第5版　2026年11月17日



使っているサービスからの漏えいは防げない。偽物も、もう見破れない。それでも、自分のアカウントへの攻撃は、今日から大きく減らせる

情報漏えいやアカウントの乗っ取りから、自分と家族を守るための冊子。偽物を見破れなくても守れる仕組みと、iPhone・Android・Mac・Windows、Google・Apple・LINE・Amazon・PayPayなど18のサービスで、パスキーや2段階認証を設定する手順を、1手ずつまとめた。55歳のケンジさんの家族の漫画4話つき。紙を横に置いて、親や家族のスマホを一緒に設定するときにも使える。

Data is CITY Media
teleport.jp/dataiscity/
AI時代のセキュリティのメディア（テレポート株式会社）。この冊子のウェブ版と最新の版も、ここから。

目次

はじめに　今までとは、次元が違う 3

1　守れるもの、守れないもの 知っておく 5

2　見破れなくても、守れる 知っておく 13

3　今日、設定する 設定する 23

4　漏れたとき・なくしたとき 起きたとき 45

チェックシート 53

奥付 55

3　今日、設定する　端末とサービス

iPhone 27
Android 28
Mac 29
Windows 30
Google アカウント 32
Apple アカウント 32
Microsoft アカウント 33
Yahoo! JAPAN ID 33
LINE アカウント 34
dアカウント（ドコモ） 35
au ID 36
SoftBank ID 37
楽天 ID（楽天会員） 37
Amazon（amazon.co.jp） 37
PayPay 38
メルカリ 38
銀行 39
証券 39
X（旧 Twitter） 39
Instagram 41
Facebook 42
TikTok 43
設定ではない、3つの約束 43

はじめに　今までとは、次元が違う

ネットの安全は、この1〜2年で、別の次元に入った。 AIが、攻撃する側の道具になったからだ。

漏えいは、この夏から桁が変わった。 調査会社のMM総研の集計では、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年の1年分（4,953万件）の**約7.6倍**で、その約94%は、7月以降に公表された事案のものだ。9月に81件だった事案は、10月には193件と倍以上になった。10月に公表されたサイバー攻撃などは233件で、月として過去最多だった。漏れたパスワードやログインIDだけで、延べ約1億6,100万件ある。2025年の**約31倍**だ。11月に入っても、公表は続いている（詳しくは特集「2026年秋の情報漏えいは、会社が使うサービスから広がった」）。あなたのメールアドレスや電話番号、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いた方がいい。

そして、攻撃する側の道具が変わった。AIだ。偽のメールが自然な日本語になり、本物そっくりの偽のサイトが安く大量に作れるようになったのは、入り口にすぎない。2025年11月、AIの会社Anthropicは、国家の後ろ盾があるとみられるグループが、同社のAIを使って世界の約30の組織に攻め込もうとし、いくつかで侵入に成功したと公表した。攻撃の仕事の8〜9割を、AIが自分で進めた。人が判断したのは、1回の攻撃につき4〜6か所ほど。多いときは1秒に何度も手を打ち、人間のハッカーには到底まねのできない速さだった。

穴を見つける力も、桁が違う。Anthropicは2026年4月、自社の新しいAIが、まだ誰も知らなかった深刻な弱点を数千見つけ、その中には、主なOS（スマホやパソコンを動かす土台のソフト）とブラウザのすべてのものがあったと発表した。同じ力は、いずれ安全に使う気のない人の手にも渡りかねないと、同社自身が書いている。英国の国のサイバーセキュリティの機関（NCSC）は、弱点が公表されてから攻撃に使われるまでがすでに数日に縮み、AIでさらに縮むのは「ほぼ確実」だと見ている。

そして、穴があれば突かれる。使い回しているパスワード、偽の画面に打ってしまうパスワード、更新していない古いスマホやパソコン。AIは、こうした穴を、休まず、速く、大勢を相手に同時に試せる。**「自分なんか狙われない」は、もう通らない。** 穴があれば、いずれ突かれる。これが、これからの前提だ。

だから、はっきりさせておく。

- **諦めるもの**：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。漏れたと知らせが来るたびに、自分を責めなくていい。
- **守れるもの**：自分のアカウントの乗っ取り。パスキー（パスワードの代わりに使う、偽のサイトでは出てこない鍵）に替え、パスワードだけで入れる入り口を閉じておけば、漏れたパスワードや偽の画面で盗まれたパスワードだけでは入られない。
- **人への迷惑**：迷惑がかかるのは、乗っ取られたときだ。あなたの名前で、友だちや家族、取引先に、お金の頼みや偽の請求書が届く。パスワードが漏れただけで、乗っ取られていなければ、同じパスワードを使っているほかのサービスも含めてすぐ変えれば、迷惑をかける心配は小さい。
- **やらなくていいこと**：パスワードを片っ端から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、漏れたと知らせが来たときでいい。

いちばんつらいのは、何が起きていて、どこまでが危ないのか分からないまま、漠然と怖がることだ。何でも怖くなって、パスワードを変え続けたり、ネットにつながらない方がいいのかと迷ったりする。でも、守れる側の話は、もう答えが出ている。2025年1月から2026年10月までに、国内の証券会社では1万782件の不正な取引があった。偽のサイトや、端末に入り込んだ不正なアプリで盗まれたIDとパスワードが使われた。金融庁は2026年4月、銀行や証券会社と一緒に、偽のサイトに強い認証（「フィッシング耐性のある多要素認証」）に切り替えるよう呼びかけた。答えは、偽物を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だ。

正しく怖がる、とは、諦めるものと守れるものを分け、守れるものを今日ちゃんと守ることだ。そのための特集を、4つに分けて組んだ。

最初の2つで、知っておくことを積み上げる。何が守れて、何が守れないのか。偽物を見破れなくても、なぜ守れるのか。3つ目で、持っている端末と使っているサービスを押すと、設定の仕方が1手ずつ、かかる時間つきで並ぶ。4つ目は、起きてしまったときにやること。漏れたと知らせが来たら、乗っ取られたら、スマホをなくしたら、だ。やってみると、楽にもなる。パスワードをスマホに覚えさせれば、サービスごとのパスワードを覚えな

くてよくなり、ふだん自分で覚えるのは、スマホの6桁　　スワードの2つになる。
と、Apple（Androidの人はGoogle）のアカウントのパ

知っておく

1　守れるもの、守れないもの

漫画　ケンジさんの家と、本物にしか合わない鍵　第1話「頼んでないのに、頼んでいた」




送信済み
田中
20:14
いま会議で手が離せない。
コンビニで電子マネー…
佐藤
20:12
いま会議で手が離せない。
コンビニで電子マネー…
鈴木
20:10
いま会議で手が離せない。
コンビニで電子マネー…
山本
20:08
いま会議で手が離せない。
コンビニで電子マネー…
おれから…… 60人に？
はい、大野です
御社から、振込先が変わったという請求書がメールで届いたのですが
請求書（振込先変更のお知らせ）
ガタッ
送ってない！
おれのせいで、部下にも、取引先にも……


父さん、乗っ取られてる
知ってる人からのメッセージは疑わないから、引っかかる人が出るんだ
怪しいメールなんか、開いてないぞ。何をしたら、乗っ取られるんだ？
ログイン
今は、AIが勝手に穴を探して、休まず攻めてくる。今までとは、次元が違うんだよ
入り口は、パスワード。父さん、全部同じでしょ
1つ漏れたら、全部開く
入り口ニ
パスワード
漏れた
偽の画面に打った
ガーン
よし、全部変える！
変えても、また漏れたら同じ。パスワードだけで守ってる限りね

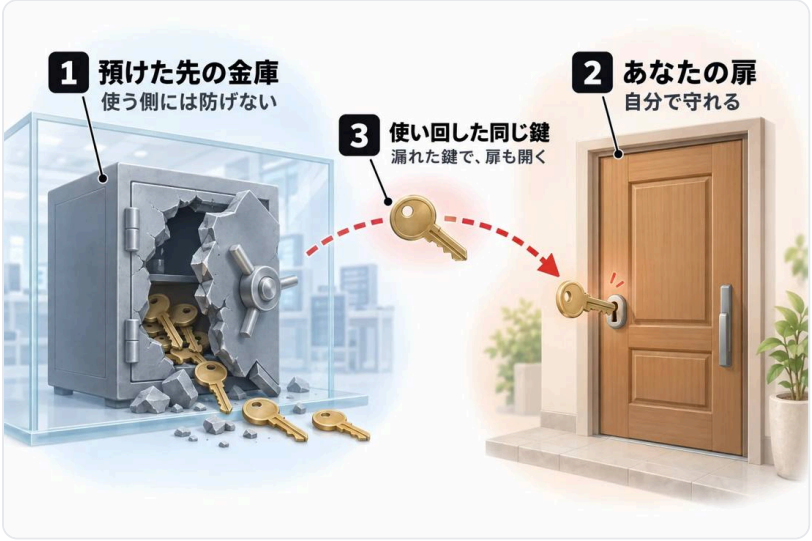

だから、パスワードとは別の鍵を作る。パスキーっていうんだ
鍵はスマホの中にできて、本物のサイトにしか合わない
パスキーを作成
最近のパソコンでも作れる。使うときは、顔か指（または暗証番号）で確かめる
顔なら、もう画面のロックで使ってるぞ？
それは、スマホが父さん本人かを確かめてるだけ。鍵は、サービスごとに作るんだ
ポイント
乗っ取りの入り口は、パスワード。
サービスごとにパスキーを作れば、
偽の画面では鍵が出ない。顔や指は、本人かを確かめるだけ

「また情報が漏れた」というニュースを見るたびに、何をすればいいのか分からなくなる。この回では、まず二つの話を分ける。自分では守れないものと、自分で守れるものだ。

サービスからの漏えいと、自分のアカウントへの攻撃は、別の話だ

「また漏れた」というニュースの多くは、使っているサービスの会社が破られた話だ。会社が守るべき金庫が破られたのであって、**使っている側が何をしても、防ぎようはない。**

自分のアカウントへの攻撃（乗っ取り）は違う。攻撃する側が狙うのは、あなたのアカウントの扉だ。扉の鍵をどうするかは、あなたが決められる。鍵を替えれば、入られる道の多くを閉じられる。



漏えいは向こうの金庫、乗っ取りはこちらの扉

1. 預けた先から漏れるのは、使う側には防げない
2. 自分のアカウントを狙う攻撃は、自分で防げる
3. 同じパスワードを使い回していると、漏れた鍵で自分の扉も開く

二つをつなぐのが、パスワードの使い回しだ。預けた先から漏れたパスワードを、ほかのサービスでも使っていれば、漏えいは自分の扉の乗っ取りに変わる。使い回していなければ、この芋づるは起きない。

ただ、それで全部が止まるわけではない。メールのアカウントが乗っ取られると、ほかのサービスで「パスワードを忘れた」を押され、再設定のメールを受け取られてしまう。パスワードが全部違っていても、そこから入られる。だから、メールのアカウントは、ほかより一段かたく守る。

守れるもの、守れないものを、表で分ける

起きることを、自分の手で守れるかどうかで3つに分けた。左の「守れる」の列は、どれも今日、自分でできることだ。

守れる（今日、自分でやる）	小さくできる（起きたあと）	守れない（しょうがない）
偽の画面でパスワードを盗まれる 見破れない メールなど大事なアカウントをパスキーに替える	**預けた先からパスワードが漏れた** 見破れない そのサービスのパスワードを変える。使い回していなければ、芋づるにはならない	**預けた先が破られる** 防げない
使い回したパスワードで芋づる式に開けられる パスワードは端末に作らせ、覚えさせる	**漏れた名前や番号で、本物そっくりの連絡が来る** 見破れない リンクを開かず、電話は一度切る	**住所や買い物の記録が漏れる** 防げない
SMSのリンクから偽の画面へ連れていかれる 見破れない 届いたリンクから入らない	**言われて入れたアプリに、画面を操作・横取りされる** 見破れない 電話やメッセージで言われたアプリは入れない。入れてしまったら、すぐ消して家族か窓口に相談	**サービスが止まる** 防げない
「はい」の通知を連打される 覚えのない通知は押さない	**AIの声の電話で、自分で操作させられる** 見破れない 切って、自分から公式の番号にかけ直す。家族の合言葉	
乗っ取られて、友だちや家族に詐欺のメッセージが送られる 見破れない メールやLINE・SNSのアカウントをパスキーか2段階認証に		
なくした端末の中を使われる・のぞかれる 画面ロックと顔・指、「探す」		
古い端末の穴を突かれる 自動で更新する。更新が来なくなった端末は買い替える		

「守れる」の列には、「見破れない」の印が付いたものが並ぶ。偽物は見破れない。それでも、守れる。その仕組みは、次の「見破れなくても、守れる」で一段ずつ説明する。

乗っ取られると、友だちや家族に迷惑がかかる。だから守ることは、周りを守ること

自分のアカウントが乗っ取られると、被害は自分だけで終わらない。乗っ取った側は、あなたの名前で、あなたの友だちや家族にメッセージを送る。LINEなら「いま手が離せないから、コンビニで電子マネーのカードを買って、番号を送って」。InstagramやXなら「このコンテストに投票して」と、偽のログイン画面へのリンクを送る。メールなら、本物の差出人のまま、取引先に偽の請求書が届く。

知らない人からのメッセージは疑えても、よく知っている人からのものは疑いにくい。だから、引っかかる人が出る。そのアカウントもまた乗っ取られ、次の人へと広がっていく。

では、使っているサービスから自分の情報が漏れたら、人に迷惑をかけるのか。**ふつうは、かけない。** あなたは被害を受けた側だ。分かれ目は、そのあと乗っ取られるかどうかにある。

自分のせいで、人に迷惑をかける？

使っているサービスから、情報が漏れたと知らせが来た

漏れただけなら、ふつうは人に迷惑はかけない。あなたは被害を受けた側だ。分かれ目は、そのあと乗っ取られるかどうか。3つの問いに答えてみよう

❶ 漏れたパスワードを、ほかのサービスでも使っている？

危ない（はいのとき）
乗っ取られる恐れがある
同じパスワードで、ほかのサービスにも入られる。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。今すぐ、同じパスワードを全部変える。

いいえなら、次の問いへ

❷ 届いたメールやSMSのリンクから入って、パスワードや番号を入れた？

危ない（はいのとき）
乗っ取られる恐れがある
偽のログイン画面だったかもしれない。すぐにそのサービスのパスワードを変え、友だちや家族に「私から来たリンクは開かないで」と知らせる。お金のサービスなら、まず金融機関に連絡する。

いいえなら、次の問いへ

❸ そのアカウントは、パスキーか2段階認証にしてある？

大丈夫（はいのとき）
迷惑をかける心配は小さい
パスワードが漏れても、それだけでは入られにくい。漏れたサービスのパスワードを変えておく。漏れた名前や番号を使った、本物そっくりの連絡には気をつける。自分のアカウントを守ることが、周りを守ることになっている。

もう一手（いいえのとき）
すぐ、パスワードを変える
漏れたサービスのパスワードを、今すぐ変える。変えるまでは、それだけで入られてしまう。あわせてパスキーか2段階認証を付ければ、次に漏れても入られにくい。

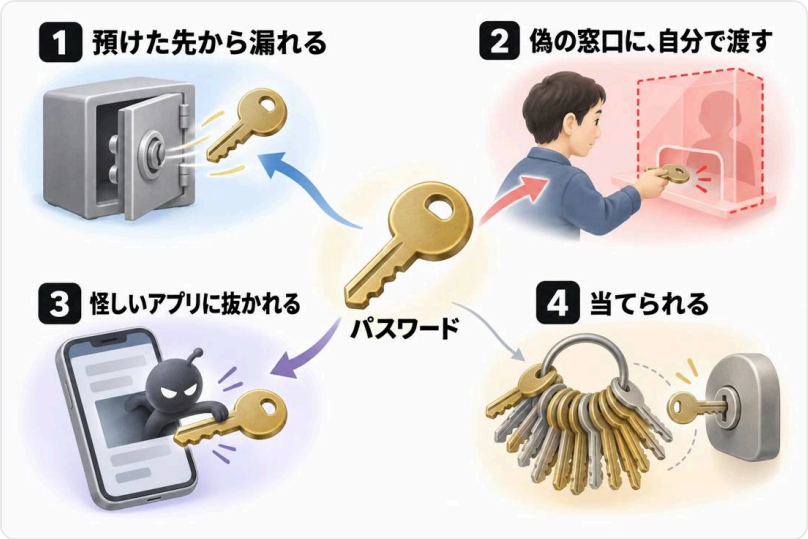
つまり、いま自分にできるのは、自分のアカウントを守ることだ。パスキーや2段階認証にしておけば、パスワードが漏れても、それだけでは入られない。自分のアカウントを守ることが、そのまま周りの人を守ることになる。

ひとつだけ例外がある。お店や教室を営んでいて、お客さんの名前や連絡先を自分のアカウントで預かっている人だ。そのアカウントから漏れれば、預かっている人たちに直接迷惑がかかる。

