RESOURCE CENTER

パスワード・セキュリティの現状 2024 レポート

連邦政府機関のパスワード・セキュリティへの取り組み

Get the full interactive view at
https://bitwarden.com/ja-jp/resources/the-state-of-password-security/

bitwarden

米国連邦政府機関におけるパスワードセキュリティの現状評価

近年、米国連邦政府全体がサイバーセキュリティに強い関心を寄せており、多くの省庁が政府機関や大小の企業、さらには消費者への啓蒙活動を主導している。

しかし、パスワードのセキュリティに関しては、すべての機関が同じ曲を歌っているわけではない。その最たるもののひとつである国立標準技術研究所（NIST）は、「米国の産業界、連邦政府機関、そしてより広範な一般市民のニーズに応えるため、サイバーセキュリティの標準、ガイドライン、ベストプラクティス、その他のリソースを開発している」。

NISTのサイバーセキュリティのページには、「NISTのサイバーセキュリティの任務は、連邦法、行政命令、政策によって定義されているものもある。例えば、行政管理予算局（OMB）は、すべての連邦政府機関に対し、国家安全保障以外のシステムに対するNISTのサイバーセキュリティ基準とガイダンスの実施を義務付けている。

残念ながら、NISTの勧告はまだすべての連邦政府機関に普遍的に受け入れられ、実施されているわけではない。また、NISTは各機関が従うべき基準を定めているが、そのNISTでさえ、ウェブサイトが乱立しているという独自の弱点を抱えている。

2024年は、ビットワーデンがこの分析を実施した3年目にあたる。この3年間、NISTのウェブサイトは、そのコンテンツは非常に健全であるにもかかわらず、混乱したままであった。前向きな動きもいくつかあった。ホワイトハウスは、パスワード・セキュリティに関するアドバイスの普及を改善し、『改善の余地あり』から『良好』へと評価を変えた。パスワード・セキュリティの推奨やサイバーセキュリティの全体的な態勢に関して、より良い方向に向かっている他の機関には、サイバーセキュリティ・インフラストラクチャ・セキュリティ協会（CISA）、連邦捜査局（FBI）、連邦取引委員会（FTC）、中小企業庁（SBA）などがある。

今年、ビットワーデンはこのレポートに証券取引委員会（SEC）も加えた。昨年、SECは企業にサイバーセキュリティに関する重大インシデントの開示を義務付ける規則を採択した。サイバーセキュリティ・コンプライアンスを実施するSECの役割を踏まえ、本レポートではSEC自身のパスワード・セキュリティに関するアドバイスを評価する。

技術の進歩は速い。ビジネスでも個人でも、楽しいエンターテインメント・サイトから銀行口座のような深刻な金融ビジネスまで、私たちの生活の多くが無数のアカウントでオンライン化されている。

このアセスメントの目的は、連邦政府からのベストプラクティスと、改善の余地がある箇所について、パスワードを使用するすべての人を巻き込み、教育することである。連邦政府内には、パスワード・セキュリティに対してしっかりとした教育的アプローチをとっているところも多いし、近代化のためにちょっとした支援が必要なところもある。

幸いなことに、パスワード・セキュリティのベスト・プラクティスについては、コンセンサスが形成されつつある。本レポートは、その詳細を集約し、評価したものである。

パスワードを見る パスワードセキュリティの現状

目次

パスワード・セキュリティ評価システムのガイドライン

格付けシステムは、以下の基準の順守に基づいて代理店をランク付けする：

Excellent

- パスワード・マネージャーの使用を推奨
- 強固なパスワードの重要性を訴える

- パスワードの安全性をさらに高める2FA/MFAの必要性を指摘
- 全体的なセキュリティに関する助言が最新で、NIST のガイドラインに準拠している。
- パスワード・セキュリティに関する推奨事項を、わかりやすく、消化しやすく、見つけやすく説明する。

Very Good

- パスワード・マネージャーの使用を推奨
- 強固なパスワードの重要性を訴える
- パスワードの安全性をさらに高める2FA/MFAの必要性を指摘
- 全体的なセキュリティに関する助言が最新で、NIST のガイドラインに準拠している。
- パスワード・セキュリティに関する推奨事項を、明確で、消化しやすく、見つけやすい方法で説明していない。

