生成AIパスポート 対策テキスト

第4章 情報リテラシー ①身を守る

だます手口と、個人情報のルール。技術の話はほとんど出てこない章。

インターネットリテラシー／だます手口（道とやり口）／悪いソフトと備え

個人情報保護法の骨組み／何が個人情報なのか／加工して使う／生成AIに入れない

重要用語 25語・確認問題 9問・図解 8点

04

AI資格ラボ

YouTubeチャンネル登録者への配布テキストです。

動画「【生成AIパスポート】第4章 情報リテラシー ①身を守る」と対応しています。

はじめに この本の使い方

この本は、YouTubeチャンネル「AI資格ラボ」の動画「**第4章 情報リテラシー ①身を守る**」に対応した、配布用のテキストです。動画を見ていない方でも、これ一冊で第4章の前半が最後まで読み切れるように書いてあります。

この本が扱う範囲

生成AIパスポートの第4章は、公式シラバス（出題範囲表）で**65語**あります。第1章の39語、第2章の62語、第3章の20語とくらべて**全5章でいちばん多い章**です。1回で扱うには多すぎるので、第2章と同じように**2冊に分けました**。

	扱う範囲	語数
①	自分の身を守る（この本）	25語
②	作ったものの権利と社会のルール（次の本）	40語

この本は**①の25語**を扱います。ネットで何が起きるのか、どうだまされるのか、個人情報はどう守られているのか。**全部、自分の身を守る話**です。

⇨ **この章は、技術の話がほとんど出てきません。**第1章から第3章までは、ニューロンや Transformer や RAG といった**中身**の話でした。第4章で出てくるのは**法律と、手口の名前と、ルール**です。頭の使い方が変わります。

この章の、いちばんしんどい所

先に正直に言います。この本の山は**だます手口の名前**です。フィッシング、スミッシング、ヴィッシング、スピアフィッシング、ベイト、ブラックメール、プレテキスト。**11語がほぼ全部カタカナ**で並びます。

名前だけを並べて覚えようとすると、まず残りません。そこでこの本では、**名前を先に出しません。何が起きるのかを先に書いて、そのあとに名前を付けます**。そのほうが残ります。

この本の構成

- **本文**……ふつうに読める文章です。まずここを読んでください。
- **試験ポイント**（青い枠）……そのまま問題になる所です。試験直前はここだけ拾い読みできます。
- ⚠**マークの枠**（赤い枠）……**間違えやすい所・引っかけが仕込まれる所**です。
- **用語**（紫の帯）……シラバスに名前が載っている用語です。この本で25語あります。
- **確認問題**（緑の枠）……テーマの区切りに3問ずつ、合計9問あります。
- **巻末**……25語のチェックリストと、用語集を付けました。

進め方

1. まず**本文を最後まで通しで読む**。分からない所で止まらず、飛ばして進んでかまいません。
2. 次に**確認問題9問**を、本文を見ずに解く。ここで落ちた所が、あなたの弱点です。
3. 落ちた所だけ本文に戻り、**自分の言葉で言い直す**。読むより言い直したほうが残ります。
4. 試験直前は、**試験ポイントの枠と、巻末の用語集だけ**を見返す。

動画と合わせて使う

- この本は、YouTubeチャンネル**AI資格ラボ**の動画 **第4章 情報リテラシー ①身を守る** と同じ順番・同じ図で作ってあります。
- **動画で流れをつかみ、この本で確かめる**。あるいは**この本を先に読んでから動画を見る**。どちらでも構いません。
- 印刷は**A4・実物大（100%）**で。図の中の文字まで読める大きさで作ってあります。

第4章① この本の全体像

25語を、**3つのかたまり**に分けて進みます。かたまりごとに確認問題が3問ずつ入ります。

	テーマ	語数
1	インターネットリテラシー	5語
2	セキュリティとプライバシー（だます手口・悪いソフト）	11語
3	個人情報保護の観点	9語

1つ目は言葉の定義だけです。5語しかなく、すぐ終わります。**2つ目が山**で、11語が全部カタカナ。**3つ目**は法律の言葉が並びます。

3つのかたまりの関係

ばらばらに見えますが、**順番につながっています**。

1. まず**何ができれば身を守れるのか**という枠組みを置く（4-1）。
2. 次に**実際にどう攻められるのか**を見る（4-2〜4-4）。攻める側を知らないと守れません。
3. 最後に**法律が何を守っているのか**を見る（4-5〜4-8）。個人情報という、いちばん狙われるものの話です。

手口の話と法律の話は、別々の暗記ではありません。盗まれると困るものがあるから法律があり、その盗み方が4-2〜4-4だ、という順で読んでください。

⇒ この本には**親子の形**が3回出てきます。①インターネットリテラシーとその中身4つ ②ソーシャルエンジニアリング攻撃とその手口4つ ③マルウェアとその一種。**親を先に置いて、子どもをぶら下げる**。この形で覚えると崩れません。

4-1 インターネットリテラシーとは

まず**インターネットリテラシー**。意味は、**インターネットを適切に使うために必要な力**です。それだけです。ひねりはありません。

> **インターネットリテラシー** Internet Literacy
> インターネットを適切に利用するために必要な力。この本の**親になる言葉**で、次に出る4つはすべてこの中身。