パスワードは、強くしても、しまっても、漏れる

パスワードを変えれば大丈夫、しっかりしまっておけば大丈夫、と思われがちだ。でも、パスワードが外へ出て

いく道は4つある。注意で減らせるものもあるが、注意だけでは防ぎきれない。



パスワードが外へ出る4つの道

1. 預けた先から漏れる。自分では防げない
2. 偽の窓口に、自分で渡してしまう。どんなに強くても、そのまま渡る
3. 端末の中の怪しいアプリに抜かれる
4. よくある言葉や、ほかで漏れた一覧で当てられる

4の「当てられる」は、長くてでたらめなパスワードにすれば、まず起きない。2と3は、気をつければ減らせる。でも、偽物は本物と見分けにくいところまで来ていて、急いでいるときの人の目では防ぎきれない（次の回）。1は、自分ではどうにもできない。

だから、パスワードは「いつか漏れるもの」として扱う。やることは二つだ。サービスごとに違うパスワードにして、使い回さない。そして、守りの主役をパスワードから、パスキー（偽のサイトでは使えない鍵。次の回）に替えていく。

ただ、サービスごとに長くてでたらめなパスワードなど、人には覚えられない。覚えなくていい。それが次の話だ。

知っておく

2　見破れなくても、守れる

漫画　ケンジさんの家と、本物にしか合わない鍵　第2話「本物にしか、見えない」




ガーン
同じじゃない！
再配達の受付
再配達の受付
yamane-unyu.jp
yamane-unyuu.jp
ぼくだって、並べなきゃ分からない
ふつうに見たら、分かりようがない……


ばあちゃん、
スマホ変えたんだ。
新しい番号、
登録しといて
あら、
リク
ばあちゃん
……同じ声
ゾクッ
URLも、
鍵の印も、
日本語も、
名前も、声も。
全部、本物に見える
だから、
見分けるのは
もうやめる。
目じゃなくて、
スマホに見分け
てもらうんだ
……ぼくのも、
SMSの
ままだった


わたしも、顔でパスワードを入れてるけど？
顔は、本人か確かめるだけ、そのあとスマホが合言葉（パスワード）を入れる。偽の画面に打てば、合言葉は犯人に渡る
本物の画面
偽の画面
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、スマホの中の鍵が答えるだけ
偽の画面には、スマホが答えない。見分けるのは、母さんの目じゃなくてスマホ
じゃあ、パスワードは覚えなくていいの？
？
サービスのパスワードを、人が覚えるのは、もうやめよう。スマホに作らせて、覚えさせる
付箋に書いたパスワードも、もういらないのね
ペリッ
ポイ
ポイント
顔や指は、本人かを確かめるだけ。
パスワードは合言葉を渡し、パスキーは渡さない。
サービスのパスワードを人が覚えるのは、もうやめる

前の回で、パスワードは「いつか漏れるもの」だと書いた。では、どうすれば守れるのか。この回では、守りを一段ずつ積んでいく。途中で、間違えやすい「顔や指で入る」と「パスキー」の違いも分ける。



この回で積む、守りの4段

見分け方は、もう効かない

これまで、偽物の見分け方として広く言われてきたことがある。どれも、もう頼れない。本物そっくりの偽サイトでも、URLは本物と少し違う。でも、急いでいるときの人の目は、その違いを見落とす。



昔の見分け方は、もう当てにならない

1. URLをよく見る：似た文字の住所や、本物をそのまま中継する偽サイトがある
2. 鍵マーク（https）を見る：偽サイトにも付いている
3. おかしな日本語を探す：AIが書くので、もう不自然にならない
4. 送り主の名前を見る：偽れる。本物のメッセージの並びに、偽物が紛れることもある
5. 声で確かめる：AIが流暢に話し、家族の声をまねることもある

見落とすのは、あなたの注意が足りないからではない。偽物の側が、本物と見分けにくいところまで来た。だから、見分けることに頼らない。人の目に頼らなくても守れる方法に替える。それを、ここから一段ずつ積む。

パスワードは、スマホやパソコンに作らせて、覚えさせる

一段目は、パスワードを自分で考えるのをやめることだ。人が覚えるのは、もうやめよう。作るのも、覚えるのも、スマホやパソコンの仕事だ。

iPhoneやMacには「パスワード」アプリ、AndroidやChromeには「Googleパスワードマネージャー」、WindowsのEdgeにはパスワードを覚える機能がある。新しくパスワードを決める画面で、端末が「強力なパスワード」を出してくれる。それを選んで、端末に覚えさせる。

こうすると、パスワードは長くてでたらめで、サービスごとに違うものになる。当てられることはまずなく、どこかで漏れても、使い回しの芋づるにはならない。前の回の、パスワードが外へ出ていく4つの道のうち、4の「当てられる」と、使い回しの芋づるが、これで消える。

覚えたパスワードは、顔・指・6桁で開けると、自動で入る

二段目は、覚えさせたパスワードを、どうやって使うかだ。

ログインの画面を開くと、端末が覚えたパスワードを出してくる。そのときに端末が求めるのが、顔か指、またはスマホを開くときの数字（iPhoneならパスコード、AndroidならPIN。6桁以上）だ。本人だと確かめられたら、パスワードが自動で入る（パソコンのブラウザは、初めの設定では確かめずに入ることもある）。

もう一つ、いいことがある。端末は、覚えたパスワードを、覚えたときと同じ住所のサイトでしか出さない。いつもは自動で入るのに出てこないときは、自分で打ち込んだり、パスワードの一覧から写したりしない。偽のサイトかもしれない。いつものアプリかブックマークから開き直す。



覚えるパスワードは、ぐっと減る

つまり、ふだん自分で覚えるのは、スマホの6桁と、Apple（Androidの人はGoogle）のアカウントのパスワードの2つになる。サービスごとのパスワードは、覚えなくていい。守りが強くなるうえに、楽になる。

AppleかGoogleのアカウントのパスワードだけは、覚えておく。スマホをなくしたときに探すのにも、新しいスマホに覚えさせたパスワードを戻すのにも要るからだ。紙に書いて、家の大事な書類と一緒にしまっておいてもいい。

ただし、この2つだけでは、スマホをなくしたときにアカウントに戻れないことがある。予備の手段を、前もって別に用意しておく。

- Googleは、再設定用の電話番号とメールアドレスを登録しておく。2段階認証を付けたら、バックアップコード（10個あり、1つずつ1回だけ使える）を印刷して、パスワードの紙とは別の封筒にしまう。財布やスマホのケースには入れない（パスワードとそろうと、2段階認証ごと入られる）
- Appleは、信頼できる家族などを「復旧用連絡先」にしておく。パスワードや6桁を忘れたときに、Appleのアカウントに戻るのを手伝ってもらえる（スマホ本体のロックは解けない）
- 自分のiPadやパソコンでも、同じアカウントにログインしておく。スマホをなくしても、そこから戻れる

Appleの「復旧キー」（28文字）は、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。ふつうは設定しなくてよい。

その代わり、6桁と顔・指が、全部の入口の鍵になる。6桁は、誕生日や「123456」のような当てやすい数字にしない。家族にも教えない。人に見られる場所では、顔か指で開ける。6桁を盗み見てから端末ごと盗む手口があるので、iPhoneは「盗難デバイスの保護」をオンにしておく（設定の仕方は「今日、設定する」に入れた）。

顔や指で入るのは、どちらも同じ。違うのは、そのあとスマホが相手に何を渡すかだ

ここが、いちばん間違えやすい。パスワードの自動入力でも、パスキーでも、画面の上では同じに見える。顔を向けるか指を当てると、ログインできる。でも、その裏でスマホがしていることは、まったく違う。

顔や指は、どちらでも「スマホが、あなた本人かを確かめる」だけだ。顔や指の形がサイトに送られることはな

い。違うのは、そのあと、スマホが相手のサイトに何を渡すかだ。

パスワードは「合言葉」だ。 ログインのたびに、あなたか、あなたの代わりのスマホが、合言葉をサイトに伝える。合言葉は、聞いた人なら誰でも使える。偽のサイトに伝えれば、犯人がそれを聞いて、本物のサイトで同じ合言葉を言うだけで入れる。スマホは、住所の違う偽のサイトでは、合言葉を自動では入れない。でも、出てこないと、人が手で打ったり、写したりして渡してしまう。サイトの会社から合言葉の控えが漏れて読み解かれても、同じことが起きる。

パスキーは、合言葉を伝えない。 パスキーを作ると、スマホの中に「鍵」が、サイトの側に、その鍵にだけ合う「錠前」が置かれる。ログインのとき、サイトは毎回ちがう問題を出し、スマホは中の鍵を使って、その回だけの答えを返す。鍵そのものは、相手のサイトには渡らない。答えは、その回、そのサイトでしか使えないので、横から盗んでも役に立たない。サイトの会社から錠前が漏れても、錠前から鍵は作れない。

そのうえ、スマホは答える前に、相手の住所（ドメイン）を確かめる。パスキーを作ったときの本物の住所と違えば、答えない。偽のサイトには、スマホが答えない。見た目がどれだけ本物そっくりでも、関係ない。そして、パスキーには、人が手で打ったり写したりして渡す方法が、そもそもない。だから、あわてていても渡しようがない。



顔や指で本人を確かめるところまでは同じ。違うのは、そのあと

自分がどちらを使っているかは、ログインの画面で見分けられる。

- パスワードの欄に「●●●」が入る → パスワード（の自動入力）。顔や指を使っていても、中身はパスワードだ
- 「パスキーでサインイン」「パスキーを使用」などと出て、パスワードの欄に何も入らない → パスキー
- パスワードの欄に●●●を入れたあとで、パスキーを求められることがある。これはパスキーを2段目に使う形で、パスワードは盗まれうる
- 銀行などのアプリの「生体認証ログイン」は、●●●も「パスキー」の字も出ないことが多い。どちらでもない仕組みのこともある
- 迷ったら、そのサービスの設定の画面に「パスキー」が登録されているかを見る

「顔でログインしているから大丈夫」と思っていても、それがパスワードの自動入力なら、まだ二段目だ。

もっと強いのが、パスキーだ。偽のサイトでは鍵が出ない

三段目が、パスキーだ。サービスごとに、スマホやパソコンの中に作る鍵で、ログインのときは顔や指（または6桁）で確かめてから使う。パスワードの代わりに使えるサービスが増えている。

仕組みは、上の図のとおりだ。鍵は相手のサービスには一度も渡らず、本物の相手にだけ答える。自分のほかの端末（同じAppleやGoogleのアカウントのiPadやパソコンなど）には、暗号をかけたまま受け渡されるだけだ。



見破るのは、目ではなく端末

1. 鍵は、相手のサービスには一度も渡らない。自分の端末どうしで、暗号をかけたまま受け渡されるだけ
2. 本物の住所の扉にだけ、鍵が回る
3. 見た目がそっくりでも、住所が違えば端末は鍵を出さない。見破るのは目ではなく端末
4. 顔や指は、端末の中の鍵を開けるだけ。顔や指紋の形は、どこにも送られない

見た目がそっくりな偽のサイトでも、住所が違えば、端末は鍵を出さない。偽物かどうかを見分けるのは、あなたの目ではなく端末だ。顔や指紋の形は、どこにも送られない。端末の中の鍵を開けるのに使うだけだ。

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）には、強さの順がある。



上ほど強い

1. パスワードだけ：盗まれたら、そのまま入られる
2. SMSの番号：電話番号を乗っ取られる。偽の画面に打てば、その場で使われる
3. 認証アプリの番号：SMSより強い。でも偽の画面に打てば、同じく使われる
4. パスキー：偽のサイトでは使えない

パスワードだけで守るのは、もう論外だ。 漏れても、偽の画面で盗まれても、そのまま入られる。

SMS（ショートメール）で届く番号は、もう安全とは言えない。 今までは、SMSの番号を足せば安全だと言われてきた。でも今の偽のサイトは、パスワードと一緒に、届いた番号まで打たせる。打った番号は、その場で犯罪者に渡り、番号が使えるうちに本物のサイトで打ち直される。そこから、あっという間に入られる。偽のサイトに打った番号は、守りにならない。盗んだパスワードだけでは入れないので、パスワードだけよりはましだが、偽の画面には効かない。実際に、銀行をかたるSMSから偽のログインサイトへ誘い、IDとパスワードに加えてワンタイムパスワードまで盗んで、預金を送金する被害が出ている。2023年は11月末までに5,147件、約80.1億円にのぼった（金融庁）。金融庁も2026年4月の広報で、メールやSMSに届く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」だと書いている。認証アプリ（Google Authenticatorなど、30秒ごとに変わる使い捨ての番号を出すアプリ）の番号も、同じ手で使われる。スマホを開く数字とは別のものだ。「はい」を押すだけの通知は、何度も鳴らして、つい押すのを待つ手口がある。自分でログインしていないときの通知は、押さない。

付けられるサービスでは、パスキーを付ける。付けられないサービスでは、そこで選べるいちばん上を選ぶ。パスキーを付けても、パスワードやSMSで入れる入口が残っていれば、攻撃する側はそちらを狙う。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、外せるサービスでは弱い入口も外す。予備がないまま外すと、スマホをなくしたときに自分も入れなくなる。

偽のサイトは、そこを突いてくる。「パスキーが使えません。パスワードで入ってください」と出すのだ。いつもパスキーで入っているサービスで、パスワードやSMSの番号を求められたら、そこで止まる。

だから、土台はスマホの6桁と顔・指だ

ここまで積んだ守りは、どれもスマホ（とパソコン）の上に乗っている。パスワードを覚えるのも、パスキーの鍵を持つのも、端末だ。その端末を開ける6桁と顔・指が、全部の土台になる。

だから、次の「今日、設定する」は、端末そのものから始める。次に、メールの受け取り先と「〇〇でログイン」の元になっているアカウント。ここが開くと、ほかの全部が開くからだ。お金とSNSは、そのあとでいい。

それでも、パスキーでも防げないものがある

パスキーは、偽のサイトでのログインを防ぐ。入ったあとと、自分の手で開けてしまう扉は、守らない。だから、パスキーにしても「絶対に安全」ではない。乗っ取られにくさが、大きく上がるということだ。



入口の外で起きること

1. 電話で「画面を共有して」「このアプリを入れて」と言われ、自分の顔で認証してしまう
2. 端末に入った怪しいアプリが、ログインしたあとの画面を横取りする。言われて入れたアプリは、公式のストアのものでも危ない

1は、電話を一度切れば、多くは防げる。銀行・役所・警察・家族を名乗っても、お金や操作の話が出たら、切って、自分から公式の番号にかけ直す。家族とは、電話で確かめ合う合言葉を決めておく。

2は、アプリを公式のストアからだけ入れ、端末をいつも最新にしておくことで、入られにくくなる。ただ、画面を遠くから操作させるアプリは、公式のストアにもある。電話やメッセージで「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。

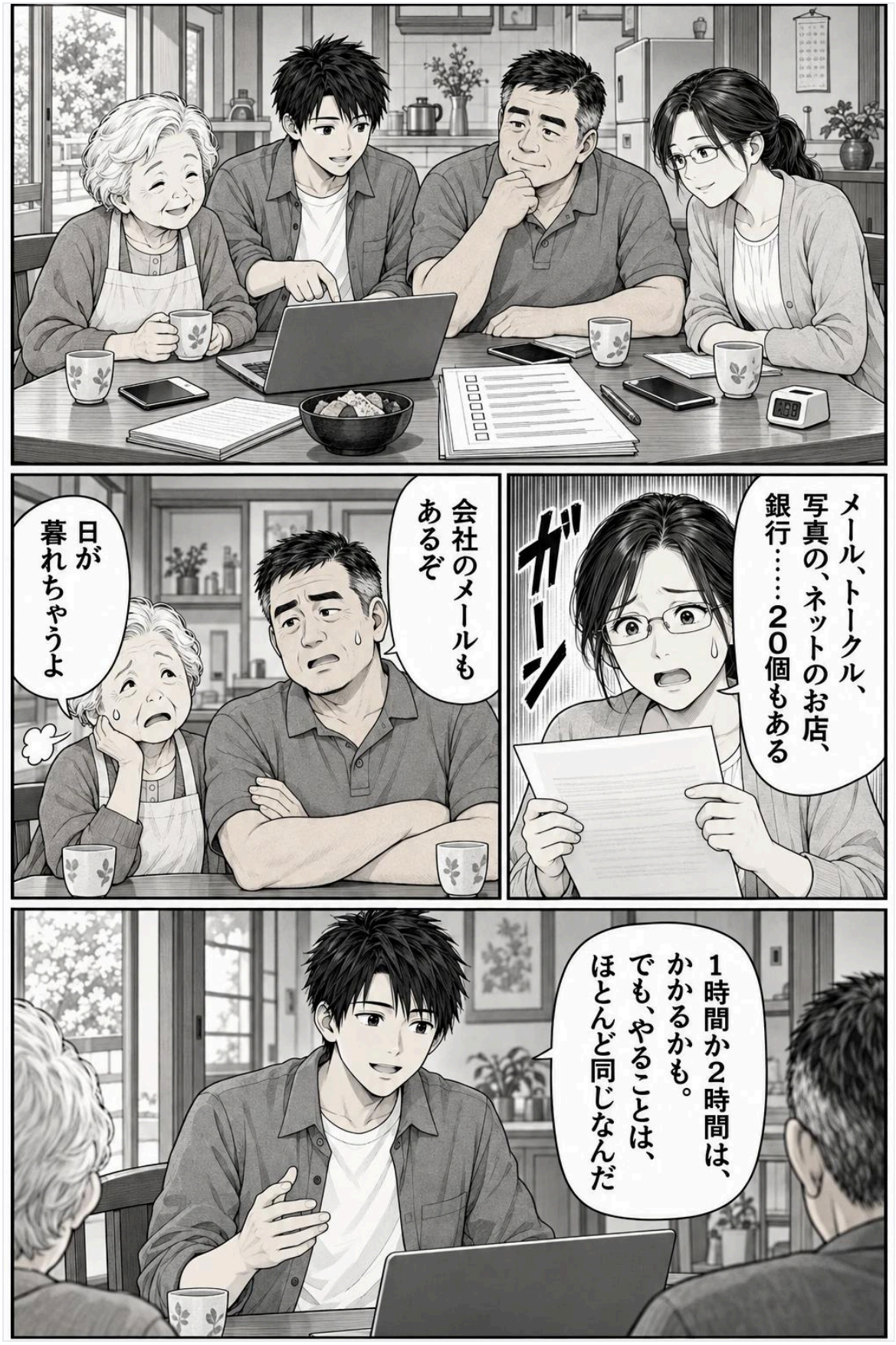
ほかに、本人のふりをして「スマホをなくした」とサービスの窓口に申し出て、アカウントを取り戻す手続きを悪用する手口もある。前の段の、予備の手段（再設定用の連絡先など）を、自分のものにしておくことが備えになる。

