） | 基盤モデルの学習に使わない              | —                   | 管理者が Microsoft Purview で保持ポリシーを設定 | 2026-10-07 |

表8 データの所在・SSO・監査ログ（2026年10月7日時点・法人向けとAPI）

| サービス（区分）                             | データの所在                                     | SSO                           | 監査ログ                                         | 確認日        |
|--------------------------------------|--------------------------------------------|-------------------------------|----------------------------------------------|------------|
| ChatGPT Business・Enterprise          | 新規の Enterprise・Edu は保存の国を選べる。Business は対象外 | SAML SSO（Business・Enterprise） | Compliance API は Enterprise のみ（Business は無し） | 2026-10-07 |
| OpenAI API                           | 有効にするとプロジェクトごとに地域を選べる（日本は保存のみ・条件あり）        | 記載なし                          | 記載なし                                         | 2026-10-07 |
| Claude Team・Enterprise（法人向け製品の説明による） | 保存は米国。処理は米・欧・アジア・豪に振り分けの場合あり               | Team・Enterprise で提供           | Enterprise のみ。書き出しは過去180日分                   | 2026-10-07 |
| Anthropic API                        | 保存は米国。処理の振り分けは同上                           | Console組織で提供                  | Compliance API で操作の記録（会話の中身は除く）              | 2026-10-07 |

表8 データの所在・SSO・監査ログ（2026年10月7日時点・法人向けとAPI）（前のページからの続き）

| サービス（区分）                     | データの所在                                         | SSO                       | 監査ログ                                             | 確認日            |
|------------------------------|------------------------------------------------|---------------------------|--------------------------------------------------|----------------|
| Google Workspace<br>の Gemini | 米国か欧州を選べる<br>（Business Standard 以上<br>など）      | SAML・OIDC に<br>対応         | 管理者向けに提供<br>（Geminiアプリと<br>Workspace アプリの操<br>作） | 2026-<br>10-07 |
| Microsoft Copilot 法<br>人向け   | 保存は日本を含む国で<br>（条件あり）。処理は<br>米・EU・他の地域の場合<br>あり | Microsoft Entra<br>ID で管理 | 組織で監査が有効な<br>ら、監査（Standard）<br>で自動記録             | 2026-<br>10-07 |

ChatGPT Business では管理者がワークスペース内の会話履歴を閲覧・書き出し・削除できますが、これは管理者機能で、監査ログとは別の項目です。多要素認証は、OpenAIが「ワークスペースの単位では必須にできない」としている一方、Googleは管理者が2段階認証を利用者やグループに強制でき、Microsoftは Entra ID の条件付きアクセスで全利用者に必須にする構成をすすめています。Anthropicの公式資料には記載がありません。確認表では「自社のID管理（SSO）の側で多要素認証を必須にできるか」を確認項目にします。個人向けプランは、この表の対象から外しています。

### 6-3 プラン名と月額

月額は、各社の日本向け料金ページの表示をそのまま写したものです（BoostXが換算・計算した値ではありません）。税の扱い・年払いか月払いか・割引で額が変わり、APIは使った量で課金されます。契約前に料金ページで確かめてください。

表9 プラン名と月額の表示（2026年10月7日時点）

| サービス       | プラン名と月額                                      | 表示の条件                               | 確認日            |
|------------|----------------------------------------------|-------------------------------------|----------------|
| ChatGPT 個人 | 無料版0円・Go 1,400円・Plus 3,000円・<br>Pro 16,800円～ | 日本の料金ページの円表示                        | 2026-<br>10-07 |
| ChatGPT 法人 | Business 1人3,050円（年額課金・月額は<br>3,850円）        | Business は2名以上。<br>Enterprise は個別見積 | 2026-<br>10-07 |

表9 プラン名と月額を表示（2026年10月7日時点）（前のページからの続き）

| サービス                 | プラン名と月額                                        | 表示の条件                       | 確認日        |
|----------------------|------------------------------------------------|-----------------------------|------------|
| Claude 個人            | Free 0ドル・Pro 22ドル（年払いは月18ドル）・Max 110ドルから       | 日本向けの表示。10%の消費税込み           | 2026-10-07 |
| Claude 法人            | Team 標準席22ドル（年払い）・Enterprise 1席20ドル＋利用量        | Team は2～150名・月払いは27.50ドル。税込 | 2026-10-07 |
| Gemini 個人            | AI Plus 725円・AI Pro 2,900円・AI Ultra 14,500円～   | 無料版あり。Ultra は2段（～32,000円）   | 2026-10-07 |
| Google Workspace     | Starter 800円・Standard 1,600円・Plus 2,500円       | 1人・年間プランの定価。割引の表示あり         | 2026-10-07 |
| Microsoft 365 個人     | Personal 2,130円・Family 2,740円・Premium 3,200円   | 月払いの表示。Copilot つきのプラン       | 2026-10-07 |
| Microsoft Copilot 法人 | Microsoft 365 Copilot 4,497円・同 Business 3,148円 | 1人・年払いの月額相当・税抜。別契約が要る       | 2026-10-07 |

## 6-4 同じ製品名でも版で扱いが違う

個人向けCopilotは、2026年8月18日からの新版では指示文・応答・ファイルの内容を基盤モデルの学習に使わず、旧版では会話を既定で18か月保存して学習に使う（止められる）と、同じ「Copilot」でも版で既定が違います。Geminiも、Workspaceでは許可なくドメインの外の学習に使わない一方、個人向けアプリではアクティビティの保存がオンのとき生成AIモデルのトレーニングを含む改良に使い、人がレビューしたチャットは削除しても最長3年保存されます。

Claudeも、個人向けで利用者が許可した場合は識別できない形で最長5年保持することがあり、法人向け製品では既定で学習に使わず、保存は米国で、通信の経路は米国・欧州・アジア・オーストラリアに振り分けることがあります。

### 決めること

自社で使うサービスとプランについて、比較表の「記載なし」の欄を営業窓口で確かめる担当と、表を最新の表示で見直す期限を決めてください。確かめられない欄がある間は、その区分の情報を入れないことにします。

# 会社の情報を入れない線を自分で引き、設定を確かめます

会社の一覧に無いサービスを個人で使うときの線引きと、使う前の6項目です。

会社が認めたサービスとプランが無い段階でも、担当者は個人で生成AIを使います。この章は、個人のアカウントで使う人のための基準です。会社全体で使う場合の管理は、次の章で分けて書きます。

## 7-1 個人で使うときの線

個人のアカウントで使うサービスは、学習利用の既定・保存・人の確認が個人向けの規約で決まります。Googleは、個人向けのGeminiアプリについて、人のレビュアーがデータの一部を確認することがあるとして、見られたくない機密情報や改良に使われたくない機密情報を入力しないよう求めています。OpenAIは、個人向けのChatGPTについて、利用者が設定で止めない限り、会話の内容をモデルの学習に使うことがあるとしています。

個人のアカウントには、会社の情報を入れないことを線にします。入れてよいのは、公開情報と、会社の情報を含まない作業（文章の言い換え・一般的な調べ物）だけで、社内情報・機密情報・個人情報・預かった情報は入れません。この線は、会社が使ってよいサービスとプランの一覧を作る前も後も同じです。一覧ができたなら、業務は会社が発行したアカウントで使います（利用ルールのひな形 第2条・第8条）。

## 7-2 設定の確かめ方

- 
- 学習を止める設定の場所を、公式資料で確かめる。ChatGPTは設定の「データコントロール」、Geminiは「アクティビティ」の設定、Claudeは個人向けの許可の設定。
- 
- 止めた後も、保存済みの会話は残る。OpenAIは、学習の設定をオフにしても保存済みのチャットは削除されないとしている。止める設定は、止める前の会話、進行中の学習、学習済みのモデルには及ばない。
- 
- 一時チャットは、学習には使われないが、短期間保持される。Geminiは72時間、ChatGPTは最大30日。
-

