Password Vault Comparison Guide

パスワード管理ソリューション比較

Table of Contents

目次

パスワード管理ソリューション比較

日付: 2026年2月20日

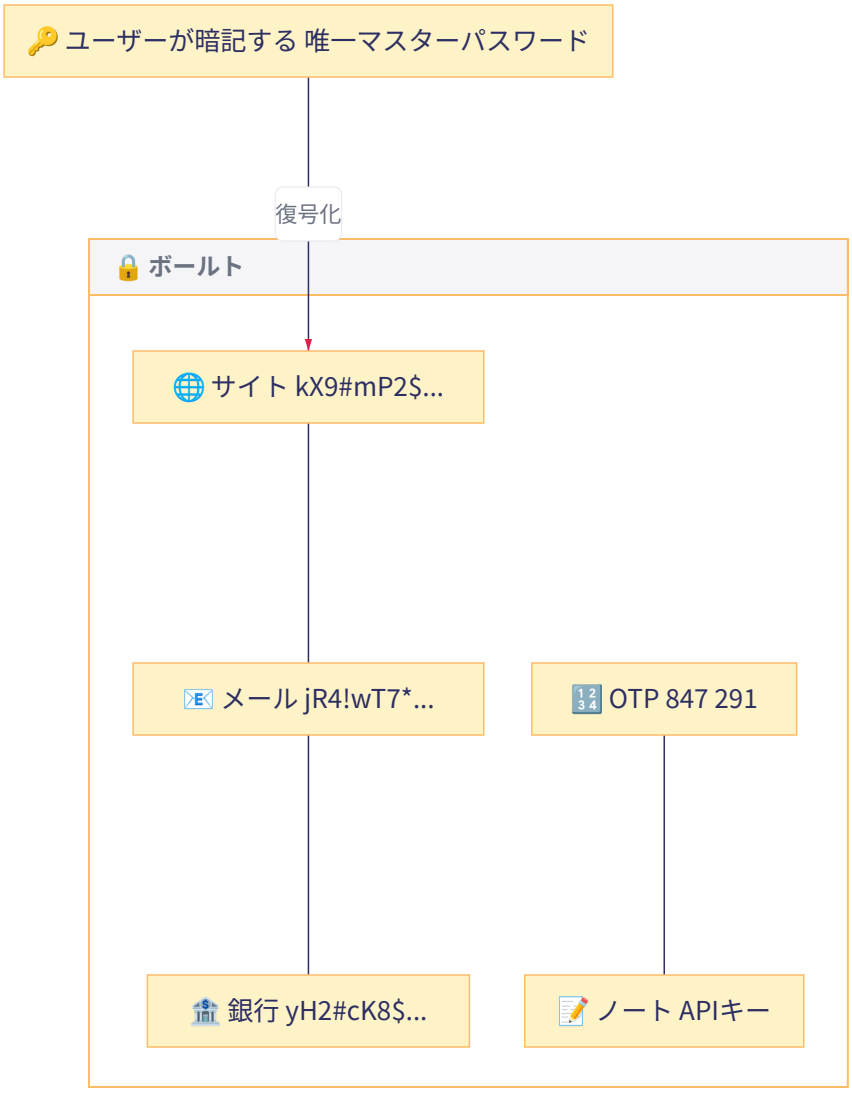
エグゼクティブサマリー

パスワードマネージャーは、デジタルアイデンティティを保護するための必須ツールです。しかし、すべてのパスワードマネージャーが同じ設計思想で作られているわけではありません。本書では、セキュリティアーキテクチャ、機能、実用的な観点から主要なソリューションを比較し、お客様のニーズに最適なソリューション選定をサポートします。

主な推奨事項: 最大限のセキュリティ、最大限の利便性、またはその両方のバランスなど、優先事項に基づいてソリューションを選択してください。本書で紹介するすべてのソリューションは、パスワードマネージャーを使用しない場合と比較して、大幅にセキュリティが向上します。

マスターパスワード：すべての鍵

マスターパスワードは、あなたが作成する最も重要な認証情報です。他のすべてのパスワードを保護します。慎重に選び、しっかり保護してください。


🔑 ユーザーが暗記する 唯一マスターパスワード
復号化
🔒 ボールト
🌐 サイト kX9#mP2$...
📧 メール jR4!wT7*...
🔢 OTP 847 291
🏦 銀行 yH2#cK8$...
📝 ノート APIキー

コンセプトはシンプルです：

- **覚えるパスワードは1つ** — マスターパスワード
- **覚えなくていいパスワードは数百** — ボールトが生成・保存

ボールト内の各パスワードは、長く、ランダムで、ユニークにできます。`kX9#mP2$vL5@nQ8&jR4!`を暗記する必要はありません。ボールトが処理します。入り方だけ覚えればいいのです。

強力なマスターパスワードの選び方

目標は、**十分に長くて安全**でありながら、**忘れないように覚えやすい**パスワードです。

推奨アプローチ：パスフレーズを使用する

`Tr0ub4dor&3`のような複雑な文字列の代わりに、ランダムな単語のフレーズを使用します：

```
correct horse battery staple
```

または、個人的な意味を持つ覚えやすい文章：

```
娘のゆきは2019年3月に生まれました!
```

なぜこれが機能するか：

- 複雑さよりも長さが重要—25文字のパスフレーズは、8文字の記号の羅列より強力
- 実際に覚えられる
- 確実にタイプできる

> **入力方法を考慮する**
>
> マスターパスワードはデスクトップとモバイルの両方で入力する必要があります。以下の点に注意してください：
>
> - **記号はモバイルで入力しにくい場合がある：** `|`、`~`、`^`、`\`などの文字は、スマートフォンのキーボードで見つけるのに複数回タップが必要なことがあります。記号を使う場合は、モバイルで簡単にアクセスできる一般的なもの（`!`、`@`、`#`、`$`など）にしましょう。
> - **スペースは使いやすい：** スペースを含むパスフレーズ（`correct horse battery staple`）は、どのデバイスでも簡単に入力できます。
> - **生体認証で入力を減らす：** ほとんどのパスワードマネージャーは、初期設定後にFace IDや指紋でロック解除できます。有効にすると、モバイルでマスターパスワードを入力することはほとんどなくなり、より長く複雑なパスワードが実用的になります。
>
> マスターパスワードを決める前に、スマートフォンでテストしてみてください。

避けるべきもの：

- 辞書の単語だけ（`password`、`sunshine`）
- オンラインで簡単に見つかる個人情報（誕生日、ペットの名前、会社名）
- パターン（`123456`、`qwerty`、`Password1!`）
- 他のアカウントのパスワードの再利用

> **重要：マスターパスワードをバックアップしてください**
>
> マスターパスワードを忘れると、保存されているすべてのパスワードへのアクセスが永久に失われます。ほとんどのプロバイダーはデータを復旧できません。これは制限ではなく、セキュリティ機能です。
>
> **マスターパスワードを紙に書いて、安全な物理的場所に保管してください**（金庫、貸金庫、または信頼できる人のもと）。デジタルで保存しないでください。この紙のバックアップは、パスワードを忘れた場合や、万が一の際に代理でアクセスが必要な場合のセーフティネットです。

ボールト内：マネージャーに任せる

パスワードマネージャーの中では、個々のパスワードを覚える必要はありません。各アカウントに長くランダムなパスワードを生成させましょう：

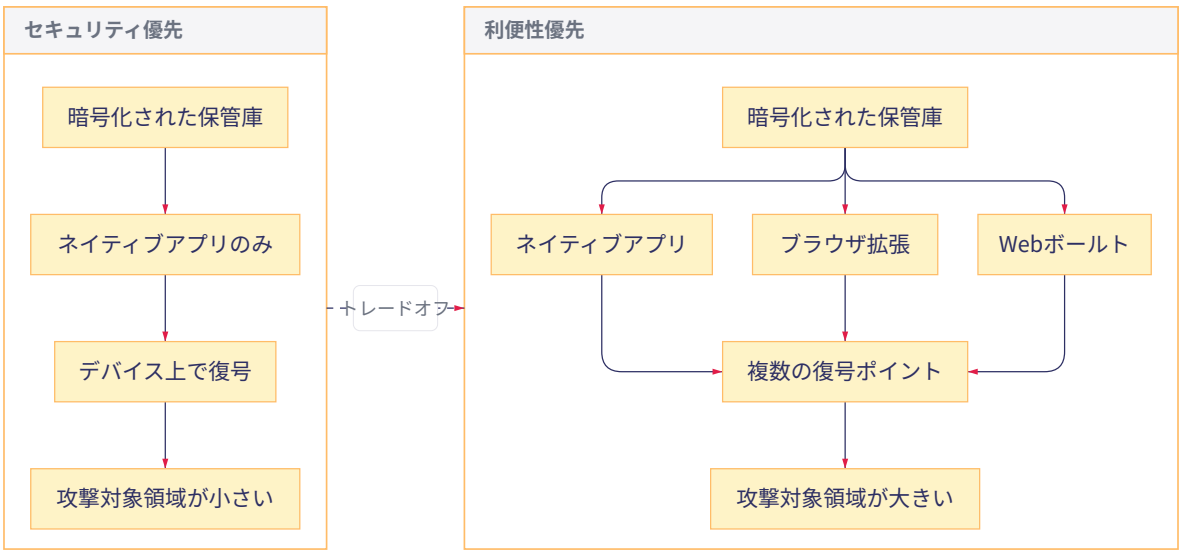
```
kX9#mP2$vL5@nQ8&jR4!wT7*
```

これらは推測不可能で覚えることも不可能ですが、それで問題ありません。マネージャーが処理してくれます。

セキュリティアーキテクチャの理解

個々の製品を比較する前に、パスワードマネージャー設計における2つの基本的なアプローチを理解することが重要です。

セキュリティ優先設計 vs 利便性優先設計



セキュリティ優先設計:

- 復号は専用アプリケーション内でのみ実行
- 侵害される可能性のあるブラウザ拡張機能やWebインターフェースなし
- 新機能の追加に慎重（各機能のセキュリティ影響を評価）
- 例: Codebook

利便性優先設計:

- シームレスなユーザー体験のための複数のアクセスポイント
- ブラウザ拡張機能によるワンクリック自動入力
- 任意のブラウザからアクセス可能なWebボールト
- 各アクセスポイントを保護するセキュリティ対策を追加
- 例: 1Password、Bitwarden

どちらのアプローチも間違いではありません。異なる優先事項を表しています。適切な選択は、脅威モデルと使いやすさの要件によって異なります。

> **「攻撃対象領域」とは？**

パスワード保管庫を家に例えてみましょう。ドアや窓を増やすほど、泥棒が侵入できる可能性のある入口が増えます。この入口の総数が「攻撃対象領域」です。

セキュリティ優先のパスワードマネージャーは、頑丈に強化された1つのドアを持つ家のようなものです。利便性優先のマネージャーは、複数のドア（玄関、裏口、ガレージ、勝手口）を持つ家のようなもので、あなたにとっては便利ですが、それぞれのドアに独自の鍵とセキュリティ対策が必要です。

どちらも安全にできますが、ドアが1つだけのアプローチは、問題が発生する可能性のある箇所が少なくなります。

クラウド同期の違い

従来型クラウドボールト（1Password、Bitwarden）：

- 任意のWebブラウザからパスワードにアクセス可能
- 共有または一時的なコンピューターでパスワードにアクセスするのに便利
- ブラウザ内でJavaScriptによる復号が実行される
- プロバイダーのサーバーが悪意のあるコードを配信しないことへの信頼が必要

真のゼロ知識同期（Codebook Cloud）：

- クラウドはデバイス間で暗号化データを移動するため**のみ**に使用
- Webインターフェースなし—パスワードはネイティブアプリでのみ表示可能
- データはサーバーに到達する前に**同期キー**で暗号化される
- **Zeteticは同期キーを持っていない**—文字通りデータを復号できない
- 法執行機関に強制されても、ハッカーに侵害されても、プロバイダーはパスワードにアクセスできない

> ⓘ **「ゼロ知識」とは？**
>
> 「ゼロ知識」とは、サービスプロバイダーがデータの内容について何も知らないことを意味します。暗号化された保管庫を保存しますが、読むことができません。
>
> **ただし、「ゼロ知識」の主張はすべて同じではありません：**

タイプ	仕組み	プロバイダーはアクセス可能？
Webボールト	パスワードでブラウザ内のデータを解除。プロバイダーのサーバーが復号コードを送信。	理論上可能—パスワードをキャプチャする悪意のあるコードを送信できる
同期専用（Codebook）	別個の同期キーがアップロード前にデータを暗号化。このキーはデバイスから離れない。	不可能—キーを持っておらず、攻撃できるWebインターフェースもない

> Codebook Cloudでは、同期キーはデバイス上で生成され、そこに留まります。Zeteticのサーバーは、復号できない暗号化されたデータの塊しか見ることができません。これは、Webアクセスを提供するサービスとはアーキテクチャ的に異なります。

> ⓘ **なぜWebボールトはリスクが高いのか？**
>
> Webボールト（1Password.comやvault.bitwarden.comなど）にログインすると、ブラウザがプロバイダーのサーバーからJavaScriptコードをダウンロードし、そのコードがパスワードを復号します。
>
> **リスク:** プロバイダーが常に正当なコードを送信することを信頼しています。サーバーが侵害された場合、不正な従業員が変更を加えた場合、または法執行機関が特定のユーザーに対してコードを変更するよう強制した場合、JavaScriptは理論的にマスターパスワードをキャプチャできます。 **これは仮定の妄想ではありません**—セキュリティ研究者がWebベースのパスワードアクセスについて長年議論してきた理由です。ほとんどのユーザーにとって、リスクは低いです。高セキュリティユーザー（経営者、ジャーナリスト、活動家）にとって、このアーキテクチャの違いは重要です。
>
> Webボールトを持たないパスワードマネージャーは、このリスクカテゴリ全体を排除します。

ソリューション比較

概要マトリックス

機能	Codebook	1Password	Bitwarden	Appleパスワード
アーキテクチャ	セキュリティ優先	利便性優先	利便性優先	プラットフォーム統合
TOTPコード	√ 内蔵	√ 内蔵	√ 内蔵	√ 内蔵
ブラウザ拡張機能	✗（設計上）	√	√	⚠ Chrome/Edgeのみ、Windowsで不安定
Webボールト	✗（設計上）	√	√	✗
対応プラットフォーム	Win, Mac, iOS, Android	全て + Linux	全て + Linux	Apple製品のみ（Windowsは不安定）
家族/チーム共有	√（2026年新機能）	√	√	Appleユーザーのみ
オープンソース	SQLCipher（暗号化）	✗	√ 完全	✗
セルフホストオプション	ローカルのみ可能	✗	√	✗
漏洩監視	√ HaveIBeenPwned	√ Watchtower	√ レポート	√ 基本的
価格（個人）	約9,000円/年	約5,500円/年	無料～約1,500円/年	無料

TOTPとは？

TOTP（Time-based One-Time Password、時間ベースのワンタイムパスワード）は、30秒ごとに変わる6桁のコードの背後にある技術です。ウェブサイトが二要素認証のオプションとして「認証アプリ」を提供している場合、TOTPを使用しています。

最新のパスワードマネージャーは、パスワードと一緒にこれらのコードを保存して生成できるため、ほとんどのアカウントで別の認証アプリは必要ありません。多くの文脈で「2FA」（二要素認証）や「MFA」（多要素認証）という用語がTOTPと互換的に使用されています。

ビジネス向け料金比較

組織向けには、3つの主要ソリューションすべてが管理機能、一括請求、オンボーディングサポートを含むビジネス専用プランを提供しています。**ビジネス目的でこれらのツールを使用する場合、ビジネスプランが必要**であり、組織管理に不可欠な機能を提供します。

チーム規模	Codebook Business	1Password	Bitwarden Teams	Bitwarden Enterprise
5ユーザー	33,750円/年*	約36,000円/年 (Starter)	約36,000円/年	約54,000円/年
10ユーザー	67,500円/年*	約36,000円/年 (Starter)	約72,000円/年	約108,000円/年
50ユーザー	337,500円/年*	約720,000円/年	約360,000円/年	約540,000円/年
ユーザー単価	$5/月 ($3.75 *)	$7.99/月	$4/月	$6/月

*Codebook Businessは$5/ユーザー/月から開始で、イソリアのディスカウントコードにて25% OFF。大規模チーム向けのボリュームディスカウントもあり。

ビジネスプランの主な機能:

機能	Codebook Business	1Password Business	Bitwarden Teams	Bitwarden Enterprise
一括請求	√	√	√	√
ユーザー管理ダッシュボード	√	√	√	√
共有権限設定	√	√	√	√
SSO連携	✗	√	✗	√
ディレクトリ同期 (SCIM)	✗	√	✗	√
セルフホストオプション	✗	✗	√	√
ユーザーへの無料Families	✗	√	✗	√

ビジネスプランのリンク:

- **Codebook Business:**https://www.zetetic.net/codebook/business/
- **1Password Teams/Business:**https://1password.com/pricing/password-manager
- **Bitwarden Business:**https://bitwarden.com/pricing/business/

注: 大規模導入（一般的に100ユーザー以上）では、すべてのベンダーからボリュームディスカウントが利用可能です。カスタム価格についてはセールスまでお問い合わせください。

詳細プロファイル

Codebook（Zetetic社）

設計思想: 最小限の攻撃対象領域による最大限のセキュリティ

強み:

- 25年以上の実績、漏洩事故なし
- SQLCipher暗号化（NASA、Samsung、Fortune 500企業が使用）
- ブラウザ拡張機能やWebボールトがないため、ブラウザベースの攻撃ベクトルなし
- **真のゼロ知識クラウド同期:** Codebook Cloudは、デバイス上で生成されアップロードされない同期キーでデータを暗号化します。Zeteticはパスワードを見ることができず、引き渡すよう強制されることもなく、データが露出するような方法でハッキングされることもありません。
- マスターパスワードはクラウド暗号化に使用されない—完全にランダムな別の同期キーがパスワードクラッキング攻撃から保護
- セキュリティに特化した企業による迅速で個人的なカスタマーサポート

> **なぜ別の同期キーが重要なのか**
>
> ほとんどの人は覚えやすい（したがって、ある程度推測可能な）マスターパスワードを選びます。高度な攻撃者は、暗号化されたデータに対して数十億回のパスワード推測を試みることができます。
>
> Codebook Cloudは、マスターパスワードで同期データを暗号化しません。代わりに、完全にランダムな同期キー—推測不可能なランダムな文字の長い文字列—を使用します。このキーはデバイス上にのみ存在します。たとえ誰かがZeteticのサーバーから暗号化されたデータを盗んだとしても、それを解読することは数学的に不可能です。

考慮事項:

- Secret Agentによる自動入力は、ブラウザ拡張機能よりやや操作が多い
- Linux非対応
- 小規模企業（ただし25年以上安定）
- 大手競合他社より知名度が低い

推奨対象: シームレスな利便性よりセキュリティアーキテクチャを優先するユーザー、厳格なセキュリティ要件を持つ組織、プライバシーを重視する個人、プロバイダーがデータにアクセスする能力をゼロにしたい方

1Password

設計思想: 強力なセキュリティ対策を備えた最高クラスのユーザー体験

強み:

- すべてのプラットフォームで優れた洗練されたユーザーインターフェース
- ブラウザ拡張機能の自動入力が確実に動作
- シークレットキーがマスターパスワード以上の暗号化レイヤーを追加
- トラベルモードで国境通過時に機密ボールトを非表示可能
- 強力なエンタープライズ管理機能
- データ漏洩の経験なし

考慮事項:

- 無料プランなし（14日間の試用版のみ）
- Webボールトはブラウザコンテキストでパスワードを復号
- クローズドソース（検証は第三者監査に依存）
- 価格帯が高い

推奨対象: シームレスな体験を優先するユーザー、簡単な共有が必要な家族、管理機能が必要な企業

Bitwarden

設計思想: 誰もがアクセスできる透明でオープンソースなセキュリティ

強み:

- 完全なオープンソースで定期的に監査
- 無制限のパスワードとデバイスを含む寛大な無料プラン
- 完全な制御のためのセルフホストオプション
- 利便性のためのブラウザ拡張機能とWebボールト
- リーズナブルな価格で強力な組織機能
- 頻繁なアップデートによるアクティブな開発

考慮事項:

- ユーザーインターフェースは1Passwordほど洗練されていない
- 一部のプラットフォームで自動入力が不安定な場合あり
- Webボールトはブラウザコンテキストでパスワードを復号（前述のWebボールトのリスクを参照）
- VC資金調達により将来の方向性に疑問（ただしオープンソースコードは会社の変化に関係なく存続）

推奨対象: 予算重視のユーザー、オープンソース支持者、セルフホストを希望する組織、洗練されていないUIを許容できる技術者

> ⓘ **「オープンソース」はセキュリティにとって何を意味するか？**
>
> オープンソースソフトウェアは、完全なコードを公開しています。誰でもセキュリティの欠陥や隠されたバックドアを検査できます。この透明性は以下を意味します：

- 独立したセキュリティ研究者がコードを監査できる（実際にしている）
- バックドアや悪意のあるコードはすぐに発見される
- 会社の主張を信頼する必要がない—検証できる

Bitwardenは完全にオープンソースです。Codebookはオープンソースの暗号化であるSQLCipherを使用していますが、アプリケーション自体はオープンソースではありません。1PasswordとAppleパスワードはクローズドソースです。

Appleパスワード（iCloudキーチェーン）

設計思想: Appleエコシステム内でのシームレスな統合

強み:

- 無料でAppleデバイスに内蔵
- Appleデバイスではセットアップ不要
- Face ID / Touch ID統合がシームレス
- パスキー対応
- 強力な暗号化

考慮事項:

- Appleエコシステム内でのみ確実に動作
- **Windowsサポートに問題あり:** iCloud for Windowsは存在しますが、多くの問題が報告されています：
  - Windows 11でパスワードアプリが頻繁にクラッシュ
  - 承認/同期プロセスがループで失敗することが多い（2FAコードは受け付けるが何も起こらない）
  - iOSやWindowsのアップデート後に同期が壊れることがある
  - Edge/Chrome拡張機能での自動入力が不安定
  - 特定の条件が必要：同一ネットワーク、VPN無効、Windows Hello有効など
  - 診断ツールが限られており、トラブルシューティングが困難
- Androidは完全に非対応
- Apple以外のユーザーとパスワード共有不可
- 制御とエクスポートオプションが限定的
- ブラウザ拡張機能はChromeとEdgeのみ（Firefox非対応）

推奨対象: Windows PCがなく、Appleエコシステム外で共有する必要のないApple製品のみの組織。信頼性の問題により、Apple/Windows混在環境には推奨しません。

ブラウザベースのマネージャー（Chrome、Edge、Firefox）

設計思想: 既存のワークフローに統合された便利さ

強み:

- すでに利用可能、追加インストール不要
- 無料
- ブラウザアカウントと同期

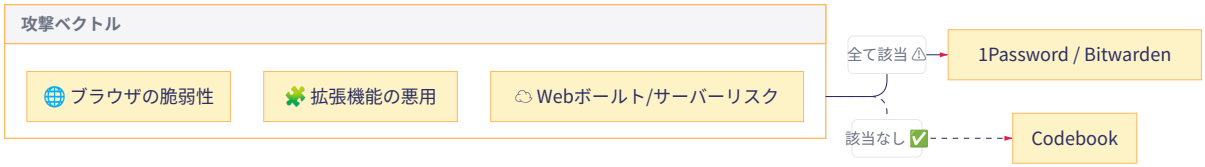
考慮事項:

- 単一障害点（ブラウザアカウントの侵害=すべてのパスワード漏洩）
- 真のゼロ知識アーキテクチャなし
- ブラウザコンテキストに限定
- TOTP非対応
- プロバイダー（Google、Microsoft）がデータにアクセスできる可能性

推奨対象: 専用ソリューションを採用しないユーザー、適切なパスワードマネージャーへの移行中の一時的な措置

> ⓘ **なぜブラウザのパスワードマネージャーは最も安全性が低いのか**
>
> Chromeでパスワードを保存すると、Googleアカウントに紐づけられます。これは以下を意味します：
>
> 1. **Googleがアクセスできる:** 専用のパスワードマネージャーとは異なり、ブラウザに保存されたパスワードは真の「ゼロ知識」ではありません。Googleは（同期目的で）このデータを処理できますし、実際にしています。
>
> 2. **1つのパスワードですべてが解除される:** 誰かがGoogle/Microsoftアカウントにアクセスした場合（フィッシング、パスワードの再利用、またはデータ漏洩を通じて）、メールとすべてのパスワードを同時に取得します。
>
> 3. **責任の分離がない:** 専用のパスワードマネージャーは単一目的のセキュリティツールです。ブラウザは、信頼できないウェブサイトを訪問し、不明なJavaScriptを実行し、巨大な攻撃対象領域を持つ複雑なアプリケーションです。
>
> ブラウザのパスワードマネージャーは何もないよりましですが、セキュリティを真剣に考える人にとっては最も弱いオプションです。

セキュリティアーキテクチャ比較



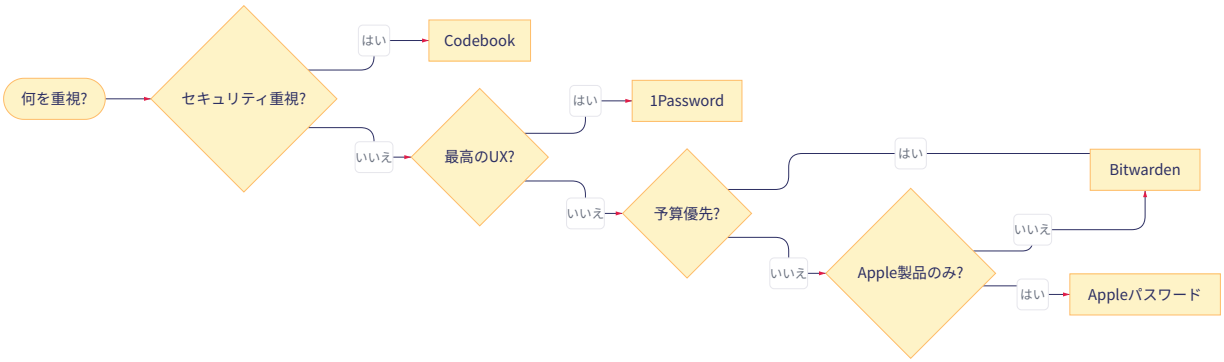
要約: Codebookのアーキテクチャは、設計によりネットワークおよびブラウザベースの脅威カテゴリ全体を排除します。ブラウザ拡張機能とWebボールトを持つソリューションは、追加の攻撃カテゴリから防御する必要があります。