ここまでで、知っておくことは全部だ。次の回で、実際に設定する。

設定する

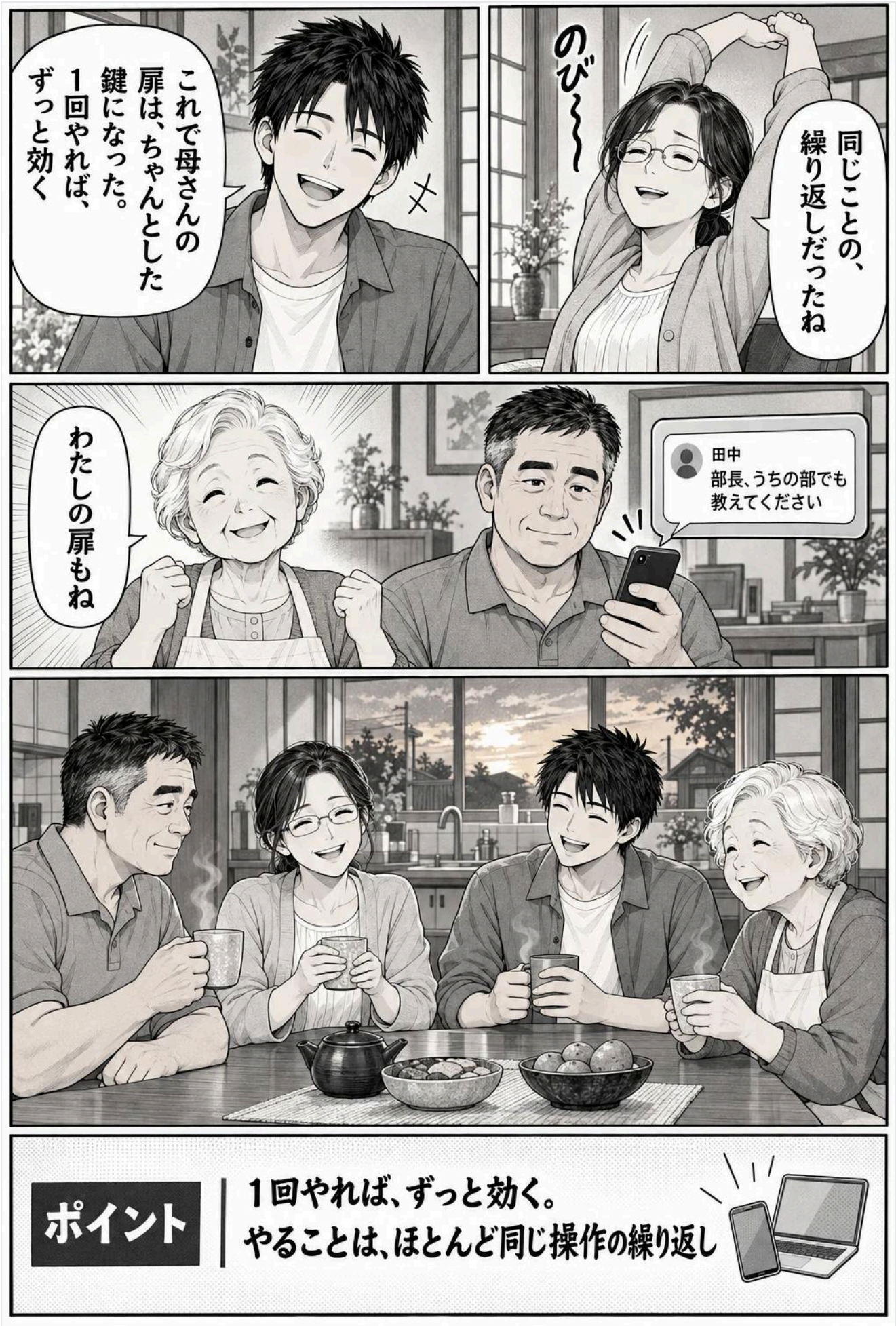
3　今日、設定する

漫画　ケンジさんの家と、本物にしか合わない鍵　第3話「1回やれば、ずっと効く鍵」




この3つの繰り返し
設定を開く
パスキーを作る
指か顔で確かめる
ピッ
パスキーを作成
パスキーを作成しました
……え、これだけ？


AAAッ
わたしのは、どこを押すの？
ばあちゃんのはAndroidだから、ここ
会社のメールは、その項目が無いぞ
会社のは、会社の管理者に聞いて。勝手に変えない
1:20


同じことの、
繰り返しだったね
のび〜〜
これで母さんの
扉は、ちゃんとした
鍵になった。
1回やれば、
ずっと効く
田中
部長、うちの部でも
教えてください
わたしの扉もね
ポイント
1回やれば、ずっと効く。
やることは、ほとんど同じ操作の繰り返し

順番は、端末そのもの → 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）→ 電話番号の元 → お金 → SNS。使っているものだけ、上から順に。済ませたら□に印を付け、日付を書いておく。もう設定してある所は、確かめるだけでいい。

端末そのもの
iPhone
済ませた日
月　日

いちばん強い方法　顔（Face ID）か指（Touch ID）と、6桁のパスコード

□ 画面ロックを、顔か指と6桁のパスコードにする

付ける

1. **設定**を開く
2. **Face IDとパスコード**をタップする（Face ID のない iPhone は**Touch IDとパスコード**）
3. **パスコードをオンにする**をタップする
4. 6桁のパスコードを入力する（**パスコードオプション**をタップすると、4桁の数字コード・カスタムの数字コード・カスタムの英数字コードに切り替えられる）
5. パスコードをもう一度入力して確定する
6. 【Face ID】照明の明るい場所で、**設定**の**Face IDとパスコード**から**Face IDを設定**をタップする
7. iPhone を縦向きに持ち、本体の前に顔が来るようにして**開始**をタップする
8. 顔がフレームの中に収まるようにし、頭をゆっくりと円を描くように動かす
9. 最初のスキャンが終わったら**続ける**をタップする
10. もう一度、円を描くようにして頭をゆっくりと動かす
11. **完了**をタップする
12. 【Touch ID の機種】**設定**で**Touch IDとパスコード**をタップしてパスコードを入力し、**指紋を追加**をタップする。センサーに指先を置き（ボタンは押さない）、画面の指示どおりに指を置いては上げるを繰り返す

画面に出ること・気をつけること
- **Face IDとパスコード**を開くと、パスコードの入力画面が表示された場合は入力する
- Face ID の設定中に頭を動かせない場合は**アクセシビリティオプション**をタップする
- Touch ID は、先にパスコードを作成しておく必要がある

□ 更新を自動にする

付ける

1. **設定**を開く
2. **一般**をタップする
3. **ソフトウェアアップデート**をタップする
4. **自動アップデート**をタップする
5. **自動インストール**と**自動ダウンロード**をオンにする
6. （今すぐ更新するとき）**ソフトウェアアップデート**の画面で、アップデートが提供されていれば**ダウンロードしてインストール**をタップし、画面の案内に従う

画面に出ること・気をつけること
- **自動インストール**：アップデートが提供されると、iPhoneが充電中で、Wi-Fiに接続されている夜間にダウンロード・インストールされる（公式の説明）
- 手動で入れる前に、iCloudまたはコンピュータでバックアップし、電源とWi-Fiにつなぐよう公式は案内している

□ なくしたときに探せるようにする

付ける

1. **設定**を開く
2. 自分の名前をタップし、**探す**をタップする
3. **iPhoneを探す**をタップし、**iPhoneを探す**をオンにする
4. **“探す”ネットワーク**をオンにする（オフラインのときでも探せるようにする）
5. **最後の位置情報を送信**をオンにする（バッテリー残量が少なくなったときに位置情報を Apple に送る）

画面に出ること・気をつけること
- サインインするよう求められた場合は、Apple Account の情報を入力する

□ パスワードを、端末に作らせて覚えさせる

付ける

1. **設定**を開き、自分の名前をタップしてから**iCloud**をタップする
2. **iCloudに保存済み**の下にある**パスワード**をタップする（iOS 17以前は**パスワードとキーチェーン**）
3. **このiPhoneを同期**をタップして、iCloudキーチェーンを有効にする
4. **設定**に戻り、**一般**→**自動入力とパスワード**の順に選ぶ
5. **パスワードとパスキーを自動入力**をオンにする
6. 保存したパスワードとパスキーは**パスワード**アプリで確かめる（iOS 18以降）

画面に出ること・気をつけること
- iCloudキーチェーンを有効にするとき、パスコードまたはApple Accountのパスワードの入力を求められる場合がある
- 事前に、ソフトウェアを最新にし、Apple Accountで2ファクタ認証を有効にしておく（公式の前提）

☐ 盗まれたときの保護（盗難デバイスの保護）をオンにする

付ける

1. **設定**を開いて、**Face IDとパスコード**をタップする
2. デバイスのパスコードを入力する
3. **盗難デバイスの保護**をタップして、**盗難デバイスの保護**をオンにする

画面に出ること・気をつけること

- 前提：Apple Accountで2ファクタ認証を使い、iPhoneでパスコード、Face IDまたはTouch ID、**利用頻度の高い場所**（位置情報サービス）を設定または有効にしておく
- 前提：**探す**を有効にしておく。**盗難デバイスの保護**が有効な間は**探す**を無効にできない
- **盗難デバイスの保護**はデフォルトで有効になっている可能性がある
- **利用頻度の高い場所**は**設定**→**プライバシーとセキュリティ**→**位置情報サービス**→**システムサービス**→**利用頻度の高い場所と経路**

☐ バックアップをオンにする（iCloudバックアップ）

付ける

1. 設定アプリを開いて、自分の名前（ユーザ名）をタップする
2. **iCloud**をタップしてから**iCloudバックアップ**をタップし、**この「デバイス**をバックアップ」がオンになっていることを確かめる
3. デバイスを電源とWi-Fiネットワークに接続し、画面をロックしておく（この状態で自動でバックアップされる）

気をつけること もう設定してある所は、確かめるだけで「済ませた」を押してよい。

公式の説明：https://support.apple.com/ja-jp/119586 https://support.apple.com/ja-jp/118575 https://support.apple.com/ja-jp/102648 https://support.apple.com/ja-jp/109016 https://support.apple.com/ja-jp/120340 https://support.apple.com/ja-jp/108366

端末そのもの Android

済ませた日 月 日

いちばん強い方法 指紋か顔と、画面ロック（PIN）

☐ 画面ロックを、指か顔と6桁以上のPINにする（パターンはのぞき見と指の跡に弱い）

付ける

1. 設定アプリを開く
2. **セキュリティとプライバシー**→**デバイスのロック解除**をタップする
3. **画面ロック**をタップする
4. 使いたい画面ロック（**PIN** **パターン** **パスワード**）を選び、画面上の手順に沿って操作する（PIN は 6 桁がおすすめ、と公式）
5. 【指紋】設定アプリで**セキュリティとプライバシー**→**デバイスのロック解除**→**指紋**をタップし、画面上の手順に沿って指紋をスキャンする
6. 【顔認証】設定アプリで**セキュリティとプライバシー**→**デバイスのロック解除**→**顔認証**をタップし、PIN・パターン・パスワードを入力する
7. **顔認証の設定**の情報を確かめて、**同意する**→**開始**をタップし、画面上の手順に沿って操作する
8. **完了**をタップする

画面に出ること・気をつけること

- すでにロックが設定されている場合は、別のロックを選ぶ前に PIN・パターン・パスワードの入力が必要
- 指紋を設定するとき、画面ロックがなければ予備の PIN・パターン・パスワードを追加するよう求められる
- 顔認証は Google Pixel 7 以降などが対象。顔認証は複雑な PIN・パターン・安全なパスワードより安全面で劣る可能性がある、と公式に注意書きがある

☐ 更新を自動にする

付ける

1. アップデートの通知が届いたら、通知を開いてアップデートの操作をタップする
2. （通知を消したとき・自分で確かめるとき）デバイスの設定アプリを開く
3. **システム**→**ソフトウェア アップデート**をタップする
4. 更新のステータスを確かめ、画面上の指示に沿って操作する
5. （適用状況の確認）設定アプリで**デバイス情報**→**Android バージョン**をタップし、**Android セキュリティ アップデート** **Google Play システム アップデート**を確かめる

画面に出ること・気をつけること

- 公式：ほとんどのシステム アップデートとセキュリティ パッチは自動的にインストールされる
- アップデートの前に Wi-Fi に接続し、75% 以上充電しておく
- Pixel では、インストールされたアップデートは次回の再起動時に有効になる

☐ なくしたときに探せるようにする

付ける

1. 設定アプリを開き、**パスワード、パスキー、アカウント**をタップして、Google アカウントのメールアドレスが表示されていることを確かめる
2. 設定アプリで**位置情報**をタップし、**位置情報の使用**をオンにする
3. 設定アプリで**セキュリティ**→**Find Hub**をタップし、**デバイスの場所の特定を許可**がオンになっていることを確かめる
4. 設定アプリで**Google**→**すべてのサービス**（このタブがある場合）→**Find Hub**をタップする
5. **オフラインのデバイスを探す**をタップし、**人通りの多い場所でのみネットワークを使用する**または**どこでもネットワークを使用する**を選ぶ
6. 別の端末から android.com/find にアクセスし、Google アカウントにログインして、デバイスが表示されるか確かめる

画面に出ること・気をつけること

- オフラインのデバイスを探すには、PIN・パターン・パスワードのいずれかの画面ロックが必要
- Google Play で非表示にしているデバイスは Find Hub にも表示されない（play.google.com/library/devices の**メニューに表示する**を確かめる）
- 紛失時に遠隔でロック・消去するには 2 段階認証プロセスを有効にし、バックアップ コードを用意しておく、と公式

☐ パスワードを、端末に作らせて覚えさせる

付ける

1. Android デバイスで Chrome を開く
2. その他アイコン →**設定**をタップする
3. **自動入力とパスワード**→**自動入力の設定**をタップし、**Google 自動入力**を選ぶ（変更したら**Chrome を再起動する**をタップ）
4. **自動入力とパスワード**→**Google パスワード マネージャー**をタップする
5. 右下の**設定**をタップし、**パスワードを保存できるようにする**をオンにする
6. サイトで新しいパスワードを入力して保存を尋ねられたら**保存**をタップする
7. 【パスキー】
   myaccount.google.com/signinoptions/passkeys にアクセスし、**パスキーを作成する**→**パスキーを作成**をタップして、デバイスのロックを解除する

画面に出ること・気をつけること

- パスキーを作成すると、パスキー優先（パスワードなし）のログイン方法に切り替わる。自分が所有し使っているデバイスでのみ作成する（共有デバイスでは作らない）
- パスキーを作る前にスマートフォンの画面ロックをオンにする
- 保存したログイン情報を守るため、再設定用情報を追加し、2 段階認証プロセスを有効にすることをおすすめ、と公式

☐ バックアップをオンにする（バックアップ）

付ける

1. デバイスの設定アプリを開く
2. **Google**→**すべてのサービス**をタップする
3. **バックアップと復元**で**バックアップ**をタップし、バックアップをオンにする（**写真と動画**、**デバイスのデータ**を選べる）

