# 指導ガイド：高等学校 情報Ⅰ／大学 初年次「正しく怖がろう：偽物を見破れなくても、自分のアカウントは守れる」

スライド：`right-fear-high-univ.pptx`（本編 17 枚＋付録 5 枚、ノートに台本）／`right-fear-high-univ.pdf`
ワークシート：`worksheet-high-univ.pdf`（A4、表と裏。直すときは `.pptx`） 元の特集：Data is CITY Media 特集「正しく怖がろう」（2026年11月17日。トップ・1「守れるもの、守れないもの」・2「見破れなくても、守れる」・3「今日、設定する」・4「漏れたとき・なくしたとき」） 作り直し：`python3 docs/dataiscity/right-fear/teach/build/build.py --pdf` 出典：Data is CITY（teleport.jp/dataiscity/）、CC BY 4.0

予習なしで使えるように、スライドのノートに、話すこと・問い・予想される答え・注意をすべて書いた。先生は、ノートを読み上げるだけで 1 コマが回る。

---

## この授業のゴール

授業の終わりに、生徒・学生が次の状態になっている。

1. 自分のスマホで、パスワードをスマホに覚えさせる設定をオンにしている 2. 使っているサービスを 1 つ、パスキーにしている（設定の画面に「パスキー」が出ているのを確かめている） 3. 「漠然と怖い」を、「諦めるもの・守れるもの（自分がやること）・やらなくていいこと」に分けて、自分の言葉で言える

---

## ねらい（評価の観点ごと）

- 知識・技能：サービスからの漏えいと、自分のアカウントの乗っ取りの違いを説明できる。顔や指（生体認証）は「本人の確かめ」で、その先に出るのがパスワードかパスキーかで、偽の画面への強さが変わることを説明できる。
- 思考・判断・表現：自分のアカウントを棚卸しし、どれが「合鍵」かを判断して、守る順番を決められる。
- 主体的に学習に取り組む態度：自分のスマホを実際に設定し、残りを家でやる日を決める。自分を守ることが周りの人を守ることだと捉え、情報社会の一員としての行動を選ぼうとしている。

---

## 学習指導要領のどこに当たるか

| 科目・項目 | 本文 | この授業での扱い |
|---|---|---|
| 情報Ⅰ 2 内容 (1) ア(イ) | 「情報に関する法規や制度、情報セキュリティの重要性、情報社会における個人の責任及び情報モラルについて理解すること。」 | 漏えいと乗っ取りは別（スライド5）、人への迷惑（15）、諦めるもの・守れるもの（16） |
| 同 (1) イ (イ) | 「情報に関する法規や制度及びマナーの意義、情報社会において個人の果たす役割や責任、情報モラルなど | AI で攻撃が変わった背景（3・4）、最初の「怖い」を分け直す（2→17） |

| 科目・項目 | 本文 | この授業での扱い |
| --- | --- | --- |
| | について、それらの背景を科学的に捉え、考察すること。」 | |
| 同 (4) ア (ア) | 「情報通信ネットワークの仕組みや構成要素、プロトコルの役割及び情報セキュリティを確保するための方法や技術について理解すること。」 | パスワードが外へ出る 4 つの道（6）、認証の強さの順（11）、パスキーの仕組み＝公開鍵暗号と電子署名（付録 A2） |
| 同 (4) イ (ア) | 「目的や状況に応じて、情報通信ネットワークにおける必要な構成要素を選択するとともに、情報セキュリティを確保する方法について考えること。」 | 合鍵のアカウントから守る順番を決める（12・ワークシート②）、自分のスマホの設定（13・14）、入口を外すか残すか（付録 A5） |
| 総則 | 第1章 第2款の2(1) 情報活用能力（情報モラルを含む） | 全体 |

