AIセキュリティ 今日からできる4つ 手順書 v1.1

Claude Code などのAIを仕事で使い始めた方のための、**パソコンを乗っ取られても大切な個人情報を守る**ための手順書です。

記事「AIセキュリティ｜Claude Codeに、パスワードを.envで渡すのも危険!?」でお話しした4つを、上から順に進められるようにまとめました。**全部を1日でやる必要はありません。**1章ずつ、終わったら □ に印を付けてください。

- 1章　自分のパソコンに外から入れる入口を、閉じる
- 2章　二段階認証を、強い種類に替える
- 3章　パスワードを、メモ帳から管理の道具に移す
- 4章　AIに鍵（APIキー・パスワード）を読ませない

このPDFは人が読むための手順書です。「Claude Codeに渡す文」は、PDFから文だけをコピーして貼ってください。

1章　自分のパソコンに外から入れる入口を、閉じる

外から入れるパソコンは、他人も入れるかもしれません。入口が開いていないかは、Claude Code に確かめさせられます。

手順1　入口の一覧を出してもらう

動かしっぱなしのパソコンで Claude Code を立ち上げ、次の文をそのまま渡します。

```
このパソコンで、外からアクセスできる仕組みが動いていないかを確かめたいです。
Cloudflare Tunnel・ngrok・Tailscale など、ローカルのサーバーやこのパソコンに外から入れるトンネルが開いていたら、すべて一覧にしてください。
それぞれ「何のために開いているか」「閉じても困らないか」も添えてください。まだ何も止めないでください。
```

私のパソコンでは、こう返ってきました。外から入れる入口は Chrome リモート デスクトップの1つだけで、ほかは「そのとき開いているだけ」の口でした。

口	中身	判断
135番	Windows 自体が使う口	ファイアウォールが3つともオンなので、外からは入れません
Zoom・Chrome	通話や通信のために、そのとき開いている口	トンネルではありません。アプリを閉じれば閉じます
Playwright	調べものの道具が、使っている間だけ開いた口	確かめている間に閉じました。常に開いている口ではありません

結論：外から入れる入口は Chrome リモート デスクトップの1つだけです。使っている入口なので、手順2（止める）は今回「止めるものなし」になります。

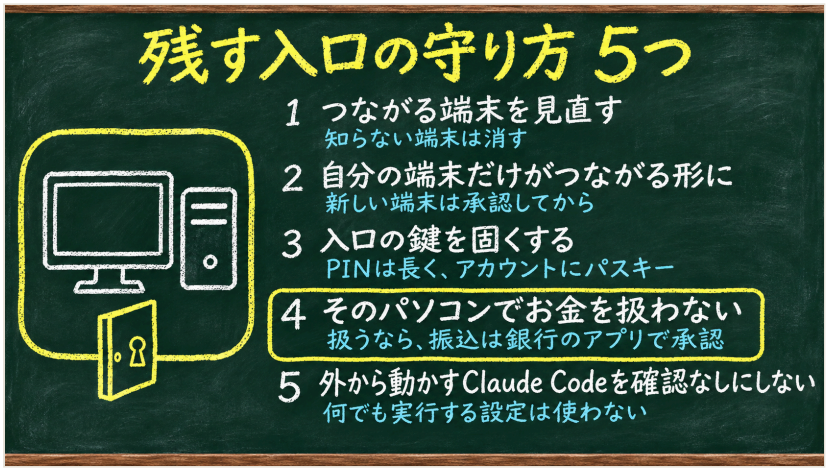
Claude Code が出した入口の一覧

手順2　使っていないものを閉じる

一覧の中で使っていないものがあれば、次の文を渡してください。

```
一覧のうち、〇〇（使っていないものの名前）を止めてください。
パソコンを立ち上げ直しても、自動で動き出さないようにしてください。
止めたあと、もう一度一覧を出して、止まったことを見せてください。
```