シラバスは、この力の中身を**4つ**に分けています。ここが5語のうちの残り4語です。

図4-1　インターネットリテラシーが親。中身が4つ

1つ目　テクノロジーの理解

仕組みを知っていることです。なぜ必要か。**知らないものは、疑えない**からです。仕組みが分かっていないと、おかしなことが起きても気づけません。

> **テクノロジーの理解**
> インターネットや情報technologyの**仕組みを知っていること**。知らないものは疑えないため、身を守る土台になる。

2つ目　情報リテラシー

情報を見極める力です。その情報は本当か。誰が言っているのか。**確かめる力**のことです。

> **情報リテラシー**
> 情報を**見極める力**。その情報は本当か、誰が発信しているのかを確かめられること。

3つ目　セキュリティとプライバシー

身を守る力です。この本ではこのあと、テーマを丸ごと1つ使って扱います。11語ぶんあります。

セキュリティとプライバシー
身を守る力。攻撃の手口を知り、設定で自分の情報を守れること。第4章①の**山になるテーマ**。

4つ目　デジタル市民権

聞き慣れない言葉だと思います。**ネット上でも、ひとりの市民として振る舞う**という考え方です。権利があり、責任もある。**匿名だから何をしてもいい、の反対**です。

デジタル市民権 Digital Citizenship
ネット上でも**ひとりの市民として振る舞う**という考え方。権利と責任がともにあるとする立場で、匿名性を理由に無責任に振る舞うことを否定する。

なぜ、この章の先頭にこれが来るのか

4つを並べると、**順番に意味がある**ことが見えてきます。仕組みを知り（テクノロジーの理解）、情報を見極め（情報リテラシー）、身を守り（セキュリティとプライバシー）、そのうえで**どう振る舞うか**を決める（デジタル市民権）。

この本の残りは、**3つ目のセキュリティとプライバシー**を丸ごと開いたものです。11語あります。そして個人情報の話が9語。つまり**4-1で出た4つのうち、1つを深く掘るのが第4章①**だと思ってください。

試験ポイント｜5語は「親と子」で出る

- **インターネットリテラシーが親**。テクノロジーの理解・情報リテラシー・セキュリティとプライバシー・デジタル市民権の**4つが子ども**。
- **情報リテラシー**と**インターネットリテラシー**を取り違えないこと。情報リテラシーは**4つのうちの1つ**で、親ではありません。
- **デジタル市民権**は名前が難しいだけで、中身は**ネットでも市民として振る舞う**。それだけです。

4-2 だます手口①　どの道で来るか

ここから手口です。まず、**何が起きるのか**から書きます。名前はそのあとです。

起きること

メールが来ます。**銀行です。口座が停止されました。こちらから手続きを**——リンクを踏むと、**本物そっくりの偽サイト**が開きます。IDとパスワードを入れると、そのまま盗まれる。

これが**フィッシング詐欺**です。偽物のメールやサイトで、個人情報を**釣り上げる**。

> **フィッシング詐欺** Phishing
> 偽物の**メールやWebサイト**で本物を装い、ID・パスワード・カード番号などの個人情報を入力させて盗む詐欺。

同じことを、別の道で

やっていることは同じで、**来る道だけが違う**手口が2つあります。ここが名前を覚える勘所です。

ショートメッセージ（SMS）で来たら——スミッシングです。**SMSとフィッシングを足した言葉**。宅配便の不在通知を装うものが、いちばん多い形です。

> **スミッシング** SMiShing
> **SMS（ショートメッセージ）**を使ったフィッシング。SMS＋Phishing の合成語。宅配便の不在通知を装う手口が代表例。

電話で来たら——ヴィッシング。**voice、つまり声のフィッシング**です。カード会社を名乗る電話がかかってきて、暗証番号を聞き出す。

> **ヴィッシング** Vishing
> **音声通話**を使ったフィッシング。Voice＋Phishing の合成語。電話で本人に喋らせて聞き出す。

図4-2　やることは同じ。違うのは来る道だけ

道はメール・SMS・電話だけではない

シラバスには、**キーワードは付いていないが学習項目として挙がっている**入口が3つあります。名前を答えさせる問題にはなりにくいものの、**どういう危険があるかは問われます**。

紙から来る　悪意のあるQRコード

QRコードは**人間の目では中身が読めません**。だからリンク先を確かめられない、という弱点があります。掲示物や請求書に貼られた正規のQRコードの上に、**偽のQRコードを重ねて貼る**手口が実際に起きています。

対策は単純で、**読み取ったあとに表示されるURLを見る**こと。そして**シールが二重に貼られていないか**を確かめることです。

回線から来る　Wi-Fiに潜む罠

暗号化されていない公衆Wi-Fiでは、**通信の中身が第三者に読まれるおそれ**があります。さらに、店舗名に似せた**偽のアクセスポイント**を立てて接続させ、そこを通る情報を抜く手口もあります。

対策は、**提供元がはっきりしない電波につながない**こと。つなぐ場合も、**ID・パスワードやカード番号を入力しない**ことです。

ファイル置き場から来る　アップロードサービスに潜む詐欺

ファイル共有サービスを装ったメールで、**ファイルを見るにはログインを**と偽のログイン画面へ誘う手口です。**中身はフィッシング詐欺と同じ**ですが、業務で日常的に使うサービスの見た目をしているぶん、警戒が緩みます。