（本文は、既存の高校の教材〈docs/dataiscity/school/high/lesson-plan.md〉と同じく、高等学校学習指導要領〈平成30年告示〉第2章第10節 情報 第2款 第1 情報Ⅰ から。） 暗号（公開鍵暗号方式・電子署名）を (4) で扱ったあとなら、付録 A2 をそのまま発展に使える。「公共」の情報化と社会、「総合的な探究の時間」（家族のスマホを一緒に設定して、何に困ったかを調べる）にも広げられる。

**大学で使うとき**：初年次教育・情報リテラシー（情報処理演習・アカデミックスキルなど）の 1 コマ（90 分）。大学のアカウント（学内のメール・学習管理システム）が「合鍵」に当たることが多いので、②の棚卸しの「学校のアカウント」の行で扱う。学生のサークルが新入生向けに開くときも、同じ 90 分の流れで使える。

---

## ことばの決まり（特集の書き方の手引き〈docs/dataiscity/editorial.md 7. の 3.〉に合わせる）

- **顔や指とパスキーを一つの言葉にまとめない**。顔・指・6桁は「スマホが持ち主本人かを確かめる」だけ。違うのは、そのあとサイトに届くもの。パスワードは「合言葉」を渡す（偽の画面に手で打てば、そのまま盗まれる）。パスキーは合言葉を渡さない：本物のサイトが出す問題に、スマホの中の鍵が**鍵は出さず、その回だけの答えを返す**。偽の画面には答えない。人の手で打ったり写したりして渡す方法もない。「顔認証の鍵」「指紋の鍵」とは言わない（スライド10。表の列の見出しは「サイトに届くもの」）。
- **何に効くかを付けて言い切る**。「パスキーなら安全」ではなく「パスキーなら、偽のサイトにはスマホが答えない」。多くのサービスではパスキーを作ってもパスワードの入口が残るので、「漏れたパスワードだけでは入られない」とは言わない。言うのは「パスキーで入り、パスワードを求められても打たない。いつもパスキーなのにパスワードを求められたら、止まる」（スライド9・14・16）。ただし玉虫色にはしない。「諦めるもの」「守れるもの」「やらなくていいこと」は分けて言い切る。漠然とした言い方が、いちばん怖がらせる。
- **数は特集の本文のまま**。「件」は「件」（「人」にしない）。いま起きていることは、いちばん新しい数（2026年の 10 月末まで）で言う。去年の年間の数で今を語らない。
- **AI のことは「後押し」程度に言わない**。攻撃の仕事そのものを AI が進める段に入った＝次元が変わった、を出典つきで言う。8〜9割は「ある攻撃では」の数（Anthropic が公表した 1 件）で、すべて

の攻撃の割合ではない（スライド4）。

- **パスキー**＝合言葉（パスワード）を渡さずに入る仕組み。本物のサイトの問題に、スマホの中の鍵がその回だけの答えを返し、偽のサイトには答えない（初出のスライド6・9で一言）。**2段階認証**＝パスワードのほかに、もう一つ確認を足すこと（11）。**認証アプリ**＝30秒ごとに変わる番号を出すアプリ（11）。**合鍵のアカウント**＝メールの受け取り先と「〇〇でログイン」の元（12）。**OS**＝スマホやパソコンを動かす土台のソフト（4）。**Anthropic（アンソロピック）**＝AI の Claude を作っている会社（4）。**NCSC**＝英国の国のサイバーセキュリティの機関（4）。
- 会社名や実在の画面は再現しない。スライド7の画面は作りもの（「マイSNS」、住所は説明用に取っておかれた `.example`）。