- 評価（いいね・よくないね）を送ると、止めた後でもその会話が学習に使われることがある。社内の文章を扱った会話では評価を送らない。
- アプリの版を確かめる。個人向けCopilotは、2026年8月18日からの新版と旧版で既定が違う。

## 個人で使う前の6項目

- ☐ 会社の情報（社内・機密・個人・預かった情報）は入れない、と決めている
- ☐ 学習を止める設定の場所を公式資料で確かめ、設定した日を控えた
- ☐ 一時チャットでも短期間は保持されることを知っている
- ☐ 社内の文章を扱った会話では、評価（いいね等）を送らない
- ☐ 使っているアプリの版と、適用される規約のページを確かめた
- ☐ 共有リンク・メモリ・ファイルの添付・アプリ連携を、会社の情報には使わない

## 個人のアカウントで、取引先から預かった見積の内訳を要約した場合

### 失敗例と防止策（想定例）

#### 何が起きるか

営業担当が、取引先から預かった見積の内訳を個人向けサービスに貼り付けて要約する。契約の守秘条項に反し、会社は把握していない。



#### なぜ起きるか

会社に使えるサービスが無く、個人で使う線も決まっていないため、本人は便利な道具として使っている。

### 防ぎ方

個人のアカウントには会社の情報を入れない線を配る。会社として使えるサービスを用意し、預かった情報は分類表で「入れない」にする。

## 決めること

個人のアカウントで入れてよい情報の線を、「公開情報と、会社の情報を含まない作業まで」のように1行で決め、従業員に伝えてください。

## 決める人・運用する人・使う人を分け、 見直す周期を決めます

会社として使うときは、役割と周期を先に決めます。対策を全部入れても安全は保証されません。

AI事業者ガイドライン（第1.2版）は、AI利用者が提供者の意図した範囲内で適正に利用し、人間の判断を介在させることで予期せぬ事故を防げるとしています。会社全体で使うときは、「誰が判断を介在させるか」を役割として決めます。

表10 会社全体で使うときの役割分担

| 役割    | 誰が           | 決めること・行うこと                               |
|-------|--------------|------------------------------------------|
| 決める人  | 経営者・責任者      | 入力の手引き、使ってよいサービスとプランの採否、事故のときの報告先、ルールの承認 |
| 運用する人 | 情報システム・総務・法務 | 確認表の記録、アカウントと権限の管理、ログの確認、ルールの周知と見直し、点検   |
| 使う人   | 各部門の担当者と責任者  | 分類表の判定、出力の確認、誤入力時の報告、聞き取りへの協力            |
| 確かめる人 | 部門責任者        | 社外に出す出力の最終確認、部下の使い方の確認                   |

### 8-1 対策を全部入れても安全を保証しない

対策を全部入れても安全を保証しない、というのがこの資料の前提です。なお、IPAの解説書は、複数の脅威に有効な共通対策を実施すれば完璧ということではなく、各脅威の解説も参照して対策を実施することが重要だとしています。だからこそ、事故が起きたときの初動と、見直しの周期を先に決めます。

#### 決めること

4つの役割に名前（部署名か役職名）を入れ、見直しの周期（推奨: 確認記録は四半期・ルールは半年・法令や指針の変更時は都度）と次の見直し日を決めてください。

# 誰が・どの権限で・何をしたかを後から追える状態にします

個人アカウントの業務利用の扱い、SSO、多要素認証、退職時の停止、監査ログの5点を点検します。

IPAの解説書は、AIの利用に関する管理者・従業員向けの対策として、多要素認証（MFA）の徹底と、通信ログ等によるAIサービスの利用状況の把握を挙げています。生成AIの事故は、何を入れたかを後から追えないと、範囲の特定も報告もできません。アカウントとログは、事故のときに最初に見る場所です。

## 9-1 点検の5点

- 1 個人アカウントの業務利用の扱い。会社の一覧にあるサービスでも、個人のアカウントで使えば個人向けの規約が適用される。業務は会社が発行したアカウントで使う、と決める。
- 2 SSO。ログインを会社のIDにまとめる仕組みで、入退社と異動がアカウントに反映されるかどうかは、作成と停止の自動連携の有無で決まるため別に確かめる。Anthropicは、SSOをTeamプラン・Enterpriseプラン・Console組織で提供している。OpenAIは、法人向けのChatGPTでSAML SSOによる認証を提供している。
- 3 多要素認証。OpenAIは、ChatGPTのワークスペースとAPIの組織の単位では多要素認証を必須にできないとしている。自社のID管理（SSO）の側で必須にできるかを先に確かめる。
- 4 退職・異動時の停止。アカウントの停止と、会話の引き継ぎ・削除の手順を決める。ID管理側を止めても、ログイン済みの端末のセッションと発行済みのAPIキーは残るため、失効を確かめる。
- 5 監査ログの有無と保存期間。Anthropicは、監査ログをEnterpriseの組織だけで提供し、書き出しの対象を過去180日以内としている。Microsoftは、組織で監査が有効な場合、Copilotに関する利用者の操作と管理の操作を、監査（Standard）の一部として自動的に記録としている。OpenAIは、ChatGPT Enterpriseなどで管理者がEnterprise Compliance APIを通じて会話に関する監査ログにアクセスできるとしている。

**BoostXの推奨**

監査ログの保存期間を、自社の規程（事故の調査にさかのぼる期間）と照らします。サービス側の期間が短ければ、定期的書き出して保管します。ログに会話の本文が含まれるかどうかプランで違うため、確認表に書きます。

## 9-2 端末とブラウザの点検

アカウントの管理が整っても、情報は端末から出ます。IPAの啓発資料は、対策の一つとして「AIブラウザは社内用と社外用を分ける」を挙げています。

- 
- 私物の端末とスマートフォンのアプリ。会社のアカウントを使うかを決め、使うなら紛失時にセッションを切る手順を持つ。
- 
- ブラウザ拡張とAIを組み込んだブラウザ。開いているページを読む拡張は社内システムの画面も読む。社内用と社外用を分ける。
- 
- デスクトップアプリの権限。ファイル・画面・クリップボードを許すと、画面共有やコピー＆ペーストの内容が渡る。
- 
- 共有PCのログイン状態。離席時のログアウトと画面の自動ロック。
- 
- 紛失・盗難。端末の遠隔ロックと、セッション切断・APIキーの失効を同時に行う。
-

## アカウントと権限の点検

---

- ☐ 業務は会社が発行したアカウントで使う、と決めて伝えた
  - ☐ SSOの対象プランを確かめ、つなげるかを決めた
  - ☐ 多要素認証を、ID管理側かサービス側で必須にした
  - ☐ 退職・異動時のアカウント停止と、会話の扱いを手順にした
  - ☐ 監査ログの対象プラン・保存期間・本文の有無を確認表に書いた
  - ☐ ログを誰が・どの頻度で見るかを決めた
  - ☐ 私物端末・ブラウザ拡張・デスクトップアプリの許す範囲と、紛失時の手順を決めた
- 

### 決めること

5点のうち、今の契約で満たせない項目を書き出し、プランの変更か、ID管理側の対策かを選んでください。

# つなぐ前に、何にアクセスさせるかと接続先の提供元を確かめます

API・プラグイン・AIエージェント・委託先は、入力と同じ扱いで確かめます。

生成AIは、社内のファイル・メール・業務システムとつなぐと便利になります。同時に、AIがアクセスできる範囲が広がり、接続先の提供元が情報を受け取ります。つなぐ前の確認を表にします。

表11 つなぐ前の確認表

| 確かめること     | 具体的に見ること                            | 誰が        |
|------------|-------------------------------------|-----------|
| 何にアクセスさせるか | 読める範囲（フォルダ・メール・顧客データ）と、書き込める範囲      | 情報システム    |
| 権限の範囲      | 最小の権限になっているか。全社の権限を渡していないか          | 情報システム    |
| 接続先の提供元    | 提供元の名前・規約・データの扱い。無名の接続先を入れていないか     | 情報システム・法務 |
| 更新情報       | 脆弱性情報と修正版の有無。更新の担当                  | 情報システム    |
| 委託に当たるか    | 個人データを渡す場合の契約と監督                    | 法務・専門家    |
| APIキー      | 発行者・保管場所・失効の手順。個人のメモや共有文書に残さない      | 情報システム    |
| 他社製の道具の規約  | APIを使う道具には、その提供元の規約と保存が適用される。別に確かめる | 情報システム・法務 |