> ⓘ **デバイス上のマルウェアについては？**
>
> 「コンピューターにマルウェアが入ったら、パスワードを盗まれるのでは？」と思うかもしれません。
>
> 答えは微妙です。強力なマスターパスワードでロックされたボールトは、非常に解読が困難です。これらのツールで使用される暗号化（AES-256、SQLCipher）は、ブルートフォースで解読するには宇宙の年齢より長い時間がかかります。
>
> **マルウェアの本当のリスクは、マスターパスワードのキャプチャです：**
>
> - キーロガーがマスターパスワードの入力を記録する可能性
> - 画面キャプチャソフトウェアが表示されたパスワードを見る可能性
> - メモリスクレイピングマルウェアがボールトのロック解除中にパスワードを読み取る可能性
>
> **自分を守る方法：**
>
> - 強力でユニークなマスターパスワードを使用する（前のセクションを参照）
> - オペレーティングシステムとソフトウェアを最新の状態に保つ
> - 信頼できないソースからソフトウェアをインストールしない
> - 積極的に使用していないときはボールトをロックする
> - モバイルでは、マスターパスワードを入力する代わりに生体認証（Face ID、指紋）を使用する
>
> **結論:** デバイスが高度なマルウェアに侵害された場合、どのパスワードマネージャーも完全には保護できません。しかし、これはどのセキュリティツールにも当てはまります。ボールトの暗号化自体は強力なままです。

注: これは1PasswordやBitwardenが安全でないことを意味するものではありません。各アクセスポイントに対して強力な保護を実装しています。この図はネットワークに面した攻撃対象領域のアーキテクチャの違いを示しています。

意思決定フレームワーク

優先事項に基づいて選択

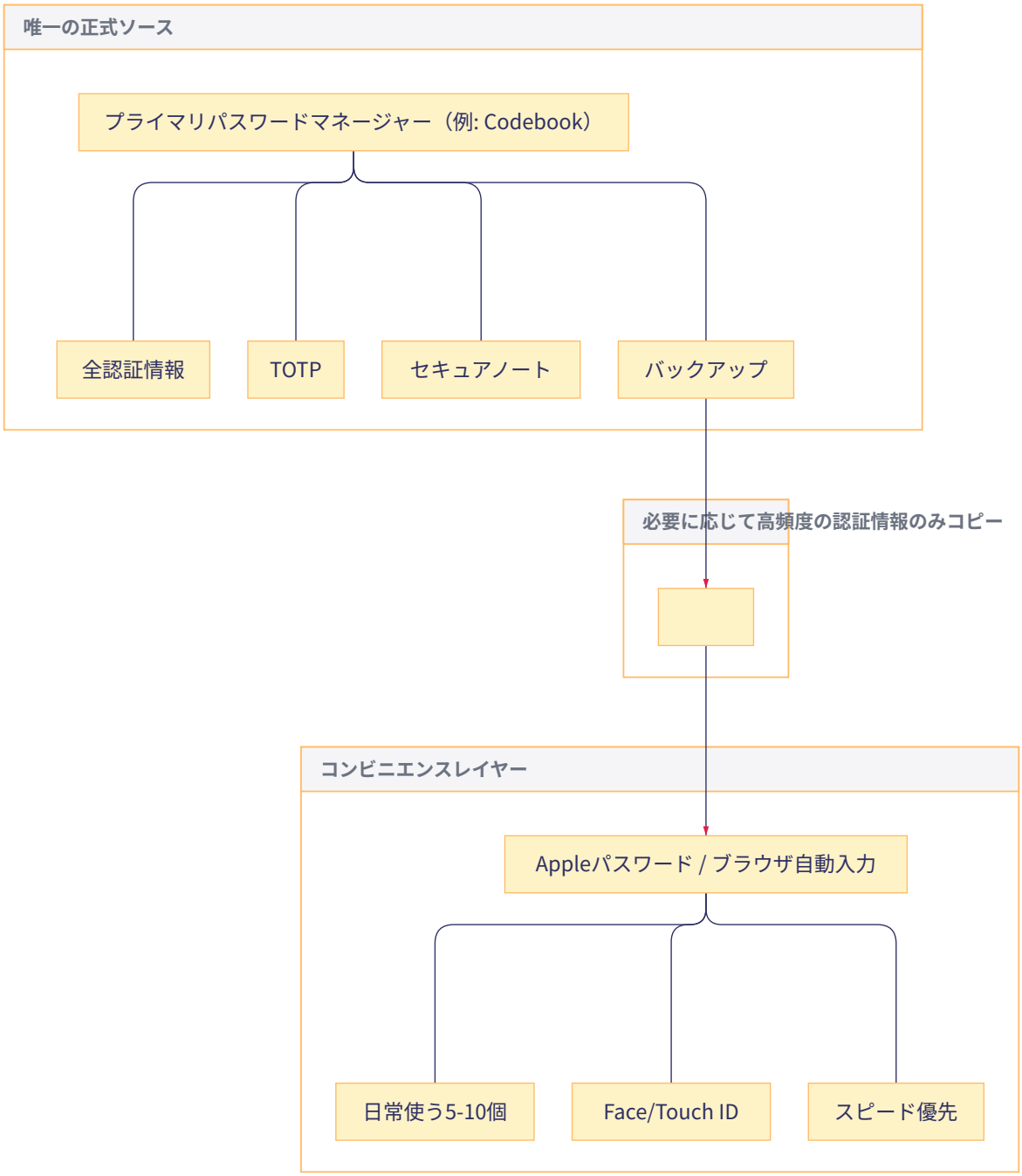


クイックリファレンス

重視する点	推奨ソリューション
最大限のセキュリティ、最小限の攻撃対象領域	Codebook
シームレスな体験、洗練されたUI	1Password
オープンソース、予算重視、セルフホスト	Bitwarden
Appleエコシステム統合、セットアップ不要	Appleパスワード

応用編: コンビニエンスレイヤーパターン

一部のユーザーは、セキュリティ優先のボールトを正式なソースとして使用しながら、頻繁にアクセスするサイト用に薄い「コンビニエンスレイヤー」を追加することで、効果的な中間点を見つけています。



なぜこれが機能するか

- **セキュリティアーキテクチャの維持:** 正式なボールトは最大限のセキュリティを維持
- **日常使用がスムーズ:** 頻繁にアクセスするサイトでFace ID自動入力
- **レジリエンス:** コンビニエンスレイヤーが壊れても問題なし—本当のデータはプライマリボールトにある
- **バージョン混乱なし:** プライマリボールトが常に正式ソース

必要な規律

1. **まずプライマリボールトを更新**し、必要に応じてコンビニエンスレイヤーにコピー
2. **コンビニエンスレイヤーは最小限に**—本当に高頻度のログインのみ
3. **コンビニエンスレイヤーにのみ保存しない**
4. **定期的なクリーンアップ**—コンビニエンスレイヤーから古いエントリを削除

このパターンを検討すべき場合

- セキュリティ優先ソリューションを選択したが、一部のサイトでよりスムーズな自動入力が欲しい
- 特定のサイトに1日に何十回もアクセスする
- プライマリ優先の習慣を維持できる規律がある

このパターンは、セキュリティ優先アーキテクチャを放棄することなく「ワンタップ自動入力が欲しい」という懸念に対応します。

重要なお知らせ

Microsoft Authenticatorの更新について

2025年8月をもって、Microsoft Authenticatorはパスワードマネージャーとして機能しなくなりました。Microsoftはすべてのパスワード保存と自動入力機能を削除しました。アプリは以下の機能を継続します：

- 多要素認証（MFA）プッシュ通知
- 時間ベースのワンタイムパスワード（TOTP）
- パスキー

以前Microsoft Authenticatorにパスワードを保存していた場合、そのデータはアクセスできなくなっています。代替ソリューションへの移行が完了していることをご確認ください。

多要素認証の推奨事項

どのパスワードマネージャーを選択する場合でも、以下を推奨します：

- ほとんどのアカウントには、パスワードマネージャー内蔵のTOTPを使用
- 条件付きアクセスポリシーで必要な場合は、Microsoft 365 MFA専用にMicrosoft Authenticatorを使用