---

## 時間配分

### 高校 50 分（出欠・配布の 2 分を含む）

生徒が口を開く・手を動かすのは、2（書く）、7（手を挙げる）、10（隣の人と30秒、必ずやる）、12（棚卸し）、13・14（自分のスマホを設定）、17（書く・言う）。

| 時間 | スライド | 活動 | 問い |
|---|---|---|---|
| 0〜2分 | — | 出欠・ワークシート配布。「スマホは後半で使う」 | — |
| 2〜3分 | 1 | 表紙：今日のゴール | — |
| 3〜5分 | 2 | 怖いことを 3 つ、ワークシート①へ。2〜3人に読ませ、板書の左へ | 「ネットの安全で、いま何が怖い？」 |
| 5〜7分 | 3 | 漏えいはこの夏から桁が変わった（2026年1〜10月 約3億7,600万件＝2025年の約7.6倍、約94%が7月以降） | — |
| 7〜10分 | 4 | ある攻撃では、AI が仕事の8〜9割を進めた・数千の未知の弱点・数日。穴があれば、いずれ突かれる | — |
| 10〜13分 | 5 | 漏えい（守れない）と乗っ取り（守れる）は別。つなぐのは使い回し。メールは合鍵 | 「同じパスワードを2つ以上で使っている？」（心の中で） |
| 13〜15分 | 6 | パスワードが外へ出る 4 つの道。「いつか漏れるもの」として扱う | — |
| 15〜17分 | 7 | どちらが本物？（30秒見せて挙手） | 「A と B、どちらが本物？」 |
| 17〜19分 | 8 | 昔の見分け方 5 つは、もう当てにならない | — |
| 19〜20分 | 9 | 守りの 4 段 | — |

| 時間 | スライド | 活動 | 問い |
|---|---|---|---|
| 20〜23分 | 10 | 顔や指は本人の確かめ。自動入力とパスキーの違い | **隣の人と30秒（必ず）**「顔でログインしているから大丈夫は本当？」 |
| 23〜25分 | 11 | パスキーは渡さない。2段階認証の強さの順 | — |
| 25〜29分 | 12 | 合鍵のアカウント。ワークシート②の棚卸し（3分） | 「『パスワードを忘れた』を押したら、メールはどこに届く？」 |
| 29〜33分 | 13 | **設定①**：画面ロックを確かめ、パスワードを覚えさせる設定をオン | — |
| 33〜41分 | 14 | **設定②**：1 つのサービスでパスキーを作り、確かめる（削らない）。手順はワークシートの QR でも。これからは「パスキーで入り、パスワードを求められたら止まる」 | — |
| 41〜43分 | 15 | 乗っ取られると友だちに届く。漏れただけなら、ふつうは迷惑をかけない | — |
| 43〜45分 | 16 | 諦めるもの・守れるもの・人への迷惑・やらなくていいこと | — |
| 45〜48分 | 17 | ワークシート③④（⑤は宿題でよい）。2〜3人に④を言わせる | 「最初の『怖い』を 3 つの箱に分け直すと？」 |
| 48〜50分 | — | 予備 | — |

計 50 分（2+1+2+2+3+3+2+2+2+1+3+2+4+4+8+2+2+3＋予備2）。**14 は削らない**。押したら 7（クイズ）と 9（4段）を 30 秒ずつにし、15 と 16 を 1 枚で 2 分にまとめる。

### 45 分版

50 分版の中身は 48 分（予備 2 分）。45 分版は中身を 44 分にして、予備を 1 分残す。

| 変える所 | 50 分版 | 45 分版 |
|---|---|---|
| 4（AI） | 3分 | 2分（Anthropic の 2 件だけ。NCSC は台本で一言） |
| 6（4 つの道） | 2分 | 1分（2 の「偽の窓口に自分で渡す」だけ詳しく） |
| 7（クイズ） | 2分 | 飛ばす（8 の「URL」の所で、1 文字違いを口で言う） |

