1Password Business

製品紹介資料

ソースネクスト株式会社

セールスDivision

Information
企業情報

1Password

SOURCENEXT

社名　　：ソースネクスト株式会社

株式市場：東証プライム（証券番号：4344）
事業内容：IoTデバイス、パソコンソフト、
　　スマホアプリの企画・開発・販売
設立　　：1996年8月
売上高　：11,455百万円（2025年3月期）
所在地　：東京都千代田区三番町３－８
　　泉館三番町３階

主要製品・サービス一覧
※クリックすると一覧カタログ資料をDLできます

音声翻訳機
「POCKETALK」

企業での採用実績
1万社以上

サッと議事録
「AutoMemo」

累計アカウント数
20万を突破

360°web会議カメラ
「KAIGIO CAM360」
「ミーティングオウル」

国内出荷台数3万台を突破
国内従業員数ベスト50社の半数以上で導入！

PCソフト	スマホアプリ	登録ユーザー	累計出荷
500タイトル	100タイトル	2,000万人以上	5,000万本以上

ソフトウェアの製品価格を1,980円に統一、セキュリティの更新料0円の「ZERO」ブランドなど、多くのパソコンソフトの常識を変えてきました。

当社は、情報セキュリティマネジメントシステム（ISMS）の国際規格である「ISO /IEC 27001」の認証取得しています。
※認証範囲：パソコン・スマートフォンソフトウェアおよびハードウェア製品の開発、及び自社ECサイトの運営、サポート業務