この分離により、パスワードボールトとMFAが単一のアプリケーションに依存しないことが保証されます。

次のステップ

1. 上記の意思決定フレームワークを使用して優先事項を**評価**
2. 希望のソリューションを**試用**（ほとんどが無料試用版を提供）
3. 既存のソース（ブラウザなど）から現在のパスワードを**エクスポート**
4. 新しいパスワードマネージャーに**インポート**
5. 重要なアカウントで二要素認証を**有効化**
6. セキュリティの低い場所（ブラウザストレージなど）からパスワードを**削除**

> **バックアップキーを忘れずに**
>
> 選択するソリューションによって、以下を安全に保管する必要があります：
>
> - **マスターパスワード:** 紙に書いて安全な場所に保管（すべてのソリューション）
> - **同期キー:** Codebook Cloudは同期用に別のキーを生成—これもバックアップ
> - **シークレットキー:** 1PasswordはEmergency Kit PDFを提供—印刷して保管
> - **リカバリーコード:** 多くのサービスがワンタイムリカバリーコードを提供—これらを保存
>
> 信頼できる家族が必要な場合に見つけられる場所にこれらの物理的バックアップを保管してください。耐火金庫や貸金庫が理想的です。

これらのソリューションの移行、セットアップ、トレーニングについてサポートいたします。

お問い合わせ

株式会社イソリア
〒105-7105
東京都港区東新橋1-5-2
汐留シティセンター5階 (Workstyling)

電話	03-4577-3380
メール	hello@esolia.co.jp
Web	https://esolia.co.jp
営業時間	月～金、9:00～18:00

Password Vault Comparison Guide

Date: February 20, 2026

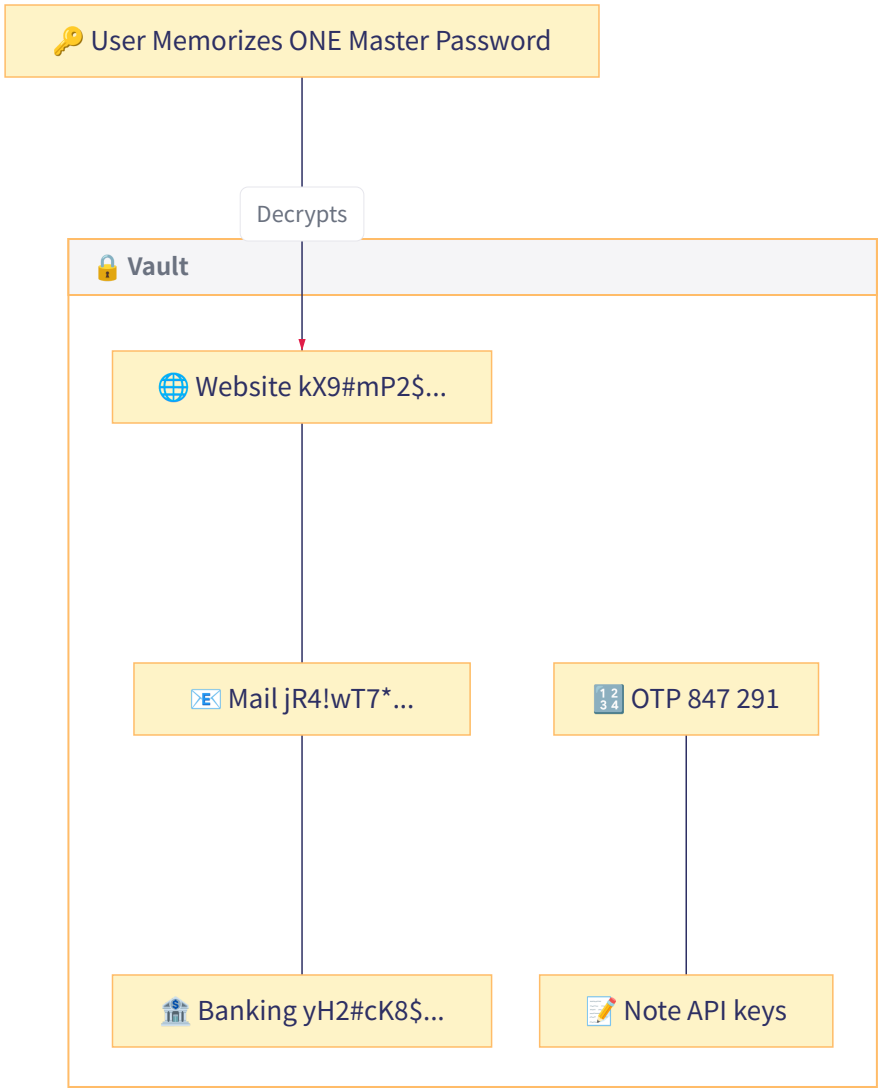
Executive Summary

Password managers are essential tools for protecting your digital identity. However, not all password managers are built the same way. This document compares leading solutions across security architecture, features, and practical considerations to help you choose the right solution for your needs.

Key Recommendation: Choose a solution based on your priorities—maximum security, maximum convenience, or a balance of both. All solutions discussed here are significantly better than not using a password manager.

Your Master Password: The Key to Everything

Your master password is the single most important credential you will ever create. It protects all your other passwords. Choose it carefully and protect it well.



The concept is simple:

- **One password to remember** — your master password
- **Hundreds of passwords you don't** — the vault generates and stores them

Each password inside the vault can be long, random, and unique. You never need to memorize `kX9#mP2$vL5@nQ8&jR4!` — the vault handles it. You only need to remember how to get in.

Choosing a Strong Master Password

The goal is a password that is **long enough to be secure** but **memorable enough that you won't forget it**.

Recommended approach: Use a passphrase

Instead of a complex string like `Tr0ub4dor&3`, use a phrase of random words:

```
correct horse battery staple
```

Or a memorable sentence with personal meaning:

```
My daughter Yuki was born in March 2019!
```

Why this works:

- Length matters more than complexity—a 25-character passphrase is stronger than an 8-character jumble of symbols
- You can actually remember it
- You can type it reliably

> **Consider How You'll Type It**
>
> You'll need to enter your master password on both desktop and mobile devices. Keep in mind:
>
> - **Symbols can be awkward on mobile:** Characters like `|`, `~`, `^`, or `\` often require multiple taps to find on phone keyboards. If you use symbols, stick to common ones easily accessible on mobile (like `!`, `@`, `#`, or `$`).
> - **Spaces work well:** A passphrase with spaces (`correct horse battery staple`) is easy to type on any device.
> - **Biometrics reduce typing:** Most password managers let you unlock with Face ID or fingerprint after the initial setup. Once enabled, you rarely type your master password on mobile—making a longer, more complex password practical.
>
> Test your master password on your phone before committing to it.

Avoid:

- Dictionary words alone (`password`, `sunshine`)
- Personal info easily found online (birthday, pet's name, company name)
- Patterns (`123456`, `qwerty`, `Password1!`)
- Reusing a password from another account

> **Critical: Back Up Your Master Password**
>
> If you forget your master password, you will lose access to all your stored passwords permanently. Most providers cannot recover your data—this is a security feature, not a limitation.
>
> **Write down your master password and store it in a secure physical location** (a safe, a safety deposit box, or with a trusted person). Do not store it digitally. This written backup is your safety net if you ever forget your password or become incapacitated and someone needs access on your behalf.

Inside the Vault: Let the Manager Do the Work

Once inside your password manager, you never need to remember individual passwords again. Let the manager generate long, random passwords for each account:

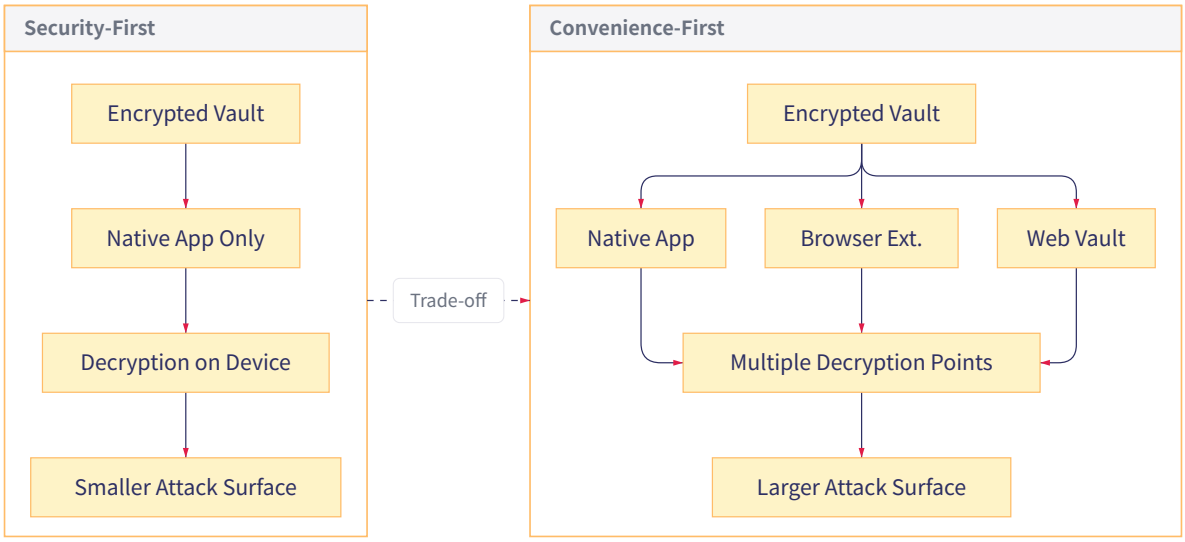
```
kX9#mP2$vL5@nQ8&jR4!wT7*
```

These are impossible to guess and impossible to remember—and that's fine, because you won't need to. The manager handles it.