Good

- パスワードマネージャーの使用は推奨しない
- 強固なパスワードの重要性を訴える
- パスワードの安全性をさらに高める2FA/MFAの必要性を指摘
- 全体的なセキュリティに関する助言が最新ではなく、NIST のガイドラインに準拠していない。
- パスワード・セキュリティに関する推奨事項を、わかりやすく、消化しやすく、見つけやすく説明していない。

Fair

- パスワードマネージャーの使用は推奨しない
- 強固なパスワードの重要性を訴える
- パスワードのセキュリティをさらにサポートする2FA/MFAの必要性を一貫して挙げていない。

- 全体的なセキュリティに関する助言が最新ではなく、NIST のガイドラインに準拠していない。
- パスワード・セキュリティに関する推奨事項を、わかりやすく、消化しやすく、見つけやすく説明していない。

- パスワードマネージャーの使用は推奨しない
- 強固なパスワードの重要性を訴えない
- パスワードのセキュリティをさらにサポートする2FA/MFAの必要性を挙げていない
- 全体的なセキュリティに関する助言が最新ではなく、NIST のガイドラインに準拠していない。
- パスワード・セキュリティに関する推奨事項を、わかりやすく、消化しやすく、見つけやすく説明していない。

米国国立標準技術研究所（NIST）

NISTリスクマネジメントフレームワーク | IA-5(18)

代理店のアドバイス

- 認証管理 | パスワード・マネージャー
  - パスワードを生成し管理するために、[課題：組織定義のパスワードマネージャー]を使用する。
    - 割り当て：組織定義のコントロール]を使用してパスワードを保護する。
    - 静的パスワードが採用されているシステムでは、パスワードが適切に複雑であること、同じパスワードが複数のシステムで採用されていないことを保証することが、しばしば課題となる。パスワード・マネージャーは、様々なアカウントのための強力で異なるパスワードを自動的に生成し、保存するので、この問題の解決策となる。パスワード・マネージャーを使用する潜在的なリスクは、敵対者がパスワード・マネージャーによって生成されたパスワードのコレクションを標的にできることである。したがって、パスワードの収集には、パスワードを暗号化し、トークンにオフラインで保管するなどの保護が必要である。
- 参考

デジタル・アイデンティティ・ガイドライン

代理店のアドバイス

- 暗記された秘密は、加入者が選択する場合、少なくとも 8 文字の長さにしなければならない。CSP または検証者が無作為に選択した暗記秘密は、少なくとも 6 文字の長さにしなければならず（SHALL）、すべて数字にしてもよい（MAY）。CSP または検証者が、危殆化した値のブラックリストに記載されていることに基づいて、選択した暗記秘密を許可しない場合、サブスクライバは別の暗記秘密を選択するよう要求されるものとする。暗記された秘密に対する他の複雑さの要件は課されるべきではない[SHOULD]。その根拠は「付録A暗記された秘密の強さ」に示されている。

- ベリファイアは、加入者が選択した暗記シークレットの長さが少なくとも 8 文字であることを要 求しなければならない (SHALL) 。
ベリファイアは、加入者が選択した、少なくとも 64 文字の長さの暗記秘密を許可すべきで ある (SHOULD) 。スペース文字と同様に、
すべての印刷ASCII[RFC 20]文字は、暗記された秘 密で許容されるべきである[SHOULD]。ユニコード[ISO/ISC 10646]
文字も受け入れるべきである(SHOULD)。誤入力の可能性を考慮し、検証者は検証の前に、
連続する複数の空白文字を1つの空白文字に置換して もよい。秘密の切り捨ては行ってはならない[SHALL NOT]。上記の長さの要件では、
Unicodeの各コード点は1文字として数えなければならない (SHALL) 。

- CSP によって (例えば、登録時に) または検証者によって (例えば、ユーザが新しい PIN を要求したときに)
ランダムに選択される暗記された秘密は、少なくとも 6 文字の長さでなければならず、承認されたランダム・ビット生成器[SP 800-90Ar1]
を使用して生成されなければならない。