手順3　出先から使うために残すなら、5つを守る



残す入口の守り方5つ

- □ **つながる端末を見直す**：Chrome リモート デスクトップなら remotedesktop.google.com/access、Tailscale なら管理画面で、登録されている端末を見る。知らない端末・もう使っていない端末は消す
- □ **入口の鍵を固くする**：Chrome リモート デスクトップの PIN は6桁より長くする。入口のアカウント（Chrome リモート デスクトップなら Google）にはパスキーを入れる（2章）
- □ **お金は承認で守る**：外から入れるパソコンで、もう銀行や証券にログインしてしまっているなら、振込・出金のときに銀行のアプリで承認する設定にしておく。パソコンに入られても、スマホの承認が無ければお金は動きません

Chrome リモート デスクトップを使っている方へ

remotedesktop.google.com/access を開くと、つながる端末の一覧が出ます。



Chrome リモート デスクトップの端末一覧（端末名は隠してあります）

- □「リモートのデバイス」に、知らない端末・もう使っていない端末があれば、右のゴミ箱で消す
- □「このデバイス」の下に「**1つ以上のクライアントが PIN の入力なしで接続できるように設定されています**」と出ていたら、「表示 / 編集」を押して、PIN なしでつなげる端末を消す。以前つないだときに「この端末では PIN を聞かない」を選ぶと、ここに残ります。残っていると、PIN をどれだけ長くしても、その端末からは素通りです

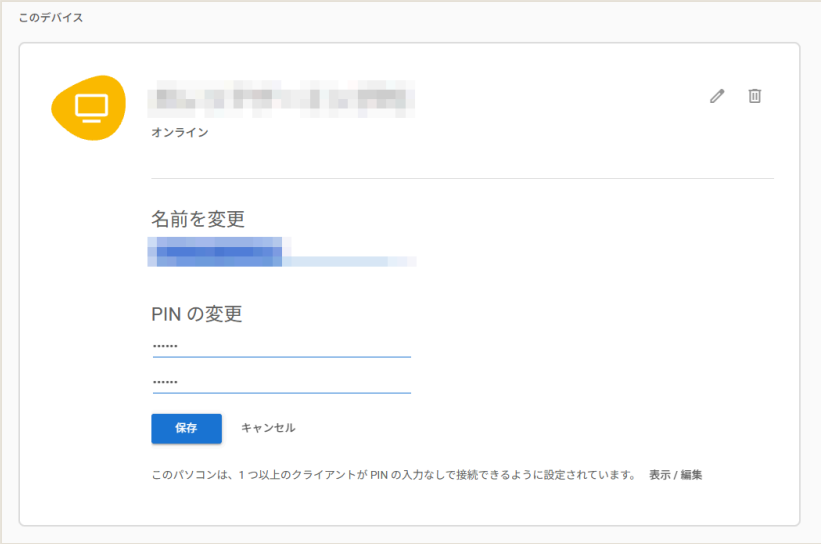


「表示 / 編集」で出る、PIN なしでつなげる端末の一覧。右のゴミ箱で1つずつ、「すべて削除」でまとめて消せます

一覧には、つないだ日と、つないだ側の種類（MacIntel＝Mac、Win32＝Windows、iPhone）が出ます。消しても、次につなぐときに PIN を1回聞かれるだけです。迷ったら「すべて削除」で構いません

- □ PIN を変えるには、「**このデバイス**」の行の鉛筆のマークを押します。「PIN の変更」の欄に新しい PIN を2回入れて「保存」。「リモートのデバイス」の鉛筆では名前しか変えられないので、PIN を変えた

いパソコンの前で、そのパソコンから開いてください



「このデバイス」の鉛筆で出る、PIN の変更の欄（パソコンの名前は隠してあります）

ツールごとの細かい設定は、次のとおりです。

- ☐ 誰でも開けるURLが出る形（ngrok など）はやめて、自分の端末どうしだけがつながる **Tailscale** にする。Cloudflare Tunnel を使うなら、前にログインの壁（Cloudflare Access）を置く
- ☐ Tailscale の管理画面で「新しい端末は承認してからつなぐ」設定（Device approval）をオンにする。Tailscale にログインするアカウント（Google や Apple）には、パスキーを入れる（2章）
- ☐ 入口は、出先に出る日だけオンにする。家にいる日は閉じておく
- ☐ 外から入れるパソコンでは、銀行や証券にログインしない。ブラウザにパスワードを保存しない（保存したままにするなら、3章の「Windows Hello」をオンにする）
- ☐ スマホの画面をパソコンに映す設定（ミラーリング）は切る。外から動かす Claude Code は、確認なしで何でも実行する設定（`--dangerously-skip-permissions`）にしない