計 45 分（2+1+2+2+2+3+1+2+1+3+2+4+4+8+2+2+3＋予備1）。14 は削らない。

### 大学 90 分

本編の間に付録を挟む。設定の時間（14）は、学生の人数と端末に合わせて 8〜12 分に伸ばしてよい（そのぶん A5 を 10 分に）。

| 時間 | スライド | 活動 |
|---|---|---|
| 0〜10分 | 1〜4 | 本編どおり（出欠を含む） |
| 10〜15分 | **A1** | 証券口座の不正な取引 1万782件・国の「偽のサイトに強い認証」への切り替え。問い「見破る目を鍛える教育と、見破れなくても守れる仕組み、どちらに時間を使う？」 |
| 15〜30分 | 5〜11 | 本編どおり |
| 30〜40分 | **A2** | パスキーの仕組み：鍵は 2 つで 1 組、秘密の鍵はスマホから出ない、毎回違う問題に署名、サイトの住所に結びつく。問い「サービスが破られたら、パスワードとパスキーで何が違う？」 |
| 40〜45分 | **A3** | パスキーでも防げないもの 3 つ（電話の声・言われて入れたアプリ・窓口の悪用）。問い「3 つに共通するのは？」 |
| 45〜62分 | 12〜14 | 棚卸しと設定（本編どおり。設定は 8〜12 分） |
| 62〜64分 | 15 | 人への迷惑 |
| 64〜69分 | **A4** | 起きてしまったら：漏れた・乗っ取られた・なくした |
| 69〜71分 | 16 | まとめ |
| 71〜86分 | **A5** | 話し合い：パスワードの入口を外す？残す？（個人2分→班8分→発表5分）。安全となくしたときに戻れること（可用性）の引っ張り合い。会社がパスワードを残す理由 |
| 86〜90分 | 17 | ふり返り（⑤まで書かせる） |

計 90 分（10+5+15+10+5+17+2+5+2+15+4）。

---

## 板書の例

``` 怖いこと（①） ｜ 諦めるもの ｜ 守れるもの（自分がやること） ｜ やらなくていいこと ・漏れる ｜ サービスからの漏えい ｜ 自分のアカウントの乗っ取り ｜ パスワードを何度も変え続ける ・乗っ取られる ｜ （自分を責めない） ｜ 1 スマホを顔・指・6桁で閉じる ｜ ネットから離れる ・偽サイト ｜ ｜ 2 パスワードはスマホが作って覚える ｜ 偽物を見破る練習 ・… ｜ ｜ 3 合鍵からパスキーに。パスワードを ｜ ｜ ｜ 求められても打たない ｜ ｜ ｜ 顔・指＝本人の確かめ（鍵ではない） ｜ ```
```

授業のはじめに左の列だけ書き、最後に生徒の言葉で右の 3 列へ移す。

---

## 端末がないとき・学校の端末で設定できないとき

- **スマホを持っていない・持ち込めない生徒**：ワークシート②の棚卸しを「家の人のスマホ」か「将来持つときの順番」で書く。設定の時間（13・14）は、スライド14の手順を見ながら、隣の人の設定を「読み上げ役」として手伝う（画面は本人が操作し、手伝う側はパスワードや番号の映った画面を見ない）。③は「家でやる日」に書き、家の人と一緒にやる。特集の冊子（印刷用 PDF）を家に持ち帰らせてよい。
- **学校がスマホの使用を認めていない**：13・14 を「家でやる宿題」にし、授業では手順の読み合わせ（どの画面のどこを押すか）までにする。次の時間の頭の 3 分で、③の✓を確かめる。
- **学校から貸している端末（1人1台端末）**：学校の端末と、学校のアカウント（学校の Google／Microsoft）は、学校の決まりに従う。生徒に設定を変えさせない。パスキーを作るのは、自分の（個人の）スマホと個人のアカウントだけ。学校のアカウントでパスキーを使えるかは、情報担当の先生や教育委員会に前日までに確かめる（管理者が止めていることがある）。
- **家族と共有している端末**：パスキーを作らない（家族が自分のアカウントに入れてしまう）。棚卸しだけにする。
- **ログインできない・パスワードを思い出せない**：授業中に無理に再設定しない。別のサービスでやるか、家で保護者と。
- **パスキーの項目が見つからない**：LINE は 2026年11月から順に使えるようになっていて、まだ届いていないことがある。X のパスキーはスマホの X アプリで（パソコンは認証アプリ）。見つからなければ別のサービスに切り替える。