## 10-1 AIエージェントに操作を任せるとき

9期生の手引書（受講生の修了成果物）は、AIエージェントが外部の仕組みとつながるための接続先の定義を書き換え、AIに危険な操作を実行させる攻撃手法が実証された事例を挙げています。エージェントに「読む」だけでなく「送る・書き換える・支払う」操作を任せるときは、操作ごとに人の確認を挟むか、任せる操作の一覧を決めます。

JPCERT/CCの週次レポート（2026年9月30日号）には、AIを組み込んだ業務基盤の製品の脆弱性と、修正済みの版への更新で解決することが掲載されています。AIの機能を持つ製品にも、ほかのソフトウェアと同じように脆弱性情報が出ます。更新の担当を決め、点検表で確かめます。

## 10-2 委託に当たるとき

個人情報保護法第27条第5項第1号は、利用目的の達成に必要な範囲内で個人データの取扱いを委託することに伴って提供される場合、提供を受ける者は第三者に当たらないと定めています。第25条は、個人データの取扱いを委託する場合、委託先に対して必要かつ適切な監督を行わなければならないと定めています。

### 専門家に確認すること

生成AIサービスやAPIの利用が「委託」に当たるかは、契約と実際の取り扱いで変わります。委託に当たるなら、委託先の選定・契約・取扱状況の把握が必要です。自社の契約と、渡すデータの種類を示して、弁護士に確かめてください。

## 決めること

今つないでいる外部連携を次の一覧に書き出し、「何にアクセスさせているか」が答えられないものを止めるか、確認表を埋めてから再開するかを決めてください。

## 外部連携の一覧

印刷して、線で囲んだ欄に書き込んで使います。

| 接続先（道具・エージェント） | アクセスさせる範囲 | 提供元 | 担当 | 確認日 |
|----------------|-----------|-----|----|-----|
|                |           |     |    |     |
|                |           |     |    |     |
|                |           |     |    |     |
|                |           |     |    |     |
|                |           |     |    |     |
|                |           |     |    |     |

# 個人アカウントの業務利用は、責めずに把握し、使える手段を用意します

把握→手段の用意→ルール→検知の順に進めます。聞き取り票と、責めない前置きの文例を付けます。

IPAの解説書は、従業員が個人で使っているAIサービスを業務に使うこと（シャドーAI）を、情報漏えいにつながるリスクとして挙げ、経営者層の対策として、シャドーAI回避のためのAIサービス利用の検討、未許可・未認可のAIサービス利用の禁止、個人アカウントにおける業務利用の制限、規程違反時の対応の明確化を挙げています。BoostXは、このうち使える手段の用意を先に置きます。禁止だけを先に出すと申告されない利用が増える、というのがBoostXの見方です。

## 11-1 進める順番

- 1 実態を把握する。部門ごとに聞き取り票で、使っているサービス・アカウントの種類・入れている情報の区分・使う理由を聞く。責めない前置きを付ける。
- 2 会社として使える手段を用意する。聞き取りで多かった用途から、会社の一覧に入れるサービスとプランを決める。
- 3 ルールを明文化して周知する。分類表・使えるサービスの一覧・報告先を1枚にして配る。
- 4 技術的に検知する。通信ログや利用状況の把握の仕組みで、一覧に無いサービスの利用を見つける。会社のネットワークを通らない端末は技術で止めにくいため、1～3を先に行う。

### BoostXの推奨

把握を先にする理由は、禁止から始めると申告されない利用が増えるためです。聞き取りは「使っている人を見つける」ためではなく、「会社が用意すべき手段を知る」ために行う、と伝えます。

## 11-2 聞き取り票

### 聞き取りの前置きの文例

生成AIをどう使っているかを教えてください。  
 使っていること自体を問題にするためではなく、  
 会社として安心して使える道具を用意するために聞きます。  
 個人のアカウントで使っている場合も、そのまま教えてください。  
 今日の内容で、個人の評価を下げることはありません。

この前置きの約束（評価を下げない）を会社として守れるかを、聞き取りの前に責任者が決めます。故意や重大な違反が見つかった場合の扱いも、先に決めておきます。

### シャドーAIの聞き取り票（1人1枚）

印刷して、線で囲んだ欄に書き込んで使います。

| 聞くこと               | 記入欄 |
|--------------------|-----|
| 使っているサービス名とプラン     |     |
| アカウントの種類（会社・個人）    |     |
| 入れている情報の区分         |     |
| 主な用途と、使う理由         |     |
| 会社の道具で置き換えるのに必要なこと |     |
| 学習を止める設定の有無        |     |
| 聞き取った日・聞き取った人      |     |

### 決めること

聞き取りを行う部門の順番（情報漏えいの影響が大きい部門から）と、聞き取る担当、結果をまとめる期限を決めてください。

# 誤り・権利侵害・なりすましは、使う前の3つの確認で止めます

事実・権利・社外に出す前の人の確認の3点と、送金や情報送付を求められたときの手順です。

AI事業者ガイドライン（第1.2版）は、AIの出力の精度とリスクの程度を理解し、リスク要因を確認したうえで利用することを求め、IPAの中小企業の情報セキュリティ対策ガイドライン（第4.0版）のコラムは、生成された成果物を必ず人間が確認し、正確性と法的リスクを確かめることを挙げています。

表12 出力を使う前の3つの確認

| 確認     | 何を見るか                                 | 誰が        |
|--------|---------------------------------------|-----------|
| 事実     | 固有名詞・数字・日付・引用が、元の資料と一致するか。元が無い記述は使わない | 作った本人     |
| 権利     | 既存の文章・画像・コードに似ていないか。他人の著作物を入力に使っていないか | 作った本人と責任者 |
| 社外に出す前 | 事実と権利の確認が済んだ印があるか。約束できない表現が無いか        | 部門責任者     |

## 12-1 架空の情報と権利侵害

出力に出てきた固有名詞・数字・法令名は、元の資料を開いて確かめ、示せない記述は社外に出す文書から外します。権利については、文化庁の考え方（令和6年3月）が、既存の著作物との類似性と依拠性が認められれば、著作権侵害として差止請求や損害賠償請求を受け得るとしています。社外に出す画像・文章・コードは、似たものが無いかを確かめ、指示文を残します。

専門家に確認すること

生成物の利用が著作権・商標権などの侵害に当たるか、他人の著作物を入力してよいかは、個別の判断です。文化庁の考え方は法的な拘束力を持たないため、社外に広く出す制作物は弁護士に確かめてください。

## 12-2 なりすまし

IPAは、ビジネスメール詐欺のなりすましで、AIによるディープフェイク等の利用が確認されているとし、啓発資料で「外見では詐欺師を見破れないと心得る」を対策に挙げています。警察庁は、経営者等になりすまして送金させる詐欺について、社内で情報を共有し、送金に関するルールを再確認するよう呼びかけています。

BoostXの推奨

送金・振込先の変更・機密情報の送付を求められたときは、声や映像で本人かどうかを判断せず、登録してある連絡先へ別の手段でかけ直す手順を決めておきます。「緊急」「秘密に」と添えられた依頼ほど飛ばしません。この章で決めることは、部門ごとの社外に出す出力の最終確認者と、送金と振込先の変更の確認手順の2つです。