気をつけること 画面の名前は機種で違う（ここはGoogle Pixelの表記）。見当たらないときは、設定の上の虫めがねで「画面ロック」「バックアップ」などと探す。パターンで開けている人は、6桁以上のPINに替えると、のぞき見に強くなる。

公式の説明：https://support.google.com/pixelphone/answer/2819522?hl=ja https://support.google.com/android/answer/7680439?hl=ja https://support.google.com/android/answer/3265955?hl=ja https://support.google.com/chrome/answer/95606?hl=ja&co=GENIE.Platform%3DAndroid https://support.google.com/android/answer/2819582?hl=ja

端末そのもの Mac

済ませた日 月 日

いちばん強い方法 指（Touch ID）と、ログインのパスワード

☐ 画面ロックを、指（Touch ID）とログインのパスワードにする

付ける

1. アップルメニュー →**システム設定**を選び、サイドバーで**ロック画面**をクリックする（下にスクロールが必要な場合がある）
2. **スクリーンセーバの開始後またはディスプレイがオフになったあとにパスワードを要求**で、パスワードが必要になるまでの時間を選ぶ
3. **バッテリー駆動時に使用していない場合はディスプレイをオフにする** **電源アダプタ接続時に使用していない場合はディスプレイをオフにする**の時間を選ぶ
4. 【Touch ID 搭載機】アップルメニュー →**システム設定**を選び、サイドバーで**Touch IDとパスワード**をクリックする
5. **指紋を追加**をクリックして、パスワードを入力し、画面に表示される指示に従う
6. Touch ID の使い方で**Macのロックを解除する**をオンにする

画面に出ること・気をつけること

- Touch ID の指紋の追加時にパスワード（Mac にログインするパスワード）の入力を求められる
- Mac の起動時、48 時間ごと、指紋認証に 5 回失敗したときなどはパスワードの再入力が必要

☐ 更新を自動にする

付ける

1. システム設定アプリを開く
2. サイドバーで**一般**をクリックする（下にスクロールが必要な場合がある）
3. **ソフトウェアアップデート**をクリックする
4. **自動アップデート**の横にある ⓘ をクリックする
5. **新しいアップデートがある場合はダウンロード**をオンにする
6. **macOSアップデートをインストール**をオンにする
7. **セキュリティ対応とシステムファイルをインストール**をオンにする
8. **完了**をクリックする

画面に出ること・気をつけること

- ノートブックは、アップデートを自動でダウンロードするには電源アダプタにつないでおく必要がある
- 手動でインストールするときは、管理者パスワード（Mac にログインする際のパスワード）の入力を求められる

☐ なくしたときに探せるようにする

付ける

1. アップルメニュー から**システム設定**を選ぶ
2. ユーザ名をクリックし、**iCloud**をクリックする
3. **すべて見る**をクリックする
4. 下にスクロールして**Macを探す**をクリックする
5. **オンにする**をクリックする

画面に出ること・気をつけること

- Apple Accountのパスワードの入力画面が表示されたら入力し、**オンにする**をクリックする
- Macの現在位置の使用を**Macを探す**に許可するかどうか確認するメッセージが表示されたら**許可**をクリックする
- 地図上で探すには、**探す**の位置情報サービスがオンになっている必要がある

☐ パスワードを、端末に作らせて覚えさせる

付ける

1. アップルメニュー から**システム設定**を選ぶ
2. ユーザ名をクリックし、**iCloud**をクリックする
3. **パスワード**をクリックする（macOS Sonoma以前は**パスワードとキーチェーン**）
4. **このMacを同期**をクリックし、**完了**をクリックする
5. **システム設定**で**一般**→**自動入力とパスワード**を選び、**パスワードとパスキーを自動入力**をオンにする
6. 保存したパスワードとパスキーは**パスワード**アプリで確かめる（macOS Sequoia以降）

画面に出ること・気をつけること

- 事前に、ソフトウェアを最新にし、Apple Accountで2ファクタ認証を有効にしておく（公式の前提）
- Apple Accountへのサインイン時に**あとで承認**を選んだ場合は、画面の指示に従って古いパスコードか別のデバイスで承認する

☐ バックアップをオンにする（Time Machine）

付ける

1. USBドライブなど外付けのストレージデバイスをMacに接続する（容量はMacの2倍以上が目安。Time Machine専用にする）
2. Appleメニューから**システム設定**を選ぶ
3. サイドバーで**一般**をクリックし、右側で**Time Machine**をクリックする
4. **バックアップディスクを追加**をクリックする
5. 接続したストレージデバイスを選び、**ディスクを設定**をクリックする（**バックアップを暗号化**を有効にするとパスワードを作る）

気をつけること もう設定してある所は、確かめるだけで「済ませた」を押してよい。

公式の説明：https://support.apple.com/ja-jp/guide/mac-help/mh11784/mac https://support.apple.com/ja-jp/guide/mac-help/mchlpx1065/mac https://support.apple.com/ja-jp/102648 https://support.apple.com/ja-jp/109016 https://support.apple.com/ja-jp/104984

端末そのもの Windows

済ませた日 月 日

いちばん強い方法 Windows Hello（顔・指紋・PIN）

☐ Windows Hello（顔・指紋・PIN）でサインインする。PINは6桁以上に

付ける

1. 設定アプリで**アカウント**→**サインイン オプション**を選ぶ
2. **サインインする方法**で、**PIN (Windows Hello)**を選ぶ
3. **設定**を選び、指示に従って設定を終える
4. 指紋リーダーがある PC は**指紋認識 (Windows Hello)**を、Hello 対応カメラがある PC は**顔認識 (Windows Hello)**を選び、同じく**設定**を選んで指示に従う

画面に出ること・気をつけること

- 顔認証でサインインするには Hello 対応カメラ、指紋認証には指紋リーダーが必要
- 次回のサインインから、パスワードの代わりに顔認識・指紋認証・PIN を選べる

☐ 更新を自動にする

付ける

1. **スタート**→**設定**→**Windows Update**を選ぶ
2. **最新の更新プログラムが利用可能になったらすぐに入手する**のトグルをオンにする
3. **Windows 更新プログラムの確認**を選ぶ
4. 利用できる更新プログラムがある場合は**ダウンロード & インストール**を選ぶ
5. 再起動を求められたら、デバイスを再起動する

画面に出ること・気をつけること

- 公式：Windows 11 では、更新プログラムが自動的にダウンロード・インストールされる。トグルがオフでも通常のセキュリティ更新プログラムは適用される（トグルはセキュリティ以外の更新をいち早く受け取るためのもの）
- トグルをオンにすると、1 か月あたりの再起動が増える場合がある
- 従量制課金接続では、一部の更新プログラムは自動的にインストールされない

▢ なくしたときに探せるようにする

付ける

1. Microsoft 個人用アカウントで PC にサインインする（アカウントの種類は**管理者**）
2. **デバイスの検索**の設定をオンにする（公式ページの**「デバイスの検索」設定を開く**」リンクから開ける）
3. デバイスの位置情報をオンにしておく
4. （確かめ方・なくしたとき）account.microsoft.com/devices に移動してサインインし、**デバイスの検索**タブを選ぶ
5. 探すデバイスを選び、**検索**を選んで地図を表示する

画面に出ること・気をつけること

- 使う前にオンにしておく必要があり、アカウントの種類は**管理者**である必要がある
- 管理者がデバイスを探すと、そのデバイスを使っている人の通知領域に毎回通知が出る
- 遠隔ロックは地図でデバイスが見つかったら**ロック**→**次へ**

▢ パスワードを、端末に作らせて覚えさせる

付ける

1. Microsoft Edge で**設定など**→**パスワード**を選ぶ
2. **パスワードとパスキーの保存前にメッセージを表示する**をオンにする
3. サインインが必要なサイトで、Edge がユーザー名とパスワードを記憶するか尋ねたら保存する
4. 【パスキー】サイトにサインインしてパスキーの作成・保存を求められたら、**続行**または**作成**を選ぶ（推奨の保存先）。保存先を選ぶときは**変更**または**保存**を選ぶ
5. 保存先（パスワード マネージャー＝Microsoft パスワード マネージャーなど／iPhone・iPad・Android デバイス／セキュリティ キー／Windows デバイス・Windows Hello）を選び、顔認識・指紋・PIN などで保存を終える
6. （パスキーへの自動アップグレード）Edge で**設定**→**Passwords とオートフィル**を選び、**Microsoft パスワード マネージャー**→**その他の設定**→**パスキーに自動的にアップグレードする**をオンにする

画面に出ること・気をつけること

- パスキーの作成時に、顔認識・指紋・PIN などのロック解除を求められる場合がある
- Microsoft アカウント自体のパスキーは account.live.com/proofs/manage で**新しいサインイン方法の追加**または**確認**から作る
- サインイン時にパスキーの作成・保存を求められないサイトは、まだ対応していない

▢ バックアップをオンにする（Windows バックアップ）

付ける

1. Microsoft アカウントでサインインする（設定アプリ → **アカウント**→**ユーザーの情報**。ローカルアカウントなら**Microsoft アカウントでのサインインに切り替える**）
2. **スタート**を選び、**backup**と入力して、結果から**Windows バックアップ**を選ぶ
3. **フォルダー**を展開し、デスクトップ、ドキュメント、ピクチャ、ビデオ、ミュージックのスイッチをオンにする
4. 設定と基本設定（インストール済みのアプリ、アカウント・Wi-Fi ネットワーク・パスワード など）を**オン**にする
5. **バックアップ**を選ぶ

気をつけること 会社から渡されたパソコンは、会社の管理者の決まりに従う。自分で設定を変えず、会社の担当者に聞く。

公式の説明：https://support.microsoft.com/ja-jp/windows/security/configure-windows-hello https://support.microsoft.com/ja-jp/windows/deployment/updates-lifecycle/get-windows-updates-as-soon-as-they-re-available-for-your-device https://support.microsoft.com/ja-jp/accounts-billing/security/find-and-lock-a-lost-windows-device https://support.microsoft.com/ja-jp/edge/save-or-forget-passwords-in-microsoft-edge https://support.microsoft.com/ja-jp/help/17143

合鍵のアカウント

Google アカウント

済ませた日
月　日

いちばん強い方法 パスキー

付ける

ブラウザ（myaccount.google.com）

1. myaccount.google.com/signinoptions/passkeys にアクセス（ログインや本人確認を求められることがある）
2. **パスキーを作成する**→**パスキーを作成**をタップ
3. デバイスのロックを解除する（指紋・顔・画面ロック）
4. iPhone・iPad・Mac で iCloud キーチェーンがまだ設定されていないときは、有効にするよう求められる
5. 複数のデバイスで使うときは、デバイスごとに同じ手順を繰り返す

別のやり方：もっと強くしたい人：セキュリティキー（別に買う鍵）

1. myaccount.google.com/signinoptions/passkeys にアクセス
2. **パスキーを作成する**→**別のデバイスを使用**をタップ
3. 画面上の指示に沿って、キーを挿入して PIN を入力するか、キーの指紋認証センサーをタップ

確かめる

ブラウザ（myaccount.google.com）

1. myaccount.google.com/signinoptions/passkeys にアクセス
2. 求められた場合は本人確認を行う（複数のアカウントにログインしているときは目的のアカウントで）
3. 登録済みのパスキーがログイン オプションに表示される

弱い入口を外す

狙われやすい人だけ：高度な保護機能（ふつうは要らない。入れるなら、セキュリティキー2本か、パスキーを2台以上に用意してから）

1. 先に、再設定用の電話番号とメールアドレスを追加し、2段階認証プロセスを有効にしておく
2. セキュリティ キーを使う場合は、対応するキーを購入する（予備にもう 1 つ以上）
3. 公式ヘルプの**高度な保護機能を有効**のリンク（account.google.com/advanced-protection/enroll/details）を開く
4. 画面上の手順に沿って高度な保護機能を有効にする（パスキーかセキュリティ キーで登録）

会社のアカウントなら 会社や学校のGoogleアカウント（Google Workspace）は、管理者が使える方法を決めていることがある。パスキーだけで入れないときや、項目が見当たらないときは、会社の管理者に聞く。

気をつけること パスキーを作っても、パスワードとSMSの入口は残る。家族と共有している端末には、パスキーを作らない。

なくしたときの備え 8桁のバックアップコード（10個）を印刷して、大事な書類と一緒にしまう。パスキーは2台以上の端末に作っておく。

公式の説明：https://support.google.com/accounts/answer/13548313?hl=ja https://support.google.com/accounts/answer/185839?hl=ja https://support.google.com/accounts/answer/183723?hl=ja https://support.google.com/accounts/answer/1187538?hl=ja https://support.google.com/accounts/answer/185834?hl=ja https://support.google.com/accounts/answer/7519408?hl=ja https://support.google.com/accounts/answer/7539956?hl=ja

合鍵のアカウント

Apple アカウント

済ませた日
月　日

いちばん強い方法 2ファクタ認証。もっと強くするならセキュリティキー（2本）

付ける

iPhone・iPad・Mac

1. **設定**（Macは**システム設定**）を開き、いちばん上の自分の名前を押す
2. **サインインとセキュリティ**を押す
3. **2ファクタ認証**が**オン**になっているか確かめる。オフなら、オンにする

iPhone（設定アプリ）

1. 設定アプリを開く
2. 自分のユーザ名をタップし、**サインインとセキュリティ**をタップ
3. **2ファクタ認証**をタップ
4. **セキュリティキー**をタップし、**セキュリティキーを追加**をタップ。画面の案内にそってキーを追加（2 本以上）
5. Apple Account に関連付けられているデバイスを確かめ、**すべてのアクティブなデバイスでサインイン状態を維持する**か、今後使わないデバイスを選んでサインアウトする

Mac（システム設定）

1. Appleメニューから**システム設定**を選び、自分のユーザ名をクリック
2. **サインインとセキュリティ**をクリックし、**2ファクタ認証**をクリック
3. **セキュリティキー**の横にある**設定**をクリックし、画面の案内にそってキーを追加（2 本以上）
4. 関連付けられているデバイスを確かめ、**すべてのデバイスでサインイン状態を維持する**か、今後使わないデバイスを選んでサインアウトする

弱い入口を外す

ウェブ（account.apple.com）

1. account.apple.com にアクセス
2. **サインインとセキュリティ**→**アカウントのセキュリティ**の順に選ぶ
3. **信頼できる電話番号**セクションで、使っていない電話番号を削除する（1 つは残す）

気をつけること Appleのアカウントは、ほとんどが最初から2ファクタ認証になっている。使っていない古い電話番号は消しておく。

なくしたときの備え セキュリティキーを使うなら、自宅と職場など別の場所に分けて置く。全部なくすと入れなくなる。

公式の説明：https://support.apple.com/ja-jp/102660 https://support.apple.com/ja-jp/102637 https://support.apple.com/ja-jp/122621 https://support.apple.com/ja-jp/guide/icloud/mm281e3e7d/icloud

合鍵のアカウント
Microsoft アカウント

済ませた日
月　日

いちばん強い方法 パスキー。できればパスワードを外す

付ける

ブラウザ（account.live.com/proofs/manage）

1. パスキーを作るデバイスで、account.live.com/proofs/manage（Microsoft アカウントの高度なセキュリティ オプション）にサインインする
2. **新しいサインイン方法の追加**または**確認**を選ぶ
3. **Face**／**フィンガープリント**／**PIN**／**セキュリティ キー**のいずれかを選ぶ
4. デバイスの指示に従う
5. **続行**または**作成**を選んで推奨の場所に保存する（別の保存場所にするときは**変更**または**保存**）
6. 顔・指紋・PIN などで保存を完了する

画面に出ること・気をつけること

- **サインインするパスキーを作成する**→**続行**または**作成**

確かめる

ブラウザ（account.live.com/proofs/manage）

1. account.live.com/proofs/manage（詳細セキュリティ オプション）にサインインする
2. パスキーを含むすべてのサインイン検証方法が一覧に出る。パスキーはパスキーのアイコンで表示される
3. パスキーの欄を展開すると、保存場所（デバイスや Microsoft パスワード マネージャーなど）と最後に使われた時刻が見られる

弱い入口を外す

パスワードを外す（パスワードレス アカウント）

1. Microsoft Authenticator アプリ（または Outlook for Android）を入れ、アプリでアカウントを設定する
2. Microsoft アカウントの**追加のセキュリティ オプション**にサインインする
3. **パスワードレス アカウント**で**オンにする**を選ぶ
4. 画面の指示に従ってアカウントを確認する
5. 認証アプリに送られた要求を承認する

別のやり方：電話番号（SMS）を外す

1. Microsoft アカウントの**追加のセキュリティ オプション**ページにサインインする
2. 外す電話番号の確認オプションを展開し、**削除**を選ぶ
3. 30 日後に削除されることを確かめるチェック ボックスをオンにして、**削除のスケジュール**を選ぶ

