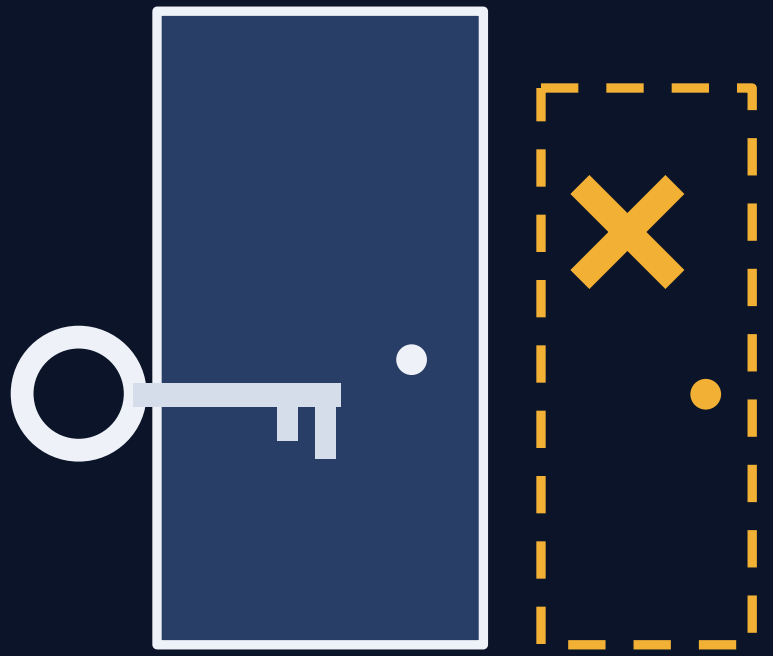
特集「正しく怖がろう」から

偽物を見破れなくても、自分のアカウントは守れる



諦めるもの・守れるもの・自分がやることを分け、
今日、自分のスマホを設定する

高等学校　情報Ⅰ（1）情報社会の問題解決／（4）情報通信ネットワークとデータの活用
大学　初年次教育・情報リテラシー（90 分）

はじめの問い（ワークシート①）

ネットの安全で、いま何が怖い？
思いつくものを3つ書く

怖いこと 1

怖いこと 2

怖いこと 3

授業の最後に、この 3 つを分け直す

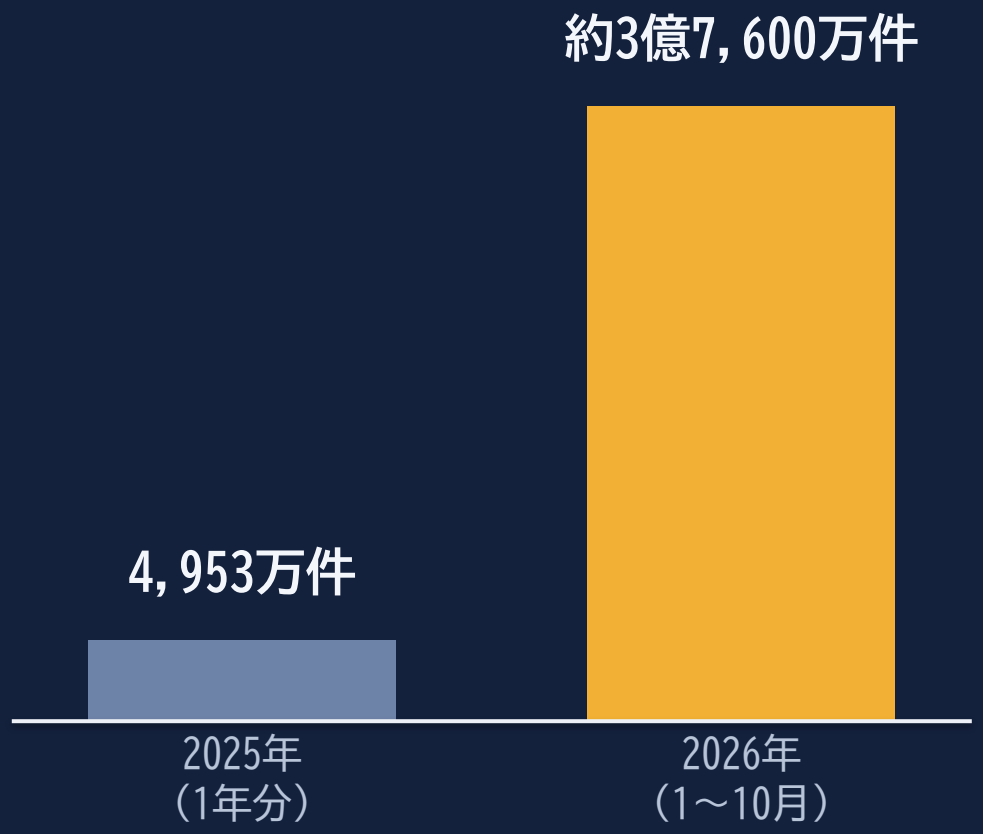
諦めるもの

守れるもの（自分がやること）

やらなくていいこと

いま起きていること①

漏えいは、この夏から桁が変わった。
2026年は10月末までに、去年1年分の約7.6倍



約94%

今年の件数のうち、
7月以降に公表された分

81→193件

事案の数（9月→10月）。
倍以上に

約31倍

漏れたパスワード・ログインID
延べ約1億6,100万件。2025年比

自分のメールアドレスや、どこかで使った
パスワードも、もう漏れていると思って動く

出典：MM総研（2026-11-04）、ANN（2026-11-09）。特集「正しく怖がろう」トップ

いま起きていること②

AI が、攻撃する側の道具になった。
ある攻撃では、仕事の8〜9割を AI が自分で進めた

8〜9割

ある攻撃で、その仕事を
AI が自分で進めた。人の判断は
1回の攻撃で4〜6か所
（2025年11月、Anthropic）

数千

まだ誰も知らなかった
深刻な弱点を、AI が見つけた。
主な OS とブラウザのすべてで
（2026年4月、Anthropic）

数日