対策は、**メールのリンクからログインしない**こと。いつも使っているブックマークや公式アプリから入り直せば、偽の画面に情報を入れずに済みます。

試験ポイント｜道で覚える

- **メールならフィッシング詐欺。SMSならスミッシング。電話ならヴィッシング。**
- 3つとも**やっていることは同じ**で、違うのは**来る道**だけ。ここを一度つかむと、二度と混ざりません。
- **スミッシング＝SMS＋Phishing**、**ヴィッシング＝Voice＋Phishing**。語源で聞かれることがあります。

4-3 だます手口②　何につけこむか

さきほどの3つは**道**の違いでした。ここからは**やり口**の違いです。まず親になる言葉から置きます。

親　ソーシャルエンジニアリング攻撃

長い名前ですが、意味は単純です。**技術ではなく、人間の心理につけこんで情報を盗む**こと。パスワードを解析するのではなく、**本人に喋らせる**。

> **ソーシャルエンジニアリング攻撃** Social Engineering
> 技術的な解析ではなく、**人間の心理や行動につけこんで**情報を盗む攻撃の**総称**。以下の4つはすべてこの中に入る。

ここが**親**です。これから出る4つは、全部この子どもです。

図4-3　親はひとつ。何につけこむかで4つに分かれる

1つ目　スピアフィッシング

スピアは、槍。ばらまくのではなく、**特定の相手を狙い撃ち**します。**経理部の○○さん**と名指しで、社内の事情を混ぜて送ってくる。**引っかかりやすさが桁違い**です。

> **スピアフィッシング** Spear Phishing
> **特定の個人や組織を狙い撃ち**にするフィッシング。spear＝槍。相手の所属や事情を調べたうえで送るため、通常のフィッシングより信じやすい。

2つ目　ベイト攻撃

ベイトは、えさ。無料でもらえます、限定公開の動画です——**欲しがる気持ちを、えさにする**手口です。USBメモリをわざと落としておく、という古典的な手口もこれにあたります。

ベイト攻撃 Baiting

えさで相手を釣る攻撃。bait＝えさ。無料・限定といった**欲を刺激する誘い**で、リンクを踏ませたり機器を使わせたりする。

3つ目　ブラックメール

黒いメール、ではありません。**脅迫**のことです。**あなたの秘密を握った。ばらされたくなければ払え**——**弱みにつけこむ**手口です。

ブラックメール Blackmail

脅迫。弱みを握ったと告げて金銭や情報を要求する。⚠ **黒いメールという意味ではない**（blackmail＝ゆすり）。

4つ目　プレテキスト

作り話、という意味です。**システム部の者ですが、確認のためパスワードを**——**役になりきって、信じ込ませてから聞き出す**。

プレテキスト Pretexting

作り話（口実）で身分をいつわり、信用させてから情報を聞き出す手口。上司・取引先・システム管理者などになりきる。

手口を知ったうえで、自分の設定を見る

手口の名前と並んで、シラバスには**守りの側の学習項目**も挙がっています。ここも名前を問う問題にはなりにくいものの、**考え方は問われます**。

プライバシー設定

SNSやスマートフォンの**公開範囲**の設定です。誰に見せるのか、位置情報を付けるのか、過去の投稿はどうするのか。**初期設定のまま使うと、意図せず全体公開になっていることがあります。**

4-3で見たスピアフィッシングは、**相手の所属や事情を調べたうえで**送られてきます。その材料は、たいてい**公開されたままの情報**から集められます。設定を見直すことが、そのまま手口への備えになります。

不適切なコンテンツへのWebアクセス

業務用の端末や、子どもが使う端末で、**見せたくないサイトに行かせない**という考え方です。**フィルタリング**と呼ばれる仕組みで、あらかじめ分類されたカテゴリごとに遮断します。

生成AIの技術的発展に潜む脅威

この章が生成AIパスポートに載っている理由のひとつです。生成AIが使えるようになったことで、**だます側の道具も良くなりました**。

- **文面が自然になった**——以前のフィッシングメールは日本語が不自然で見分けられました。いまは**その手がかりが消えつつあります**。
- **声や映像をまねられる**——本人そっくりの音声で電話をかけ、送金を指示する事件が起きています。ヴィッシングの精度が上がった形です。
- **下調べが速くなった**——公開情報を集めて相手に合わせた文面を作る作業が、短時間でできるようになりました。スピアフィッシングと相性が悪い変化です。

手口そのものは、これまでと同じです。変わったのは**質と量**だけ。だからこそ、名前と形で覚えておく意味があります。

試験ポイント｜何につけこむかで分かれる

- **親**がソーシャルエンジニアリング攻撃。**狙い撃ち**がスピアフィッシング、**えさ**がベイト攻撃、**脅し**がブラックメール、**作り話**がプレテキスト。
- **ブラックメール**を「黒いメール」と読まないこと。**脅迫**です。ここは引っかけになります。
- **4-2は道の違い、4-3はやり口の違い**。この2本の軸で整理すると、7語がきれいに並びます。