2章　二段階認証を、強い種類に替える

二段階認証は、入れているかどうかより、どの種類かで守れる範囲が変わります。弱い順に、こうなります。

1. SMS（ショートメッセージで届く数字）
2. 6桁の数字（認証アプリで30秒ごとに変わる数字）
3. プッシュ通知（スマホに出る「はい」を押す）
4. **パスキー・物理キー**（偽サイトでは、そもそも反応しない）

1〜3は、偽サイトに打ち込んだ数字をその場で本物のサイトへ中継されると破られます。4は本物のサイトにしか反応しません。

手順1　親玉の3つにパスキーを入れる

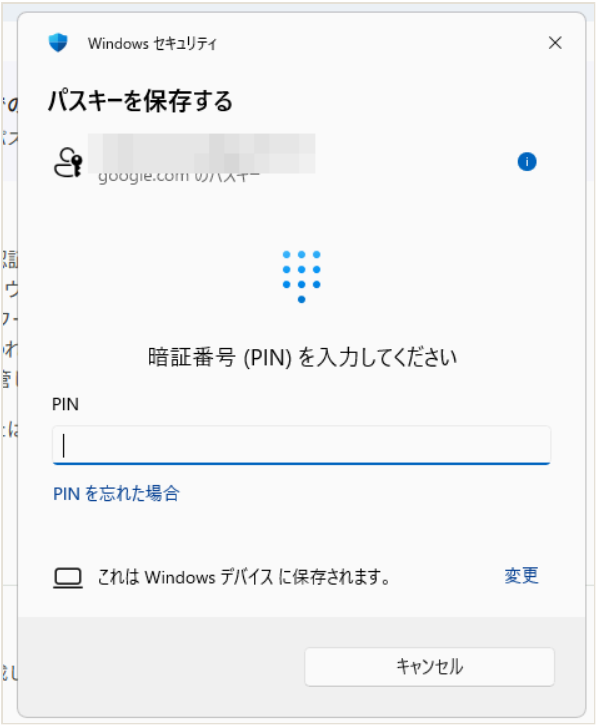
ほかのサービスのログインは、この3つから広がっています。ここから始めます。

- □ **Googleのアカウント**：Googleアカウントの管理画面 →「セキュリティ」→「パスキーとセキュリティキー」→「パスキーを作成」



Googleの「パスキーとセキュリティキー」の画面

「パスキーを作成」を押すと、Windows なら PIN（パソコンを開くときの暗証番号）を聞かれます。入れれば、このパソコンにパスキーが保存されます。



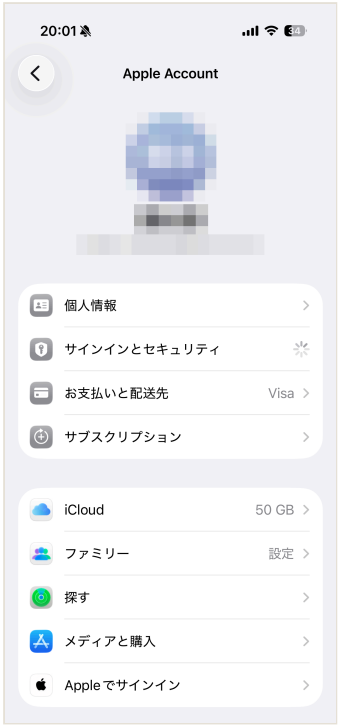
Windowsにパスキーを保存する



パスキーが作成されました

パスキーは、作った端末で使うものです。iPhone で作ったパスキーでパソコンからログインしようとすると、「Bluetooth をオンに」と出て、iPhone をパソコンの近くに置く必要があります。面倒に見えますが、近くにいないと使えないので、遠くにいる犯人にも使えません。ふだん使う端末ごとに1つずつ作るか、どの端末にも挿せる物理キーを使ってください。