弱点の公表から、攻撃に使われる
まで。AI でさらに縮むのは
「ほぼ確実」（英国 NCSC）

穴があれば、いずれ突かれる。「自分なんか狙われない」は、もう通らない

出典：Anthropic（2025-11-13、2026-04-07）、英国 NCSC（2025-05-07）。特集「正しく怖がろう」トップ

まず分ける

サービスからの漏えいと、自分のアカウントの乗っ取りは、別の話



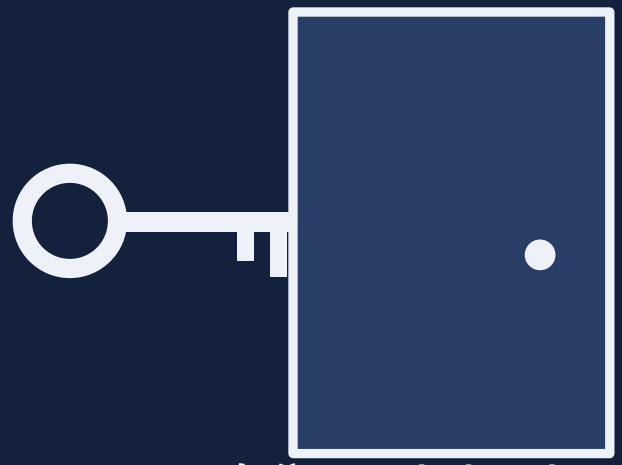
破られる

使っているサービスの会社
（預けた先の金庫）

守れない

パスワードの使い回し

漏れたパスワードを
ほかでも使っていると、
漏えいが乗っ取りに変わる



自分のアカウントの扉
（鍵は自分で決められる）

守れる

パスワードが外へ出る、4 つの道

パスワードは、強くしても、しまっても、漏れる

パスワードは
「いつか漏れるもの」



1　預けた先から漏れる
自分ではどうにもできない

2　偽の窓口に、自分で渡す
見破れない

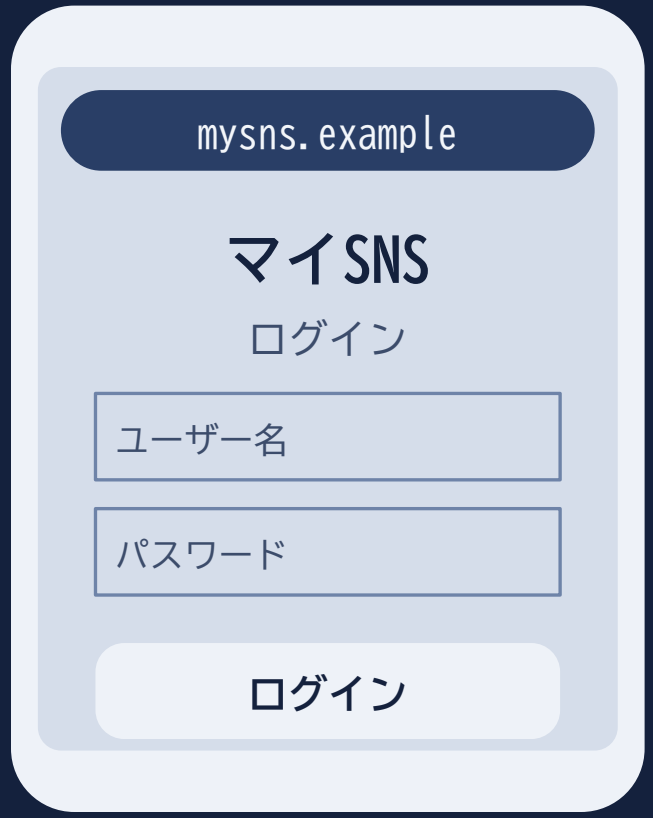
どんなに強くても、そのまま渡る

3　怪しいアプリに抜かれる
端末の中で。気をつければ減らせる

4　当てられる
よくある言葉や、漏れた一覧で。
長くでたらめなら、まず起きない

やってみる（30秒）

どちらが本物のログイン画面？



A

?

画面は授業のための
作りもの



B

見破れない

昔の見分け方は、もう当てにならない。だから、見分けることに頼らない

URL	鍵マーク	日本語	送り主の名前	声
1文字違い・本物を中継する偽サイト	偽サイトにも付いている	AI が書くので不自然にならない	偽れる。本物の並びに紛れる	AI が流暢に話し、家族の声もまねる
✕	✕	✕	✕	✕