確認問題① だます手口

確認問題①

第1問　SMSで送られてくる偽メッセージの詐欺を何といいますか。電話の場合、メールの場合はどうですか。

答

スミッシング。電話なら**ヴィッシング**、メールなら**フィッシング詐欺**。

3つとも中身は同じで、違うのは来る道だけです。

確認問題①

第2問　技術ではなく、人の心理につけこんで情報を盗む攻撃の総称を何といいますか。

答

ソーシャルエンジニアリング攻撃。

これが親で、スピアフィッシング・ベイト攻撃・ブラックメール・プレテキストが子どもです。

確認問題①

第3問　特定の相手を狙い撃ちするフィッシングは何ですか。えさで釣る手口は何ですか。

答

スピアフィッシングと**ベイト攻撃**。

スピアは槍、ベイトはえさ。語源で覚えると取り違えません。

4-4 悪いソフトと、その備え

手口の次は**もの**です。ここも親子の形が出てきます。

親　マルウェア

悪意のあるソフトウェアの総称です。**mal は「悪い」**という意味で、ソフトウェアと足してマルウェア。ウイルス、ワーム、トロイの木馬——**全部この中に入ります**。

> **マルウェア** Malware
> **悪意のあるソフトウェアの総称**。malicious（悪意のある）＋software。ウイルス・ワーム・トロイの木馬・ランサムウェアなどをすべて含む。

その中で、試験に出るのが1つ

ランサムウェア。**ランサムは、身代金**。ファイルを勝手に暗号化して開けなくし、**元に戻す代わりに金を要求する**。病院やインフラが止まる事件は、たいていこれです。

> **ランサムウェア** Ransomware
> ファイルを**暗号化して使えなくし**、復旧と引き換えに金銭を要求するマルウェア。ransom＝身代金。

⇒ ⚠ **払っても戻る保証はありません。**復旧できなかった例も、払ったうえで再び要求された例もあります。だから**備えのほうが大事**です。

備えの側の語

アンチウイルスソフトウェア。**マルウェアを見つけて、止めて、取り除くソフト**です。

> **アンチウイルスソフトウェア** Antivirus Software
> マルウェアを**検出・遮断・駆除**するソフトウェア。⚠ 名前は「アンチウイルス」だが、**ウイルスだけを見るわけではない**。

⇒ ⚠ 名前は**アンチウイルス**ですが、**ウイルスだけを相手にするわけではありません**。マルウェア全般が相手です。ここは地味に引っかけになります。

図4-4　マルウェアが親。ランサムウェアがその一種。備えがアンチウイルスソフトウェア

マルウェアの中身

マルウェアは総称なので、中に何が入っているかも押さえておくと、問題文の言い回しに強くなります。

	どう広がるか	特徴
ウイルス	他のファイルに寄生する	単独では動けず、宿主が要る
ワーム	自分で複製して広がる	宿主が要らず、勝手に増える
トロイの木馬	役に立つソフトを装う	入り込むまで悪さをしない
ランサムウェア	経路はさまざま	暗号化して身代金を要求する

名前を答えさせる問題として出るのはランサムウェアだけですが、選択肢に他が並ぶことはあります。

備えは、ソフトだけではない

アンチウイルスソフトウェアは**入口**の備えです。ランサムウェアに対しては、それだけでは足りません。

- **バックアップ**——暗号化されても、別に控えがあれば戻せます。**払わずに済む唯一の道**です。
- **更新**——古いままのソフトの穴から入られます。
- **怪しいファイルを開かない**——結局ここに戻ります。4-2と4-3で見た手口が入口になります。

ランサムウェアの被害は、こう進む

名前だけでは実感が湧きにくいので、起きることを順に書きます。

1. メールの添付や、古いままの機器の穴から**入り込む**。
2. 気づかれないうちに**社内へ広がる**。
3. ある朝いっせいに**ファイルが開かなくなる**。画面に要求の文面が出る。
4. **業務が止まる**。病院なら診療、工場なら生産、自治体なら窓口が止まります。

近年は**暗号化する前に中身を盗み出しておき、払わなければ公開すると迫る**やり方も増えました。バックアップがあっても、**公開されると困る**という別の圧力をかける形です。

⇨ ⚠️ 試験で問われるのは**定義**です。**ファイルを暗号化して、復旧と引き換えに金銭を要求する**——ここを一文で言えるようにしてください。

試験ポイント｜3語セットで出る

- **マルウェアが親。ランサムウェアがその一種。アンチウイルスソフトウェアが対策。**この3語はセットで問われます。
- **ランサム＝身代金**。暗号化して金を要求する、が定義。**払っても戻る保証はない**ことまで押さえます。
- **アンチウイルスソフトウェアはウイルス専用ではない**。マルウェア全般が対象です。

4-5 個人情報保護法の骨組み

ここからテーマが変わります。**個人情報**です。法律の言葉が並びますが、**誰が何をする立場なのか**で整理すると入ります。

法律の名前

個人情報保護法。個人情報を扱うときのルールを決めた法律です。

> **個人情報保護法**
> 個人情報の**取得・利用・保管・提供**のルールを定めた法律。正式名称は個人情報の保護に関する法律。

そして**改正個人情報保護法**という語も、別に載っています。**3年ごとに見直す**と決められていて、時代に合わせて何度も改正されているからです。

> **改正個人情報保護法**
> 改正を重ねている個人情報保護法を指す言い方。**3年ごとの見直し**が定められており、技術や社会の変化に合わせて内容が更新される。