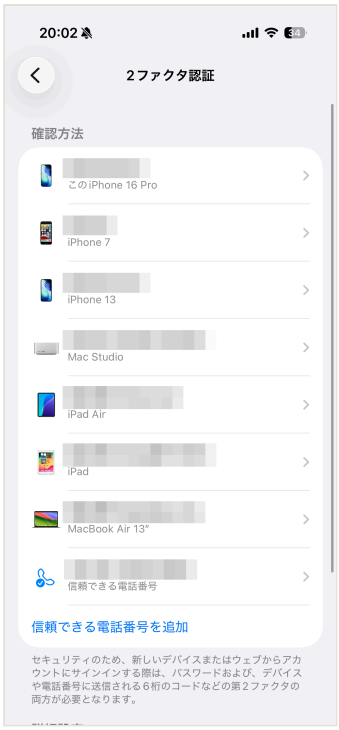
- □ **Appleのアカウント**：iPhone の「設定」→ いちばん上の自分の名前 →「サインインとセキュリティ」→「2ファクタ認証」の矢印を押す。信頼できる端末の一覧が出れば、オンになっています（いまの iOS は「オン」の文字が出ません。オフなら、オンにするボタンが出ます）。物理キーを持っていれば「セキュリティキー」から登録できる



Apple Account の画面。いちばん上の自分の名前から入る（名前とメールは隠してあります）



「サインインとセキュリティ」の画面



「2ファクタ認証」の矢印を押すと出る、信頼できる端末の一覧。これが出ればオン（端末の名前と電話番号は隠してあります）

知らない端末や、もう使っていない端末があれば、押して外しておきます。

- □ **パスワード管理の道具（3章）**：ログインに二段階認証をかけ、パスキーか物理キーを選ぶ

二段階認証の設定で出る QR コードと英数字のキーは、撮らない・人に見せない。6桁の数字は30秒で切れますが、QR とキーがあれば、誰でも同じ6桁を作り続けられます。

手順2　お金まわりを固める

- □ 銀行・証券の二段階認証を、使える中でいちばん強い種類に替える（パスキー → 物理キー → プッシュ通知の順に選ぶ）
- □ 出金先を固定し、ログインと取引の通知をオンにする
- □ 振込・出金の承認を、銀行のアプリ（スマホ）でする設定にする。パソコンでログインしたままでも、スマホで承認しなければお金は動きません

手順3　予備を用意する

- □ 認証アプリ（Google Authenticator など）のコードを、Googleのアカウントに同期しているかを見る。同期は、**Googleにパスキーか物理キーを入れたあとなら、そのままで構いません。**Googleのログインが SMS だけのまま同期していると、Googleが破られたときに一緒に破られます。順番が大事です

- ☐ バックアップコードは紙に書いて、パソコンから離れた場所に置く

3章　パスワードを、メモ帳から管理の道具に移す

パソコンに入られた瞬間、メモ帳やスプレッドシートの鍵は全部読まれます。だから、置き場所をパスワード管理の道具に移すのです。

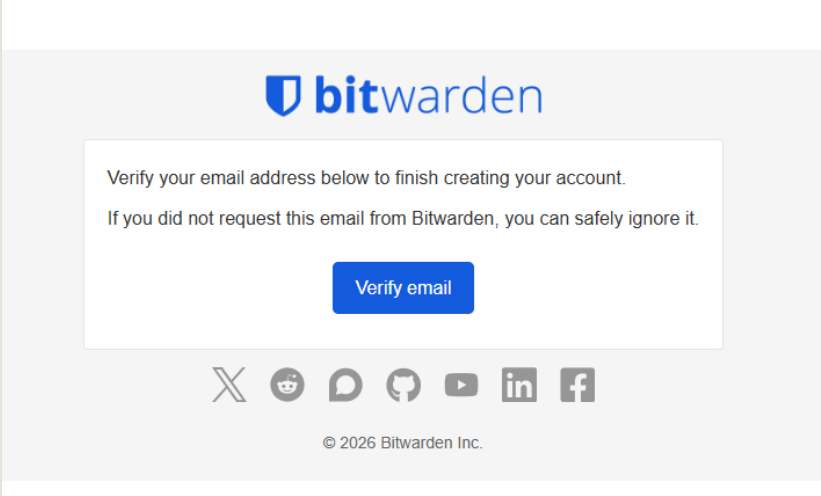
	1Password	Bitwarden
料金	有料	無料のプランあり
AIとの組み合わせ	AIにパスワードを渡さないまま、ログインだけさせられる	「シークレットマネージャー」で、APIキーを使うときだけ取ってこられる