## 社長の声で振込先の変更を指示され、担当者がその場で送金した場合

失敗例と防止策（想定例）

何が起きるか

経理担当者に、社長の声と名前で「急ぎで振込先を変えて送金してほしい」と電話が入り、担当者はその場で送金する。

なぜ起きるか

声で本人と判断し、送金前にかけ直す手順が無い。「緊急」「秘密に」と言われて確認を飛ばしている。

防ぎ方

送金と振込先の変更は、登録済みの連絡先へ別の手段でかけ直してからにする。確認なしの送金はしない、と社内で共有する。

# 気づいた人と管理者の動きを、1ページに決めます

覚知→事実の確保→社内の報告→速報の要否判断→速報→確報の順と期限を、1ページに決めます。

個人情報保護委員会のガイドラインは、漏えい等の事案が発覚したとき、責任ある立場の者への報告と拡大防止、調査と原因の究明、影響範囲の特定、再発防止などの措置を求めています。この章の最後の1ページはそれを生成AIへの誤入力に当てはめた手順で、期限は法令と指針の定めとBoostXの目安を見出しで分けます。

## 13-1 法令とガイドラインで決まっている期限（2026年10月時点）

個人情報保護法施行規則第7条が個人情報保護委員会への報告が必要と定める事態は、要配慮個人情報を含む漏えい等、財産的被害のおそれがある漏えい等、不正の目的によるおそれがある漏えい等、本人の数が1,000人を超える漏えい等の4つ（高度な暗号化等の措置を講じた個人データは除く）で、いずれも「発生したおそれがある事態」を含みます。

表13 漏えい等の報告・通知の期限と起算点

| 区分                   | 期限                             | 起算点                | 根拠                     |
|----------------------|--------------------------------|--------------------|------------------------|
| 速報                   | 知った後、速やかに。目安は個別の事案によるが概ね3～5日以内 | 法人では、いずれかの部署が知った時点 | 施行規則第8条第1項、通則編         |
| 確報                   | 知った日から30日以内                    | 同じ。知った時点を1日目と数える   | 施行規則第8条第2項、通則編         |
| 確報（不正の目的によるおそれがある事態） | 知った日から60日以内                    | 同じ                 | 施行規則第8条第2項             |
| 本人への通知               | 状況に応じて速やかに（困難なら代わりの措置）         | —                  | 法第26条第2項、規則第10条        |
| 委託元への通知（預かった個人データ）   | 知った後速やかに。目安は個別の事案によるが概ね3～5日以内  | 委託先が知った時点          | 法第26条第1項ただし書、規則第9条、通則編 |

## 初動の連絡先（記入して手順の横に貼る）

印刷して、線で囲んだ欄に書き込んで使います。

| 連絡先          | 部署・氏名 | メール・内線 | 記入日 |
|--------------|-------|--------|-----|
| 窓口（最初に知らせる先） |       |        |     |
| 管理者（保全・削除）   |       |        |     |
| 責任者（報告を決める人） |       |        |     |
| 専門家（弁護士など）   |       |        |     |
| 委託元（預かった情報）  |       |        |     |

### 専門家に確認すること

誤入力が法令上の「漏えい等」に当たるか、報告と本人通知が要るかは事案ごとの判断です。情報の区分・件数・保存と削除の状況を示して弁護士に確かめてください。不正アクセスが疑われる場合は、JPCERT/CCが報告の受け付けと対応の支援を行っています。個人情報の保護に関する法律等の一部を改正する法律（2026年7月17日公布、施行は原則として公布から2年以内）には委託先の義務と本人通知の見直しが含まれ、施行後に直す箇所もあわせて確かめてください。

## 13-2 BoostXが推奨する社内の目安

手順の「いつまでに」の印は、（目安）＝BoostXの推奨、（指針）＝ガイドライン通則編の目安、（法令）＝法と施行規則の期限です。報告と本人通知の要否の判断は、知った日を1日目として2日目までに終わります（速報の目安を判断で使い切らないため）。不正アクセスが疑われるときは消さずに専門家へ、個人のアカウントで起きた場合は本人が窓口の立ち会いで同じ手順を行います。

手順

## 誤入力したときの初動（印: 目安・指針・法令）

- |   |                                           |                                                  |                               |
|---|-------------------------------------------|--------------------------------------------------|-------------------------------|
| 1 | <b>入力を止める</b><br><b>誰が</b><br>入力した本人      | <b>何を</b><br>同じ会話への追加の入力をやめ、画面を閉じない              | <b>いつまでに</b><br>気づいた直後（目安）    |
| 2 | <b>記録と失効</b><br><b>誰が</b><br>入力した本人       | <b>何を</b><br>画面の写し・日時・サービス名・入れた情報を控え、認証情報は失効     | <b>いつまでに</b><br>気づいた直後（目安）    |
| 3 | <b>窓口へ報告する</b><br><b>誰が</b><br>入力した本人     | <b>何を</b><br>決めておいた窓口へ、記録を添えて知らせる                | <b>いつまでに</b><br>当日中（目安）       |
| 4 | <b>保全してから削除する</b><br><b>誰が</b><br>管理者     | <b>何を</b><br>会話を書き出して保全し、削除の日時と操作者を記録する          | <b>いつまでに</b><br>当日中（目安）       |
| 5 | <b>範囲を特定する</b><br><b>誰が</b><br>管理者と責任者    | <b>何を</b><br>情報の区分・件数・本人の有無・委託元を書き出す             | <b>いつまでに</b><br>翌営業日まで（目安）    |
| 6 | <b>報告の要否を判断する</b><br><b>誰が</b><br>責任者と専門家 | <b>何を</b><br>漏えい等に当たるか、報告と本人通知が要るかを定める（知った日が1日目） | <b>いつまでに</b><br>2日目まで（目安）     |
| 7 | <b>速報と関係先・本人への通知</b><br><b>誰が</b><br>責任者  | <b>何を</b><br>委員会へ速報、委託元・契約先へ通知。本人へは状況に応じ速やかに（法令） | <b>いつまでに</b><br>知ってから3～5日（指針） |
| 8 | <b>確報と再発防止</b><br><b>誰が</b><br>責任者と管理者    | <b>何を</b><br>確報（不正目的なら60日）を出す。ルールの直しも同じ時期を目安に    | <b>いつまでに</b><br>30日以内（法令）     |

# 条文の例を自社の言葉で埋め、配れる形にします

適用範囲・サービス・入力・出力・禁止・連絡・見直し・端末・外部連携・確認・責任者の11条です。

次のひな形は、中核人材育成プログラム9期生の手引書（受講生の修了成果物）が全社の利用ガイドラインの記載事項として挙げる7観点（適用範囲・利用できるAI・入力基準・出力の取扱い・禁止事項・インシデント時の対応・責任分界）を基に、BoostXが見直し・アカウントと端末・外部連携・利用状況の確認の4条を足した11条です。〔 〕の中を自社の言葉で埋めてください。

## 14-1 利用ルールのひな形

### 利用ルールのひな形（第1条～第3条）

#### 第1条（適用範囲）

このルールは、〔会社名〕の役員・従業員・派遣社員・業務委託先の担当者が、業務で生成AIを使うすべての場合に適用する。  
個人のアカウントで業務の情報を扱う場合も含む。

#### 第2条（使ってよいサービス）

業務で使う生成AIは、〔管理部門名〕が確認し、別表「使ってよいサービスとプランの一覧」に載せたものに限る。  
一覧ができるまでは、個人のアカウントで公開情報と、会社の情報を含まない作業に限って使える。一覧ができた後も同じとする（第8条）。  
一覧に無いサービスを業務で使いたいときは、〔管理部門名〕に申請する。  
一覧は〔四半期〕ごとに見直し、確認日を記録する。

#### 第3条（入力の基準）

入力する情報は、別表「入力情報の分類表」の4区分に当てはめる。  
公開情報は入力してよい。社内情報は、一覧にあるサービスで、分類表の条件を満たす場合に入力できる。  
機密情報、個人情報、顧客から預かった情報は入力しない。  
分類表で条件つきとした個人情報・預かった情報は、〔法務担当〕の確認が済んだ範囲でだけ入力できる。  
判定に迷ったときは入力せず、〔相談窓口〕に相談する。