- 暗記型秘密検証機は、サブスクライバが、認証されていない請求者がアクセス可能な「 ヒント 」を保 存することを許可してはならない。
ベリファイアは、暗記された秘密を選択する際に、特定の種類の情報(例えば、"What was your first pet? "など)を使用するよう、
加入者に促してはならない(SHALL NOT)。

- 暗記された秘密を設定および変更する要求を処理する際、検証者は、一般的に使用され、予期され、
または危殆化されることが知られている値を含むリストと、将来の秘密を比較しなければならない (SHALL) 。例えば、リストには、
これらに限定されるものではないが、以下を含めてもよい :
  - 過去の違反コーパスから得られたパスワード。
  - 辞書の単語。
  - 繰り返しまたは連続する文字 (例 : 'aaaaaa'、'1234abcd') 。
  - サービス名、ユーザー名、およびその派生語など、コンテキスト固有の単語。

- 選択した秘密がリストに含まれている場合、CSP または検証者は、別の秘密を選択する必要がある ことをサブスクライバに通知し、
拒否の理由を提示し、サブスクライバに別の値の選択を要求するものとする。

- ベリファイアは、パスワード強度計[Meters]などのガイダンスを加入者に提 供し、
ユーザーが強力な暗記秘密を選択できるように支援すべきである[SHOULD]。このことは、
上記のリストで暗記された秘密が拒絶された後に特に重要である。なぜなら、リストアップされた(そしておそらく非常に弱い)
暗記された秘密の些細な改変を阻止するからである[Blacklists]。

- ベリファイアは、セクション5.2.2に記載されるとおり、サブスクライバのアカウントで行える認証試行
の失敗回数を効果的に制限するレート制限メカニズムを実装しなければならない (SHALL) 。

- ベリファイアは、暗記された秘密に対して他の構成規則 (異なる文字種の混在を要求する、 連続して繰り返される文字を禁止するなど) を課すべきでない (SHOULD NOT) 。検証者は、暗記された秘密を任意に(例えば定期的に)変更することを 要求すべきではない(SHOULD NOT)。ただし、ベリファイアは、認証者の危殆化の証拠がある場合、強制的に変更しなければならな い (SHALL) 。

- ベリファイアは、暗記された秘密を入力する際、請求者が「 ペースト 」機能を使用することを許可す べきである (SHOULD) 。
これによって、広く使われているパスワード・マネージャーの使用が容易になり、多くの場合、
ユーザーがより強力な暗記秘密を選択する可能性が高まる。

- 請求者が暗記した秘密をうまく入力できるように、検証者は、秘密が入力されるまで、一連のド ットやアスタリスクではなく、
秘密を表示するオプションを提供すべきである (SHOULD) 。これにより、請求者は、画面が観察されにくい場所にいる場合、
入力を確認することができる。ベリファイアはまた、正しい入力を確認するために、各文字が入力された後に短時間、
ユーザーの機器に個々の入力された文字を表示することを許可してもよい (MAY) 。これは特にモバイル機器に当てはまる。

- ベリファイアは、盗聴やMitM攻撃への耐性を提供するために、暗記された秘密を要求する 際に、
承認された暗号化と認証された保護チャネルを使用しなければならない[SHALL]。

- 検証者は、記憶した秘密をオフライン攻撃に耐性のある形式で保存しなければならない（SHALL）。暗記された秘密鍵は、適切な一方向性鍵導出関数を使用して、塩付けおよびハッシュ化されなければ ならない（SHALL）。鍵導出関数は、パスワード、ソルト、コスト係数を入力とし、パスワードハッシュを生成する。その目的は、パスワード・ハッシュ・ファイルを入手した攻撃者によるパスワード推測の各試行を高価なものにすることであり、したがって推測攻撃のコストを高くするか、禁止することである。適切な鍵導出関数の例としては、パスワードベースの鍵導出関数2(PBKDF2)[SP 800-132]やBalloon[BALLOON]がある。メモリハードな関数は、攻撃のコストを増加させるので、使用すべきです（SHOULD）。鍵導出関数は、鍵付きハッシュメッセージ認証コード(HMAC)[FIPS 198-1]、SP 800-107 において承認されたハッシュ関数、セキュアハッシュアルゴリズム 3(SHA-3)[FIPS 202]、CMAC[SP 800-38B]または Keccak メッセージ認証コード(KMAC)、カスタマイズ可能な SHAKE(cSHAKE)、または ParallelHash[SP800-185]などの承認された一方向性関数を使用しなければならない(SHALL)。鍵導出関数の選択された出力長は、基礎となる一方向性関数の出力長と同じであるべき である[SHOULD]。