Understanding Security Architecture

Before comparing individual products, it's important to understand the two fundamental approaches to password manager design.

Security-First vs. Convenience-First Design



Security-First Design:

- Decryption occurs only within the dedicated application
- No browser extensions or web interfaces that could be compromised
- Slower to add new features (each feature evaluated for security impact)
- Example: Codebook

Convenience-First Design:

- Multiple access points for seamless user experience
- Browser extensions enable one-click autofill
- Web vault allows access from any browser
- Security measures added to protect each access point
- Examples: 1Password, Bitwarden

Neither approach is wrong—they represent different priorities. The right choice depends on your threat model and usability requirements.

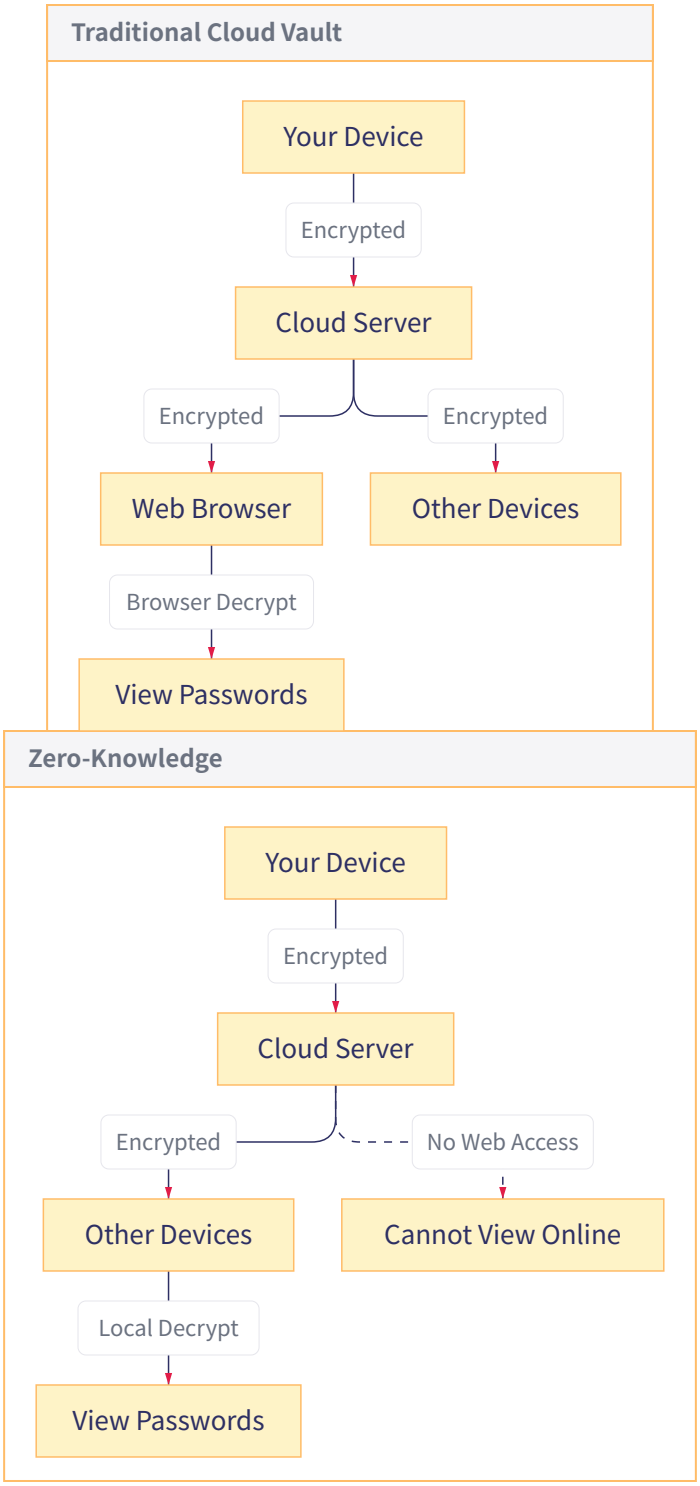
What is "Attack Surface"?

Think of your password vault like a house. The more doors and windows you add, the more entry points a burglar could potentially use. Each entry point is part of the "attack surface."

A security-first password manager is like a house with one heavily reinforced door. A convenience-first manager is like a house with multiple doors (front, back, garage, side)—more convenient for you, but each door needs its own locks and security measures.

Both can be secure, but the single-door approach has fewer things that could go wrong.

How Cloud Sync Differs by Solution



Traditional Cloud Vault (1Password, Bitwarden):

- Access your passwords from any web browser
- Convenient for accessing passwords on shared or temporary computers
- Decryption happens in the browser via JavaScript
- Requires trusting that the provider's servers won't serve malicious code

True Zero-Knowledge Sync (Codebook Cloud):

- Cloud is used **only** to move encrypted data between your devices
- No web interface—passwords can only be viewed in the native app
- Your data is encrypted with a **Sync Key** before it ever reaches their servers
- **Zetetic does not have your Sync Key**—they literally cannot decrypt your data
- Even if compelled by law enforcement or compromised by hackers, the provider cannot access your passwords

What is "Zero Knowledge"?

"Zero knowledge" means the service provider knows nothing about the contents of your data. They store your encrypted vault but cannot read it.

However, not all "zero knowledge" claims are equal:

Type	How it works	Provider Can Access?
Web Vault	Your password unlocks data in your browser. Provider's servers send you the decryption code.	Theoretically yes—they could send malicious code that captures your password
Sync-Only (Codebook)	A separate Sync Key encrypts data before upload. This key never leaves your devices.	No—they don't have the key and there's no web interface to attack

With Codebook Cloud, your Sync Key is generated on your device and stays there. Zetetic's servers only ever see encrypted blobs they cannot decrypt. This is architecturally different from services that offer web access.

Why Are Web Vaults Riskier?

When you log into a web vault (like 1Password.com or vault.bitwarden.com), your browser downloads JavaScript code from the provider's server, and that code decrypts your passwords.

The risk: You're trusting that the provider will always send you legitimate code. If their servers were compromised, or if a rogue employee made changes, or if law enforcement compelled them to modify the code for a specific user, the JavaScript could theoretically capture your master password. **This is not hypothetical paranoia**—it's why security researchers have long debated web-based password access. For most users, the risk is low. For high-security users (executives, journalists, activists), this architectural difference matters.

Password managers without web vaults eliminate this entire category of risk.

Solution Comparison

Overview Matrix

Feature	Codebook	1Password	Bitwarden	Apple Passwords
Architecture	Security-first	Convenience-first	Convenience-first	Platform-integrated
TOTP Codes	✓ Built-in	✓ Built-in	✓ Built-in	✓ Built-in
Browser Extension	✗ (by design)	✓	✓	⚠ Chrome/Edge only, unreliable on Windows
Web Vault	✗ (by design)	✓	✓	✗
Platforms	Win, Mac, iOS, Android	All + Linux	All + Linux	Apple only (Windows buggy)
Family/Team Sharing	✓ (new in 2026)	✓	✓	Apple users only
Open Source	SQLCipher (encryption)	✗	✓ Full	✗
Self-Host Option	Local-only available	✗	✓	✗
Breach Monitoring	✓ HaveIBeenPwned	✓ Watchtower	✓ Reports	✓ Basic
Price (Individual)	$60/year	$36/year	Free–$10/year	Free

What is TOTP?

TOTP (Time-based One-Time Password) is the technology behind those 6-digit codes that change every 30 seconds. When a website offers "authenticator app" as a two-factor option, it's using TOTP.

Modern password managers can store and generate these codes alongside your passwords, so you don't need a separate authenticator app for most accounts. You'll still see the term "2FA" (two-factor authentication) or "MFA" (multi-factor authentication) used interchangeably with TOTP in many contexts.