1Passwordとは

企業と個人のセキュリティを守るパスワード管理ツール

覚えるパスワードは1つだけ

「マスターパスワード」1つだけで、すべてのログイン情報にアクセス。記憶の負担から解放されます。

強力なパスワード自動生成・入力

推測困難なランダムパスワードを生成し、安全に保存。ログイン時は自動入力でスムーズに認証。

デバイス間の一元管理

PC、スマホ、タブレットで即座に同期。オフィスでも外出先でも、常に最新情報へアクセス可能。

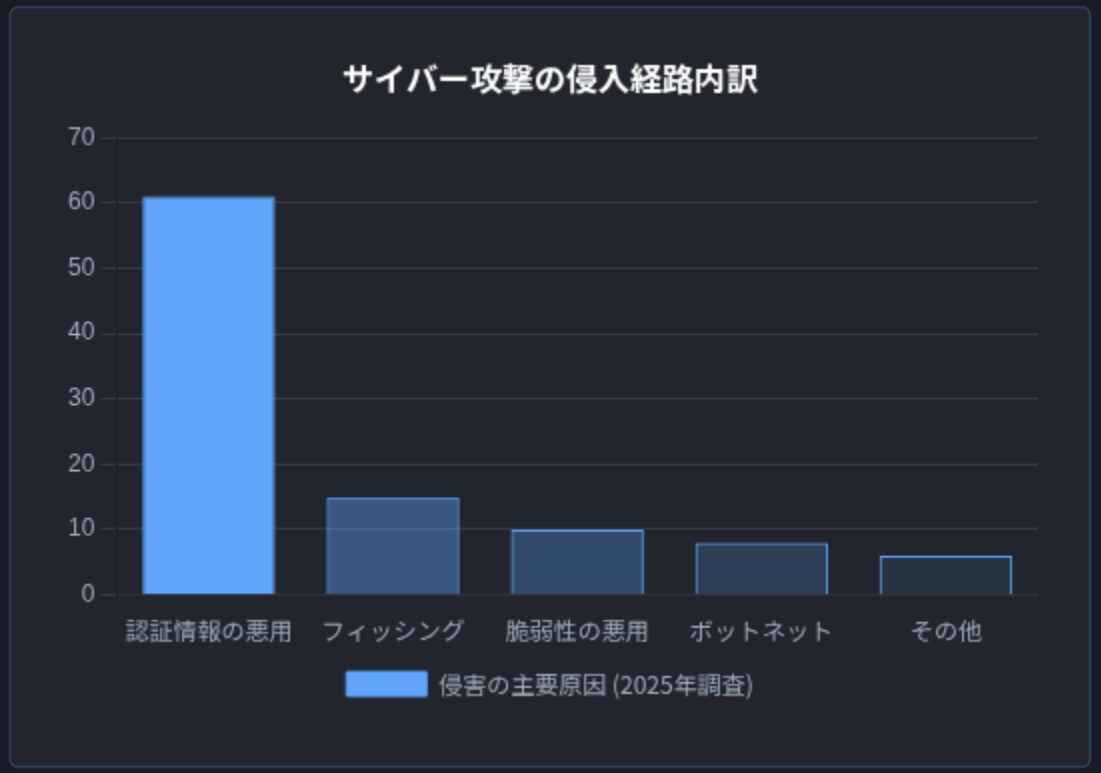
強固なセキュリティ保護

データは端末内で暗号化され、マスターパスワードとシークレットキーで二重に保護されます。

なぜ今、パスワード管理が必要か

働き方の変化とサイバー攻撃の高度化により、従来のパスワード管理手法は限界を迎えています。セキュリティリスクは経営課題として直結する問題となっています。

61%
侵害原因は認証情報悪用



リモートワークの常態化社外からのアクセスが増加し、ID管理が複雑化

SaaS利用の急増とパスワード数爆発1人あたり管理すべきパスワード数が激増（中小：平均85個）

従来管理（Excel・付箋）の限界使い回しや脆弱なパスワード設定が常態化するリスク

ランサムウェア攻撃の急増と対策強化2025年には某有名企業が**74万件以上**のデータ漏洩発生。 攻撃の高度化に伴い、大手企業の**75.9%**がセキュリティ予算を増額

ターゲット＆

導入実績

企業規模

大企業 ～ 中小企業まで幅広く対応

主要連携サービス

日本国内導入実績

500～600社以上

LY Corporation　Nintendo　その他多数の大手企業

世界導入実績

200,000社以上

Slack　IBM　GitLab　Salesforce　PagerDuty　Under Armour

Main Features

1Passwordで できること

ログイン情報の一元管理

散在するIDとパスワードを安全な保管庫（Vault）に集約し、整理して管理します。

自動入力でスムーズにログイン

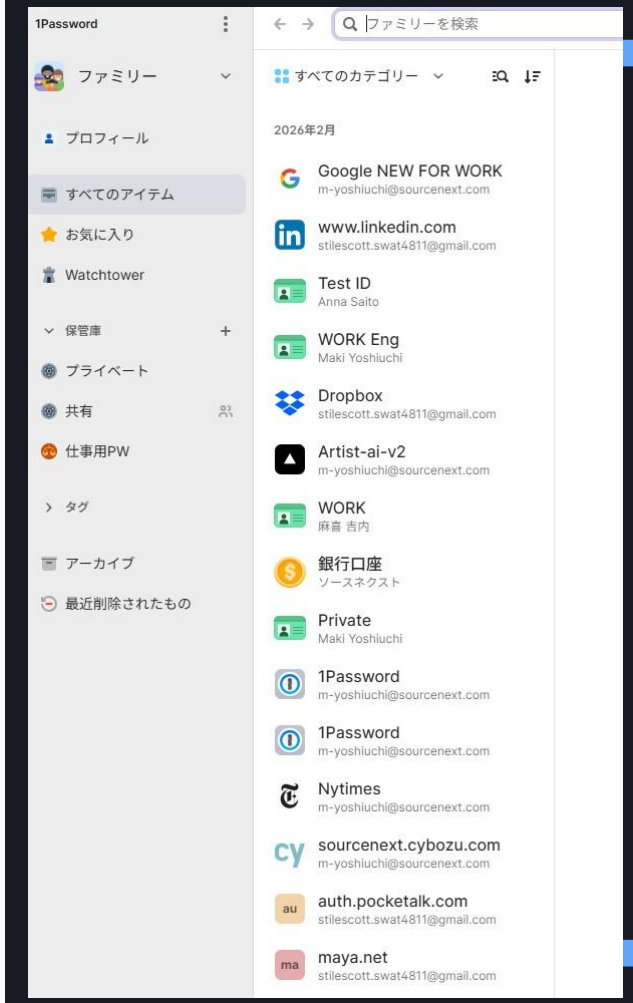
ブラウザやアプリでID・パスワードを自動入力。手入力の手間とミスをゼロにします。