会社のアカウントなら 会社のMicrosoft 365のアカウントは、組織が許可したときだけパスキーを作れる。項目が見当たらなければ、会社のヘルプデスクに聞く。

気をつけること パスキーを消すときは、先に別の方法を足してから。

なくしたときの備え 確かめ済みのメールアドレスを足し、パスキーも設定しておく。

公式の説明：https://support.microsoft.com/ja-jp/accounts-billing/security/create-save-passkey https://support.microsoft.com/ja-jp/accounts-billing/security/manage-your-saved-passkeys https://support.microsoft.com/ja-jp/accounts-billing/security/how-to-go-passwordless-with-your-microsoft-account https://support.microsoft.com/ja-jp/accounts-billing/manage/microsoft-to-stop-sending-sms-codes-for-personal-accounts https://support.microsoft.com/ja-jp/accounts-billing/manage/removing-a-sign-in-verification-method https://support.microsoft.com/ja-jp/accounts-billing/manage/microsoft-account-security-info-verification-codes https://support.microsoft.com/ja-jp/accounts-billing/security/how-to-use-two-step-verification-with-your-microsoft-account https://support.microsoft.com/ja-jp/accounts-billing/security/what-are-passkeys-why-they-matter

合鍵のアカウント
Yahoo! JAPAN ID

済ませた日
月　日

いちばん強い方法 パスキー。付けたらパスワードを無効に

付ける

iPhone（ブラウザ（Safari・Google Chrome・Firefox））

1. **パスキーの設定**ページ（https://account.edit.yahoo.co.jp/authdevice）を開く
2. **パスキーを追加**を押す
3. 指紋・顔認証をする
4. **追加が完了しました**と出れば完了

別のやり方：iPhone（Yahoo! JAPAN 公式アプリ（対象のアプリ））

1. 対象の公式アプリを開く
2. **指紋・顔・パスコード認証**または**パスキーの設定**を選ぶ
3. **指紋・顔・パスコード認証**なら**設定する**を押す。**パスキーの設定**なら**パスキーを追加**を押して認証する

Android（ブラウザ（Google Chrome））

1. **パスキーの設定**ページ（https://account.edit.yahoo.co.jp/authdevice）を開く
2. **パスキーを追加**を押す
3. 指紋・顔・画面ロック認証をする
4. **追加が完了しました**と出れば完了

別のやり方：Android（Yahoo! JAPAN 公式アプリ（対象のアプリ））

1. 対象の公式アプリを開く
2. マイページや設定で**指紋・顔・画面ロック認証**または**パスキーの設定**を選ぶ
3. **指紋・顔・画面ロック認証**なら**設定する**を押して認証する。**パスキーの設定**なら**パスキーを追加**を押して認証する

Mac（ブラウザ（Google Chrome・Safari））

1. 先に Mac で Touch ID を設定しておく
2. **パスキーの設定**ページ（https://account.edit.yahoo.co.jp/authdevice）を開く
3. **パスキーを追加**を押す
4. 画面の指示に従って認証する
5. **追加が完了しました**と出れば完了

Windows（ブラウザ（Microsoft Edge・Google Chrome・Firefox。シークレットモードは不可））

1. 先に Windows Hello（顔認識・指紋認証・PIN のどれか）を設定しておく
2. **パスキーの設定**ページ（https://account.edit.yahoo.co.jp/authdevice）を開く
3. **パスキーを追加**を押す
4. 画面の指示に従って認証する
5. **追加が完了しました**と出れば完了

> **画面に出ること・気をつけること**
> - **このサイトへのセキュリティキーを表示できるようにしますか**→**許可**（推奨。**スキップ**でも登録はできる。Windows 10 を最新にすると出ない）

確かめる

ブラウザ

1. **パスキーの設定**ページ（https://account.edit.yahoo.co.jp/authdevice）を開く
2. **ご利用可能なパスキー**に出ているものが使えるパスキー

弱い入口を外す

ブラウザ

1. 先に**SMS認証**を設定しておく（https://account.edit.yahoo.co.jp/manage_msn?src=id）
2. Yahoo! JAPAN ID ガイドの**パスワード無効設定**で**今すぐ設定する**を押し、設定ページ（https://account.edit.yahoo.co.jp/password?src=id）を開く
3. **無効にする**を選ぶと完了

気をつけること パスキーを付けても、パスワードのログインは残る。下の「弱い入口を外す」で無効にする。家族と共有している端末には登録しない。

なくしたときの備え 機種変更や初期化の前に、ほかにログインに使えるパスキーが残っているか確かめる。

公式の説明：https://support.yahoo-net.jp/SccLogin/s/article/H000004626 https://support.yahoo-net.jp/PccLogin/s/article/H000014121 https://id.yahoo.co.jp/security/manage_auth_device_ios.html https://id.yahoo.co.jp/security/inactive_pw.html https://id.yahoo.co.jp/security/otp.html https://www.lycorp.co.jp/ja/news/release/020333/

合鍵のアカウント

LINE アカウント

済ませた日 月 日

いちばん強い方法 パスキー。「メールアドレス・パスワードでログイン」はオフ

付ける

iPhone（LINE アプリ）

1. LINE アプリで**設定**をタップ
2. **アカウント**をタップ
3. **パスキー**をタップ
4. **パスキーを作成**をタップ
5. 画面の案内に沿って顔認証または指紋認証をする

Android（LINE アプリ）

1. LINE アプリで**設定**をタップ
2. **アカウント**をタップ
3. **パスキー**をタップ
4. **パスキーを作成**をタップ
5. 画面の案内に沿って顔認証または指紋認証をする

Mac（パソコン版 LINE（スマホの生体認証でログイン。パソコン版 6.5.0 以上・スマホ版 10.18.0 以上））

1. スマホ本体で生体情報を設定しておく（iPhone は**設定**＞**Touch ID/Face ID**、Android は**設定**＞**セキュリティ**）
2. スマホ版 LINE で**設定**＞**アカウント**を開き、iPhone は**Face ID, Touch ID**、Android は**生体情報**をタップ
3. **許可する**をタップし、生体情報で認証する
4. **アカウント**画面の**ログイン許可**をオンにする
5. パソコン版 LINE で電話番号を入力し、**スマートフォンを使ってログイン**をクリック
6. 案内を確かめて**認証番号を確認する**を押す
7. スマホで**設定**＞**アカウント**＞**他の端末と連携**をタップし、パソコンに出た 6 桁の番号を入力
8. スマホに出た端末情報を確かめて**ログイン**をタップし、生体情報で認証する（2 回目からは 5 と 8 だけ）

Windows（パソコン版 LINE（スマホの生体認証でログイン。パソコン版 6.5.0 以上・スマホ版 10.18.0 以上））

1. スマホ本体で生体情報を設定しておく（iPhone は**設定**＞**Touch ID/Face ID**、Android は**設定**＞**セキュリティ**）
2. スマホ版 LINE で**設定**＞**アカウント**を開き、iPhone は**Face ID, Touch ID**、Android は**生体情報**をタップ
3. **許可する**をタップし、生体情報で認証する
4. **アカウント**画面の**ログイン許可**をオンにする
5. パソコン版 LINE で電話番号を入力し、**スマートフォンを使ってログイン**をクリック
6. 案内を確かめて**認証番号を確認する**を押す
7. スマホで**設定**＞**アカウント**＞**他の端末と連携**をタップし、パソコンに出た 6 桁の番号を入力
8. スマホに出た端末情報を確かめて**ログイン**をタップし、生体情報で認証する（2 回目からは 5 と 8 だけ）

確かめる

iPhone（LINE アプリ）

1. **設定**＞**アカウント**＞**パスキー**を開く
2. 登録したパスキーが一覧に出ていれば付いている（登録・削除のたびに本人宛てに通知が届く）

Android（LINE アプリ）

1. **設定**＞**アカウント**＞**パスキー**を開く
2. 登録したパスキーが一覧に出ていれば付いている（登録・削除のたびに本人宛てに通知が届く）

弱い入口を外す

iPhone（LINE アプリ）

1. スマホ版 LINE で**設定**＞**アカウント**を開く
2. **メールアドレス・パスワードでログイン**をオフにする

Android（LINE アプリ）

1. スマホ版 LINE で**設定**＞**アカウント**を開く
2. **メールアドレス・パスワードでログイン**をオフにする

気をつけること パスキーは2026年11月から順に使えるようになっている。項目が見当たらなければ、まだ届いていない。パスキーを作れるのはスマホのアプリだけ。

なくしたときの備え 機種変更の前に、トーク履歴のバックアップと、バックアップ用の6桁のPINを用意する。

公式の説明：https://guide.line.me/ja/account-and-settings/passkey.html https://guide.line.me/ja/security/bio-auth.html https://guide.line.me/ja/account-and-settings/account-transfer.html https://help.line.me/line/smartphone/?contentId=20000104&lang=ja https://www.lycorp.co.jp/ja/news/release/020967/

電話番号の元（携帯会社）

dアカウント（ドコモ）

済ませた日 月 日

いちばん強い方法 パスキーと、「いつもパスキー設定」

付ける

iPhone（ブラウザ（ドコモ回線の契約がある人））

1. **パスキー端末設定のお手続きへ進む**を押す（**ログイン**が出たら案内に従ってログイン）
2. **パスキー端末設定**を押す
3. 本人認証：モバイル回線ならネットワーク暗証番号（4桁）を入れて**次へ**。Wi-Fi で、ほかに設定済みの端末があれば**本人確認へ**を押し、出た QR コードを設定済みの端末で読み取ってパスキー認証
4. 確認画面で**次へ**を押す
5. 画面の指示に従ってパスキーを登録する

別のやり方：iPhone（ブラウザ（ドコモ回線の契約がない人））

1. **パスキー端末設定のお手続きへ進む**を押す（**ログイン**が出たら案内に従ってログイン）
2. **パスキー端末設定**を押す
3. 連絡先携帯電話番号で**セキュリティコードを送信**を押し、届いたコードを入れて**次へ**。続けて連絡先メールアドレスでも同じようにする（コードが自動入力されたときは省略）。最後に**次へ**
4. 画面の指示に従ってパスキーを登録する
5. **「パスキー端末設定**が完了しました。」と出れば完了

Android（ブラウザ（ドコモ回線の契約がある人））

1. **パスキー端末設定のお手続きへ進む**を押す（**ログイン**が出たら案内に従ってログイン）
2. **パスキー端末設定**を押す
3. 本人認証：モバイル回線ならネットワーク暗証番号（4桁）を入れて**次へ**。Wi-Fi で、ほかに設定済みの端末があれば**本人確認へ**を押し、出た QR コードを設定済みの端末で読み取ってパスキー認証
4. 確認画面で**次へ**を押す
5. 画面の指示に従ってパスキーを登録する

別のやり方：Android（ブラウザ（ドコモ回線の契約がない人））

1. **パスキー端末設定のお手続きへ進む**を押す（**ログイン**が出たら案内に従ってログイン）
2. **パスキー端末設定**を押す
3. 連絡先携帯電話番号で**セキュリティコードを送信**を押し、届いたコードを入れて**次へ**。続けて連絡先メールアドレスでも同じようにする（コードが自動入力されたときは省略）。最後に**次へ**
4. 画面の指示に従ってパスキーを登録する
5. **「パスキー端末設定**が完了しました。」と出れば完了

Mac（パソコンのブラウザ（スマホのパスキーで QR コード認証。macOS 13 以上の Safari））

1. 先にスマホでパスキー端末設定をしておく
2. パソコンとスマホの両方で Bluetooth をオンにする
3. ログイン画面で ID を入れて**次へ**をクリック
4. パソコンに出た QR コードをスマホで読み取る
5. スマホの画面ロック解除の方法（顔・指紋・PIN など）で認証すると、パソコンでログインできる

Windows（パソコンのブラウザ（スマホのパスキーで QR コード認証。Windows 11 以上の Edge・Chrome 122 以上））

1. 先にスマホでパスキー端末設定をしておく
2. パソコンとスマホの両方で Bluetooth をオンにする
3. ログイン画面で ID を入れて**次へ**をクリック
4. パソコンに出た QR コードをスマホで読み取る
5. スマホの画面ロック解除の方法（顔・指紋・PIN など）で認証すると、パソコンでログインできる

確かめる

iPhone（ブラウザ）

1. **パスキー端末設定のお手続きへ進む**を押す
2. **登録済みの端末**に機種名が出ていれば設定済み（設定が終わったときは、登録したメールアドレスか SMS に完了の通知が届く）

Android（ブラウザ）

1. **パスキー端末設定のお手続きへ進む**を押す
2. **登録済みの端末**に機種名が出ていれば設定済み（設定が終わったときは、登録したメールアドレスか SMS に完了の通知が届く）

弱い入口を外す

ブラウザ

1. 先に、使う端末でパスキー端末設定をしておく
2. **「いつもパスキー設定**のお手続きへ進む」を押す（https://id.smt.docomo.ne.jp/aif/auth/flow/v1.0/always-passkeys-set。**ログイン**が出たら案内に従ってログイン）
3. **設定する**を選ぶ
4. **次へ**を押し、画面の指示に従ってパスキー認証をする（ドコモ回線の契約があればネットワーク暗証番号でも可）
5. **いつもパスキー設定完了**と出れば完了

気をつけること パスキーはスマホで設定する。家族が使う端末には付けない。「いつもパスキー設定」をすると、パスワードでは入れなくなる。

なくしたときの備え 画面ロックは人に当てられにくいものに。パスキーが使えないときは、連絡先のメールか携帯に届くコードで解除できる。

公式の説明：https://www.docomo.ne.jp/service/bio/ https://id.smt.docomo.ne.jp/src/utility/passkeys.html https://id.smt.docomo.ne.jp/src/utility/regpasskey_flow.html https://id.smt.docomo.ne.jp/src/utility/passwordless_flow_web.html https://id.smt.docomo.ne.jp/src/utility/passwordless_flow2_web.html https://id.smt.docomo.ne.jp/src/utility/passwordless.html https://id.smt.docomo.ne.jp/src/utility/passwordless_flow_app.html https://id.smt.docomo.ne.jp/src/utility/use_passkey_pc_qr.html https://id.smt.docomo.ne.jp/src/utility/twostepauth.html

電話番号の元（携帯会社）
au ID
済ませた日
月　日

いちばん強い方法 指紋・顔認証によるログイン（パスキーと同じ仕組み）

付ける

iPhone（ブラウザ（Safari））

1. au／UQ mobile／povo1.0 の回線の au ID なら、Wi-Fi をオフにしてご契約中の回線で接続する
2. **au ID会員情報サイト**にアクセスし、**指紋・顔認証によるログイン設定**から au ID でログインする
3. **この端末を登録する**をタップする
4. **次へ**をタップする
5. **次へ**をタップし、設定を完了する

Android（ブラウザ（Chrome））

1. au／UQ mobile／povo1.0 の回線の au ID なら、Wi-Fi をオフにしてご契約中の回線で接続する
2. **au ID会員情報サイト**にアクセスし、**指紋・顔認証によるログイン設定**から au ID でログインする
3. **この端末を登録する**をタップする
4. **次へ**をタップする
5. **次へ**をタップし、設定を完了する

Mac（（パソコン単体では設定できない））

1. パソコン単体では設定できない。スマートフォンで設定する（公式：**パソコンやタブレット単体では利用できません**）
2. パソコンからは、スマートフォンで QR コードを読み取ってログインする（Bluetooth が必要。事前にパスワードによるログインの有効化を求められる場合がある）

Windows（（パソコン単体では設定できない））

1. パソコン単体では設定できない。スマートフォンで設定する（公式：**パソコンやタブレット単体では利用できません**）
2. パソコンからは、スマートフォンで QR コードを読み取ってログインする（Bluetooth が必要。事前にパスワードによるログインの有効化を求められる場合がある）

確かめる

ブラウザ（指紋・顔認証でログインできる端末で）

1. au ID会員情報サイトに au ID でログインする
2. **指紋・顔認証によるログイン設定**をタップする
3. 画面が出た場合は**OK**をタップする
4. 指紋または顔認証で本人確認をする
5. 登録済みの端末が並ぶ（各端末に**解除**の欄がある。覚えのない端末は**登録済端末を解除**で外す）

弱い入口を外す

ブラウザ

1. (a) の**指紋・顔認証によるログイン**を設定する（これでパスワードによるログインは無効になる）
2. パソコンなどで使うために**パスワードによるログイン設定**を一時的に有効にした場合は、ログインのあと無効（オフ）に戻す（MENU →**ログインとセキュリティ**→**パスワードによるログイン設定**）

気をつけること auでは「パスキー」ではなく「指紋・顔認証によるログイン」と呼ぶ。設定はWi-Fiを切り、携帯の回線で行う。SMSとメールの2段階認証は外せない。

なくしたときの備え 登録できる端末は10台まで。使わなくなった端末の登録は外す。

公式の説明：https://www.au.com/au-id/auth-biometric/ https://www.au.com/support/faq/details/00/0000/000020/pg00002000/ https://www.au.com/support/faq/details/00/0000/000019/pg00001999/ https://www.au.com/au-id/auth-two-factor/ https://id.auone.jp/id/sp/security/pw_login.html https://www.au.com/support/faq/details/00/0000/000032/pg00003242/ https://www.au.com/support/faq/details/00/0000/000026/pg00002638/