Business Pricing Comparison

For organizations, all three major solutions offer business-specific plans with administrative controls, centralized billing, and onboarding support. **If you are using these tools for business purposes, the business plans are required** and provide features essential for organizational management.

Team Size	Codebook Business	1Password	Bitwarden Teams	Bitwarden Enterprise
5 users	$225/year*	$240/year (Starter)	$240/year	$360/year
10 users	$450/year*	$240/year (Starter)	$480/year	$720/year
50 users	$2250/year*	$4,794/year	$2,400/year	$3,600/year
Per-user rate	From $5/user/mo	$7.99/user/mo	$4/user/mo	$6/user/mo

- Codebook Business starts at $5/user/month. Prices shown are 25% off, **with eSolia affiliate code**. Large teams may be eligible for a bigger discount.

Key Business Plan Features:

Feature	Codebook Business	1Password Business	Bitwarden Teams	Bitwarden Enterprise
Centralized billing	✓	✓	✓	✓
User management dashboard	✓	✓	✓	✓
Sharing permissions	✓	✓	✓	✓
SSO integration	✗	✓	✗	✓
Directory sync (SCIM)	✗	✓	✗	✓
Self-hosting option	✗	✗	✓	✓
Free Families for users	✗	✓	✗	✓

Business Plan Links:

- **Codebook Business:**https://www.zetetic.net/codebook/business/
- **1Password Teams/Business:**https://1password.com/pricing/password-manager
- **Bitwarden Business:**https://bitwarden.com/pricing/business/

Note: Volume discounts are typically available from all vendors for larger deployments (generally 100+ users).

Detailed Profiles

Codebook (by Zetetic)

Philosophy: Maximum security through minimal attack surface.

Strengths:

- 25+ year track record with no breaches
- SQLCipher encryption (used by NASA, Samsung, Fortune 500 companies)
- No browser extension or web vault means no browser-based attack vectors
- **True zero-knowledge cloud sync:** Codebook Cloud encrypts your data with a Sync Key that is generated on your device and never uploaded. Zetetic cannot see your passwords, cannot be compelled to hand them over, and cannot be hacked in a way that exposes your data.
- Even your master password isn't used for cloud encryption—a separate, fully random Sync Key protects against password-cracking attacks
- Responsive, personal customer support from a company focused solely on security

> ⓘ **Why the Separate Sync Key Matters**
>
> Most people choose memorable (and thus somewhat guessable) master passwords. Advanced attackers can try billions of password guesses against encrypted data.
>
> Codebook Cloud doesn't encrypt your sync data with your master password. Instead, it uses a completely random Sync Key—a long string of random characters that's impossible to guess. This key lives only on your devices. Even if someone stole the encrypted data from Zetetic's servers, cracking it would be mathematically infeasible.

Considerations:

- Autofill via Secret Agent requires slightly more interaction than browser extensions
- No Linux support
- Smaller company (though stable for 25+ years)
- Less brand recognition than larger competitors

Best for: Users who prioritize security architecture over seamless convenience; organizations with strict security requirements; privacy-conscious individuals; anyone who wants their provider to have zero ability to access their data.

1Password

Philosophy: Best-in-class user experience with strong security measures.

Strengths:

- Excellent, polished user interface across all platforms
- Browser extension autofill works reliably
- Secret Key adds extra encryption layer beyond master password
- Travel Mode can hide sensitive vaults when crossing borders
- Strong enterprise management features
- Never experienced a data breach

Considerations:

- No free tier (14-day trial only)
- Web vault means passwords can be decrypted in browser context
- Closed-source (relies on third-party audits for verification)
- Higher price point

Best for: Users who prioritize seamless experience; families who need easy sharing; enterprises requiring management features.

Bitwarden

Philosophy: Transparent, open-source security accessible to everyone.

Strengths:

- Fully open-source and regularly audited
- Generous free tier with unlimited passwords and devices
- Self-hosting option for complete control
- Browser extension and web vault for convenience
- Strong organizational features at reasonable prices
- Active development with frequent updates

Considerations:

- User interface less polished than 1Password
- Autofill can be inconsistent on some platforms
- Web vault means passwords can be decrypted in browser context (see earlier section on web vault risks)
- VC funding raises questions about future direction (though open-source code would survive any company changes)

Best for: Budget-conscious users; open-source advocates; organizations wanting self-hosted option; technical users comfortable with less polished UI.

> **What Does "Open Source" Mean for Security?**
>
> Open-source software publishes its complete code publicly. Anyone can inspect it for security flaws or hidden backdoors. This transparency means:
>
> - Independent security researchers can (and do) audit the code
> - Backdoors or malicious code would be discovered quickly
> - You don't have to trust the company's claims—you can verify
>
> Bitwarden is fully open-source. Codebook uses SQLCipher, which is open-source encryption, though the application itself is not. 1Password and Apple Passwords are closed-source.

Apple Passwords (iCloud Keychain)

Philosophy: Seamless integration within Apple ecosystem.

Strengths:

- Free and built into Apple devices
- Zero setup required for Apple devices
- Face ID / Touch ID integration is seamless
- Passkey support
- Strong encryption

Considerations:

- Only works reliably within Apple ecosystem
- **Windows support is problematic:** iCloud for Windows exists but has well-documented issues:
  - Passwords app frequently crashes on Windows 11
  - Approval/sync process often fails in a loop (2FA codes accepted but nothing happens)
  - Sync can break after iOS or Windows updates
  - Autofill in Edge/Chrome extensions is inconsistent
  - Requires specific conditions: same network, VPN disabled, Windows Hello enabled
  - Troubleshooting is difficult with limited diagnostic tools
- No Android support whatsoever
- Cannot share passwords with non-Apple users
- Limited control and export options
- Browser extension only available for Chrome and Edge (not Firefox)

Best for: Apple-only organizations with no Windows PCs and no need to share outside Apple ecosystem. Not recommended for mixed Apple/Windows environments due to reliability issues.

Browser-Based Managers (Chrome, Edge, Firefox)

Philosophy: Convenient, integrated with existing workflow.

Strengths:

- Already available, no additional installation
- Free
- Syncs with browser account

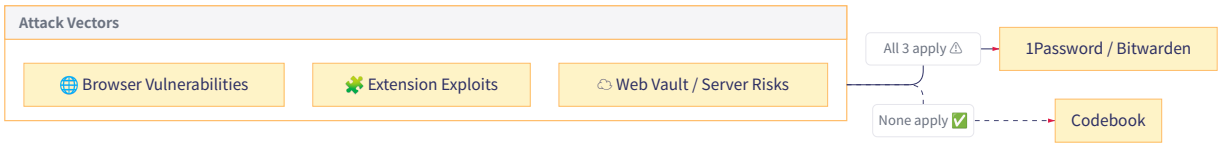
Considerations:

- Single point of failure (browser account compromise = all passwords exposed)
- No true zero-knowledge architecture
- Limited to browser context
- No TOTP support
- Provider (Google, Microsoft) can potentially access data

Best for: Users who will not adopt a dedicated solution; temporary measure while transitioning to a proper password manager.

> ⓘ **Why Browser Password Managers Are the Least Secure Option**
>
> When you save passwords in Chrome, they're tied to your Google account. This means:
>
> 1. **Google can access them:** Unlike dedicated password managers, browser-stored passwords are not truly "zero knowledge." Google can (and does, for sync purposes) process this data.
>
> 2. **One password unlocks everything:** If someone gains access to your Google/Microsoft account (through phishing, password reuse, or a data breach), they get your email AND all your passwords simultaneously.
>
> 3. **No separation of concerns:** A dedicated password manager is a single-purpose security tool. A browser is a complex application that visits untrusted websites, runs unknown JavaScript, and has a massive attack surface.
>
> Browser password managers are better than nothing, but they're the weakest option for anyone taking security seriously.

Security Architecture Comparison



Summary: Codebook's architecture eliminates entire categories of network and browser-based threats by design. Solutions with browser extensions and web vaults have additional vectors that must be defended.

What About Malware on Your Device?

You may wonder: "If malware gets on my computer, can't it steal my passwords?"

The answer is nuanced. A locked vault with a strong master password is extremely difficult to crack—the encryption used by these tools (AES-256, SQLCipher) would take longer than the age of the universe to brute-force.