見落とすのは、注意が足りないからではない。目に頼らなくても守れる方法に替える

守りを積む

守りを4段で積む。いちばん上がパスキー

右の段（上の段）ほど強い



1

スマホを、顔か指と
6桁で閉じる

全部の土台

2

パスワードは、
スマホが作って覚える

使い回しが消える

3

顔や指で確かめると、
パスワードが自動で入る

楽。でも中身はパスワード

4

パスキーで入る。
パスワードは打たない

偽のサイトには答えない

いちばん間違えやすいところ

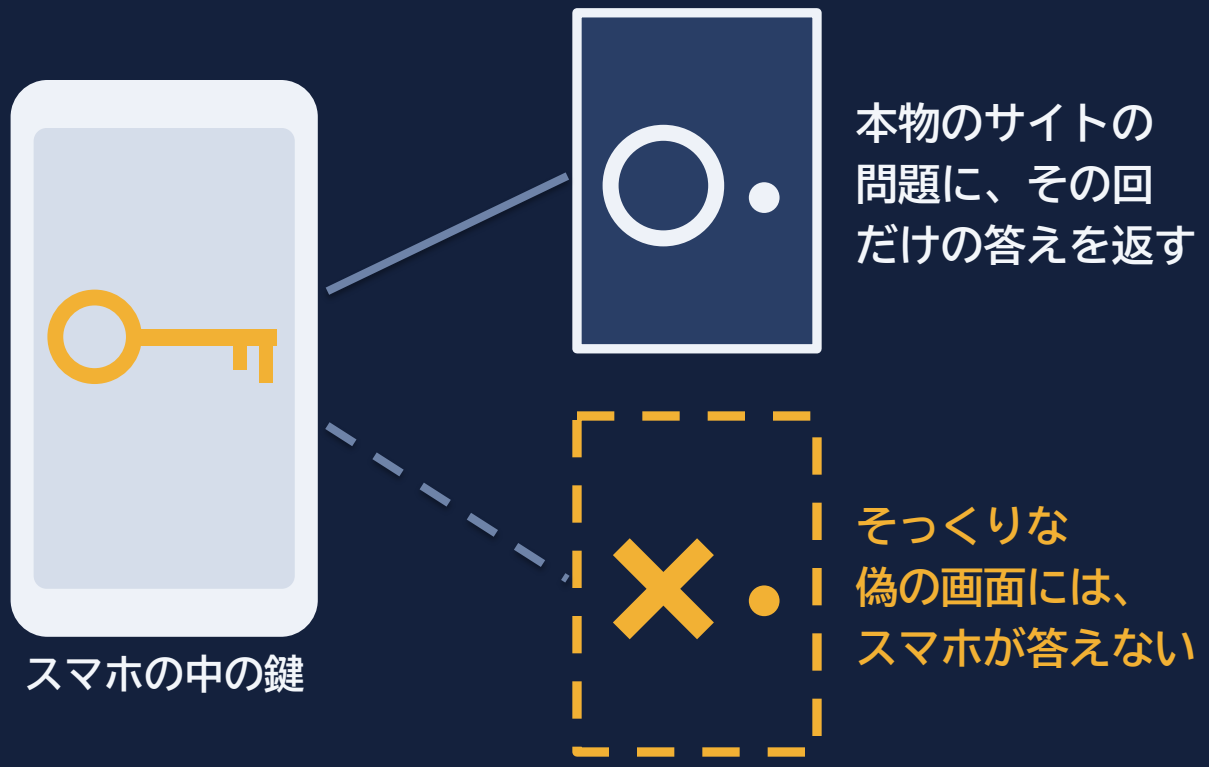
顔や指は「持ち主本人か」を確かめるだけ。守りの強さは、そのあとサイトに届くもので決まる

	確かめたあと	サイトに届くもの	偽の画面では
顔・指・6桁 スマホが「持ち主本人か」を確かめる	パスワードの自動入力（3段目）	合言葉（パスワード）そのもの	手で打てば、そのまま盗まれる
	パスキー（4段目）	鍵は出さず、その回だけの答え	スマホが答えない。手で渡す方法もない