電話番号の元（携帯会社）

SoftBank ID

済ませた日 月 日

いちばん強い方法 パスキー（スマホのWeb版 My SoftBank・My Y!mobile）

付ける

iPhone（ブラウザ（Safari・スマートフォン向け Web 版 My SoftBank））

1. 公式のお知らせのページにある**パスキーを設定する**を押す
2. **パスキーの登録・設定**を選択する

Android（ブラウザ（Google Chrome・スマートフォン向け Web 版 My SoftBank））

1. 公式のお知らせのページにある**パスキーを設定する**を押す
2. **パスキーの登録・設定**を選択する

Mac（(パソコンでは設定できない)）

1. パソコンでは設定できない（公式：**スマートフォンからのみ設定いただけます**）。スマートフォンで設定する

Windows（(パソコンでは設定できない)）

1. パソコンでは設定できない（公式：**スマートフォンからのみ設定いただけます**）。スマートフォンで設定する

弱い入口を外す

公式の説明では、外す手順が見当たらない。

気をつけること パスキーは2026年5月から。使えるのは、スマホのWeb版のMy SoftBank・My Y!mobile・My Menuのログインだけ。パスワードの入口を止められるかは、公式の説明に書かれていない。

公式の説明：https://www.softbank.jp/mobile/info/personal/news/service/20260525a/ https://www.softbank.jp/support/faq/view/196500 https://www.softbank.jp/support/faq/view/196501 https://www.softbank.jp/mobile/special/kaizen-action/topics-115/

お金

楽天 ID（楽天会員）

済ませた日 月 日

いちばん強い方法 パスキー

付ける

ブラウザ（端末の標準ブラウザ。SNS アプリなどのアプリ内ブラウザは使わない）

1. **パスキー管理ページ**にアクセスし、**新しいパスキーを設定する**を押す（パスキーに対応した楽天のサービスにログインしたときに出る登録画面からでもよい）
2. **パスキーを設定する**を押す
3. 表示されたメールアドレスに届いた認証コードを入力し、**認証して設定に進む**を押す
4. **続ける**を押す
5. 指紋・顔・PIN など端末のロック解除と同じ方法で本人確認をする
6. **パスキーが設定されました**と表示されたら完了

画面に出ること・気をつけること

- **パスキーが設定されました**→ 完了

確かめる

ブラウザ

1. **パスキー管理ページ**を開く
2. 登録済みの端末名・パスキーの登録日時・パスキーに紐づいた OS 端末とブラウザ名が並ぶ（ブラウザ名から、どのクラウドのアカウントに保存されたかが分かる）

弱い入口を外す

外せない。

気をつけること 楽天IDのパスキーは、楽天のパスキー対応サービスで共通。楽天証券は楽天IDと別のIDなので、楽天証券の画面で別に作る（2026年6月から順に必須）。パスワードの入口は外せない。

なくしたときの備え 機種変更のときは、新しい端末でパスキーで入れるのを確かめてから、古い端末のパスキーを消す。

公式の説明：https://jp.account.rakuten.com/device-management/faq/ja/ https://jp.account.rakuten.com/device-management/faq/ja/passkey/device-registration/ https://jp.account.rakuten.com/device-management/faq/ja/passkey/sign-in/device-not-supporting-passkey/ https://jp.account.rakuten.com/device-management/faq/ja/passkey/device-unlink/ https://static.id.rakuten.co.jp/static/passkey/desktop_guide.pdf

お金

Amazon（amazon.co.jp）

済ませた日 月 日

いちばん強い方法 パスキーと、2段階認証（認証アプリ）

付ける

アカウントサービス（ウェブ）

1. アカウントサービスで、**ログインとセキュリティ**を選択する
2. **パスキー**の横にある**設定**を選択する
3. **設定**を選択する
4. 画面上の簡単な指示に従って設定を完了する

別のやり方：別のパスキープロバイダーの端末に足すとき

1. アカウントサービスで、**ログインとセキュリティ**を選択する
2. **パスキー**の横にある**編集**を選択する
3. **パスキーを追加**を選択する
4. 画面上の指示に従う（自分が所有するデバイスにのみ追加する）

別のやり方：2段階認証（認証アプリ）を有効にする

1. アカウントサービスで、**ログインとセキュリティ**を選択する
2. **2段階認証 (2SV)の設定**の横にある**編集**を選択する
3. **はじめる**を選択する
4. 画面上の指示に従う（ワンタイムパスワードの受け取りは、テキストメッセージか認証アプリを選べる）

確かめる

アカウントサービス（ウェブ）

1. アカウントサービスに移動し、**ログインとセキュリティ**を選択する
2. **パスキー**を選択する
3. 作ったパスキーが並ぶ（それぞれの横に削除アイコンがある。覚えのないものは削除する）

弱い入口を外す

外せない。

気をつけること パスキーを付けても、パスワードのサインインは残る。だから2段階認証も認証アプリで付けて、パスワードの入口も守る。認証アプリは、Google AuthenticatorやMicrosoft Authenticatorなど、使い捨ての6桁の番号を出すアプリ。

なくしたときの備え 2段階認証のバックアップの方法を登録しておく。

公式の説明：https://www.amazon.co.jp/gp/help/customer/display.html?nodeId=TPphmhSWBgcI9Ak87p https://www.amazon.co.jp/gp/help/customer/display.html?nodeId=TsfzMlkp9pNh0GzriE https://www.amazon.co.jp/gp/help/customer/display.html?nodeId=TDKJ0Bccq0arCj4EKU https://www.amazon.co.jp/gp/help/customer/display.html?nodeId=G3PWZPU52FKN7PW4 https://www.amazon.co.jp/gp/help/customer/display.html?nodeId=GLEC8Z5M8NNXC9B2 https://www.amazon.co.jp/gp/help/customer/display.html?nodeId=GU3SL3GTHLHPDQ2H https://www.amazon.co.jp/gp/help/customer/display.html?nodeId=G9MX9LXNWXFKMJYU

お金 PayPay

済ませた日 月 日

いちばん強い方法 ログイン中の端末を確かめ、知らない端末を消す（パスキーは公式の説明に無い）

確かめる

PayPay アプリ

1. ホーム画面の右下の**アカウント**（または右上のベルマーク横のアイコン）をタップ
2. **セキュリティとプライバシー**をタップ
3. **ログイン管理**または**端末の管理**をタップ（アプリのバージョンで名前が違う）
4. **認証済みの端末**タブを確かめる
5. 心当たりのない端末は、右側の**削除**をタップしてログアウトさせる

弱い入口を外す

外せない。

気をつけること ログインし直すときは、必ずSMSの認証が要り、外せない。SMSの認証コードと認証用のQRコードは、誰にも教えない。

なくしたときの備え 登録している電話番号を確かめておく。番号を変えたら、PayPayの電話番号も変える。

公式の説明：https://paypay.ne.jp/help/c0295/ https://paypay.ne.jp/help/c0374 https://paypay.ne.jp/help/c0028/ https://paypay.ne.jp/help/c0022/ https://paypay.ne.jp/help/c0370/

お金 メルカリ

済ませた日 月 日

いちばん強い方法 パスキー

付ける

アプリ（1 台目）

1. **マイページ＞設定＞アカウント設定（個人情報設定）＞パスキー設定**を開く
2. **パスキーを登録する**をタップする
3. 登録した電話番号に届いた認証番号を**認証番号**欄に入力する
4. 再度**パスキーを登録する**をタップし、表示される生体認証を行う。表示された画面で**続ける**を押す（iOS の Face ID は、メルカリアプリへの使用許可が要る場合がある）
5. 登録した端末でログインできるようになる

別のやり方：2 台目以降の端末

1. 追加したい端末でメルカリにログインし、**生体認証**設定画面を開いて**パスキーを追加する**をタップする
2. 生体認証を求められたらパスキー認証をする。QR コードの読み取り画面が出たら、パスキー登録済みの端末で読み込む
3. 追加したい端末で顔認証・指紋認証・パスコードなどを求められるので、画面の指示に従って認証する

確かめる

アプリ

1. **マイページ＞設定＞アカウント設定＞パスキー設定**を開く
2. **生体認証**設定画面に登録した端末（パスキー）が追加されていれば完了

弱い入口を外す

アプリ

1. 上の**付ける**でパスキーを登録する（これでログインにパスキー認証が必須になる）
2. パスキーは最低１端末を残す（全部消すと不正アクセスのリスクが高まると公式）

気をつけること パスキーを登録すると、ログインにパスキーが必須になる。電話番号（SMS）は外せない。

なくしたときの備え 2台目の端末にもパスキーを足しておく。

公式の説明：https://help.jp.mercari.com/guide/articles/1876/ https://help.jp.mercari.com/guide/articles/1483/ https://help.jp.mercari.com/guide/articles/1103/ https://help.jp.mercari.com/guide/articles/1860/ https://help.jp.mercari.com/guide/articles/1874/ https://help.jp.mercari.com/guide/articles/1875/ https://about.mercari.com/press/news/articles/20240129_passkeys/

お金 銀行

済ませた日 月 日

いちばん強い方法 その銀行のパスキー。無ければ、銀行の専用アプリの認証

付ける

どの端末でも

1. 銀行の公式アプリか、ブックマークから入る（メールやSMSのリンクから入らない）
2. **セキュリティ** **ログイン設定** **認証方法**のような項目を探す
3. **パスキー** **生体認証** **アプリ認証**があれば、それを設定する
4. メールやSMSのワンタイムパスワードしか無ければ、もっと強い方法の予定を銀行に問い合わせる

気をつけること 金融庁は2026年4月の広報で、メールやSMSに届く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」と書いている。

公式の説明：https://www.fsa.go.jp/news/r7/sonota/20260416-2/20260416-2.html https://www.fsa.go.jp/news/r7/sonota/20260416-2/02.pdf

お金 証券

済ませた日 月 日

いちばん強い方法 パスキー（またはマイナンバーカードなどの認証）

付ける

どの端末でも

1. 証券会社の公式アプリか、ブックマークから入る（メールやSMSのリンクから入らない）
2. **セキュリティ設定** **ログイン設定**を開く
3. **パスキー**（またはマイナンバーカードなどの認証）を設定する。会社からのお知らせがあれば、その手順に従う
4. 出金先の口座の変更にも、同じ認証がかかっているか確かめる

気をつけること 日本証券業協会のガイドラインで、ログイン・出金・出金先の変更に、偽のサイトに強い認証（フィッシング耐性のある多要素認証）が必須になった（2025年10月施行。金融庁は2026年6月末までの対応を求めた）。

公式の説明：https://www.jsda.or.jp/about/hatten/inv_alerts/alearts04/files/20251015_internetgl.pdf https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html

SNS X（旧 Twitter）

済ませた日 月 日

いちばん強い方法 iPhoneとAndroidはパスキー（Xアプリで）。パソコンは認証アプリ

付ける

iPhone（X アプリ（パスキー））

1. パスキーを有効にするアカウントを使用してXアプリにログインします。
2. ナビゲーションバーにある**アカウント**をクリックします。
3. **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**の順に選択します。
4. **追加のパスワード保護**の**パスキー**を選択します。
5. 画面の指示に沿って、パスワードを入力します。
6. **パスキーの追加**を選択し、表示された手順を実行します。

Android（X アプリ（パスキー））

1. パスキーを付けたいアカウントで、Xアプリにログインします。
2. ナビゲーションバーの**アカウント**（プロフィールアイコン）をタップします。
3. **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**の順に選択します。
4. **追加のパスワード保護**の**パスキー**を選択します。
5. 画面の指示に沿って、パスワードを入力します。
6. **パスキーの追加**を選択し、表示された手順を実行します（指か顔、またはスマホのPINで確かめる）。

別のやり方：Android（X アプリ（2要素認証も付けるなら、認証アプリ））

1. トップメニューのナビゲーションメニューアイコンまたはプロフィールアイコンをタップして、**設定とプライバシー**を選択します。
2. **アカウント**、**セキュリティ**の順にタップします。
3. **2要素認証**をタップします。
4. **認証アプリ**のチェックボックスをタップします。
5. 手順を確認し、**始める**をタップします。
6. メッセージが表示されたら、パスワードを入力して**認証する**をタップします。
7. QRコードを認証アプリでスキャンしたら、**次へ**をタップします（Google Authenticator、Authy、Duo Mobile、1Password など、どの TOTP 認証アプリでも使える）。
8. 認証アプリにより生成されたコードを入力し、**認証する**をタップします。
9. 確認画面が表示されます。**OK**をタップして設定を完了します。

> **画面に出ること・気をつけること**
> - Xアカウントのメールの確認がまだ完了していない場合、確認を求めるメッセージ → メールアドレスを入力して［次へ］→ メールで届いた認証コードを入力して［認証］

Mac（ブラウザ（x.com・認証アプリ））

1. サイドメニューの**もっと見る**をクリックし、**設定とプライバシー**をクリックします。
2. **セキュリティとアカウントアクセス**をクリックし、**セキュリティ**をクリックします。
3. **2要素認証**をクリックします。
4. **認証アプリ**のチェックボックスをクリックします。
5. 手順を確認し、**始める**をクリックします。
6. メッセージが表示されたら、パスワードを入力して**認証する**をクリックします。
7. QRコードを認証アプリでスキャンしたら、**次へ**をクリックします。
8. 認証アプリにより生成されたコードを入力し、**認証する**をクリックします。
9. 確認画面が表示されます。**OK**をクリックして設定を完了します。

> **画面に出ること・気をつけること**
> - Xアカウントのメールの確認がまだ完了していない場合、確認を求めるメッセージ → メールアドレスを入力して［次へ］→ メールで届いた認証コードを入力して［認証］

Windows（ブラウザ（x.com・認証アプリ））

1. サイドメニューの**もっと見る**をクリックし、**設定とプライバシー**をクリックします。
2. **セキュリティとアカウントアクセス**をクリックし、**セキュリティ**をクリックします。
3. **2要素認証**をクリックします。
4. **認証アプリ**のチェックボックスをクリックします。
5. 手順を確認し、**始める**をクリックします。
6. メッセージが表示されたら、パスワードを入力して**認証する**をクリックします。
7. QRコードを認証アプリでスキャンしたら、**次へ**をクリックします。
8. 認証アプリにより生成されたコードを入力し、**認証する**をクリックします。
9. 確認画面が表示されます。**OK**をクリックして設定を完了します。

> **画面に出ること・気をつけること**
> - Xアカウントのメールの確認がまだ完了していない場合、確認を求めるメッセージ → メールアドレスを入力して［次へ］→ メールで届いた認証コードを入力して［認証］

確かめる

Android（X アプリ）

1. トップメニューのナビゲーションメニューアイコンまたはプロフィールアイコンをタップして、**設定とプライバシー**を選択します。
2. **アカウント**、**セキュリティ**の順にタップします。
3. **2要素認証**をタップし、付けた方法（**認証アプリ**など）がオンになっているかを見る。セキュリティキーは**セキュリティキーを管理**セクションに表示されます。

Mac（ブラウザ（x.com））

1. サイドメニューの**もっと見る**をクリックし、**設定とプライバシー**をクリックします。
2. **セキュリティとアカウントアクセス**をクリックし、**セキュリティ**をクリックします。
3. **2要素認証**をクリックし、付けた方法のチェックボックスが入っているかを見る。セキュリティキーは**セキュリティキーを管理**セクションに表示されます。

Windows（ブラウザ（x.com））

1. サイドメニューの**もっと見る**をクリックし、**設定とプライバシー**をクリックします。
2. **セキュリティとアカウントアクセス**をクリックし、**セキュリティ**をクリックします。
3. **2要素認証**をクリックし、付けた方法のチェックボックスが入っているかを見る。セキュリティキーは**セキュリティキーを管理**セクションに表示されます。

弱い入口を外す

iPhone（X アプリ）

1. トップメニューのプロフィールアイコンをタップし、**設定とプライバシー**をタップします。
2. **アカウント**、**セキュリティ**の順にタップします。
3. **2要素認証**をタップし、**ショートメール**のスイッチをタップしてオフにします。
4. **オフにする**を2回タップして確定します。

> **画面に出ること・気をつけること**
> - ［オフにする］を2回タップして確定

Android（X アプリ）

1. トップメニューのプロフィールアイコンをタップし、**設定とプライバシー**をタップします。
2. **アカウント**、**セキュリティ**の順にタップします。
3. **2要素認証**をタップします。
4. **ショートメール**のチェックボックスをタップしてオフにします。
5. **オフにする**をタップして確定します。

> **画面に出ること・気をつけること**
> - ［オフにする］をタップして確定

Mac（ブラウザ（x.com））

1. サイドメニューの**もっと見る**をクリックし、**設定とプライバシー**をクリックします。
2. **セキュリティとアカウントアクセス**をクリックし、**セキュリティ**をクリックします。
3. **2要素認証**をクリックします。
4. **ショートメール**のチェックボックスをオフにします。