⇒ ⚠ **改正◯年版の中身までは問われません。改正され続けている、という事実**を押さえてください。

誰が見張っているのか

個人情報保護委員会です。**国の機関**で、監督や指導をするところ。**委員会という名前ですが、国の組織**です。ここは覚えるだけです。

> **個人情報保護委員会**
> 個人情報保護法にもとづき、事業者を**監督・指導する国の機関**。⚠ 民間の団体ではない。

誰がルールを守る側か

個人情報取扱事業者。**個人情報をデータベースにして事業に使っている者**、という意味です。

> **個人情報取扱事業者**
> 個人情報を**データベース化して事業に使っている者**。法律上の義務を負う側。⚠ **規模の下限はない**。

⇒ ⚠ ここに**引っかけ**があります。**大企業だけでしょ**と思いますよね。**違います。**1件でも扱っていれば、個人事業主でも当てはまります。**規模の下限はありません。**

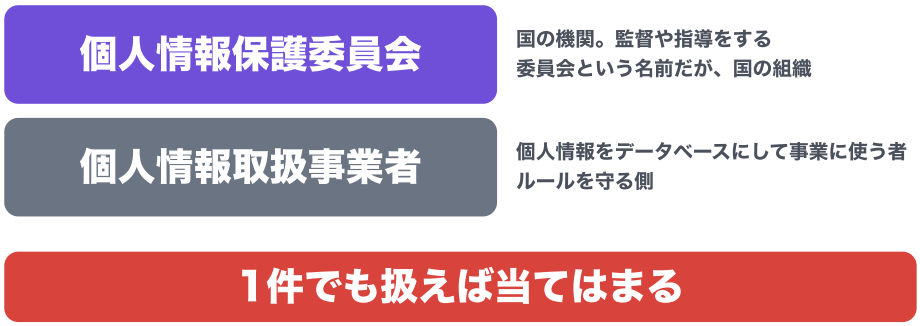

図4-5　見張る側が委員会。守る側が事業者

そもそも「個人情報」とは何か

法律は、個人情報を**2つの形**で定義しています。

1. **生存する個人に関する情報**であって、氏名や生年月日などにより**特定の個人を識別できるもの**。他の情報と**容易に照合できて**識別できるようになるものも含みます。
2. **個人識別符号が含まれるもの**。こちらは4-6で扱います。

⇒ ⚠ **生存する**という条件が付いています。また**容易に照合できれば含む**という書き方なので、**単体では誰か分からない情報でも、社内の名簿と突き合わせれば分かる場合は個人情報にあたります**。ここは考え方として問われます。

試験ポイント｜立場で覚える

- **見張るのが個人情報保護委員会（国の機関）、守るのが個人情報取扱事業者**。
- **個人情報取扱事業者に規模の下限はない**。**1件でも扱えば当てはまる**——ここが最頻出の引っかけです。
- **改正個人情報保護法**は、3年ごとの見直しがある、まで。改正年ごとの中身は問われません。

4-6 何が「個人情報」なのか

ここが**この章でいちばん細かい**所です。3語ありますが、うち2つはほぼ同じ意味なので、実質2つと思ってかまいません。

それ単体で個人が分かるもの

個人識別符号。**それ単体で個人を特定できる符号**のことです。

ひとつは**体の特徴をデータにしたもの**。指紋、顔、虹彩（こうさい）など。もうひとつは**公的な番号**。マイナンバー、旅券番号、運転免許証番号など。

名前が無くても、これだけで誰か分かる。だから個人情報として扱われます。

> **個人識別符号**
> それ**単体で特定の個人を識別できる**符号。①**身体の特徴**をデータ化したもの（指紋・顔・虹彩など）②**公的な番号**（マイナンバー・旅券番号・運転免許証番号など）。

特に配慮が要るもの

要配慮個人情報。**本人が不当な差別や偏見を受けないよう、特に配慮が要る情報**です。人種、信条、社会的身分、病歴、犯罪の経歴、犯罪被害の事実。

扱いが特別で、**原則、本人の同意なしに取得できません**。**そこが普通の個人情報との違い**です。

> **要配慮個人情報**
> 本人が**不当な差別や偏見を受けないよう特に配慮を要する**個人情報。人種・信条・社会的身分・病歴・犯罪の経歴・犯罪被害の事実など。**原則、本人の同意なしに取得できない**。

ほぼ同じ意味の、もうひとつの言い方

機微（センシティブ）情報。**要配慮個人情報と、ほぼ同じ意味**です。

違いはどこか。**要配慮個人情報が法律の言葉**で、**機微情報のほうが、もっと広い一般的な言い方**です。**両方載っているので、両方覚える**。それだけです。

> **機微（センシティブ）情報**
> 取り扱いに配慮が要る情報の**一般的な呼び方**。要配慮個人情報とほぼ同じ意味だが、**こちらは法律用語ではなく、より広い言い方**。