隣の人と30秒：「顔でログインしているから大丈夫」は本当？

パスキーの強さ

パスワードは相手に渡す。パスキーは渡さない。偽物を見分けるのは、目ではなくスマホ



ログインの守りの強さの順（上ほど強い）

パスキー
偽のサイトには、スマホが答えない

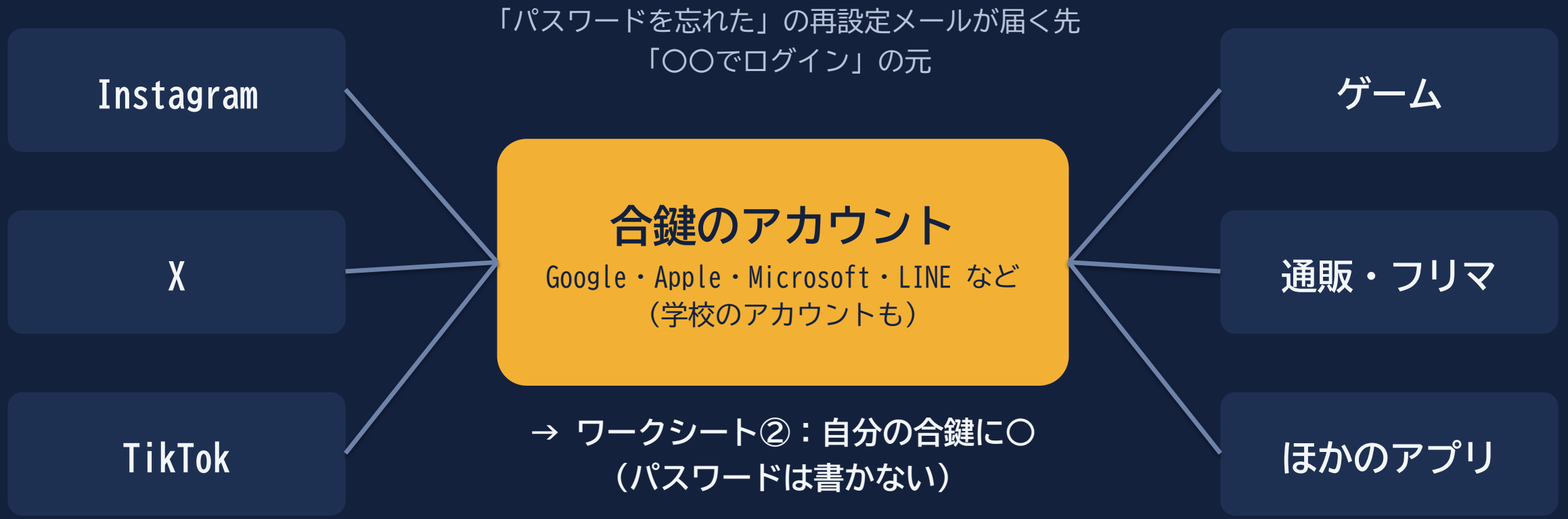
認証アプリの番号
偽の画面に打てば、奪われる

SMS の番号
偽の画面に打てば、奪われる

パスワードだけ
盗まれたら、そのまま入られる

順番を決める（ワークシート②）

最初に守るのは「合鍵のアカウント」。ここが開くと、ほかの全部が開く



いま、設定する①（4分）

パスワードを、スマホに覚えさせる

先に：画面ロックが「顔か指」と「6桁以上」になっているか確かめる

iPhone

「設定」→「一般」
→「自動入力とパスワード」
→「パスワードとパスキーを
自動入力」をオン

Android

Chrome を開く →「設定」
→「自動入力とパスワード」
→「Google パスワード マネージャー」
→「設定」→「パスワードを保存
できるようにする」をオン