- ソルトは少なくとも32ビット長でなければならず[SHALL]、保存されたハッシュ間のソルト値の衝突を最小化するように、任意に選択されなければならない[SHALL]。ソルト値と結果のハッシュの両方は、記憶された秘密認証子を使用して、各サブスクライバごとに保存されなけれ ばならない[SHALL]。

- PBKDF2の場合、コスト要因は反復回数である。PBKDF2関数の反復回数が多ければ多いほど、パスワードハッシュの計算にかかる時間は長くなる。したがって、反復回数は検証サーバーの性能が許す限り大きくすべきであり、通常は少なくとも10,000回反復すべきである。

- 加えて、検証者は、検証者だけが知っている秘密のソルト値を使用して、鍵導出関数の 追加反復を実行すべきである[SHOULD]。このソルト値は、使用される場合、承認されたランダム・ビット・ジェネレーター[SP 800-90Ar1]によって生成され、SP 800-131Aの最新リビジョンで規定された最小セキュリティ強度（本書の日付現在 112 ビット）を提供しなければならない。秘密のソルト値は、ハッシュ化された記憶された秘密とは別に(例えば、 ハードウェアセキュリティモジュールのような特別なデバイスに)保存しなければならない[SHALL]。この追加反復により、ハッシュ化された記憶された秘密に対するブルートフォース攻撃は、秘密のソルト値が秘密のままである限り、現実的ではない。

- サイバーセキュリティ啓発月間2023ブログシリーズ
  - 代理店のアドバイス
    - パスワードは、関心のあるリソースにアクセスするための認証メカニズムとして、今でも最も広く使われている。パスワードは、サイバー犯罪者やデータ侵害からデータの機密性と完全性を守るための最前線の防御手段である。良質で強力なパスワードは、人々がオンラインで安全かつプライベートに過ごすのに役立ちます。