#### 利用ルールのひな形（第4条～第7条）

##### 第4条（出力の確認）

生成AIの出力は、事実（固有名詞・数字・日付・引用）と、他人の著作物との類似の有無を、作った本人が確かめる。  
社外に出す文書・画像・コードは、〔部門責任者〕の確認を受ける。  
送金・振込先の変更・機密情報の送付を求める連絡は、登録済みの連絡先へ別の手段でかけ直してから対応する。

##### 第5条（禁止事項）

認証情報（パスワード・鍵・トークン）の入力。  
一覧に無いサービスへの、公開情報以外の入力。  
出力をそのまま社外に送ること。  
会社の情報を扱った会話での評価（いいね等）の送信。

##### 第6条（誤入力・事故のときの連絡）

入れてはいけない情報を入力したと気づいたときは、追加の入力をやめ、画面と日時を記録し、〔連絡先〕に当日中に知らせる。  
報告した本人の不利益にはしない。  
以後の手順は、別紙「誤入力したときの初動」による。

##### 第7条（見直し）

このルールは、〔半年〕ごと、および法令・公的な指針・利用するサービスの規約が変わったときに、〔管理部門名〕が見直す。  
改定日と版を記録し、全員に知らせる。

#### 利用ルールひな形（第8条～第11条）

##### 第8条（アカウントと端末）

業務は、会社が発行したアカウントで使う。

私物の端末と個人のアカウントでは、公開情報と、会社の情報を含まない作業に限る。

ブラウザ拡張、AIを組み込んだブラウザ、デスクトップアプリは、〔管理部門名〕が認めたものだけを使う。

共有の端末ではログアウトする。端末を紛失したときは〔連絡先〕に知らせ、セッションを切る。

##### 第9条（外部連携）

社内のファイル・メール・業務システムとの接続と、AIエージェントへの操作の委任は、〔管理部門名〕に申請し、別表「外部連携の一覧」に載せたものに限る。

APIキーは〔管理部門名〕が発行し、個人で保管しない。

##### 第10条（利用状況の確認）

会社は、監査ログと通信ログで利用状況を確認することがある。

確認の範囲は〔 〕とし、このルールで全員に知らせる。

##### 第11条（責任者）

このルールの責任者は〔役職名〕とする。入力の手引き、サービスの採否、事故のときの報告は責任者が決め、運用は〔管理部門名〕、確認は〔部門責任者〕が担う。

#### 専門家に確認すること

第3条の「条件」と第5条の禁止事項は、業務で実際に扱う書類名で書き足してください。第10条の利用状況の確認（ログの確認）が労務上認められる範囲と、懲戒の扱いは、社会保険労務士または弁護士に確かめてから書きます。

#### 決めること

〔 〕の中を埋める担当と、第1版を配る日を決めてください。配るときは、分類表・使ってよいサービスとプランの一覧・外部連携の一覧・初動の1ページを別表として付け、配った日を点検表の「教育」の欄に書きます。

# サービス・設定・権限・ログ・教育・規約を、 頻度を決めて点検します

点検表は2枚と担当表1枚です。頻度は印字済みで、担当と次の点検日は担当表に書き込みます。

点検は、事故を防ぐためだけでなく、規約と法令の更新に気づくために行います。更新日の表示がある各社の公式ページは、2026年1月から9月の間に更新されています。IPAは、AIに関するセキュリティの動向と事例をまとめた「AIセキュリティ短信」を継続して公開しており、最新号は2026年9月号です。管理者が定期的に確認する情報源として、点検表に入れます。

## 管理者の点検表（1）サービスと設定

- 
- ☐ 使ってよいサービスとプランの一覧が最新で、確認日が四半期以内（四半期）
  - ☐ 各サービスの学習利用の既定と、止める設定の状態を確かめた（四半期）
  - ☐ 保存期間の設定と、削除の運用を確かめた（四半期）
  - ☐ データの所在を確認表に書き、変更が無いが公式資料を見た（四半期）
  - ☐ 名称・プランの変更を公式資料で確かめ、旧名称を併記した（四半期）
  - ☐ 外部連携の一覧に、アクセス範囲と提供元が書かれている（四半期）
  - ☐ AIの機能を持つ製品の脆弱性情報と更新を確かめた（毎月）
  - ☐ AIセキュリティ短信など、公的機関の更新情報を見た（毎月）
-

## 管理者の点検表（2）人と運用

- ☐ 業務は会社が発行したアカウントで使われている（四半期）
- ☐ SSOと多要素認証の設定に例外が無い（四半期）
- ☐ 退職・異動した人のアカウントが停止されている（毎月）
- ☐ 監査ログで、契約中のサービスの操作を決めた頻度で確かめた（毎月）
- ☐ 通信ログで、一覧に無いサービスの利用が無いことを確かめた（毎月）
- ☐ 分類表・ルール・初動の1ページを、新しく入った人に配った（入社時）
- ☐ 誤入力の報告が、責めずに受け付けられている（半年）
- ☐ 規約・法令・指針の更新と改正個人情報保護法の施行日を確認、ルールを直した（半年・都度）
- ☐ 私物端末・ブラウザ拡張・デスクトップアプリの許す範囲に例外が無い（四半期）

### 15-1 点検の担当表

頻度ごとに、点検する担当と次の点検日を書き込んでください。点検したら確認者が日付を入れます。

#### 点検の担当表

印刷して、線で囲んだ欄に書き込んで使います。

| 頻度           | 担当 | 次の点検日 | 点検した日と確認者 |
|--------------|----|-------|-----------|
| 毎月           |    |       |           |
| 四半期          |    |       |           |
| 半年           |    |       |           |
| 入社時          |    |       |           |
| 都度（法令・規約の変更） |    |       |           |

## 自社に無いものを見つけ、戻る章を決めます

点数で安全を判定しません。「いいえ」の問いごとに、戻る章を示します。

1つ目は、自社にあるか・無いかを「はい・いいえ」で答える12の問いです。「いいえ」が付いた問いの章に戻ってください。2つ目は、読んだ内容の確認です。

### 自社に無いものを見つける12の問い

---

- ☐ 入力情報の分類表があり、従業員に配られている（いいえ → 入力情報の分類）

---
- ☐ 預かった情報の契約の守秘条項を読む担当が決まっている（いいえ → 情報の種類と確認）

---
- ☐ 使ってよいサービスとプランの一覧があり、確認日が書かれている（いいえ → サービスと契約の確認）

---
- ☐ 学習・保存・人の確認・所在を分けて確認している（いいえ → 学習・保存・所在）

---
- ☐ 個人のアカウントで入れてよい情報の線が決まっている（いいえ → 個人で使う基準）

---
- ☐ 決める人・運用する人・使う人・確かめる人が決まっている（いいえ → 会社全体の管理）

---
- ☐ 多要素認証と監査ログの対象プランを確かめている（いいえ → アカウントとログ）

---
- ☐ 外部連携の一覧に、アクセス範囲と提供元が書かれている（いいえ → 外部連携と委託）

---
- ☐ 個人アカウントの業務利用を、聞き取りで把握した（いいえ → シャドーAI）

---
- ☐ 送金と振込先の変更の確認手順が決まっている（いいえ → 出力の確認）

---
- ☐ 誤入力したときの連絡先が決まり、貼り出されている（いいえ → 誤入力の初動）

---
- ☐ 利用ルール第1版が配られ、見直しの周期が決まっている（いいえ → 利用ルールのひな形）

---

## 16-1 読んだ内容の確認

---

**Q1** 法人契約のサービスに、顧客から預かった資料を入力する前に、最初に確かめることはどれですか

- ☐ ア 法人契約なので確認は要らない
  - ☐ イ 学習を止める設定がオンになっているか
  - ☐ ウ 契約の秘密保持条項と再委託の制限
- 

**Q2** 「学習を止める設定にした」とき、あわせて確かめることはどれですか

- ☐ ア 保存期間・人の確認・データの所在
  - ☐ イ 何も要らない。学習に使われなければ安全
  - ☐ ウ サービスの料金プラン
- 

**Q3** 個人向けのChatGPTで「すべての人のためにモデルを改善する」をオフにした後の扱いとして正しいものはどれですか

- ☐ ア 保存済みのチャットも削除される
  - ☐ イ 新しい会話は学習に使われないが、保存済みのチャットは残る
  - ☐ ウ 一時チャットは保持されない
- 