守りの強さはほぼ同じです。迷ったら、まず無料で始められる Bitwarden で構いません。

手順1　Bitwarden を始める

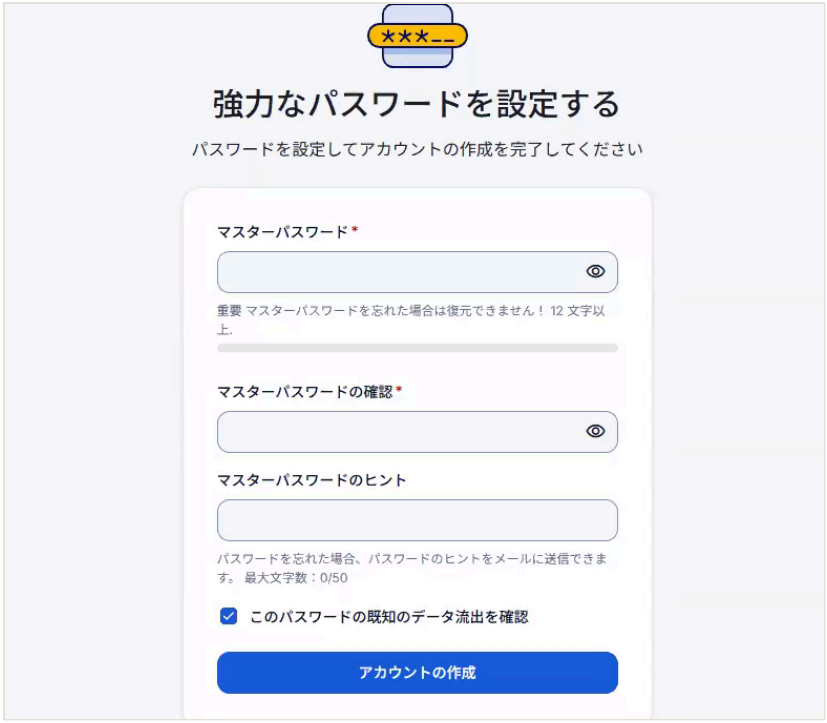
ここでは Bitwarden で進めます（1Password も流れは同じです）。

- ☐ bitwarden.com で「アカウントを作成」→ メールアドレスを入れる → 届いたメールの「Verify email」を押す



Bitwardenから届く確認のメール

- ☐ **マスターパスワード**を決める。Bitwarden のすべての鍵を開ける、ただ1つの鍵です。長い文（言葉を4つ以上つなげたもの）にして、紙に書いて家の中の決めた場所に置く。**忘れると、Bitwarden の会社でも戻せません**