- 参考

bitwarden

米国国立標準技術研究所（NIST）
ビットワルデンの総合評価非常に良い

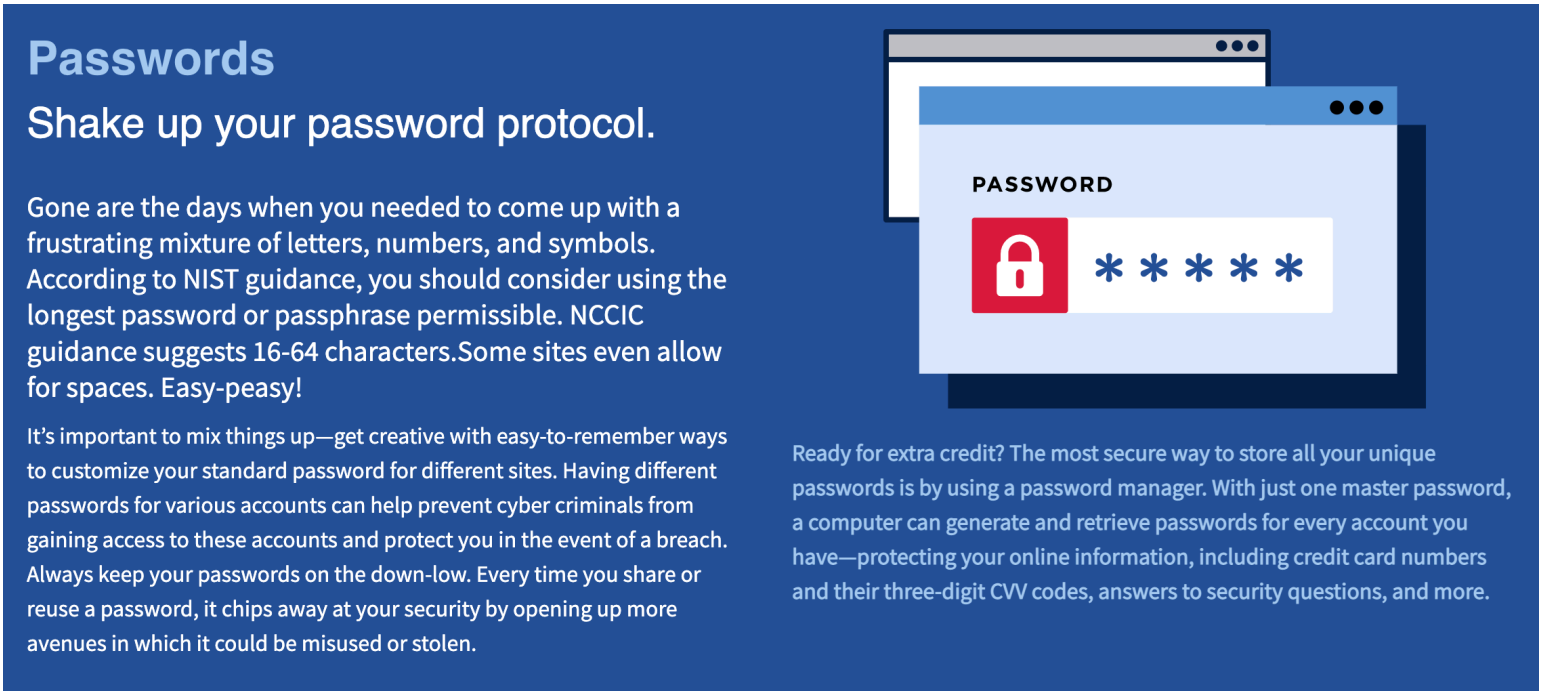
- パスワード・マネージャーの使用を推奨
- 強固なパスワードの重要性を訴える
- パスワードの安全性をさらに高める2FA/MFAの必要性を指摘
- セキュリティに関するアドバイス全体が最新で、NIST のガイドラインに準拠している（NIST は連邦政府のセキュリティに関するアドバイスの基準を定めている）。
- パスワード・セキュリティに関する推奨事項を、明確で、消化しやすく、見つけやすい方法で説明していない。

助言は徹底しており、代理店の基準を定めているが、
ウェブサイトからパスワードガイドラインにアクセスするのは直感的ではない。アドバイスは非常に長いPDFに埋もれており、使い勝手の悪い書き方をしている。

"Verifiers SHOULD permit claimants to use “paste” functionality when entering a memorized secret. This facilitates the use of password managers, which are widely used and in many cases increase the likelihood that users will choose stronger memorized secrets."

NIST

サイバーセキュリティ・インフラセキュリティ機構（CISA）
サイバー・レッスン



パスワード、CISAに関するサイバー・レッスン

- 参考

ランサムウェア対策ガイド

代理店のアドバイス

- 少なくとも15文字のユニークなパスワードを要求するパスワードポリシーを導入する。
  - パスワード・マネージャーは、安全なパスワードの作成と管理に役立ちます。使用中のパスワード・マネージャーへのアクセスを安全かつ制限し、MFAなど、使用中の製品で利用可能なすべてのセキュリティ機能を有効にする。

- 参考

世界を守れ強力なパスワードの要求

代理店のアドバイス

- 中小企業は悪意のあるハッカーの常習的な標的であり、デジタル窃盗犯の一般的な侵入口は、盗まれたパスワードや脆弱なパスワードである。

- しかし、従業員に強力なパスワードとパスワード・マネージャーの使用を義務づけることで、ビジネスの安全を守ることができるのは朗報だ。

- 個人とビジネスのすべてのアカウントで、長くてランダムなユニークなパスワードを使い、パスワード・マネージャーを使って忘れないようにすることで、模範を示しましょう！そして、ITスタッフやプロバイダーと協力して、従業員がシステムにアクセスする際に強力なパスワードを使用するよう義務付けましょう。これにより、データは安全に保護される。