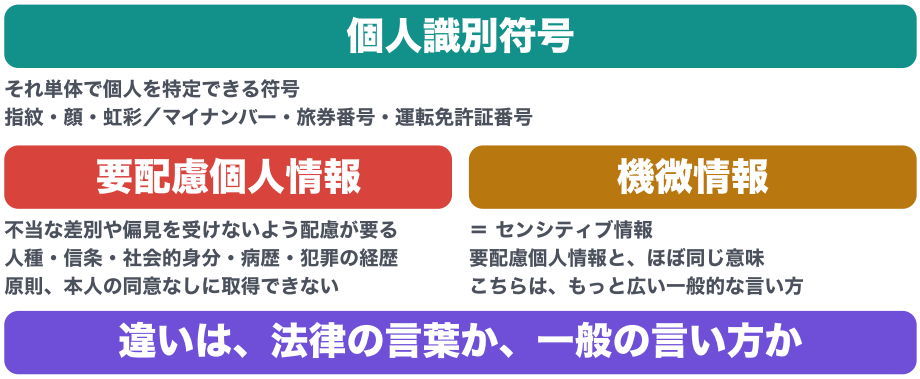

図4-6　単体で分かるものと、特に配慮が要るもの

具体例で確かめる

言葉の定義だけでは判断できないので、代表的なものを並べておきます。

例	どれにあたるか	理由
氏名	個人情報	それだけで特定できる
指紋・顔・虹彩のデータ	個人識別符号	体の特徴で特定できる
マイナンバー・旅券番号	個人識別符号	公的な番号で特定できる
病歴・信条・犯罪の経歴	要配慮個人情報	差別や偏見につながりうる
社員番号だけ	場合による	社内名簿と照合できるなら個人情報

⇒ ⚠ **要配慮個人情報は、個人情報の一種**です。別のものではありません。**個人情報のうち、特に扱いが厳しいもの**という関係になります。ここも親子の形です。

試験ポイント｜違いを一言で

- **個人識別符号**＝それ単体で個人が分かるもの（体の特徴／公的な番号）。
- **要配慮個人情報**＝差別につながりうるので特に配慮が要る情報。**原則、本人の同意なしに取得できない**。
- **機微（センシティブ）情報**＝要配慮個人情報とほぼ同義。**法律の言葉か、一般的な言い方か**の違い。

確認問題② 個人情報の骨組み

確認問題②

第4問 指紋や顔、マイナンバーのように、それ単体で個人を特定できるものを何といいますか。

答

個人識別符号。

体の特徴をデータにしたものと、公的な番号の2種類があります。

確認問題②

第5問 病歴や信条のように、差別につながりうるので特に配慮が要る情報を何といいますか。

答

要配慮個人情報。

原則、**本人の同意なしに取得できません**。そこが普通の個人情報との違いです。

確認問題②

第6問 個人情報保護法を監督する国の機関は何ですか。ルールを守る側の呼び名は何ですか。

答

個人情報保護委員会と**個人情報取扱事業者**。

事業者は**1件でも扱えば当てはまります**。規模の下限はありません。

4-7 加工して、使えるようにする

個人情報は、**守るだけでは終わりません**。使いたい。でも、本人が分かってはいけない。**そこで出てくるのが、次の2語**です。

匿名加工情報

特定の個人を識別できないように加工して、元に戻せないようにした情報です。

ここが大事です。「戻せない」ことが条件。**名前を消しただけでは足りません**。

何が嬉(うれ)しいか。**本人の同意なしに、第三者へ提供できる**ようになります。だから統計や研究、AIの学習データとして使えます。

> **匿名加工情報**
> 特定の個人を識別できないように加工し、**元に戻せないようにした**情報。この条件を満たせば**本人の同意なしに第三者提供ができる**。

マスキング

情報の一部を隠すことです。名前を**山田＊＊**にする、カード番号の下4桁だけ残す、顔にぼかしを入れる。

> **マスキング** Masking
> 情報の**一部を隠す処理**。氏名の一部を伏せる、番号の一部だけ残す、顔にぼかしを入れるなど。

⇒ ⚠ **この2つを混ぜないこと。**マスキングは**隠す手口**。匿名加工情報は**加工した結果できあがったもの**で、法律上の区分です。**手口か、区分か**。そこで分けてください。

図4-7　手口としてのマスキング、区分としての匿名加工情報

どうやって作るのか

匿名加工情報は、**気持ちの上で匿名にした**というものではありません。決められた基準にしたがって加工します。

- **氏名などを削除する**——特定の個人が分かる記述を消す。
- **個人識別符号を削除する**——指紋データやマイナンバーは、残っていると4-6のとおり単体で特定できてしまいます。
- **珍しい値をならす**——たとえば年齢116歳のように**1人しかいない値**は、消すか丸めます。
- **元に戻すための情報を残さない**——対応表を持っていたら、それは戻せるということです。

何に使えるのか

条件を満たすと、**本人の同意なしに第三者へ提供できます**。統計、研究、そして**AIの学習データ**。ここが生成AIの話につながります。

ただし、提供する側には**作ったことを公表する**などの義務があり、受け取った側は**元に戻そうとしてはいけません**。自由に使ってよい、という意味ではありません。