The real risk from malware is capturing your master password:

- A keylogger could record you typing your master password
- Screen capture software could see your passwords when displayed
- Memory-scraping malware could read passwords while your vault is unlocked

How to protect yourself:

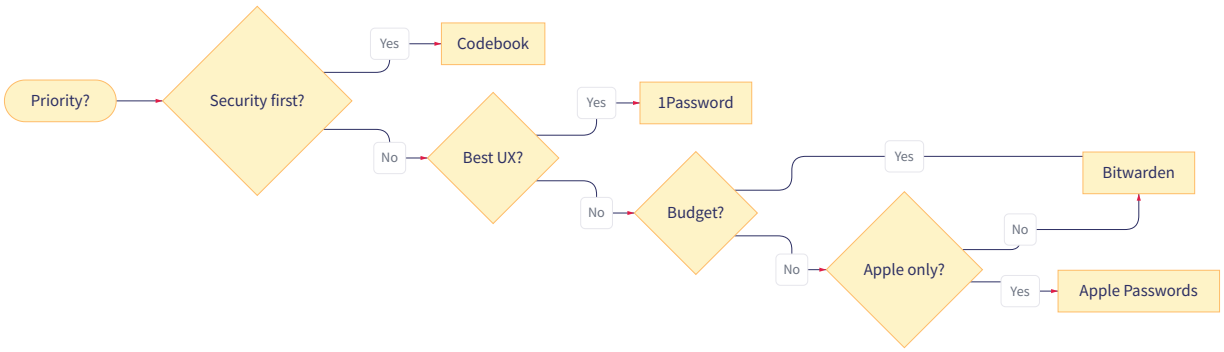
- Use a strong, unique master password (see previous section)
- Keep your operating system and software updated
- Don't install software from untrusted sources
- Lock your vault when not actively using it
- On mobile, use biometrics (Face ID, fingerprint) instead of typing your master password

Bottom line: If your device is compromised by sophisticated malware, no password manager can fully protect you. But this is true of any security tool. The vault encryption itself remains strong.

Note: This does not mean 1Password or Bitwarden are insecure—they implement strong protections for each access point. The diagram shows the architectural difference in network-facing attack surface.

Decision Framework

Choose Based on Your Priorities

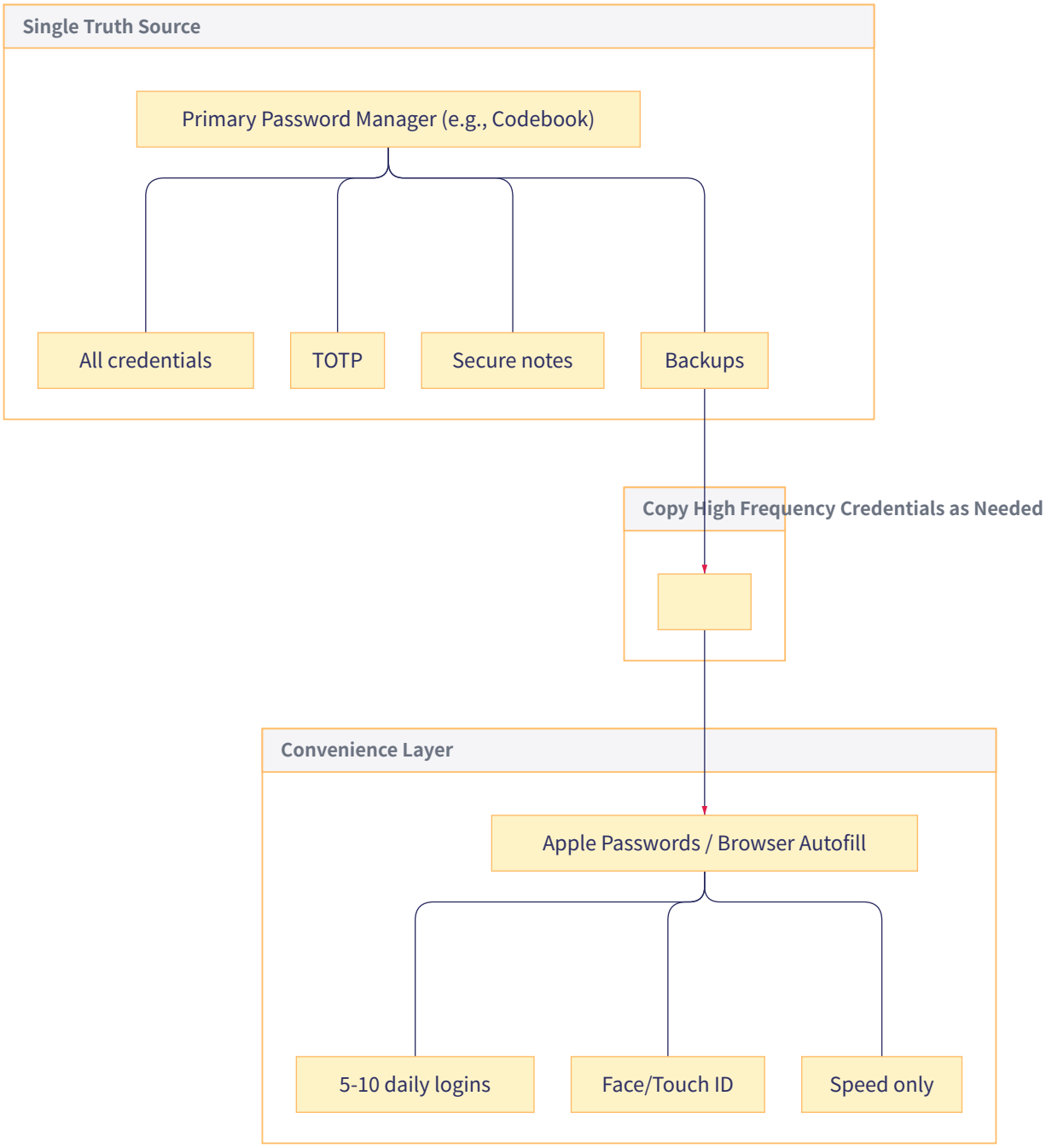


Quick Reference

If you value...	Choose...
Maximum security, minimal attack surface	Codebook
Seamless experience, polished UI	1Password
Open source, budget-friendly, self-host option	Bitwarden
Apple ecosystem integration, zero setup	Apple Passwords

Advanced: The Convenience Layer Pattern

Some users find an effective middle ground by using a security-first vault as their authoritative source while adding a thin "convenience layer" for frequently-accessed sites.



Why This Works

- **Security architecture preserved:** Your authoritative vault maintains maximum security
- **Frictionless daily use:** Face ID autofill for the handful of sites you access constantly
- **Resilience:** If the convenience layer breaks, you don't care—the real data is in your primary vault
- **No version confusion:** Primary vault is always the source of truth

The Discipline Required

1. **Update primary vault first**, then copy to convenience layer if needed
2. **Keep the convenience layer minimal**—only truly high-frequency logins
3. **Never store anything exclusively in the convenience layer**
4. **Periodic cleanup**—remove stale entries from convenience layer

When to Consider This Pattern

- You've chosen a security-first solution but want smoother autofill for a few sites
- You access certain sites dozens of times daily
- You're disciplined enough to maintain the primary-first habit

This pattern addresses the "but I want one-tap autofill" concern without abandoning security-first architecture.

Important Notes

Microsoft Authenticator Update

As of August 2025, Microsoft Authenticator no longer functions as a password manager. Microsoft removed all password storage and autofill features. The app continues to work for:

- Multi-factor authentication (MFA) push notifications
- Time-based one-time passwords (TOTP)
- Passkeys

If you previously stored passwords in Microsoft Authenticator, that data is no longer accessible. Please ensure you have migrated to an alternative solution.

Multi-Factor Authentication Recommendation

Regardless of which password manager you choose, we recommend:

- Using your password manager's built-in TOTP for most accounts
- Using Microsoft Authenticator specifically for Microsoft 365 MFA where required by Conditional Access policies

This separation ensures your password vault and MFA are not dependent on a single application.

Next Steps

1. **Evaluate** your priorities using the decision framework above
2. **Trial** your preferred solution (most offer free trials)
3. **Export** your current passwords from existing sources (browser, etc.)
4. **Import** into your new password manager
5. **Enable** two-factor authentication on critical accounts
6. **Delete** passwords from less secure locations (browser storage, etc.)

> **Don't Forget Your Backup Keys**
>
> Depending on which solution you choose, you may need to securely store:
>
> - **Master Password:** Write it down and store in a safe place (all solutions)
> - **Sync Key:** Codebook Cloud generates a separate key for sync—back this up too
> - **Secret Key:** 1Password provides an Emergency Kit PDF—print and store it
> - **Recovery Codes:** Many services provide one-time recovery codes—save these
>
> Store these physical backups where a trusted family member could find them if needed. A fireproof safe or safety deposit box is ideal.

We are available to assist with migration, setup, and training for any of these solutions.

Contact Us

eSolia Inc.
Shiodome City Center 5F (Workstyling)
1-5-2 Higashi-Shimbashi, Minato-ku
Tokyo 105-7105, Japan

Phone	03-4577-3380
Email	hello@esolia.co.jp
Web	https://esolia.co.jp/en
Hours	Monday-Friday, 9:00-18:00 JST