- 参考

セキュア・アワ・ワールド脆弱なパスワード

代理店のアドバイス

- パスワード・マネージャーに任せましょう！パスワード・マネージャーは、私たちのために自動的にパスワードを作成し、保存し、入力する。そうすれば、私たちはそれぞれ、パスワード・
  マネージャー自体のための強力なパスワードを1つだけ覚えておけばいいことになる。高評価のパスワード・
  マネージャーを紹介しているConsumer Reportsのような「パスワード・マネージャー」の信頼できる情報源を検索する。
  レビューを読んでオプションを比較し、評判の良いプログラムを見つけましょう。

- 参考

bitwarden

サイバーセキュリティ・インフラセキュリティ機構（CISA）

ビットワルデンの総合評価非常に良い

- パスワード・マネージャーの使用を推奨
- 強固なパスワードの重要性を訴える
- パスワードの安全性をさらに高める2FA/MFAの必要性を指摘
- 全体的なセキュリティに関する助言が最新で、NIST のガイドラインに準拠している。
- パスワード・セキュリティに関する推奨事項を、明確で、消化しやすく、見つけやすい方法で説明していない。

国家安全保障局（NSA）

ランサムウェア対策ガイド

代理店のアドバイス

- 少なくとも15文字のユニークなパスワードを要求するパスワードポリシーを導入する。
  - パスワード・マネージャーは、安全なパスワードの作成と管理に役立ちます。使用中のパスワード・マネージャーへのアクセスを安全かつ制限し、MFAなど、使用中の製品で利用可能なすべてのセキュリティ機能を有効にする。
- 参考

シスコパスワードの種類ベストプラクティス

代理店のアドバイス

- 近年、ネットワーク・インフラに対する侵害が増加していることは、ネットワーク・デバイスに対する認証が重要な考慮事項であることを再認識させるものである。ネットワーク機器は、以下のような原因で危険にさらされる可能性がある：
  - パスワードの選択が悪い（ブルートフォースパスワードスプレーに弱い）
  - 暗号化されていない電子メールで送信されたルーターの設定ファイル（ハッシュ化されたパスワードを含む）。
  - パスワードの再利用（侵害されたデバイスから復元されたパスワードが、他のデバイスを侵害するために使用される可能性がある）。
- パスワードを単独で使用すると、デバイスが悪用されるリスクが高まる。NSAは、重要なデバイスを管理する管理者に多要素認証を強く推奨しているが、パスワードだけでなければならない場合もある。優れたパスワード保存アルゴリズムを選択することで、搾取をより困難にすることができる。
- 可能な限り保護するため、強力なパスワードを使用し、クラックされて平文に変換されるのを防ぐ。以下のパスワードポリシーに従うこと：
  - 小文字、大文字、記号、数字の組み合わせからなる；
  - 英数字15文字以上。

- そうでないパターン：
  - キーボードの散歩道
  - ユーザー名と同じ
  - デフォルトのパスワード
  - 他の場所で使用されるパスワードと同じ
  - ネットワーク、組織、場所、その他の機能識別子に関連するもの
  - 辞書に載っているもの、一般的な略語、推測しやすいもの
- 参考

ソーシャルメディアにおける安全確保

代理店のアドバイス

- パスワードの保護と強化
  - 各オンラインアカウントには、ユニークで強力なパスワードを使用する。複数のアカウントでパスワードを再利用すると、パスワードが発見された場合、すべてのアカウントのデータが流出する可能性がある。パスワードは、文字、数字、特殊文字を組み合わせて、適切な長さと複雑さを持たせてください。可能であれば、認証トークンやアプリを使った多要素認証を導入し、パスワードが漏えいしてもアカウントにアクセスできないようにしましょう。パスワードは決して共有せず、ソーシャルメディアのプロフィールや公開情報から推測されるような情報は使わないようにしましょう。
- 参考