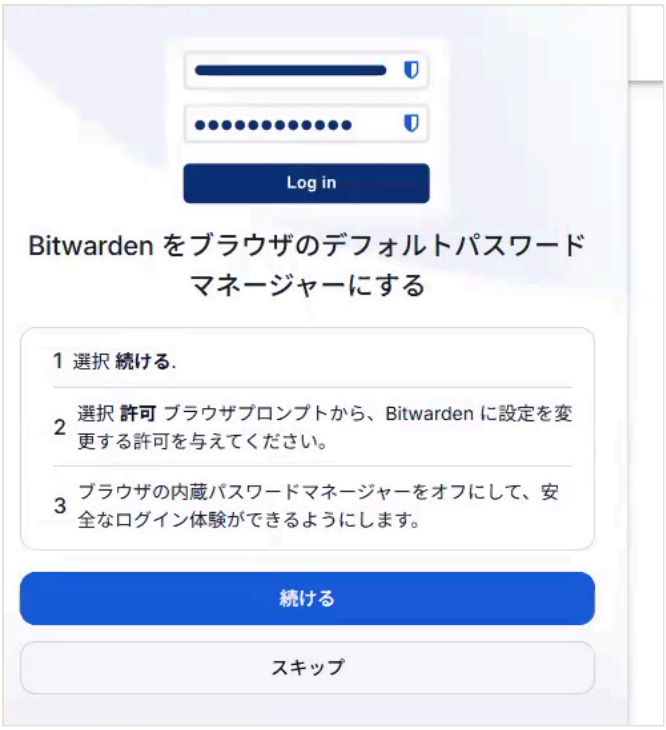
マスターパスワードを設定する画面

- ☐ Chrome に拡張機能「Bitwarden パスワードマネージャー」を入れて、ログインする



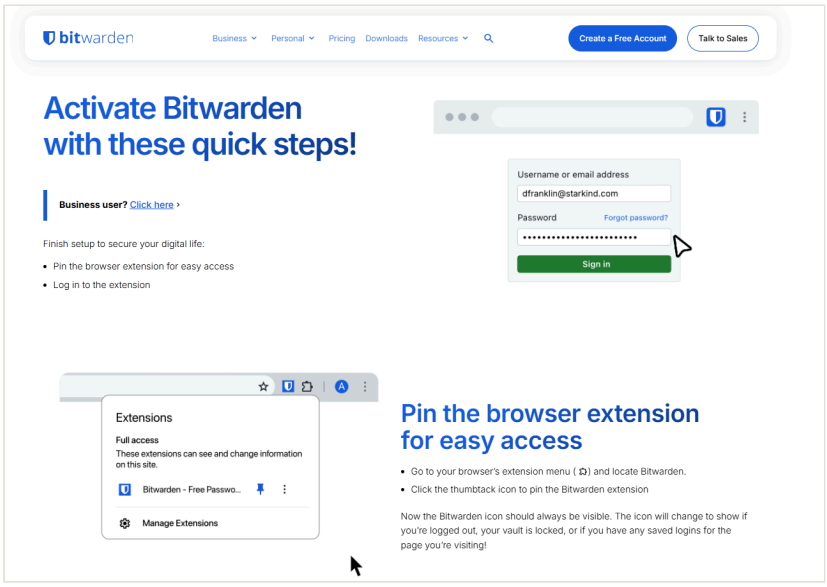
Bitwardenの拡張機能のログイン画面

- □「Bitwarden をブラウザのデフォルトパスワードマネージャーにする」が出たら「続ける」→「許可」。Chrome がパスワードを保存しに来なくなります



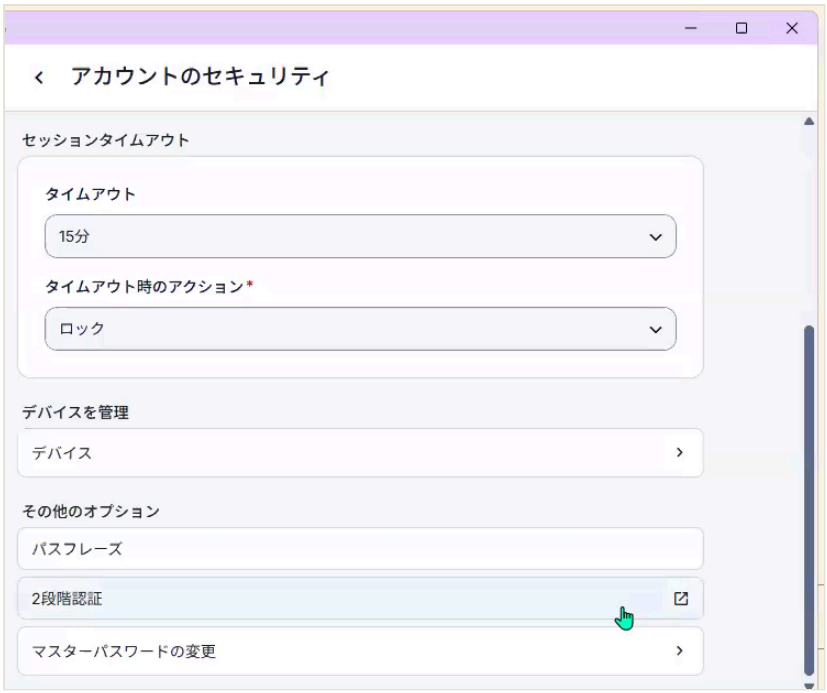
Bitwardenを既定のパスワードマネージャーにする

- □ 拡張機能をツールバーに固定する（右上のパズルのマーク → Bitwarden のピン）



拡張機能を固定する案内

- □ **自動ロックを15分に。**拡張機能の「設定」→「アカウントのセキュリティ」→「タイムアウト」を15分、「タイムアウト時のアクション」を「ロック」にする。席を離れても、15分でまたマスターパスワードが要るようになります



タイムアウトを15分・ロックにする

- ☐ **Bitwarden 自体にも二段階認証をかける。**ウェブの保管庫 →「設定」→「セキュリティ」→「2段階認証」。物理キーがあれば「FIDO2 WebAuthn」、無ければ「認証アプリ」を選ぶ



2段階認証の種類の一覧

