Engineer

パスワード

＊ログインする本人を確かめるための秘密の文字列

どのようなものか

パスワードは、人が覚えるかパスワードマネージャーに保存し、そのアカウントが自分のものだと示すために提示する文字列です。NIST用語集の定義は、文字、数字、その他の記号を「本人の認証、またはアクセス認可の検証に使う」という中心部分で一致し、一部の文書では暗号鍵の導出にも使います。現在のデジタルID指針SP 800-63-4は、「本人が知っているもの」の要素と呼び、初版では記憶する秘密という名前を使ったと記します。単語を並べたパスフレーズも、十進数字だけのPINも、広い意味ではパスワードです。

同じ文字列でも、似て見える二つの役割があります。ログイン用なら検証者へ送り、検証者は判別に足りる情報を保存しても、パスワードそのものは決して保存すべきではありません。手元のものを解除するパスワードは、端末内にとどまります。SP 800-63Bは、これをアクティベーションシークレット（有効化用の秘密情報）と呼び、典型例に多要素認証器の解除PINを挙げます。端末上で使い、認証器が保持する秘密にアクセスするためのものです。

難しさは、パスワードが共有された秘密であることです。利用者が知り、サービスが判別し、知ってしまった人なら誰でも、本人と同じように使えます。文字列自体には、要求したサイトと結び付くものがありません。SP 800-63Bが、フィッシングへの耐性はないと明言する理由です。周辺の設計の大半は、この共有された知識が漏れたときの損失を抑えるためにあります。

概念を判断に生かす

「パスワードとは？」を実際の判断に生かしましょう。その概念を、開発または購入するシステムに結び付けて考えるお手伝いをします。 アカウント、パスワード、権限を整理し、業務に必要なアクセスだけを付与し、退職者の権限は当日に解除します。

サービスを見る お問い合わせ →

用語の背後にある前提を検証する

解説とリンク先の実績を参考に、プロジェクトについての質問を整理してください。ツールを選ぶ前に、前提を一緒に検討できます。 Linuxサーバーを守る1,000件のRBACルールを作成 — 1,000 セキュリティ上の穴を塞ぐアクセスルール

Linuxサーバーを守る1,000件のRBACルールを作成 お問い合わせ →

なぜ重要なのか

アカウントを守るものが、パスワードだけということもよくあります。問題となる推測攻撃は二種類あり、抑える方法も違います。

オンラインの推測は、実際のログインフォームで試すことで、速さはサービスが決めます。SP 800-63Bは、一つのアカウントに一つの認証器で行う連続した失敗を100回までとし、新しいパスワードを、よくある値、予測しやすい値、漏えい済みの値を集めた拒否リストで検査するよう求めます。攻撃者が最初に試す候補を受け付けないためです。

保存したパスワードデータのコピーが外へ出ると、オフラインの推測が始まります。フォームも上限もありません。指針は、オフラインなら毎秒何十億ものハッシュを計算でき、それに耐えるパスワードは、ログインフォームだけに向き合うものより「桁違いに複雑」である必要があると記します。保存方式が結果を決めるのは、そのためです。SP 800-63Bは、ソルトを加え、パスワード専用のハッシュ方式を使うよう求めます。パスワード、ソルト、コスト係数を入力とし、試すたびの負担を大きくする方式です。ソルトは少なくとも32ビットで、同じ値がめったに出ないように選び、同じパスワードの二つのアカウントが、保存ハッシュまで同じになるのを防ぎます。コスト係数は検証者が許容できる限り高くし、時とともに引き上げるべきです。指針は、後で強い方式へ移れるよう、各ハッシュに使った方式とコストを記録することも勧めます。

RFC 9106は、この目的のために作られた、メモリー使用の負担が大きい関数Argon2を説明し、そのArgon2id方式を推奨します。すべての環境での既定値は、2 GiBのメモリーを一回走査する設定で、メモリーが乏しければ、64 MiBを三回走査する設定です。RFCは、前者が、総当たり専用ハードウェアを使う攻撃者の費用を最大にするとします。ハッシュファイルが漏れた後で重要になる性質です。OWASPのPassword Storage Cheat Sheetは、より低い実用上の最小値と、Argon2idを使えないシステムの代替案を挙げ、共通する原則も示します。SHA-256のような高速ハッシュでは、短時間に大量の推測ができるので不適切です。暗号化は逆向きに戻せて元を復元できるため、パスワードは暗号化でなく、ハッシュ化して保存します。