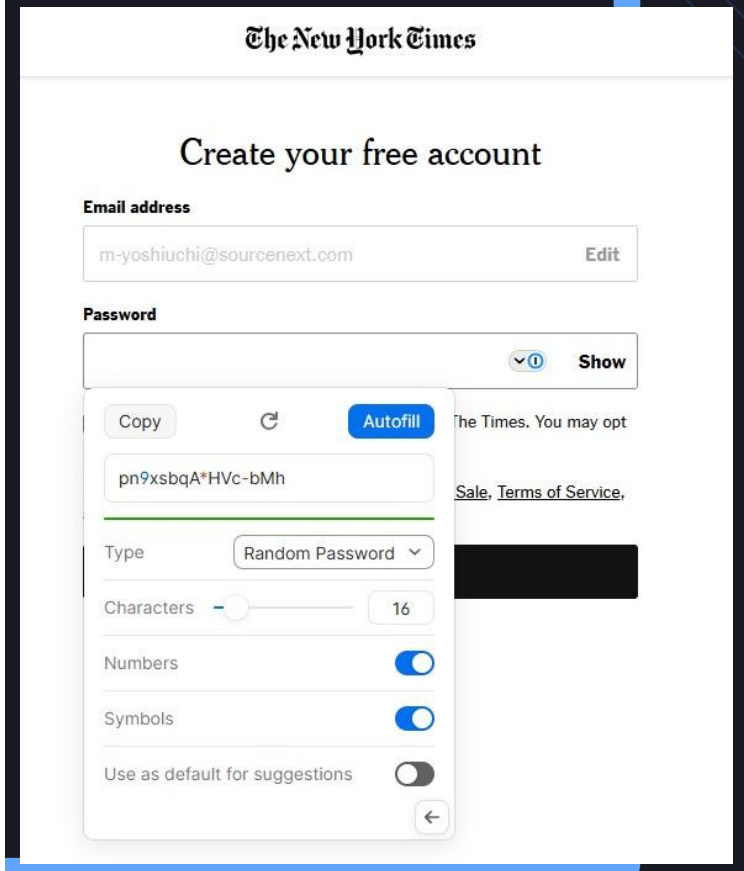
強固なパスワードを自動生成

文字数、記号、数字の組み合わせを自由にカスタマイズ可能。推測されにくい複雑なパスワードをワンクリックで作成。

暗号化してクラウド保存

データは強力に暗号化されて同期。デバイスを紛失してもデータは安全に守られます。





Beyond Passwords

パスワード以外の情報も管理可能

1Passwordは単なるパスワード管理ツールではありません。デジタルライフにおけるあらゆる重要情報を、安全な保管庫（Vault）に一元管理できます。

覚えるのが面倒な情報や、漏洩したら困る情報をまとめて保護。必要な時にいつでも安全にアクセスできます。

クレジットカード
番号、有効期限、CVCを保存し、オンライン決済時に入力

銀行口座
口座番号、支店コード、暗証番号などを安全に記録

住所情報
自宅や配送先の住所を登録し、フォーム入力を自動化

パスポート
旅券番号や有効期限を管理し、紛失時の控えとしても活用

運転免許証
免許証番号や更新日を記録し、期限切れを防止

マイナンバー
マイナンバーカードや通知カードの情報を厳重に保管

ライセンスキー
ソフトウェアのプロダクトキーや購入情報を一括管理

セキュアノート
Wi-Fiパスワードや秘密の質問など、任意のテキスト情報を保存

Security & Trust

1Passwordは本当に安全？

3重のセキュリティ設計

業界標準を超える堅牢な保護メカニズムを採用。

- 2つの鍵管理 (2SKD)
- SRP対応
- AES-GCM-256bit

Watchtower による監視

パスワードの使い回しや脆弱性、漏洩事故を24時間365日監視し、危険な状態を即座にユーザーへ警告します。