認証アプリを選ぶと、QR コードとキーが出ます。スマホの認証アプリで読み取り、出た6桁を入れて「有効化」を押します。**この QR とキーは撮らない・人に見せない**（2章）。下の画像は、QR とキーを隠してあります。



認証アプリの設定（QRとキーは隠してあります）

「2段階認証」の画面にある「リカバリーコードを確認」で出るコードは、紙に書いてマスターパスワードと別の場所に置いてください。スマホをなくしたときの、ただ1つの戻り道です。

なお、拡張機能の設定に出てくる「アカウントのパスフレーズ」（言葉が5つ並んだもの）は、ログインのときに本物の Bitwarden かを見分けるための目印です。秘密の言葉ではないので、覚えなくて大丈夫です。

手順2　Chromeに保存したパスワードを移す

- ☐ Chrome の「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」→「パスワードをエクスポート」で、CSVファイルに書き出す

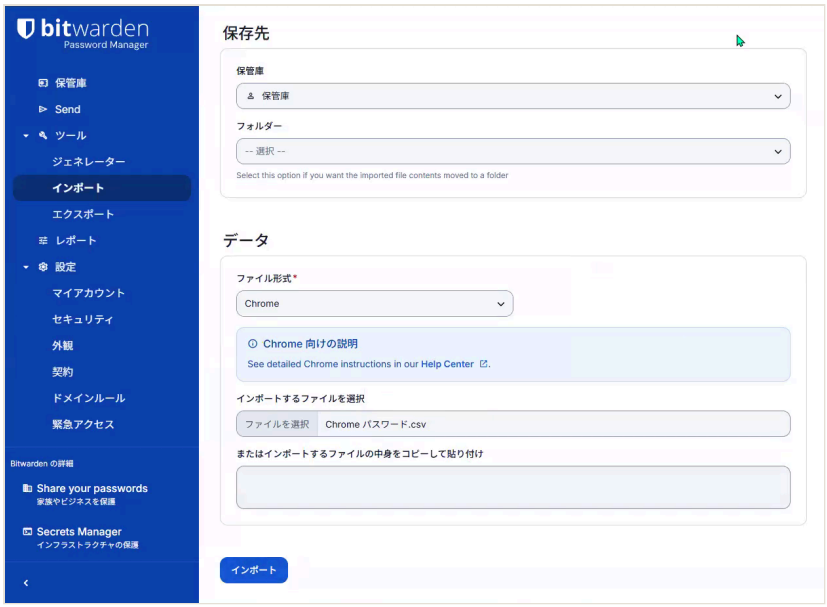


Chromeの「自動入力とパスワード」



Googleパスワードマネージャーの設定。下の方に「パスワードをエクスポート」

- □ 取り込む
- Bitwarden：ウェブの保管庫 →「ツール」→「インポート」→ ファイル形式で Chrome（csv）を選び、書き出したファイルを選んで「インポート」
- 1Password：1Password.com にログイン → 右上の自分の名前 →「インポート」→ Chrome を選ぶ