Windows（ブラウザ（x.com））

1. サイドメニューの**もっと見る**をクリックし、**設定とプライバシー**をクリックします。
2. **セキュリティとアカウントアクセス**をクリックし、**セキュリティ**をクリックします。
3. **2要素認証**をクリックします。
4. **ショートメール**のチェックボックスをオフにします。

気をつけること パスキーは、英語版の公式ヘルプ（2026年9月更新）でiPhoneとAndroidの両方に対応と書かれている。日本語版のヘルプには「iOSのみ」の古い記述が残っている。SMSの2要素認証は、先に認証アプリを付けてから外す。認証アプリは、Google AuthenticatorかMicrosoft Authenticatorを公式のストアから入れる。サービスの画面に出る四角い模様（QRコード）をアプリで読み取ると、30秒ごとに変わる6桁の番号が出る。

なくしたときの備え 2要素認証を付けたときに出るバックアップコードを、印刷するか紙に書いて、大事な書類と一緒にしまう（写真で残すと、スマホと一緒になくす）。

公式の説明：https://help.x.com/en/managing-your-account/how-to-use-passkey https://help.x.com/ja/managing-your-account/two-factor-authentication https://help.x.com/ja/managing-your-account/how-to-use-passkey https://help.x.com/en/managing-your-account/two-factor-authentication

SNS Instagram

済ませた日 月 日

いちばん強い方法 パスキー（2段階認証も付けるなら認証アプリで）

付ける

Instagram アプリ・ブラウザ（Meta アカウント設定）

1. 使用しているアプリ内で**設定**に移動します。
2. **Metaアカウント設定**をタップまたはクリックします。
3. **ログインとセキュリティ**をタップまたはクリックします。
4. **パスキー**をタップまたはクリックし、**パスキーを作成**をタップまたはクリックします。

確かめる

Instagram アプリ・ブラウザ（Meta アカウント設定）

1. 使用しているアプリ内で**設定**に移動します。
2. **Metaアカウント設定**をタップまたはクリックします。
3. **ログインとセキュリティ**をタップまたはクリックします。
4. **パスキー**をタップまたはクリックし、作ったパスキーが出ているかを見る（各パスキーに、関連付けられたメールアドレスまたは電話番号、保存場所、作成日が表示される）。

弱い入口を外す

iPhone（Instagram アプリ）

1. 右下にある**プロフィール**またはプロフィール写真をタップして、プロフィールに移動します。
2. 右上の**メニュー**をタップします。
3. **アカウントセンター**をタップしてから、**パスワードとセキュリティ**をタップします。
4. **二段階認証**をタップし、アカウントを選択します。
5. オフにするセキュリティ強化方法（SMS）を選択し、画面の指示に沿って操作します。

Android（Instagram アプリ）

1. 右下にある**プロフィール**またはプロフィール写真をタップして、プロフィールに移動します。
2. 右上の**メニュー**をタップします。
3. **アカウントセンター**をタップしてから、**パスワードとセキュリティ**をタップします。
4. **二段階認証**をタップし、アカウントを選択します。
5. オフにするセキュリティ強化方法（SMS）を選択し、画面の指示に沿って操作します。

Mac（ブラウザ（instagram.com））

1. 左下の**その他**をクリックし、**設定**をクリックします。
2. **アカウントセンターでもっと見る**をクリックし、**パスワードとセキュリティ**をクリックします。
3. **二段階認証**をクリックし、アカウントを選択します。
4. オフにするセキュリティ強化方法（SMS）を選択し、画面の指示に沿って操作します。

Windows（ブラウザ（instagram.com））

1. 左下の**その他**をクリックし、**設定**をクリックします。
2. **アカウントセンターでもっと見る**をクリックし、**パスワードとセキュリティ**をクリックします。
3. **二段階認証**をクリックし、アカウントを選択します。
4. オフにするセキュリティ強化方法（SMS）を選択し、画面の指示に沿って操作します。

気をつけること InstagramとFacebookは、Metaの「アカウントセンター」でまとめて管理する。画面は「アカウントセンター」か「Metaアカウント設定」のどちらか。SMSは、先に認証アプリを付けてから外す。認証アプリは、Google AuthenticatorかMicrosoft Authenticatorを公式のストアから入れる。サービスの画面に出る四角い模様（QRコード）をアプリで読み取ると、30秒ごとに変わる6桁の番号が出る。

なくしたときの備え バックアップコードを取り、印刷するか紙に書いて、大事な書類と一緒にしまう。

公式の説明：https://help.instagram.com/566810106808145 https://help.instagram.com/1582474155197965 https://help.instagram.com/843785199163974 https://help.instagram.com/1006568999411025 https://www.meta.com/ja-jp/help/meta-account/1991801474748071/ https://www.meta.com/ja-jp/help/meta-account/553000504008092/

SNS

Facebook

済ませた日
月　日

いちばん強い方法 パスキーと、二段階認証（セキュリティキーか認証アプリ）

付ける

Facebook アプリ・ブラウザ（Meta アカウント設定）

1. 使用しているアプリ内で**設定**に移動します。
2. **Metaアカウント設定**をタップまたはクリックします。
3. **ログインとセキュリティ**をタップまたはクリックします。
4. **パスキー**をタップまたはクリックし、**パスキーを作成**をタップまたはクリックします。

確かめる

Facebook アプリ・ブラウザ（Meta アカウント設定）

1. 使用しているアプリ内で**設定**に移動します。
2. **Metaアカウント設定**をタップまたはクリックします。
3. **ログインとセキュリティ**をタップまたはクリックします。
4. **パスキー**をタップまたはクリックし、作ったパスキーが出ているかを見る（各パスキーに、関連付けられたメールアドレスまたは電話番号、保存場所、作成日が表示される）。

弱い入口を外す

iPhone（Facebook アプリ）

1. Facebook画面の左上にある**メニュー**をタップします。
2. **設定とプライバシー**＞**設定**の順にタップします。
3. **アカウントセンター**をタップしてから、**パスワードとセキュリティ**をタップします。
4. **二段階認証**をタップしてから、更新するアカウントをタップします。
5. 使用をやめる携帯電話番号の横にある**オフにする**をタップします。

Android（Facebook アプリ）

1. Facebook画面の左上にある**メニュー**をタップします。
2. **設定とプライバシー**＞**設定**の順にタップします。
3. **アカウントセンター**をタップしてから、**パスワードとセキュリティ**をタップします。
4. **二段階認証**をタップしてから、更新するアカウントをタップします。
5. 使用をやめる携帯電話番号の横にある**オフにする**をタップします。

Mac（ブラウザ（facebook.com））

1. 画面右上のプロフィール写真をクリックしてから、**設定とプライバシー**をクリックします。
2. **設定**をクリックします。
3. **アカウントセンター**をクリックしてから、**パスワードとセキュリティ**をクリックします。
4. **二段階認証**をクリックしてから、更新するアカウントをクリックします。
5. 使用をやめる携帯電話番号の横にある**オフにする**をクリックします。

Windows（ブラウザ（facebook.com））

1. 画面右上のプロフィール写真をクリックしてから、**設定とプライバシー**をクリックします。
2. **設定**をクリックします。
3. **アカウントセンター**をクリックしてから、**パスワードとセキュリティ**をクリックします。
4. **二段階認証**をクリックしてから、更新するアカウントをクリックします。
5. 使用をやめる携帯電話番号の横にある**オフにする**をクリックします。

気をつけること Instagramと同じく、Metaの「アカウントセンター」で管理する。SMSは、先に認証アプリを付けてから外す。認証アプリは、Google AuthenticatorかMicrosoft Authenticatorを公式のストアから入れる。サービスの画面に出る四角い模様（QRコード）をアプリで読み取ると、30秒ごとに変わる6桁の番号が出る。

なくしたときの備え 10個のリカバリーコードを取り、印刷するかメモする。

公式の説明：https://www.facebook.com/help/148233965247823 https://www.facebook.com/help/1181045243159511 https://www.facebook.com/help/358336074294704 https://www.facebook.com/help/1756727521321961 https://www.facebook.com/help/401566786855239 https://www.facebook.com/help/148104135383285 https://www.meta.com/ja-jp/help/meta-account/1991801474748071/

SNS
TikTok

済ませた日
月　日

いちばん強い方法　パスキーと、2段階認証（認証アプリとメール）

付ける

iPhone（TikTok アプリ）

1. TikTokアプリで、画面下部の**プロフィール**をタップします。
2. 画面上部のメニュー≡ボタンをタップします。
3. **設定とプライバシー**をタップします。
4. **アカウント**をタップします。
5. パスキーをタップして、次の画面で設定をタップし、表示される指示に従います。

Android（TikTok アプリ）

1. TikTokアプリで、画面下部の**プロフィール**をタップします。
2. 画面上部のメニュー≡ボタンをタップします。
3. **設定とプライバシー**をタップします。
4. **アカウント**をタップします。
5. パスキーをタップして、次の画面で設定をタップし、表示される指示に従います。Googleパスワードマネージャーでパスキーを作成する場合は、その画面に移動して設定を完了します。

確かめる

iPhone（TikTok アプリ（セキュリティチェック））

1. 画面下部のプロフィールをタップします。
2. 画面上部のメニュー（≡）ボタンをタップし、**設定とプライバシー**を選択します。
3. セキュリティとアクセス許可をタップします。
4. セキュリティチェックをタップし、**アカウントにパスキーを追加する**　**2段階認証を有効にする**に緑色のチェックマークが付いているかを見る。

Android（TikTok アプリ（セキュリティチェック））

1. 画面下部のプロフィールをタップします。
2. 画面上部のメニュー（≡）ボタンをタップし、**設定とプライバシー**を選択します。
3. セキュリティとアクセス許可をタップします。
4. セキュリティチェックをタップし、**アカウントにパスキーを追加する**　**2段階認証を有効にする**に緑色のチェックマークが付いているかを見る。

弱い入口を外す

iPhone（TikTok アプリ（2段階認証を SMS なしで付ける））

1. 画面下部のプロフィールをタップします。
2. 画面上部のメニュー（≡）ボタンをタップし、**設定とプライバシー**を選択します。
3. セキュリティとアクセス許可をタップします。
4. 2段階認証をタップして、認証方法を2つ以上選択します（電話番号ではなく、メールアドレスと認証アプリを選ぶ）。
5. 認証アプリは、次の画面に表示される指示に従ってQRコードをスキャンするか、表示されるキーをコピーして認証アプリに入力し、認証アプリに表示されるコードをTikTokアプリに入力します。
6. オンにするをタップして確定します。
7. 続行をタップして、メールに送信された認証コードを入力します。

Android（TikTok アプリ（2段階認証を SMS なしで付ける））

1. 画面下部のプロフィールをタップします。
2. 画面上部のメニュー（≡）ボタンをタップし、**設定とプライバシー**を選択します。
3. セキュリティとアクセス許可をタップします。
4. 2段階認証をタップして、認証方法を2つ以上選択します（電話番号ではなく、メールアドレスと認証アプリを選ぶ）。
5. 認証アプリは、次の画面に表示される指示に従ってQRコードをスキャンするか、表示されるキーをコピーして認証アプリに入力し、認証アプリに表示されるコードをTikTokアプリに入力します。
6. オンにするをタップして確定します。
7. 続行をタップして、メールに送信された認証コードを入力します。

気をつけること　設定はスマホのアプリで行う。2段階認証は「メールアドレス」と「認証アプリ」を選べば、SMSを使わずに済む。認証アプリは、Google AuthenticatorかMicrosoft Authenticatorを公式のストアから入れる。サービスの画面に出る四角い模様（QRコード）をアプリで読み取ると、30秒ごとに変わる6桁の番号が出る。

なくしたときの備え　認証アプリを付けたときのリカバリーコードを控える。

公式の説明：https://support.tiktok.com/ja/safety-hc/account-and-user-safety/account-safety　https://support.tiktok.com/ja/log-in-troubleshoot/log-in/log-in-with-a-passkey

設定ではない
3つの約束

- [ ] **届いたリンクからは入らない**
  メールやSMSのリンクは、本物らしく見えても開かない。いつものアプリかブックマークから入る
- [ ] **覚えのない「はい」は押さない**
  自分でログインしていないときに届く確認の通知は、何度鳴っても押さない

- [ ] **お金と操作の電話は、一度切る**
  銀行・役所・警察・家族を名乗っても、切って、自分から公式の番号にかけ直す。家族とは合言葉を決めておく

起きたとき

4　漏れたとき・なくしたとき

漫画　ケンジさんの家と、本物にしか合わない鍵　第4話「なくしても、慌てない」




人のパソコンからでも探せるって、リクが言ってたな
GUEST PC
ロックして、画面に連絡先を出せる
音を鳴らす
紛失としてマーク
タクシー会社の営業所


タクシー会社
夜中に鳴っていたので、預かっていました
助かった……
はぁ…
このスマホは紛失中です。ご連絡ください
携帯会社にも連絡して、回線を止める
戻ってこないと決めたら、遠くから中身を消すこともできる。急がなくていいけどね
中身は、どうなる？
バックアップしてあるから、新しいスマホに戻せる


かばんごと
なくしても、
これで場所が
分かる
スマホを
全部なくしたら？
人のスマホや
パソコンからでも、
探せるよ
ポイント
なくしても慌てない。
バックアップ
探す
遠くから鍵
探し物タグ

漏れたと知らせが来たら、3つだけやる

「守れるもの、守れないもの」の表の真ん中の列、「小さくできる」の中身だ。サービスの会社から「情報が漏れたおそれがあります」と知らせが来たら、慌てずに、これだけやる。

- そのサービスのパスワードを変える。同じパスワードをほかで使っていたら、全部変える
- 知らせのメールやSMSのリンクからは入らない。いつものアプリか、ブックマークから入って確かめる
- 漏れた名前や電話番号を使った、本物そっくりの連絡が来る前提で待つ。来ても、リンクは開かず、電話は一度切る

預けた先のそのまた先で漏れた件は、特集「委託先のその先で起きた漏えいは、会社からは防ぎきれない」で読める。

乗っ取られたら、お金の口座は、まず金融機関へ

何が乗っ取られたかで、最初にやることが違う。

銀行・証券・クレジットカード・決済アプリで、身に覚えのないログインや取引の知らせが来たら、最初にその会社の公式の窓口に連絡する。取引や出金を止めてもらうのが先だ。電話番号は、届いたメールやSMSではなく、カードの裏や公式のアプリ、ブックマークした公式のサイトで確かめる。金融庁も2026年11月6日、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するよう呼びかけている。被害があったら、警察の相談窓口（警察相談専用電話 #9110 か、都道府県警察のサイバー犯罪の窓口）にも相談する。

メール・LINE・SNSなら、次の二つを一緒に進める。

- 各サービスの公式の手順で、アカウントを取り戻す。取り戻したら、パスワードを変え、パスキーか2段階認証を付ける。ログインしている端末の一覧を開き、知らない端末を外す。メールの自動転送の設定と、再設定用の電話番号・メールアドレスが自分のものかも確かめる（乗っ取った人が書き換えていることが多い）
- 電話や家族など、乗っ取られたのとは別の手段で、友だちや家族に「私から来たメッセージのリンクは開かないで。お金やカードの頼みにも応じないで」と知らせる

メールのアカウントが乗っ取られていたら、そのメールで再設定できるほかのサービス（お金のものから先に）も、パスワードを変える。

なくしたら、探す、ロックする、最後に消す

スマホやパソコンをなくしても、前もって設定しておけば、慌てなくていい。やることは、探す、ロックする、最後の手段として消す、の順だ。



なくしたら、探す・ロック・最後に消去

1. 別のスマホかパソコンで、なくした端末の場所を地図で見る。近くなら音を鳴らす
2. ロックして、画面に連絡先とメッセージを出す。拾った人が連絡でき、中のものも使われない
3. 戻ってこないと決めたら、遠くから中身を消す。急がなくていい（盗まれて6桁を見られたかもしれないときは、急ぐ）

ロックすると、画面に連絡先が出るので、拾った人が連絡しやすい。iPhoneなら、Apple Payのカードも止まる。6桁を知られていなければ、中のものは使われにくい。消すのは、戻ってこないと決めてからでいい。

あわせて、携帯会社に連絡して、回線を止めてもらう。SIMを抜かれると、SMSの確認の番号を受け取られてしまうからだ。

ただし、盗まれたうえに、スマホを開く6桁を見られていたかもしれないときは、急ぐ。すぐに消去し、AppleかGoogleのアカウントのパスワードを変える。

端末ごとに、探す・ロック・消す

端末ごとの手順は下のとおり。押すと開く。前もってオンにしておくことも、最初に書いた。

なくしたら
iPhone

使うもの 「探す」

地図で探す

1. 別の信頼できるApple製デバイスの**探す**アプリか、ブラウザで icloud.com/find を開き、Apple Accountにサインインする（icloud.com/find は認証コード不要。求められたら**デバイスを探す**ボタンを選ぶ）
2. **すべてのデバイス**の下のリストから、なくしたiPhoneを選ぶ
3. 地図で位置を確かめる。オフラインならデバイス名の下に**オフライン**と出て、最後の位置が最大24時間表示される。**検出時に通知**を選ぶと、オンラインに戻ったときにメールが届く