**Q4** 誤入力に気づいた本人が、最初にすることはどれですか

- ☐ ア 会話の履歴を削除する
  - ☐ イ 研修の内容を見直す
  - ☐ ウ 同じ会話への追加の入力をやめ、画面を閉じずに記録する
- 

**Q5** 社長の声で急ぎの送金を指示されたとき、取る行動はどれですか

- ☐ ア 登録済みの連絡先へ別の手段でかけ直してから対応する
- ☐ イ 声が本人なのでその場で送金する
- ☐ ウ 金額が小さければ送金する

**Q6** 個人情報保護委員会への報告が必要な事態の確報の期限として、2026年10月時点の条文で正しいものはどれですか

- ☐ ア 知った日から7日以内
- ☐ イ 知った日から30日以内（不正の目的によるおそれがある事態は60日以内）
- ☐ ウ 知った日から1年以内

## 確認テストの正解と解説

**Q1** 正解 ウ

預かった情報は、法令より先に契約で入力できない場合があります。契約の条項を読み、不明なら契約先に確かめます。

**Q2** 正解 ア

学習に使わないことと、保存されないこと、人が確認しないこと、国内に置かれることは別の項目です。4つを分けて確認します。

**Q3** 正解 イ

この設定をオフにしても保存済みのチャットは削除されません。一時チャットも、安全上の理由から最大30日間保持される場合があります。

**Q4** 正解 ウ

最初に入力を止め、画面の写し・日時・サービス名・入れた情報を控えてから、決めておいた窓口へ報告します。削除は、管理者が書き出して保全してから行います。

**Q5** 正解 ア

外見や声では本人かどうかを見分けられない前提で、別の手段でかけ直す手順を決めておきます。「緊急」「秘密に」と添えられた依頼ほど飛ばしません。

**Q6** 正解 イ

施行規則第8条の定めです。速報は、知った後速やかに（目安は個別の事案によるものの概ね3～5日以内）行います。報告の要否は専門家と確かめます。

## 確認テストの結果とサービスの一覧を手元に、相談の形を選びます

「いいえ」の問いのうち最初に戻る章を1つ決めたら、読者の状態に合う相談の形を選びます。

全部を同時に整えようとせず、分類表を使ってよいサービスの一覧から始めることをおすすめします。この資料の道具は製品に依らず自社で使えますが、分類表の条件を自社の業務に当てはめる、使ってよいサービスを選ぶ、従業員に浸透させる、社内で作ったAIの仕組みを第三者の目で見ると、いう場面では、相談が近道になることがあります。

表14 確認テストの結果と、相談の中身

| 読者の状態                               | 相談の中身                         | サービス         |
|-------------------------------------|-------------------------------|--------------|
| ルールと使ってよいサービスの一覧がまだ無い               | 分類表・ルール・サービス選定を、自社の業務に合わせて決める | AI顧問         |
| ルールはあるが従業員に浸透していない                  | 自社の業務とルールを題材にした研修             | 生成AI研修       |
| 社内でAIの仕組み（API・RAG・エージェント・自動化）を作っている | 権限・データ・外部連携の第三者レビューと本番化の前の審査  | AI開発セキュリティ顧問 |

相談の前に、確認テストの「いいえ」が付いた問いの一覧、使っているサービスとプランの一覧（個人のアカウントで使っているものも含む）、判定に迷っている情報の区分の3つを手元に用意してください。

### ▶ 自社の線引きとサービスの選び方を、一緒に決めます

無料相談では、まず貴社の状況をお伺いし、そのうえで貴社の課題に当てはめて、どう解決していくかをご提案します。オンラインで最大45分です。お申し込みは下のボタンからできます。

無料相談を予約する



## 参考文献と出典

原典に日付の記載が無いページは「日付の記載なし」とし、閲覧した日だけを示します。各社のサービスの仕様と料金は2026年10月7日時点のもので、契約前に最新の公式資料で確かめてください。

- 
- 1** 総務省 「AI事業者ガイドライン」掲載ページ（AIネットワーク社会推進会議）  
版 第1.2版 公開 2026年3月31日 閲覧 2026年10月7日 関連する章 入力情報の分類  
[https://www.soumu.go.jp/main\\_sosiki/kenkyu/ai\\_network/02ryutsu20\\_04000019.html](https://www.soumu.go.jp/main_sosiki/kenkyu/ai_network/02ryutsu20_04000019.html)

---

  - 2** 総務省・経済産業省 AI事業者ガイドライン（第1.2版）本編  
版 第1.2版 公開 2026年3月31日 閲覧 2026年10月7日 関連する章 入力情報の分類、出力の確認  
[https://www.soumu.go.jp/main\\_content/001064279.pdf](https://www.soumu.go.jp/main_content/001064279.pdf)

---

  - 3** IPA（独立行政法人情報処理推進機構） 中小企業の情報セキュリティ対策ガイドライン（公開ページ）  
版 第4.0版 公開 2026年3月27日 更新 2026年9月30日 閲覧 2026年10月7日  
関連する章 サービスと契約の確認  
<https://www.ipa.go.jp/security/guide/sme/about.html>

---

  - 4** IPA 中小企業の情報セキュリティ対策ガイドライン 第4.0版（本編）  
版 第4.0版 公開 2026年3月27日 閲覧 2026年10月7日 関連する章 入力情報の分類、出力の確認  
[https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/sme\\_guideline\\_v4.0.pdf](https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/sme_guideline_v4.0.pdf)

---

  - 5** IPA 情報セキュリティ10大脅威 2026  
版 2026 公開 2026年1月29日 更新 2026年5月21日 閲覧 2026年10月7日 関連する章 起きる事故  
<https://www.ipa.go.jp/security/10threats/10threats2026.html>

---

  - 6** IPA 「情報セキュリティ10大脅威 2026」解説書〔組織編〕  
版 2026年3月 公開 2026年3月 閲覧 2026年10月7日 関連する章 起きる事故、会社全体の管理  
[https://www.ipa.go.jp/security/10threats/omgdg50000008fi8-att/kaisetsu\\_2026\\_soshiki.pdf](https://www.ipa.go.jp/security/10threats/omgdg50000008fi8-att/kaisetsu_2026_soshiki.pdf)

---

  - 7** IPA 産業サイバーセキュリティセンター 中核人材育成プログラム 9期生 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  
版 第1版（受講生の修了成果物・IPAの意見を代表しないと明記） 公開 2026年7月31日 閲覧 2026年10月7日  
関連する章 起きる事故、入力情報の分類  
[https://www.ipa.go.jp/jinzai/ics/core\\_human\\_resource/final\\_project/2026/rcu1hd0000018kkn-att/rcu1hd0000019kwj.pdf](https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2026/rcu1hd0000018kkn-att/rcu1hd0000019kwj.pdf)
-