これから：新しいパスワードは、スマホが出す「強力なパスワード」を選ぶ。いまのを全部変えなくていい

手順は各社の公式の説明（特集の編集部が 2026-11-16 に確かめたもの）。画面が違っていたら、公式の説明を正とする

いま、設定する②（8分）

使っているサービスを、1つパスキーにする

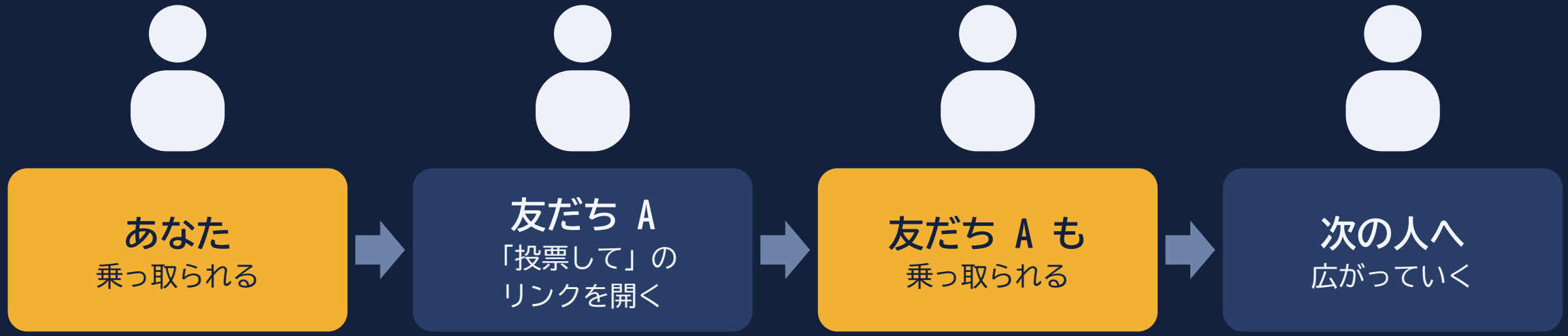
Google	myaccount.google.com/signinoptions/passkeys →「パスキーを作成する」 →「パスキーを作成」→ 画面ロックを解く 合鍵。使えるならここから
Instagram	「設定」→「Metaアカウント設定」→「ログインとセキュリティ」 →「パスキー」→「パスキーを作成」
TikTok	「プロフィール」→ メニュー（三本線）→「設定とプライバシー」 →「アカウント」→「パスキー」→「設定」
X	「設定とプライバシー」→「セキュリティとアカウントアクセス」→「セキュリティ」 →「追加のパスワード保護」の「パスキー」→「パスキーの追加」 スマホの X アプリで
LINE	「設定」→「アカウント」→「パスキー」→「パスキーを作成」 2026年11月から順に。項目がなければ、まだ届いていない