実際の活用例

組織全体にパスワード管理システムを導入する前、資格情報は、それぞれの好みで保存、共有していました。日々の姿は、大きな侵入事件というより、チャットに書いたパスワード、誰も更新しない共有ログイン、小さな露出の緩やかな積み重ねです。導入により、組織は一貫した保存、共有方法を得ました。利用は個人の任意にはしませんでした。半分だけが使っても、使わない半分にリスクがあれば、ほとんど役に立たないためです。一つの管理された場所に資格情報を置くと、アクセス制御も簡単で一貫したものになりました。SP 800-63Bも、サービス側から同じ方向を示します。検証者は、パスワードマネージャーと自動入力を認めなければならず、貼り付けも認めるべきです。サービスごとに別のパスワードを持つ方法として、マネージャーを挙げています。

二台目のサーバーをコードから構築したとき、一台目の来歴が、その理由を示しました。手で作った後でファイアウォールを追加しており、既定のパスワード方針の新しいホストへ、インターネットから接続できる時間ができていました。対策は順序です。ファイアウォールのplayをサーバーのplayより先に動かすため、新しいマシンは最初から、その内側に作られます。

大手メールプロバイダーへのログインでは、アプリケーションが、パスワードが違うと利用者に伝えていました。実際は違っていませんでした。その提供元は第三者のクライアントに、アプリ専用パスワードを求めます。一つのアカウントに二種類のパスワードがあり、一方だけを知るメッセージが、何度入力しても動かない値の入れ直しを促していたのです。書き換えたメッセージは、提供元の名前、アプリ専用のものが必要なこと、作成場所を示し、テストが提供元名と資格情報の種類を検査します。

問題が起きるところ

一つのパスワードを、複数のアカウントに使います。 同じものが複数のサービスを守ると、最も弱い一つの漏えいが、残りも開きます。SP 800-63Bは、あるサイトで得たパスワードを、他のサイトの同じ人のアカウントへ試すことを、パスワードスタッフィングと呼びます。利用者はサービスごとに違うものを使い、実際にはマネージャーを利用して防ぎます。サービス側は、新しいパスワードを、過去の漏えいの値と照合します。

規則が、かえってパスワードを弱くします。 文字の組み合わせを強制すると、厳しく見えて、予測しやすい結果を生みます。指針自身の例では、passwordを選ぶはずだった人が、大文字と数字を求められるとPassword1を、記号も求めら

れるとPassword1!を選びます。組み合わせの規則、定期的な変更、ログイン前に読めるヒント、最初のペットの名前のような秘密の質問は認めません。ただし、漏えいなどの侵害の証拠があれば、直ちに変更する必要は残ります。

高速なハッシュか、全行に同じソルトを使います。 パスワードテーブルを汎用関数でハッシュ化したり、全行を同じソルトにしたりすると、オフラインの攻撃者が安く推測し、一度に全アカウントへ照合できます。古いハッシュを引き継いだシステムでも、OWASPが説明するように、次回ログイン時に、新しい方式で再ハッシュ化できます。保存した方式への参照で、古いものが残る行も分かります。

パスワードを途中で切るか、貼り付けを認めません。 SP 800-63Bは、送られた全体を検証し、切り詰めた一部だけを調べてはいけないとし、自動入力が動かない場所でもマネージャーを使えるよう、貼り付けを認めるべきだとしています。ハッシュ関数自身に上限がある場合もあります。OWASPは、多くの実装でbcryptの入力は最大72バイトと記し、使うサービスに、その上限を守らせるよう求めます。

本来置くべきでない場所に、パスワードが残ります。 チャットへの貼り付け、チケットへの記入、ログへの出力は、正規の保存先が持つ、すべての管理から外れたコピーです。そのコピーを使えなくする唯一の方法は、パスワードを変えることです。見た目を決めるどんな規則より、一つの管理された保存先の方が重要なのは、そのためです。

参考資料

- NIST CSRC用語集のパスワード — FIPS 140-2、SP 800-63-4などの定義と、特殊な形としてのパスフレーズです。
- NIST SP 800-63B-4 — 選び方、検査、保存の現在の規則と、付録Aにある根拠です。
- RFC 9106 — Argon2と、パスワードのハッシュ化向けに推奨する、二つのArgon2id設定です。
- OWASPのパスワード保存チートシート — Argon2id、scrypt、bcrypt、PBKDF2の実用的なパラメーターと、古いハッシュの更新方法です。

用語集

実際の制約に合わせて選ぶ

デプロイの流れ、運用上のリスク、緊急対応の担当者をお知らせください。検査、復旧手段、明確な責任の所在を伴う変更の範囲を定められます。

料金を見る お問い合わせ →

用語を実務に結び付ける

「パスワードとは？」がお客様の組織にどう当てはまるかをご相談ください。現在のシステムの具体例が一つあれば、話を始められます。

サービスを見る

welcome@engineer.company +45 50 10 61 84 デンマーク、コペンハーゲン

このページを持ち歩く

連絡先カード

心を込めて丁寧に制作： D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

著作権 © 2025 – 現在 · Engineer ApS · すべての権利を留保します。

印刷元： https://engineer.company/ja/glossary/password/