Bitwardenのインポートの画面



取り込みが終わった画面

- □ **書き出したCSVファイルは、取り込んだらすぐに消す（ゴミ箱も空にする）**。パスワードがそのままの文字で入っています
- □ Chrome に残したパスワードは、全部消さなくても構いません。代わりに、上の設定画面の「**Windows Hello を使用してパスワードを入力する**」をオンにします。外から入った人は、パソコンの PIN が無いと自動入力できなくなります。銀行・証券のパスワードだけは、Chrome から消しておくと安心です

手順3　メモ帳・スプレッドシートの鍵を移す

- □ パソコンのメモ帳、スプレッドシート、Googleドキュメントに書いたパスワードやAPIキーを、1件ずつ管理の道具に入れる
- □ 入れ終わったら、元のメモは消す

- ☐ パスワードを人に渡すときは、メールやチャットに貼らず、Bitwarden の「Send」（開ける回数と、開けなくなる日を決めて渡せるリンク）を使う

手順4　大事な所のパスワードを替える

- ☐ 銀行・お金・お客さんの情報がからむ所は、今日のうちに、管理の道具が作る強いパスワードに替える
- ☐ 同じパスワードを使い回している所を、そこから先に替える
- ☐ 漏れていないかを調べる（1Password は「Watchtower」、Bitwarden はレポート機能）

4章　AIに鍵（APIキー・パスワード）を読ませない

Claude Code に鍵を貼るのも、「.envに書いてあるから読みに行って」と頼むのも、AIが鍵を読むことに変わりはありません。読んだものは、会話としてAIの会社に送られ、履歴として自分のパソコンにも残ります。

手順1　鍵のファイルを読みに行けないようにする

Claude Code に、次の文をそのまま渡します。

```
Claude Codeの設定を見直したいです。
.env や .pem など、パスワード・APIキー・トークンが入っているファイルは、あなたが直接読みに行かないようにしてください。
グローバルの設定（settings.json）も含めて確認し、いま読みに行ける状態の場所があれば教えてください。

今後、鍵の保存・管理・取得は、あなたが直接読むのではなく、プログラムやコマンドを実行して行う形にしたいです。
会話の中に、パスワードやトークンがそのまま出てこないようにしてください。
```

- ☐ 設定を直してもらったら、確かめる。中身が空の .env を試しのフォルダに置き、「この .env を読んで」と頼んで、断られることを見る

手順2　鍵は、プログラムに取ってこさせる

APIキーを使う作業（画像を作る、など）は、プログラムが管理の道具から鍵を取ってくる形にします。
Claude Code はそのプログラムを動かすだけなので、鍵の中身を一度も目にしません。

```
○○（作業の名前）のプログラムで使っているAPIキーを、.env ではなく 1Password（または Bitwarden）から取ってくる形に作り直してください。
鍵の中身は、会話にも画面にも出さないでください。
作り直したら、鍵を出さずに動くかを1回試して、結果だけ教えてください。
```

手順3　漏れても困らない形にしておく

- ☐ APIキーには、使える金額の上限を決めておく。または、先に入れた分しか使えない払い方にする
- ☐ 漏れたかもしれないと思ったら、すぐに新しいキーに作り直し、古いキーは消す

手順4　Claude Code を最新にする

- ☐ ターミナルで **claude update** と打つ。最新でなければ新しくなり、最新ならそのままです

最後に：やったことの記録

やったこと	日付
1章　入口の一覧を出し、使っていないものを閉じた	
2章　Google・Apple・パスワード管理の道具を固めた	
2章　銀行・証券の二段階認証と通知を見直した	
3章　パスワードを管理の道具に移し、CSVを消した	
3章　大事な所のパスワードを替えた	
4章　鍵のファイルを読めないようにして、確かめた	
4章　APIキーに上限を決めた	

わからないところがあれば、受け取った公式LINEにそのまま返信してください。どの章の、どの手順で止まったかを書いていただければ、こちらで確認します。

株式会社スターストリーム・スタジオ