PROVEN TRACK RECORD

大規模情報漏洩なし

サービス開始以来、顧客情報の重大な漏洩事故ゼロを継続中。

第三者機関による監査

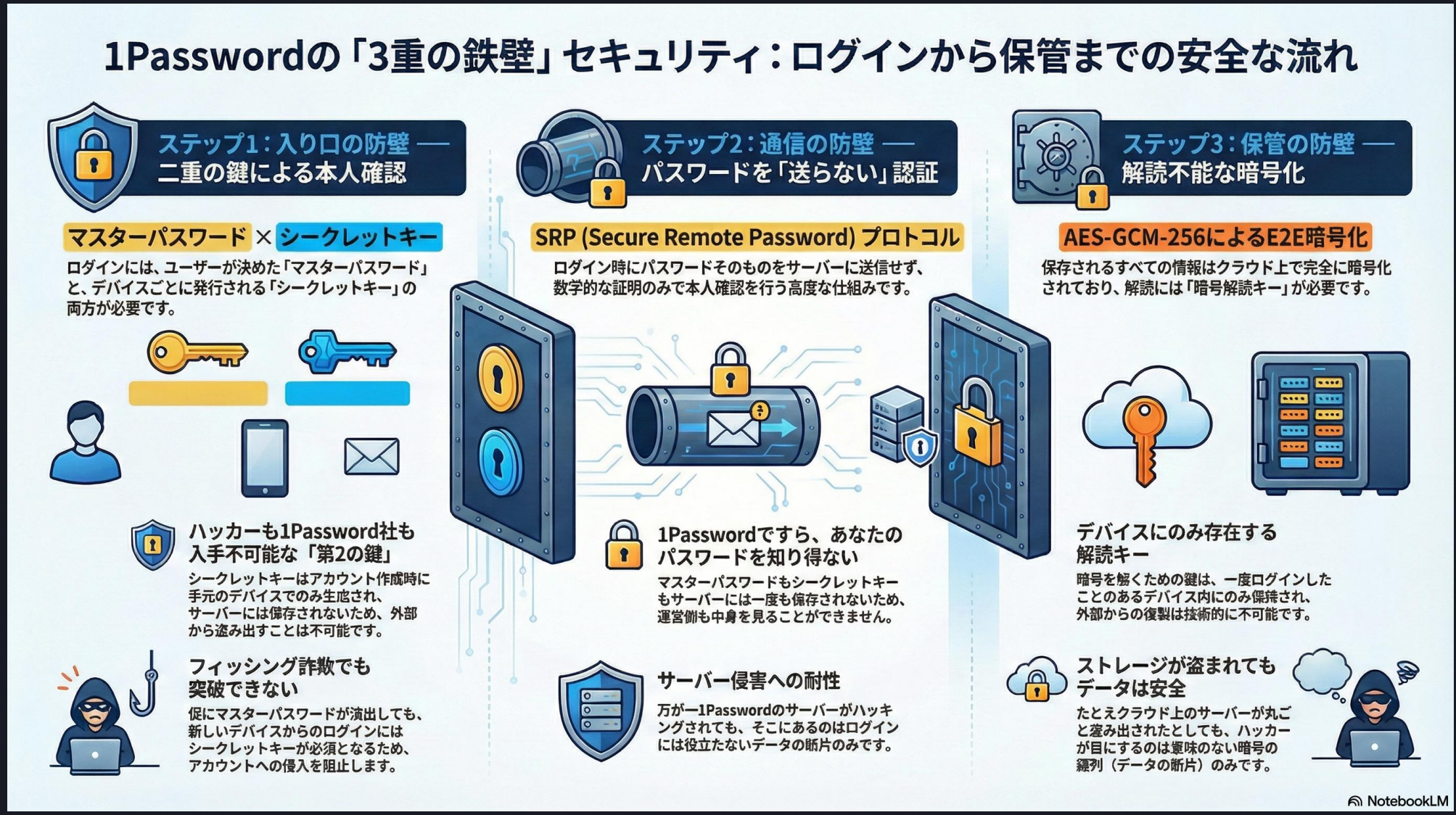
毎年外部専門家によるペネトレーションテスト（侵入テスト）を実施。

国際基準・認証の取得

SOC 2 Type 2、ISO 27001など、厳格なセキュリティ基準に準拠。

1Passwordの「3重の鉄壁」セキュリティ

ログインから保管までの安全な流れ



2つの鍵管理（2SKD）とは

強固なセキュリティを支える「2つの秘密」

マスター パスワード

ユーザーが作成・記憶する唯一のパスワード。
サーバーには決して送信されません。

記憶ベースの 認証要素

頭の中だけにある情報。
あなたの記憶が鍵の一部となります。

シークレット キー

デバイス内で自動生成される128bitの鍵。
設定時のみ表示され、自動保存されます。

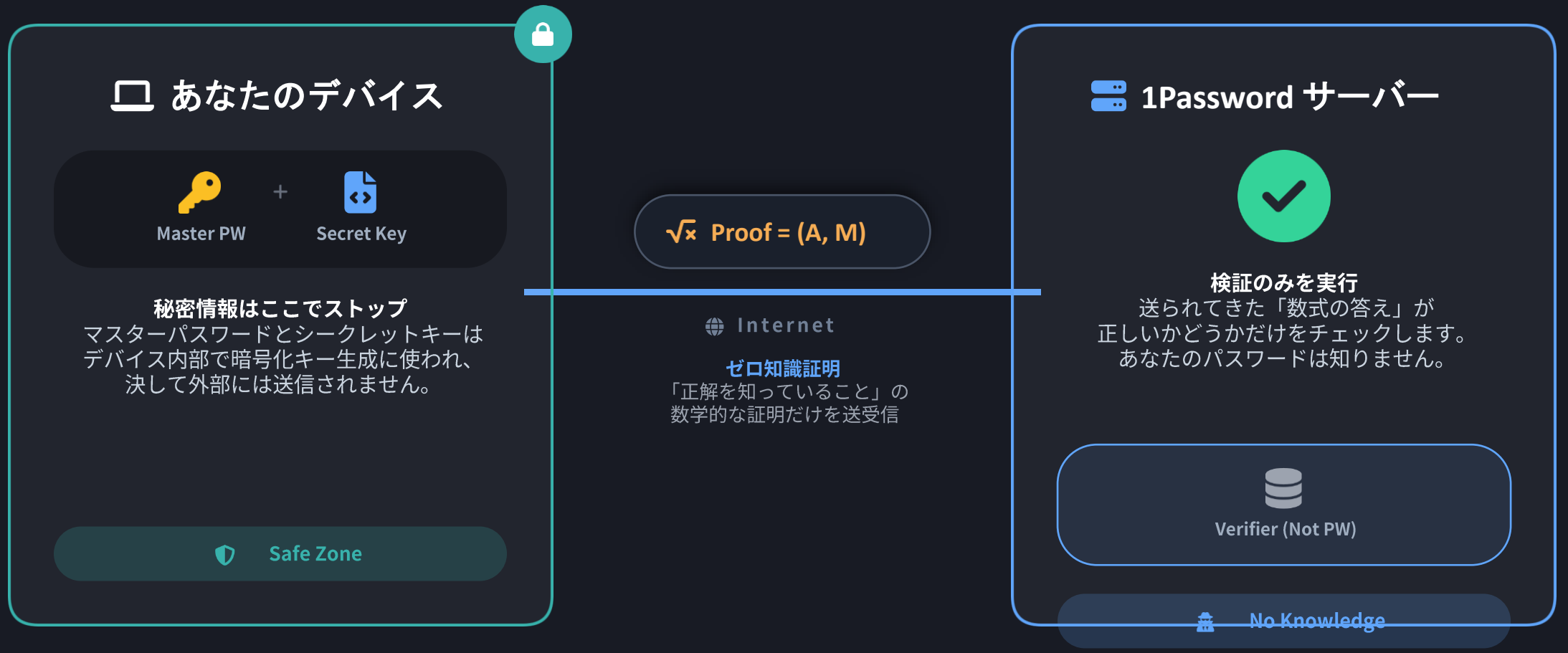
デバイスベースの 認証要素

端末の中だけにある情報。
登録済みデバイス自体が鍵となります。

両方が揃わない限り、データは数学的に解読不可能です

SRP（Secure Remote Password）とは

パスワードを「送らず」に認証する、ゼロ知識証明の仕組み



AES-GCM-256とは

強固なエンドツーエンド暗号化の仕組み

1. ユーザー端末で暗号化

すべてのデータは、あなたのデバイスから送信される前に暗号化されます。この時点でデータは「解読不能な文字列」に変換されており、平文の情報は一切ネットワークに出ません。

2. 暗号化データの保管