- 
- 8** IPA セキュリティセンター AI利用者のためのセキュリティ豆知識  
版 2026年4月公開 公開 2026年4月2日 閲覧 2026年10月7日  
関連する章 情報の種類と確認、アカウントとログ  
[https://www.ipa.go.jp/digital/ai/security/ai\\_security\\_tips.html](https://www.ipa.go.jp/digital/ai/security/ai_security_tips.html)
- 
- 9** IPA セキュリティセンター AIセキュリティ短信  
版 2026年9月号 公開 2026年9月28日 閲覧 2026年10月7日 関連する章 管理者の点検表  
<https://www.ipa.go.jp/digital/ai/security/ai-security-bulletin.html>
- 
- 10** 個人情報保護委員会 生成AIサービスの利用に関する注意喚起等（別添1）  
版 令和5年6月2日 公開 2023年6月2日 閲覧 2026年10月7日 関連する章 情報の種類と確認  
[https://www.ppc.go.jp/files/pdf/230602\\_alert\\_generative\\_AI\\_service.pdf](https://www.ppc.go.jp/files/pdf/230602_alert_generative_AI_service.pdf)
- 
- 11** e-Gov法令検索（デジタル庁） 個人情報の保護に関する法律（平成15年法律第57号）第25条～第28条  
施行 2026年10月1日 閲覧 2026年10月7日 関連する章 情報の種類と確認、外部連携と委託  
<https://laws.e-gov.go.jp/law/415AC0000000057>
- 
- 12** e-Gov法令検索（デジタル庁） 個人情報の保護に関する法律施行規則 第7条～第10条  
施行 2026年6月14日 閲覧 2026年10月7日 関連する章 誤入力の初動  
<https://laws.e-gov.go.jp/law/428M60020000003>
- 
- 13** 個人情報保護委員会 個人情報の保護に関する法律についてのガイドライン（通則編）  
版 平成28年11月（令和8年6月一部改正） 改訂 2026年6月 閲覧 2026年10月7日 関連する章 誤入力の初動  
[https://www.ppc.go.jp/personalinfo/legal/guidelines\\_tsusoku/](https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/)
- 
- 14** 個人情報保護委員会 「個人情報の保護に関する法律についてのガイドライン」に関するQ&A  
版 令和7年7月1日更新 更新 2025年7月1日 閲覧 2026年10月7日 関連する章 情報の種類と確認  
[https://www.ppc.go.jp/personalinfo/faq/APPI\\_QA/](https://www.ppc.go.jp/personalinfo/faq/APPI_QA/)
- 
- 15** 個人情報保護委員会 令和8年 改正個人情報保護法について  
公布 2026年7月17日 閲覧 2026年10月7日 関連する章 誤入力の初動  
<https://www.ppc.go.jp/personalinfo/legal/r8kaiseihogohou>
- 
- 16** 個人情報保護委員会 個人情報保護法等の一部を改正する法律について（概要）  
版 2026年7月 公開 2026年7月17日 閲覧 2026年10月7日 関連する章 誤入力の初動  
[https://www.ppc.go.jp/files/pdf/260717\\_kaiseihounitsuite.pdf](https://www.ppc.go.jp/files/pdf/260717_kaiseihounitsuite.pdf)
-

---

**17 経済産業省 営業秘密管理指針**

版 最終改訂 令和7年3月31日 改訂 2025年3月31日 閲覧 2026年10月7日 関連する章 情報の種類と確認  
<https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/r7ts.pdf>

---

**18 文化庁（文化審議会著作権分科会法制度小委員会） AIと著作権に関する考え方について**

版 令和6年3月15日 公開 2024年3月15日 閲覧 2026年10月7日 関連する章 情報の種類と確認、出力の確認  
[https://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/pdf/94037901\\_01.pdf](https://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/pdf/94037901_01.pdf)

---

**19 文化庁著作権課 AIと著作権に関するチェックリスト&ガイダンス**

版 令和6年7月31日 公開 2024年7月31日 閲覧 2026年10月7日 関連する章 情報の種類と確認、出力の確認  
[https://www.bunka.go.jp/seisaku/chosakuken/pdf/94097701\\_01.pdf](https://www.bunka.go.jp/seisaku/chosakuken/pdf/94097701_01.pdf)

---

**20 デジタル庁（デジタル社会推進会議幹事会決定） 行政の進化と革新のための生成AIの調達・利活用に係るガイドライン**

版 2026年6月12日改定（初版 2025年5月27日） 公開 2025年5月27日 改訂 2026年6月12日  
閲覧 2026年10月7日 関連する章 サービスと契約の確認  
[https://www.digital.go.jp/assets/contents/node/information/field\\_ref\\_resources/dec64eb-f26e-41cb-8d37-f3dd173108b8/59054b35/20260612\\_resources\\_standard\\_guidelines\\_guideline\\_01.pdf](https://www.digital.go.jp/assets/contents/node/information/field_ref_resources/dec64eb-f26e-41cb-8d37-f3dd173108b8/59054b35/20260612_resources_standard_guidelines_guideline_01.pdf)

---

**21 内閣官房国家サイバー統括室ほか関係省庁 AI性能の高度化を踏まえたサイバーセキュリティ対策の強化について**

公開 2026年5月18日 閲覧 2026年10月7日 関連する章 事故の経路  
[https://www.cyber.go.jp/pdf/press/20260518\\_AI\\_CS\\_Package.pdf](https://www.cyber.go.jp/pdf/press/20260518_AI_CS_Package.pdf)

---

**22 JPCERT/CC インシデント対応とは**

更新 2026年6月30日 閲覧 2026年10月7日 関連する章 誤入力 of 初動  
<https://www.jpcert.or.jp/ir/>

---

**23 JPCERT/CC Weekly Report 2026-09-30号**

版 JPCERT-WR-2026-0930 公開 2026年9月30日 閲覧 2026年10月7日 関連する章 外部連携と委託  
<https://www.jpcert.or.jp/wr/2026/wr260930.html>

---

**24 警察庁 法人を対象とした詐欺（ニセ社長詐欺）に注意！**

公開 2026年2月13日 閲覧 2026年10月7日 関連する章 出力の確認  
<https://www.npa.go.jp/bureau/safetylife/sos47/new-topics/260213/01.html>

---

**25 OpenAI OpenAI におけるエンタープライズプライバシー**

更新 2026年1月8日 閲覧 2026年10月7日 関連する章 学習・保存・所在、アカウントとログ  
<https://openai.com/ja-JP/enterprise-privacy/>

---

---

**26** OpenAI モデルのパフォーマンスを向上させるためのデータの使用方法

更新 2026年3月13日 閲覧 2026年10月7日 関連する章 サービスと契約の確認、個人で使う基準

<https://openai.com/ja-JP/policies/how-your-data-is-used-to-improve-model-performance/>

---

**27** OpenAI ChatGPT のデータ管理 (OpenAI Help Center)

更新 2026年9月 閲覧 2026年10月7日 関連する章 学習・保存・所在、個人で使う基準

<https://help.openai.com/ja-jp/articles/7730893-data-controls-in-chatgpt>

---

**28** OpenAI Data controls in the OpenAI platform (開発者向け文書)

日付の記載なし 閲覧 2026年10月7日 関連する章 学習・保存・所在

<https://developers.openai.com/api/docs/guides/your-data>

---

**29** Anthropic Is my data used for model training? (Consumers)

更新 2026年3月16日 閲覧 2026年10月7日 関連する章 学習・保存・所在

<https://privacy.claude.com/en/articles/10023580-is-my-data-used-for-model-training>

---

**30** Anthropic Is my data used for model training? (Commercial Customers)

更新 2026年8月18日 閲覧 2026年10月7日 関連する章 学習・保存・所在

<https://privacy.claude.com/en/articles/7996868-is-my-data-used-for-model-training>

---

**31** Anthropic How long do you store my organization's data?

更新 2026年7月1日 閲覧 2026年10月7日 関連する章 学習・保存・所在

<https://privacy.claude.com/en/articles/7996866-how-long-do-you-store-my-organization-s-data>

---

**32** Anthropic How long do you store my data? (Consumers)

更新 2026年7月1日 閲覧 2026年10月7日 関連する章 学習・保存・所在

<https://privacy.claude.com/en/articles/10023548-how-long-do-you-store-my-data>

---

**33** Anthropic Where are your servers located? (Anthropic Privacy Center)

更新 2026年6月15日 閲覧 2026年10月7日 関連する章 学習・保存・所在

<https://privacy.claude.com/en/articles/7996890-where-are-your-servers-located-do-you-host-your-models-on-e-u-servers>