確かめる：同じ画面に「パスキー」が出ていれば完了 ／ これから：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

手順は各社の公式の説明（特集の編集部が 2026-11-16 に確かめたもの）。画面が違っていたら、公式の説明を正とする

人への迷惑

乗っ取られると、あなたの名前で
友だちや家族に、詐欺のメッセージが届く



漏れただけなら、
ふつうは人に迷惑をかけない

分かれ目は、乗っ取られるかどうか。
自分を守ることが、周りを守る

まとめ：正しく怖がる

諦めるもの、守れるもの、やらなくていいことを分ける

諦めるもの	守れるもの	人への迷惑	やらなくていいこと
使っているサービスの会社からの漏えい。使う側には止められない。自分を責めなくていい	自分のアカウントの乗っ取り。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求められたら、止まる	かかるのは、乗っ取られたとき。漏れただけなら、すぐ変えれば心配は小さい	パスワードを何度も変え続けることも、ネットから離れることもいらない。変えるのは、知らせが来たとき

ふり返り（ワークシート③④⑤）

最初の「怖い」を、自分の言葉で分け直す

③ 今日やったことに✓。できなかったことは、家でやる日を書く

④ ①の「怖いこと」を、3つの箱に分け直す

⑤ 友だちや家族に、一つ伝えるなら？（一文）　← 宿題でよい

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

正しく怖がる＝諦めるものと守れるものを分け、守れるものを今日守る

この作品は クリエイティブ・コモンズ 表示 4.0 国際 ライセンスで提供されています。
出典：Data is CITY（teleport.jp/dataiscity/）
https://creativecommons.org/licenses/by/4.0/deed.ja