混ざりやすいのは、ここ

マスキングは**手口**で、匿名加工情報は**区分**——と書きましたが、実際には**マスキングは匿名加工情報を作るときの手口のひとつ**でもあります。

ただし**マスキングをすれば匿名加工情報になる、わけではありません**。**戻せないこと**という条件を満たして初めて匿名加工情報です。名前の一部を伏せただけなら、それはただのマスキングです。

試験ポイント｜条件と効果

- **匿名加工情報**の条件は**元に戻せないこと**。名前を消しただけでは足りません。
- 満たすと**本人の同意なしに第三者提供ができる**。ここが効果です。
- **マスキングは手口、匿名加工情報は区分**。取り違えを狙った問題が出ます。

4-8 生成AIに個人情報を入れない

最後に、**この章が生成AIパスポートに載っている理由**です。**生成AIに、個人情報を入力してはいけない**。理由は2つあります。

理由1　学習に使われることがある

入力した内容が**学習に使われることがある**からです。そうすると、**他の人への回答に出てくるおそれ**があります。

理由2　社外に渡していることになる

そもそも**社外に渡している**ことになるからです。**個人情報を第三者に提供している**と見なされうる。

やりがちな例

- **顧客名簿を貼り付けて「分析して」**とやる。
- **履歴書を丸ごと入れて「要約して」**とやる。
- **社外の生成AIに、社内の問い合わせ記録をそのまま入れる。**

やりがちです。でも**アウト**です。

対策は2つ

1. **個人が分かる部分を消してから入れる**——4-7で出た**マスキング**です。
2. **学習に使わない設定のサービスを選ぶ**。

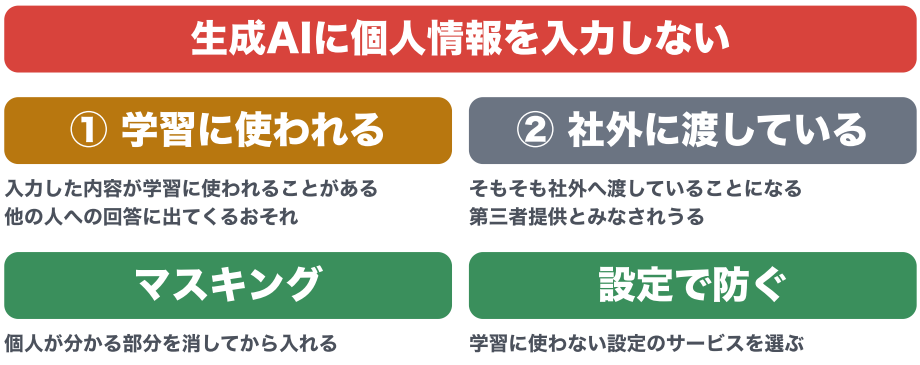

図4-8　入れてはいけない理由と、その対策

試験ポイント｜技術ではなく運用

- 理由は2つ。**①学習に使われうる ②第三者提供にあたりうる。**
- 対策も2つ。**①マスキングしてから入れる ②学習に使わない設定を選ぶ。**
- **技術の話ではなく、運用の話**です。試験でもそう聞かれます。

確認問題③ 加工と、生成AI

確認問題③

第7問　個人を識別できないよう加工し、元に戻せないようにした情報を何といいますか。

答

匿名加工情報。

戻せないことが条件です。名前を消しただけでは足りません。

確認問題③

第8問　情報の一部を隠すことを何といいますか。

答

マスキング。

こちらは**手口**です。匿名加工情報は**区分**でした。

確認問題③

第9問　ファイルを暗号化して身代金を要求するマルウェアを何といいますか。

答

ランサムウェア。

ランサムは身代金。マルウェアが親で、これはその一種です。

まとめ　25語、全部出ました

前半で出た25語を、**3つのかたまり**で並べ直します。ここだけ見返せば全体が戻ります。

1　インターネットリテラシー（5語）

インターネットリテラシーが親。中身が**テクノロジーの理解／情報リテラシー／セキュリティとプライバシー／デジタル市民権**の4つ。

2　セキュリティとプライバシー（11語）

道の違いが3つ——メールなら**フィッシング詐欺**、SMSなら**スミッシング**、電話なら**ヴィッシング**。

やり口の違いが4つ——親が**ソーシャルエンジニアリング攻撃**で、狙い撃ちが**スピアフィッシング**、えさが**ベイト攻撃**、脅しが**ブラックメール**、作り話が**プレテキスト**。

ものの話が3つ——**マルウェア**が親、**ランサムウェア**がその一種、**アンチウイルスソフトウェア**が対策。

3　個人情報保護の観点（9語）

法律が**個人情報保護法**と**改正個人情報保護法**。見張る側が**個人情報保護委員会**、守る側が**個人情報取扱事業者**。

何が個人情報かが**個人識別符号／要配慮個人情報／機微（センシティブ）情報**。加工して使う話が**匿名加工情報**と**マスキング**。

⇒ **後半（②）へ続きます。**次は**作ったものの権利**と**社会のルール**です。知的財産権、肖像権とパブリシティ権、不正競争防止法、そしてAI社会原則とAI新法。40語あります。