---

**34** Anthropic Set up single sign-on (SSO) (Claude Help Center)

更新 2026年9月2日 閲覧 2026年10月7日 関連する章 アカウントとログ

<https://support.claude.com/en/articles/13132885-set-up-single-sign-on-sso>

---

---

**35** Anthropic Access audit logs (Claude Help Center)

更新 2026年6月15日 閲覧 2026年10月7日 関連する章 アカウントとログ

<https://support.claude.com/en/articles/9970975-access-audit-logs>

---

**36** Google Gemini アプリのプライバシー ハブ

更新 2026年9月24日 閲覧 2026年10月7日 関連する章 学習・保存・所在、個人で使う基準

<https://support.google.com/gemini/answer/13594961?hl=ja>

---

**37** Google Google Workspace の生成 AI に関するプライバシー ハブ

更新 2026年10月6日 閲覧 2026年10月7日 関連する章 学習・保存・所在

<https://knowledge.workspace.google.com/admin/gemini/generative-ai-in-google-workspace-privacy-hub>

---

**38** Microsoft Data, Privacy, and Security for Microsoft Copilot

更新 2026年9月30日 閲覧 2026年10月7日 関連する章 サービスと契約の確認、学習・保存・所在

<https://learn.microsoft.com/en-us/microsoft-365/copilot/microsoft-365-copilot-privacy>

---

**39** Microsoft Copilot および AI アプリケーションの監査ログ (Microsoft Purview)

更新 2026年8月27日 閲覧 2026年10月7日 関連する章 アカウントとログ

<https://learn.microsoft.com/ja-jp/purview/audit-copilot>

---

**40** Microsoft 個人向け Microsoft Copilot: アクティビティの履歴

日付の記載なし 閲覧 2026年10月7日 関連する章 学習・保存・所在、個人で使う基準

<https://support.microsoft.com/ja-jp/privacy/microsoft-copilot/activity-history>

---

**41** Microsoft Microsoft Copilot のプライバシーに関する FAQ (旧版アプリ向け)

日付の記載なし 閲覧 2026年10月7日 関連する章 学習・保存・所在、個人で使う基準

<https://support.microsoft.com/ja-jp/topic/privacy-faq-for-microsoft-copilot-27b3a435-8dc9-4b55-9a4b-58eeb9647a7f>

---

**42** OpenAI ChatGPT の料金

日付の記載なし 閲覧 2026年10月7日 関連する章 学習・保存・所在

<https://chatgpt.com/ja-JP/pricing/>

---

**43** OpenAI Deleting and archiving chats in ChatGPT (OpenAI Help Center)

日付の記載なし 閲覧 2026年10月7日 関連する章 学習・保存・所在

<https://help.openai.com/en/articles/8809935-deleting-and-archiving-chats-in-chatgpt>

---

---

**44** OpenAI Data residency and inference residency for ChatGPT

日付の記載なし 閲覧 2026年10月7日 関連する章 学習・保存・所在

<https://help.openai.com/en/articles/9903489-data-residency-and-inference-residency-for-chatgpt>

---

**45** OpenAI Managing multi-factor authentication (MFA)

日付の記載なし 閲覧 2026年10月7日 関連する章 学習・保存・所在、アカウントとログ

<https://help.openai.com/en/articles/7967234-managing-multi-factor-authentication-mfa>

---

**46** Anthropic プランと料金 (Claude)

日付の記載なし 閲覧 2026年10月7日 関連する章 学習・保存・所在

<https://claude.com/ja/pricing>

---

**47** Anthropic Access the Compliance API (Claude Help Center)

日付の記載なし 閲覧 2026年10月7日 関連する章 学習・保存・所在

<https://support.claude.com/en/articles/15167101>

---

**48** Google Google AI のプラン (Gemini)

日付の記載なし 閲覧 2026年10月7日 関連する章 学習・保存・所在

<https://gemini.google/jp/subscriptions/?hl=ja>

---

**49** Google Google Workspace の料金

日付の記載なし 閲覧 2026年10月7日 関連する章 学習・保存・所在

<https://workspace.google.com/intl/ja/pricing.html>

---

**50** Google データ リージョンの対象となるデータ (Google Workspace)

日付の記載なし 閲覧 2026年10月7日 関連する章 学習・保存・所在

<https://knowledge.workspace.google.com/admin/compliance/data-covered-by-data-regions>

---

**51** Google SSO について (Google Workspace)

更新 2026年10月7日 閲覧 2026年10月7日 関連する章 学習・保存・所在

<https://knowledge.workspace.google.com/admin/apps/about-ssso>

---

**52** Google 2段階認証プロセスを導入する (Google Workspace)

更新 2026年9月3日 閲覧 2026年10月7日 関連する章 学習・保存・所在

<https://knowledge.workspace.google.com/admin/security/deploy-2-step-verification>

---

---

**53** Google Gemini API 追加利用規約

日付の記載なし 閲覧 2026年10月7日 関連する章 学習・保存・所在

<https://ai.google.dev/gemini-api/terms>

---

**54** Google Gemini API の不正使用のモニタリング

日付の記載なし 閲覧 2026年10月7日 関連する章 学習・保存・所在

<https://ai.google.dev/gemini-api/docs/usage-policies>

---

**55** Microsoft Microsoft 365 のプランと価格の比較

日付の記載なし 閲覧 2026年10月7日 関連する章 学習・保存・所在

<https://www.microsoft.com/ja-jp/microsoft-365/buy/compare-all-microsoft-365-products>

---

**56** Microsoft Microsoft 365 Copilot（エンタープライズ）の価格

日付の記載なし 閲覧 2026年10月7日 関連する章 学習・保存・所在

<https://www.microsoft.com/ja-jp/microsoft-365-copilot/enterprise>

---

**57** Microsoft Microsoft 365 Copilot Business の価格

日付の記載なし 閲覧 2026年10月7日 関連する章 学習・保存・所在

<https://www.microsoft.com/ja-jp/microsoft-365-copilot/business>

---

**58** Microsoft Data Residency for Microsoft 365 Copilot Offerings

更新 2026年9月3日 閲覧 2026年10月7日 関連する章 学習・保存・所在

<https://learn.microsoft.com/en-us/microsoft-365/enterprise/m365-dr-service-copilot-offerings>

---

**59** Microsoft Apply Zero Trust principles to Microsoft Copilot

更新 2026年9月11日 閲覧 2026年10月7日 関連する章 学習・保存・所在

<https://learn.microsoft.com/en-us/security/zero-trust/copilots/zero-trust-microsoft-365-copilot>

---

# 発行情報



|             |                                                                                                               |
|-------------|---------------------------------------------------------------------------------------------------------------|
| 発行元         | 株式会社BoostX                                                                                                    |
| 所在地         | 〒812-0011 福岡県福岡市博多区博多駅前二丁目17-1 博多プレステージ<br>本館1F・2F                                                            |
| Web         | <a href="https://boostx-inc.com">boostx-inc.com</a>                                                           |
| 執筆・監修       | 株式会社BoostX（監修 吉元大輝・代表取締役社長）                                                                                   |
| 版番号         | 第1.0版                                                                                                         |
| 発行日         | 2026年10月6日                                                                                                    |
| 最終確認日       | 2026年10月7日                                                                                                    |
| 適用範囲        | 特定の業界に依らず、生成AIを業務で使う会社の、入力の線引き・サービスと契約の確認・アカウントと権限・外部連携・従業員向けのルール・誤入力時の初動に適用します。個別の事案の法的な判断には適用しません。          |
| この資料の扱い     | 社内での共有と、表・ひな形の自社用への書き換えは自由です。社外へ配るときは、発行元へご連絡ください。各社のサービスの仕様と料金は2026年10月7日時点の公式資料によるもので、契約前に最新の公式資料で確かめてください。 |
| 更新方針        | 法令・公的な指針・各社の規約が変わったときと、半年ごとに見直します。改正個人情報保護法の施行時には、報告と通知の扱いを見直します。誤りや更新情報は、下の連絡先までお知らせください。                    |
| 誤りや更新情報の連絡先 | 株式会社BoostX お問い合わせフォーム（ <a href="https://boostx-inc.com/contact/">boostx-inc.com/contact/</a> ）                |