1Passwordのクラウドサーバーには、暗号化されたデータのみが保管されます。運営会社であっても、中身を見ることは技術的に不可能です。

3. 解読には2つの鍵が必要

データを復号（解読）するには、「マスターパスワード」と「シークレットキー」の両方が必要です。この2つを持つあなただけが、データにアクセスできます。

Point: ハッカーがサーバーに侵入しても、手に入るのは意味のない暗号化データのみ。あなたの情報は安全に守られます。

Watchtower

パスワードの健全性を24時間自動監視

Watchtowerは、あなたの保管庫に潜む**セキュリティリスク**を常に監視します。

侵害されたサイトのパスワードや、強度の低いパスワードを即座に特定し、改善を促すことで、アカウントの安全性を最高レベルに保ちます。

漏洩パスワード検知

「Have I Been Pwned」と連携し、世界中のデータ侵害を監視。流出したパスワードを使用している場合、即座に警告します。

弱いパスワード検知

「123456」や辞書にある単語など、推測されやすく強度が不足しているパスワードを自動的に特定します。

使い回しパスワード検知

複数のサイトで同一のパスワードを使用しているリスクを検知。1つの漏洩が全体に波及する「リスト型攻撃」を防ぎます。

脆弱性レポート

2要素認証（2FA）が未設定のサイトや、暗号化されていないHTTP接続のサイトなど、セキュリティ上の問題を定期レポートします。

管理者とユーザーの違い

役割に応じた適切な権限管理と機能提供

1 一般ユーザー

基本機能は共通

- パスワードの保存・自動入力・生成などの基本機能
- 個人用保管庫（プライベート）の利用
- 共有された保管庫へのアクセス（権限範囲内）
- マルチデバイスでの同期・利用