巻末 25語チェックリスト

自分の言葉で説明できたら✓を入れてください。読めるだけでは足りません。

- [ ] インターネットリテラシー
- [ ] テクノロジーの理解
- [ ] 情報リテラシー
- [ ] セキュリティとプライバシー
- [ ] デジタル市民権
- [ ] フィッシング詐欺
- [ ] スミッシング
- [ ] ヴィッシング
- [ ] ソーシャルエンジニアリング攻撃
- [ ] スピアフィッシング
- [ ] ベイト攻撃
- [ ] ブラックメール
- [ ] プレテキスト
- [ ] マルウェア
- [ ] ランサムウェア
- [ ] アンチウイルスソフトウェア
- [ ] 個人情報保護法
- [ ] 改正個人情報保護法
- [ ] 個人情報保護委員会
- [ ] 個人情報取扱事業者
- [ ] 個人識別符号
- [ ] 要配慮個人情報
- [ ] 機微（センシティブ）情報
- [ ] 匿名加工情報
- [ ] マスキング

巻末 用語集

インターネットリテラシー p.5
インターネットを適切に利用するために必要な力。テクノロジーの理解・情報リテラシー・セキュリティとプライバシー・デジタル市民権の4つを含む親の言葉。

テクノロジーの理解 p.5
インターネットや情報技術の仕組みを知っていること。知らないものは疑えないため、身を守る土台になる。

情報リテラシー p.5
情報を見極める力。その情報が本当か、誰が発信しているのかを確かめられること。

フィッシング詐欺 p.7
偽のメールやWebサイトで本物を装い、ID・パスワード・カード番号などを入力させて盗む詐欺。

スミッシング p.7
SMS（ショートメッセージ）を使ったフィッシング。SMS＋Phishing。宅配便の不在通知を装う手口が代表例。

ヴィッシング p.7
音声通話を使ったフィッシング。Voice＋Phishing。電話で本人に喋らせて聞き出す。

ブラックメール p.10
脅迫。弱みを握ったと告げて金銭や情報を要求する。黒いメールという意味ではない。

プレテキスト p.10
作り話（口実）で身分をいつわり、信用させてから情報を聞き出す手口。上司・取引先・システム管理者などになりきる。

マルウェア p.13
悪意のあるソフトウェアの総称。malicious＋software。ウイルス・ワーム・トロイの木馬・ランサムウェアなどをすべて含む。

セキュリティとプライバシー p.6
身を守る力。攻撃の手口を知り、設定によって自分の情報を守れること。

デジタル市民権 p.6
ネット上でもひとりの市民として振る舞うという考え方。権利と責任がともにあるとし、匿名を理由にした無責任な振る舞いを否定する。

ソーシャルエンジニアリング攻撃 p.9
技術的な解析ではなく、人間の心理や行動につけこんで情報を盗む攻撃の総称。スピアフィッシング・ベイト攻撃・ブラックメール・プレテキストを含む。

スピアフィッシング p.9
特定の個人や組織を狙い撃ちにするフィッシング。spear＝槍。相手の所属や事情を調べたうえで送るため信じやすい。

ベイト攻撃 p.10
えさで相手を釣る攻撃。bait＝えさ。無料・限定といった欲を刺激する誘いで、リンクを踏ませたり機器を使わせたりする。

ランサムウェア p.13
ファイルを暗号化して使えなくし、復旧と引き換えに金銭を要求するマルウェア。ransom＝身代金。払っても戻る保証はない。

アンチウイルスソフトウェア p.13
マルウェアを検出・遮断・駆除するソフトウェア。名前に反して、ウイルスだけでなくマルウェア全般が対象。

個人情報保護法 p.16
個人情報の取得・利用・保管・提供のルールを定めた法律。正式名称は個人情報の保護に関する法律。

改正個人情報保護法 p.16
改正を重ねている個人情報保護法を指す言い方。3年ごとの見直しが定められており、社会や技術の変化に合わせて更新される。

個人情報保護委員会 p.16
個人情報保護法にもとづき事業者を監督・指導する国の機関。名前に反して民間団体ではない。

個人情報取扱事業者 p.16
個人情報をデータベース化して事業に使っている者。法律上の義務を負う側で、規模の下限はなく1件でも該当する。

個人識別符号 p.18
それ単体で特定の個人を識別できる符号。身体の特徴をデータ化したもの（指紋・顔・虹彩など）と、公的な番号（マイナンバー・旅券番号・運転免許証番号など）。

要配慮個人情報 p.18
本人が不当な差別や偏見を受けないよう特に配慮を要する個人情報。人種・信条・社会的身分・病歴・犯罪の経歴・犯罪被害の事実など。原則、本人の同意なしに取得できない。

機微（センシティブ）情報 p.18
取り扱いに配慮が要る情報の一般的な呼び方。要配慮個人情報とほぼ同義だが、法律用語ではなくより広い言い方。

匿名加工情報 p.21
特定の個人を識別できないように加工し、元に戻せないようにした情報。条件を満たせば本人の同意なしに第三者提供ができる。

マスキング p.21
情報の一部を隠す処理。氏名の一部を伏せる、番号の一部だけ残す、顔にぼかしを入れるなど。