---

## 指導の注意

- **パスワードそのもの、スマホの6桁、バックアップコード、メールアドレスや電話番号は、ワークシートに書かせない・人に見せない。**ワークシートを回収するときも、書いてあるのはサービスの名前と○だけ。回収せず、写真で③④だけ提出させてもよい。
- 生徒どうしで画面を見せ合うときは、パスワードや番号が映っていないか、先に一言注意する。
- **弱い入口（パスワードや SMS の入口）は、授業中には外させない。**予備（バックアップコード、別の端末のパスキー、再設定用の連絡先）を用意してからでないと、スマホをなくしたときに自分も入れなくなる。外すのは家で、予備を確かめてから（大学では付録 A5 で考える）。
- Apple の「復旧キー」は、ふつうは設定しない（設定すると Apple の窓口での復旧の手続きが使えなくなり、なくすとアカウントに二度と入れなくなることがある。特集2）。
- 怖がらせて終わらない。3・4 の数は「だから、穴をふさぐ。ふさぎ方は分かっている」につなぐ。最後は自分がやったことで閉じる。
- 「偽物の見分け方を練習しよう」で終わらせない。特集の主張は、見分けられなくても守れる方法に替えること。
- 実在の偽サイトを探したり、開いたりする課題は出さない。スライド7は作りもの。

- お金がからむとき、どうしていいか分からないときは、一人で抱えずに保護者や先生に、と伝える（付録 A4・ワークシートの裏）。
- 漏えいの件数・不正な取引の件数は、特集の公開時（2026年11月）の数。授業の前日に、新しい数が出ていないか見る。

---

## よく出る質問と答え

- 「顔でログインしているから大丈夫？」→ 顔はスマホが本人かを確かめるだけ。そのあとサイトに届くのがパスワード（合言葉）なら、偽の画面で打ち込めば盗まれる。見分け方：ログインの画面でパスワードの欄に「●●●」が入ればパスワード、「パスキーでサインイン」などと出て欄に何も入らなければパスキー。迷ったら、設定の画面に「パスキー」があるかを見る（スライド10）。
- 「パスキーを作ったら、もうパスワードは漏れても平気？」→ 平気とは言えない。多くのサービスでは、パスキーを作ってもパスワードの入口が残る。だから、パスキーで入り、パスワードを求められても打たない。パスワードはスマホに作らせて使い回さない。弱い入口を外すのは、予備を用意してから家で（付録 A5）。
- 「顔の形がサービスに送られるの？」→ 送られない。スマホの中で確かめるのに使うだけ（特集2）。
- 「パスキーにすれば絶対安全？」→ 絶対ではない。偽のサイトでのログインに強くなる。電話で言われて自分で操作する、言われて入れたアプリに画面を操作される、は別に防ぐ（付録 A3）。
- 「スマホをなくしたら、パスキーも消える？」→ パスキーは、同じ Apple か Google のアカウントの自分のほかの端末に、暗号をかけたまま受け渡される。新しいスマホに Apple か Google のアカウントで入れば戻る。だから Apple か Google のアカウントのパスワードは覚えておき、予備（再設定用の連絡先など）を用意しておく（特集2）。
- 「パスワードは何か月ごとに変えればいい？」→ 変え続けなくていい。変えるのは、漏れたと知らせが来たとき（特集トップ）。
- 「SMS の番号でも 2 段階認証なら十分？」→ ないよりはずっといい。でも、偽の画面に番号を打てば、その場で使われる。金融庁も2026年4月の広報で「リアルタイムフィッシングに脆弱」と書いている。付けられるならパスキー（スライド11）。
- 「ゲームのアカウントは？」→ Google・Apple・X・LINE などと連携しているなら、その元が合鍵。元のアカウントをパスキーにする（スライド12）。
- 「友だちから『投票して』とリンクが来た」→ 開かない。お金の頼みに応じない。電話など別の手段で本人に確かめる（スライド15）。