前もって、オンにしておく

1. 設定アプリを開く
2. 自分の名前をタップし、**探す**をタップする
3. **「デバイス**を探す」をタップし、**「デバイス**を探す」をオンにする
4. オフラインのときでも探せるように**“探す”ネットワーク**をオンにする
5. バッテリーが少なくなったときに位置をAppleに送るなら**最後の位置情報を送信**をオンにする

音を鳴らす

1. icloud.com/find にアクセスし、Apple Accountにサインインする（必要な場合）
2. デバイスのリストから、サウンドを再生するデバイスを選ぶ
3. **サウンドを再生**を選ぶ

サイレントモードや消音でも鳴る。オンラインなら徐々に大きくなって約2分間。オフラインなら次にWi-Fiかモバイルデータ通信につながったときに鳴る。「探す」アプリからも同じ操作ができる。

ロックして、連絡先を出す

1. **探す**アプリで、**デバイスを探す**タブを表示する
2. 下にスクロールして、紛失したiPhoneを選ぶ
3. **詳細**ボタンをタップする
4. 下にスクロールして**「デバイス**を紛失」を表示し、**紛失モード**をオンにする
5. 連絡先情報を表示したい場合は、画面の案内に従う
6. **有効にする**をタップする

ロックすると

- パスコードでロックされる
- Apple Payで使っている決済カードやパスは使用停止になる
- 入れた電話番号とメッセージが、オンラインである限りロック画面に表示される（オフラインならネットにつながるまで出ない）
- メッセージや通知、アラームの音やアラートは出なくなるが、電話やFaceTime通話は受けられる
- 現在位置と移動履歴が地図上に表示される
- **盗難デバイスの保護**を使っている場合、紛失モードの解除にFace IDかTouch IDが要る

最後の手段：消去（急がなくていい）

1. icloud.com/find にアクセスし、Apple Accountにサインインする（必要な場合）
2. デバイスのリストから、消去するデバイスを選ぶ
3. **このデバイスを消去**を選ぶ
4. 画面の指示に従う（電話番号とメッセージを入れると、ロック画面に表示される）

消す前に

- 消去すると元に戻せない。それ以外のすべての手段を試し尽くしてから（Apple）
- 消去したあとも**探す**からは削除しない。削除するとアクティベーションロックが外れ、盗んだ人が再販しやすくなる
- アクティベーションロックはオンのまま。再び使うにはApple Accountとパスワードが要る
- 消去したあとも**デバイスを探す**で位置の確認とサウンドの再生はできる（iCloudユーザガイドの記述）
- オフラインなら、次にオンラインになったときに消去が始まる。始まる前なら**消去リクエストを中止**で取り消せる
- 見つかりそうにないときは、通話料金などを請求されないよう携帯電話会社に連絡してサービスを止める。警察にも届ける（シリアル番号を聞かれることがある）

気をつけること Appleが「iPhoneが見つかった」と連絡することはない。パスコード・パスワード・認証コードは誰に聞かれても教えない（Apple公式101593）。

なくしたら
Android

使うもの Find Hub

地図で探す

1. 別の Android スマートフォンかタブレットで、Find Hub アプリを開く（未インストールなら Google Play でダウンロード）。別の Android デバイスがないときは、ブラウザで android.com/find（Find Hub）にアクセスする
2. ログインする。自分のデバイスなら **[あなたの名前** として続行]、友だちの端末を借りるなら **ゲストとしてログイン** をタップして自分でログインする
3. 表示されたデバイスの中から、探しているデバイスを選ぶ（なくしたデバイスに通知が送られる）
4. 地図で現在地を確かめる。わからなくても、最後に確認された位置が出ることがある。**ルートを検索する** で道順、10メートル以内なら **付近を探す**

前もって、オンにしておく

1. Google アカウントにログインしているか確かめる（設定アプリ → **パスワード、パスキー、アカウント**）
2. 位置情報をオンにする（設定アプリ → **位置情報** → **位置情報の使用** をオン）
3. Find Hub をオンにする（設定アプリ → **セキュリティ** → **Find Hub** → **デバイスの場所の特定を許可** がオン）。Google アカウントを追加済みなら最初からオン
4. オフラインでも探せるようにする（設定 → **Google** → **すべてのサービス** → **Find Hub** → **オフラインのデバイスを探す** で **人通りの多い場所でのみネットワークを使用する** か **どこでもネットワークを使用する**）
5. 画面ロック（PIN、パターン、パスワード）を設定する。ネットワークで探すのに必要
6. Google Play で非表示にしていないか確かめる（play.google.com/library/devices の **メニューに表示する**）
7. 2 段階認証プロセスのバックアップ コードを作っておく（スマホが確認コードの受け取り先のことがあるため）

音を鳴らす

1. Find Hub で、なくしたデバイスを選ぶ
2. **音を鳴らす** を選ぶ

最大音量で5分間鳴る。マナーモードやバイブレーション モードでも鳴る。

ロックして、連絡先を出す

1. Find Hub で、なくしたデバイスを選ぶ
2. **紛失としてマーク** → **次へ** をタップする
3. 紛失したデバイスのロック画面に表示する連絡先情報とメッセージを入れる
4. **紛失としてマーク** をタップする

ロックすると

- PIN、パターン、またはパスワードでロックされる
- ロック画面に連絡先情報とメッセージが出る
- Android 17 以降で指紋認証か顔認証に対応している機種は、解除に PIN 等に加えて指紋か顔が要り、通知・ウィジェット・クイック アクセスも使えなくなる

最後の手段：消去（急がなくていい）

1. Find Hub アプリを開く（ウェブや、友だちの Android のゲストモードでも使える）
2. リセットするデバイスを選ぶ
3. **設定** を選ぶ
4. **初期状態へのリセット** をタップする

消す前に

- デバイス上のすべてのデータが完全に削除される（SD カードのデータは削除されない場合がある）
- 出荷時の設定にリセットすると、Find Hub で利用できなくなる（＝探せなくなる）
- 消去後に見つかった場合、再び使うには Google アカウントのパスワードが要る

なくしたら

Mac

使うもの 「探す」／「Macを探す」

地図で探す

1. icloud.com/find にアクセスし、Apple Accountにサインインする（必要な場合）。別のApple製デバイスの **探す** アプリでもよい
2. デバイスのリストから、なくしたMacを選ぶ
3. 地図で位置を確かめる（オフラインなら **オフライン** と出て、最後の位置が最大24時間表示される）

前もって、オンにしておく

1. Appleメニューから **システム設定** を選ぶ
2. ユーザ名をクリックし、**iCloud** をクリックする
3. **すべて見る** をクリックする
4. 下にスクロールして **Macを探す** をクリックする
5. **オンにする** をクリックする（Apple Accountのパスワードを求められたら入れる）。位置の使用の確認が出たら **許可**

音を鳴らす

1. icloud.com/find にアクセスし、サインインする
2. デバイスのリストから、Macを選ぶ
3. **サウンドを再生** を選ぶ

Macで止めるときは「探す」のアラートの「OK」をクリック。

ロックして、連絡先を出す

1. icloud.com/find にアクセスし、サインインする
2. デバイスのリストから、Macを選ぶ
3. **紛失としてマーク** を選ぶ
4. 画面上の指示に従う（電話番号とメッセージを入れる）

ロックすると

- Intelプロセッサ搭載Macは、パスワードがあっても数字のパスコードを新たに作ってロックする
- Appleシリコン搭載Macは、Apple Accountとパスワードでロックされる
- オンラインや他のデバイスからはロックを解除できない。解除できるのはそのMacの上だけ
- 該当するデバイスでは、支払い用のカードやその他のサービスは停止される
- 電話番号とメッセージは、オンラインである限りロック画面に表示される

最後の手段：消去（急がなくていい）

1. icloud.com/find にアクセスし、サインインする
2. デバイスのリストから、Macを選ぶ
3. **このデバイスを消去**を選ぶ
4. 画面の指示に従う

消す前に

- 元に戻せない。アクティベーションロックはオンのまま
- 消去後も**デバイスを探す**で位置の確認・サウンドの再生はできる。Macはかつてつないだ Wi-Fi の近くにあれば場所を特定できる可能性がある
- オフラインなら次にオンラインになったときに消去が始まる

なくしたら

Windows

使うもの デバイスの検索

地図で探す

1. account.microsoft.com/devices に移動し、サインインする
2. **デバイスの検索**タブを選ぶ
3. 検索するデバイスを選び、**検索**を選んで、デバイスの場所を示すマップを表示する

前もって、オンにしておく

1. Microsoft 個人用アカウントでデバイスにサインインする（アカウントの種類は**管理者**）
2. 設定の**デバイスの検索**をオンにする（公式ページの**デバイスの検索**設定を開く のリンク先は ms-settings:findmydevice）
3. デバイスの位置情報をオンにしておく

音を鳴らす

Microsoft の公式ページに音を鳴らす機能の記載はない（探す・ロックのみ）。

ロックして、連絡先を出す

1. https://account.microsoft.com/devices に移動し、サインインする
2. マップ上でデバイスが見つかったら、**ロック**→**次へ**を選ぶ
3. ロックしたあと、セキュリティを強めるためにパスワードをリセットする

最後の手段：消去（急がなくていい）

個人向けの「デバイスの検索」に遠隔で消去する機能の記載はない。盗難は警察と保険会社に届ける（シリアル番号は account.microsoft.com/devices の [情報とサポート]）と公式が勧めている。

バックアップをオンにしておけば、なくしても壊しても戻せる

壊したときやなくしたときに、中身を戻せるのがバックアップだ。iPhoneはiCloudバックアップ、AndroidはGoogleのバックアップ、MacはTime Machine、WindowsはWindowsバックアップ。オンにする手順は、「今日、設定する」の端末のカードに入れた。

探し物タグを付けておけば、落としても場所が分かる

鍵やかばん、財布に付けておく小さなタグがある。落としても、スマホの地図で場所が分かる。iPhoneならAirTag、AndroidならGoogleの「Find Hub」に対応したタグを選ぶ。評価の高いものを、iPhone用とAndroid用で2つずつ挙げる。

- **Apple AirTag（第2世代）1個**（iPhoneで使える。評価 4.4・5,468円前後）
  https://www.amazon.co.jp/dp/B0GJTW9CL8
- **Apple AirTag 4個入り（第2世代）**（iPhoneで使える。評価 4.5・16,430円前後）
  https://www.amazon.co.jp/dp/B0GJTXZHDX
- **Xiaomi Tag（1個）**（Android・iPhoneで使える。評価 4.1・2,181円前後）
  https://www.amazon.co.jp/dp/B0G5B5DM5P
- **Anker Eufy (ユーフィ) SmartTrack Link（Android用）**（Android のみで使える。評価 4.0・2,650円前後）
  https://www.amazon.co.jp/dp/B0D9VTLK47

評価と値段は2026年11月16日のAmazon.co.jpの表示。タグは自分の持ち物を探すためのもの。人の後をつけるのに使ってはいけない。

まとめ

チェックシート

使っているものに印を付け、済ませた日を書く。家族のスマホを一緒に設定するときは、人ごとに1枚ずつ。

	段	端末・サービス	いちばん強い方法	済ませた日
☐	端末そのもの	**iPhone**	顔（Face ID）か指（Touch ID）と、6桁のパスコード	
☐	端末そのもの	**Android**	指紋か顔と、画面ロック（PIN）	
☐	端末そのもの	**Mac**	指（Touch ID）と、ログインのパスワード	
☐	端末そのもの	**Windows**	Windows Hello（顔・指紋・PIN）	
☐	合鍵のアカウント	**Google アカウント**	パスキー	
☐	合鍵のアカウント	**Apple アカウント**	2ファクタ認証。もっと強くするならセキュリティキー（2本）	
☐	合鍵のアカウント	**Microsoft アカウント**	パスキー。できればパスワードを外す	
☐	合鍵のアカウント	**Yahoo! JAPAN ID**	パスキー。付けたらパスワードを無効に	
☐	合鍵のアカウント	**LINE アカウント**	パスキー。「メールアドレス・パスワードでログイン」はオフ	
☐	電話番号の元（携帯会社）	**dアカウント（ドコモ）**	パスキーと、「いつもパスキー設定」	
☐	電話番号の元（携帯会社）	**au ID**	指紋・顔認証によるログイン（パスキーと同じ仕組み）	
☐	電話番号の元（携帯会社）	**SoftBank ID**	パスキー（スマホのWeb版 My SoftBank・My Y!mobile）	
☐	お金	**楽天 ID（楽天会員）**	パスキー	
☐	お金	**Amazon（amazon.co.jp）**	パスキーと、2段階認証（認証アプリ）	
☐	お金	**PayPay**	ログイン中の端末を確かめ、知らない端末を消す（パスキーは公式の説明に無い）	
☐	お金	**メルカリ**	パスキー	
☐	お金	**銀行**	その銀行のパスキー。無ければ、銀行の専用アプリの認証	
☐	お金	**証券**	パスキー（またはマイナンバーカードなどの認証）	
☐	SNS	**X（旧 Twitter）**	iPhoneとAndroidはパスキー（Xアプリで）。パソコンは認証アプリ	
☐	SNS	**Instagram**	パスキー（2段階認証も付けるなら認証アプリで）	
☐	SNS	**Facebook**	パスキーと、二段階認証（セキュリティキーか認証アプリ）	
☐	SNS	**TikTok**	パスキーと、2段階認証（認証アプリとメール）	
☐	約束	**届いたリンクからは入らない**		
☐	約束	**覚えのない「はい」は押さない**		
☐	約束	**お金と操作の電話は、一度切る**		

この冊子をつくったところ

Data is CITY Media

teleport.jp/dataiscity/

AI時代のセキュリティのメディア。情報漏えいやサイバー攻撃のニュースを、自分でできる守り方と一緒に読み解く。

特集「正しく怖がろう」のウェブ版

teleport.jp/dataiscity/right-fear/

端末とサービスを押すと、設定の手順が1手ずつ並ぶ。最新の版の冊子も、ここから落とせる。

セナリ学院

teleport.jp/scenari/

生成AIを学んで実践するオンラインスクール。ChatGPT、Claude、Geminiなどの生成AIを、仕事や暮らしで使いながら学ぶ。攻撃にも守りにもAIが使われる今、AIを自分で使ってみることが、AIを正しく怖がる近道になる。

Data is CITY Media とセナリ学院は、どちらもテレポート株式会社が運営している。

正しく怖がろう

自分のアカウントを守る設定の手引き

版	第5版（2026年11月17日 発行）
文	平野友康（テレポート株式会社）、マモル（Data is CITY Media 編集部のAIエージェント）
編集・発行	Data is CITY Media（テレポート株式会社）
ウェブ版	teleport.jp/dataiscity/right-fear/　最新の版は、ここから落とせる
運営	テレポート株式会社（Data is CITY Media teleport.jp/dataiscity/・セナリ学院 teleport.jp/scenari/）
手順の確かめ	各社の公式の説明を、編集部が開いて確かめた（2026年11月16日）。画面や手順は変わることがあるので、違っていたら公式の説明を正とする
出典	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年11月4日）、ANN「10月のサイバー攻撃が233件で過去最多」（2026年11月9日）、Anthropic「Disrupting the first reported AI-orchestrated cyber espionage campaign」（2025年11月13日）・「Project Glasswing」（2026年4月7日）、英国NCSC「Impact of AI on cyber threat from now to 2027」（2025年5月7日）、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」、金融庁「フィッシング耐性のある多要素認証」の広報（2026年4月16日）、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」（2025年10月15日施行）、各社の公式ヘルプ
画像	イラストと漫画はAIで生成した。画面の絵は再現で、実際の画面の写しではない。漫画の人物・会社・アプリ・出来事は架空
探し物タグ	評価と値段は 2026年11月16日 のAmazon.co.jpの表示。編集部は、売り上げから報酬を受け取っていない

版の履歴

第1版	2026年11月17日	初めて発行
第2版	2026年11月17日	専門家の確認を受けて直した（顔や指でのパスワードの自動入力とパスキーの違い、復旧の予備、乗っ取られたときの順番、XのAndroidのパスキーほか）。冒頭に、攻撃が増えた背景を足した
第3版	2026年11月17日	漫画「ケンジさんの家と、本物にしか合わない鍵」の4話を、1〜4の回の頭に入れた
第4版	2026年11月17日	「はじめに」を書き直した（AIで攻撃が別の次元に入ったこと、諦めるものと守れるもの）。表紙の題の重なりを直した
第5版	2026年11月17日	表紙と最後のページにData is CITY MediaのURL、最後のページにセナリ学院のURLを載せた

この冊子は、個人や家庭、学校や職場で、印刷して配ってよい。中身を書き換えて配るときは、書き換えたことが分かるようにしてほしい。