付録 A1（大学 90 分で足す・時間があれば）

証券口座の乗っ取りで、不正な取引は1万782件。国は「偽のサイトに強い認証」への切り替えを求めた

1万782件

証券会社での不正な取引（2025年1月～2026年10月）。
偽のサイトや不正なアプリで盗まれた ID とパスワードが使われた

国と業界の動き

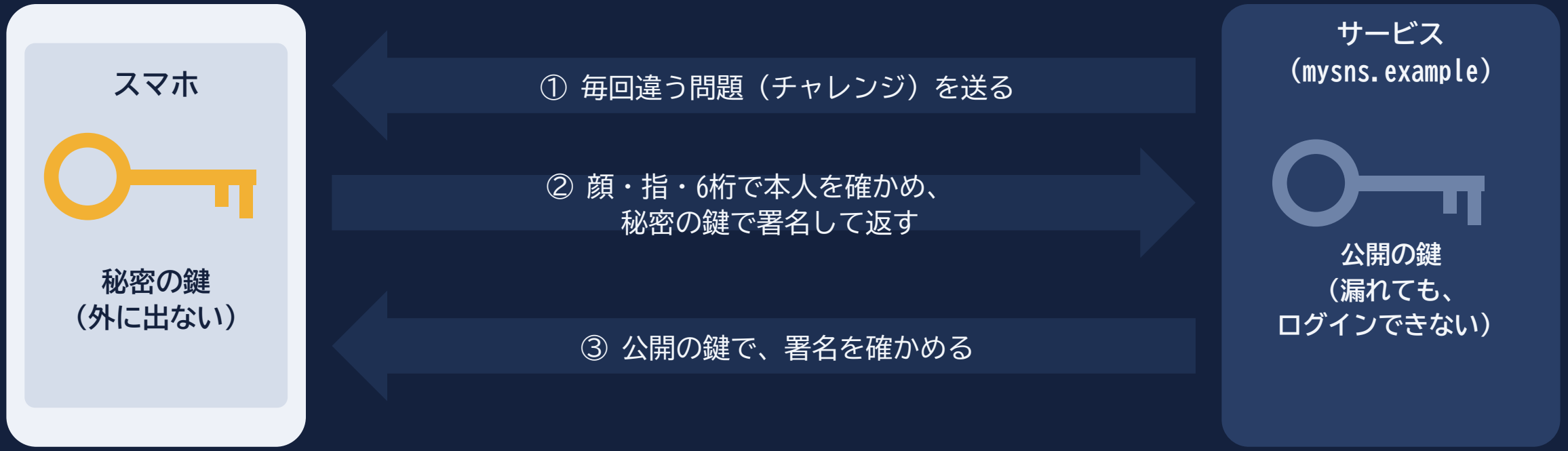
- 金融庁が、銀行や証券会社と一緒に「フィッシング耐性のある多要素認証」への切り替えを呼びかけ（2026年4月）
- 証券のログインと出金に必須に（日本証券業協会、2025年10月施行）

答えは、見破る目を鍛えることではなく、**見破れなくても守れる鍵に替えること**

出典：金融庁（2026-11-13 更新の資料・2026-04-16 の広報）、日本証券業協会（2025-10-15 施行）。特集トップ・3

付録 A2（大学 90 分・情報Ⅰの暗号の発展）

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ず、サイトの住所に結びつく



鍵の組は、作ったサイトの住所に結びつく → 住所が違う偽のサイトには、スマホが答えない

出典：W3C「Web Authentication（WebAuthn）」、FIDO Alliance「Passkeys」。特集の本文の外の補足（指導ガイドに出典）

付録 A3（大学 90 分で足す・質問が出たら）

それでも、パスキーでも防げないものがある。入ったあとと、自分の手で開けてしまう扉

1　電話の声に言われて、自分で認証してしまう	2　言われて入れたアプリに、画面を操作される	3　窓口に「なくした」と申し出て、取り戻す手口
一度切って、自分から公式の番号にかけ直す。家族とは合言葉	「このアプリを入れて」と言われたら、どのアプリでも入れない。端末は最新に	再設定用の電話番号・メールを、自分のものにしておく

パスキーは「絶対に安全」ではない。偽のサイトでの乗っ取られにくさが、大きく上がる

付録 A4（大学 90 分で足す・時間があれば）

起きたら：漏れた・乗っ取られた・なくした

漏れたと知らせが来た

- そのサービスのパスワードを変える（同じものは全部）
- 届いたリンクから入らない
- そっくりな連絡が来る前提で待つ

乗っ取られた

- お金は、まず公式の窓口へ
- 公式の手順で取り戻し、パスキーか2段階認証
- 電話など別の手段で、友だちに知らせる

なくした

- 探す → ロック → 最後に消す
- 携帯会社に連絡して、回線を止める
- 6桁を見られたかもしれないなら、急いで消し、パスワードを変える

付録 A5（大学 90 分の話し合い：個人2分 → 班8分 → 発表5分）

パスキーを付けたあと、パスワードの入口を外す？ 残す？

外す

- 攻撃は、残った弱い入口に来る
- パスキーだけなら、偽の画面に渡せるものがない

残す

- 予備がないと、なくしたときに自分も入れない
- パスキーに対応していない端末で入れなくなる

考える：

・外すなら、前もって用意する予備は？　・サービスの会社は、なぜパスワードの入口を残すのか？