---

## 授業の前日に確かめること

- 自分のスマホで、スライド13・14 の手順を一度たどる（画面の名前が変わっていないか。違っていたら公式の説明を正とする。特集3〈teleport.jp/dataiscity/right-fear-setup/〉は各社の公式の説明へのリンクつき）。
- 学校のスマホの持ち込み・使用の決まり。学校のアカウントでパスキーを使えるか（情報担当の先生・教育委員会）。

- 校内の Wi-Fi に生徒のスマホがつながるか（つながらなければ、モバイル回線で）。
- 漏えいの数（MM 総研）・不正な取引の数（金融庁）に新しい発表がないか。
- ワークシートの印刷（A4 両面、1 人 1 枚）。

---

## ワークシート（worksheet-high-univ.pdf）

表

- 書かないことの注意（パスワード・6桁・バックアップコード・メールアドレスや電話番号）
- ① はじめの「怖いこと」3 つ　← スライド2
- ② 自分のアカウントの棚卸し（サービスの名前・合鍵か・いまの入り方〈パスワードだけ／SMS／認証アプリ／パスキー〉・使い回し・今日やった）。いちばん先に守る合鍵を一つ　← スライド12

裏

- ③ 今日やったことに✓（画面ロック・パスワードを覚えさせる・パスキーを作った〈サービスの名前〉・確かめた・【家で】合鍵の再設定用の電話番号とメール・家でやる日）　← スライド13・14・17。再設定用の連絡先は、14 で早く終わった生徒だけが授業中にやり、ほかは家で（台本にも書いた）
- ③の横に、特集3「今日、設定する」（teleport.jp/dataiscity/right-fear-setup/）の QR コード。スライド14の手順は字が小さいので、後ろの席の生徒は手元のスマホでこれを読み、サービスを押して手順を1手ずつ見る
- ④ ①の「怖いこと」を、諦めるもの／守れるもの（自分がやること）／やらなくていいこと に分け直す　← スライド17
- ⑤ 友だちや家族に、一つ伝えるなら（一文。宿題でよい）
- 持ち帰り用：起きてしまったら（漏れた・乗っ取られた・なくした）

評価の目安：知識・技能は ④ で「漏えい（諦める）」と「乗っ取り（守れる）」を取り違えずに分けられているか、⑤ や発言で「顔や指＝本人の確かめ」と「パスキー」を区別できているか。思考・判断・表現は ② で合鍵のアカウントを選べているか。主体的に学習に取り組む態度は ③ で設定を 1 つ以上済ませ、残りを「いつ」やるかまで書けているか（端末がなかった生徒は、家でやる日と、誰とやるかで見る）。

---

## 使った事実と出典（スライドの隅にも記載）

数はすべて特集「正しく怖がろう」の本文のもの（特集の編集部が一次の出典を開いて確かめた）。付録 A2 の仕組みだけは特集の本文の外の補足で、下の W3C・FIDO Alliance の文書で確かめた（2026-11-17）。

| 事実 | 出典 |
| --- | --- |
| 2026年に国内で公表されたサイバー攻撃による漏えいは10月末までに約3億7,600万件、2025 | MM総研「サイバー攻撃による漏えい情報は10月末までに約3.8億件」（2026-11-04）https://www.m2ri.jp/release/detail.htm |