2 管理者（Admin）

ユーザー管理
社員の追加・削除、退職時のアクセス権即時停止

インサイト機能
全社員のパスワード強度や使い回し状況の可視化

セキュリティポリシー設定
マスターパスワードの要件や2要素認証の強制設定

保管庫の権限管理
部署やチームごとの共有設定、アクセスログの確認

FREE TRIAL

まずは14日間、
無料でお試しください

クレジットカード登録不要

お支払情報の登録は不要です。
期間終了後に自動課金されることはありません。

スムーズな本契約移行

試用期間中のデータや設定はそのまま引き継げるため、再設定の手間はかかりません。

お申し込み方法

お申し込みフォームURL

start.1password.com/sign-up/business

上記URLよりお申し込み後、弊社まで
以下の3点をご連絡ください。

氏名 **職場メールアドレス** **会社名**

※会社名は英語でご記入ください。

「1Password Business」を14日間無料でお試しいただけます。

ビジネス版

Teams / Business / Enterprise

- **高度な管理コンソール**
  ユーザー追加・削除、権限設定を一元管理
- **SSO / SCIM 連携**
  Okta, Azure AD等との統合、自動プロビジョニング
- **セキュリティポリシー設定**
  MFA強制、パスワード強度要件などの組織全体適用
- **詳細な監査ログ**
  誰がいつ何にアクセスしたかの追跡・レポート
- **共有ボールトと権限管理**
  チーム・部署ごとの柔軟な共有設定
- **優先サポート**
  ビジネスユーザー向けの優先的な技術支援

VS

個人版

Individual / Families

- **基本的なパスワード管理**
  保存、自動入力、生成などの基本機能のみ
- **管理機能なし**
  組織的なユーザー管理やポリシー設定は不可
- **SSO連携なし**
  企業認証システムとの統合機能は非搭載
- **監査ログなし**
  アクセス履歴や操作ログの確認機能なし
- **限定的な共有**
  家族間や小規模な共有に限定される

パスワード管理ツール 機能比較（1/3）

◎ 最高　○ 良好　△ 限定的　× 非対応

機能 / 製品	1Password	A社	B社	C社	D社
セキュリティ機能					
暗号化方式 AES-256 + 独自技術	◎	◎	◎	◎	◎
シークレットキー (2SKD) 128-bit追加鍵でゼロ知識保証	◎	×	×	×	△
パスワード漏洩検知 Watchtower / HIBP連携	◎	◎	○	○	◎
使い回しパスワード検知 Vault Healthレポート	◎	◎	○	○	◎
脆弱性・評価レポート セキュリティダッシュボード	◎	◎	△	△	○

パスワード管理ツール 機能比較（2/3）

◎ 最高　○ 良好　△ 限定的　× 非対応

機能 / 製品	1Password	A社	B社	C社	D社
管理・運用機能					
SSO連携 SAML 2.0 / SCIM Bridge	○	◎	○	○	△
オフラインモード 全プラットフォーム対応	◎	◎	○	△	○
パスワード自動生成 高度な生成機能（最大100桁）	◎	◎	◎	◎	◎
パスワード自動入力 Passkey対応・アプリ連携	◎	◎	◎	○	◎
シークレット管理 1Password Dev統合	◎	○	△	△	◎
提供形態 クラウド / ローカルキャッシュ	◎	◎	○	◎	◎

パスワード管理ツール 機能比較（3/3）

◎ 最高　○ 良好　△ 限定的　× 非対応

機能 / 製品	1Password	A社	B社	C社	D社
サポート体制・クライアント環境					
日本語対応（管理画面） 完全対応	◎	○	○	△	×
日本語マニュアル サポートサイト完備/検索性高い	◎	△	○	△	△
ユーザートレーニング オンラインビデオ・記事充実	○	◎	△	×	△
サポート体制 リソース充実/セルフサービス強力	◎	◎	○	○	○
クライアント対応 全OS・全ブラウザ対応	◎	◎	○	◎	◎