| 事実 | 出典 |
| --- | --- |
| 年（4,953万件）の約7.6倍、約94%が7月以降の公表、事案は9月81件→10月193件、認証情報は延べ約1億6,100万件で2025年の約31倍 | l?id=745 |
| 10月に公表されたサイバー攻撃などは233件で月の過去最多 | ANN（2026-11-09）https://news.ksb.co.jp/ann/article/17033815 |
| AI が攻撃の80〜90%を進め、人の判断は1回の攻撃につき4〜6か所、約30の組織を狙いいくつかで成功 | Anthropic「Disrupting the first reported AI-orchestrated cyber espionage campaign」（2025-11-13）https://www.anthropic.com/news/disrupting-AI-espionage |
| 新しい AI が、主な OS とブラウザのすべてで数千の未知の弱点を見つけた。同じ力がいずれ広がるとの見通し | Anthropic「Project Glasswing」（2026-04-07）https://www.anthropic.com/glasswing |
| 弱点の公表から攻撃に使われるまでは数日に縮み、AI でさらに縮むのは「ほぼ確実」 | 英国 NCSC「Impact of AI on cyber threat from now to 2027」（2025-05-07）https://www.ncsc.gov.uk/report/impact-ai-cyber-threat-now-2027 |
| 証券会社での不正な取引 1万782件（2025年1月〜2026年10月の累計） | 金融庁「インターネット取引サービスへの不正アクセス・不正取引による被害にご注意ください」（2026-11-13 更新の資料）https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html |
| 「フィッシング耐性のある多要素認証」への切り替えの呼びかけ。メールや SMS のワンタイムパスワードは「リアルタイムフィッシングに脆弱」 | 金融庁の広報（2026-04-16）https://www.fsa.go.jp/news/r7/sonota/20260416-2/20260416-2.html |
| 証券のログイン・出金・出金先の変更に、偽のサイトに強い認証が必須（2025年10月施行。金融庁は2026年6月末までの対応を求めた） | 日本証券業協会「インターネット取引における不正アクセス等防止に向けたガイドライン」https://www.jsda.or.jp/about/hatten/inv_alerts/alearts04/files/20251015_internetgl.pdf |
| 身に覚えのない取引の知らせがあれば、すぐ金融機関に連絡 | 金融庁「現下の情勢を踏まえた金融機関利用者へのお願い」（2026-11-06）https://www.fsa.go.jp/news/r8/sonota/20261106/20261106.html |
| 漏えいと乗っ取りの区別、4 つの道、見分け方 5 つ、守りの 4 段、自動入力とパスキーの違い、強さの順、合鍵のアカウント、人への迷惑、起きたときにやること | 特集「正しく怖がろう」トップ・1〜4（Data is CITY Media、2026-11-17）https://teleport.jp/dataiscity/right-fear/ |
| 設定の手順（iPhone・Android のパスワード、Google・Instagram・TikTok・X・LINE のパスキー） | 各社の公式の説明（特集の編集部が 2026-11-16 に確かめたもの。リンクは特集3と docs/dataiscity/right-fear/guard.yaml） |
| 再設定用の連絡先・バックアップコード、Apple の復旧用連絡先・復旧キー | Google アカウント ヘルプ https://support.google.com/accounts/answer/183723?hl=ja ・ https://support.google.com/accounts/answer/1187538?hl=ja ／ Apple サポート https://support.apple.com/ja-jp/102641 ・ https://support.apple.com/ja-jp/109345 |

| 事実 | 出典 |
| --- | --- |
| 〔付録 A2〕パスキーは公開鍵暗号を使い、秘密の鍵は利用者の端末側、サービスは公開の鍵で署名を確かめる。鍵はサービス（RP ID）に結びつき、ほかの住所では使えない | W3C「Web Authentication: An API for accessing Public Key Credentials - Level 3」（W3C 勧告、2026-08-25）https://www.w3.org/TR/webauthn-3/ ／ FIDO Alliance「Passkeys」https://fidoalliance.org/passkeys/ |

---

## ライセンス

この教材（スライド・ワークシート・指導ガイド）は、クリエイティブ・コモンズ 表示 4.0 国際（CC BY 4.0）で提供する。改変も配布も、営利目的の利用も自由。使うときは「出典：Data is CITY（teleport.jp/dataiscity/）」と表示する。https://creativecommons.org/licenses/by/4.0/deed.ja

出典：Data is CITY（teleport.jp/dataiscity/）、CC BY 4.0