安全な多要素認証ソリューションの選択

代理店のアドバイス

- 単一応答、多要素認証のメカニズムでは、PIN/パスワードまたはバイオメトリクスのいずれかを使用してデバイスをアクティブにする必要があります。デバイスは「あなたが持っているもの」を提供し、デバイスの起動は「あなたが知っているもの」あるいは「あなたがいるもの」が確認されたことを意味する。
- 一方、多段階認証には、「知っていること」を提供するパスワードと、「持っていること」を提供する別の認証が含まれることが多い。米国政府機関は、「What-you-know」を提供するために直接使用されるパスワードだけでなく、PIN/パスワードの有効化に関する要件も検討すべきである。SP 800-63-3 Part B のガイドラインでは、暗記秘密鍵（アクティベーション用と単一要素認証用 の両方）は少なくとも 6-8 文字でなければならず、ユーザが選択したパスワードにはより高いパ スワード強度を推奨している。パスワード要件を決定する場合、多要素デバイスはパスワード推測攻撃に対処するために厳密な閾値を組み込むべきであるが、検証者は、直接使用されるパスワードがより高い強度要件を持つことを保証する、より厳しくない閾値メカニズムを採用する可能性があることに注意すること。
- 参考

Very Good

bitwarden

国家安全保障局（NSA）

ビットワルデンの総合評価良い

- パスワードマネージャーの使用は推奨しない
- 強固なパスワードの重要性を訴える
- パスワードの安全性をさらに高める2FA/MFAの必要性を指摘
- 全体的なセキュリティに関する助言が最新ではなく、NIST のガイドラインに準拠している。
- パスワード・セキュリティに関する推奨事項を、明確で、消化しやすく、見つけやすい方法で説明していない。

"Disable the feature that allows web browsers to remember your passwords. Secure your passwords in a password manager."

NSA

国土安全保障省

CISAはDHSの管轄下にある。

サイバーセキュリティのページ

代理店のアドバイス

- バイデン大統領は、国土安全保障省（DHS）の重要な任務であるサイバーセキュリティを、バイデン＝ハリス政権のあらゆるレベルにおける最優先事項としている。
- マヨルカス長官は、大統領のコミットメントを推進し、国家のサイバーセキュリティの回復力強化がDHSの最優先事項であることを反映させるため、就任後1カ月でサイバーセキュリティに特化した行動を呼びかけた。この行動の呼びかけは、ランサムウェアの差し迫った脅威への取り組みと、より強固で多様な労働力の構築に焦点を当てたものだった。
- 2021年3月、マヨルカス長官は、ハンプトン大学およびガールスカウト・オブ・USAとの協力のもと、RSAカンファレンスが主催したバーチャル講演で、同省のサイバーセキュリティへの取り組みに関する広範なビジョンとロードマップについて概説した。
- プレゼンテーションの後、長官はガールズスカウトのジュディス・バティ暫定CEOとともに、現在米国が直面している前例のないサイバーセキュリティの課題について熱く語り合った。ハンプトン大学コンピューターサイエンス学部のChutima Boonthum-Denecke博士が事務局長を紹介し、質疑応答でプログラムを締めくくった。
  - DHSサイバーセキュリティ・スプリントの概要

bitwarden

国土安全保障省

ビットワルデンの総合評価改善の余地

- パスワードマネージャーの使用は推奨しない
- 強固なパスワードの重要性を訴えない
  - 不正確で見当違いなパスワード・セキュリティのアドバイスを提供する、あるいはパスワードやパスワード・セキュリティについて言及しない
  - パスワードに関するアドバイスを明確に呼び出さない
- パスワードのセキュリティをさらにサポートする2FA/MFAの必要性を一貫して挙げていない。
- 全体的なセキュリティに関する助言が最新ではなく、NIST のガイドラインに準拠していない。
- パスワード・セキュリティに関する推奨事項を、わかりやすく、消化しやすく、見つけやすく説明していない。

連邦捜査局（FBI）

サイバー脅威

代理店のアドバイス

- インターネットを利用した犯罪やサイバー侵入はますます巧妙になっており、それらを防ぐには、接続されたデバイスの各ユーザーが意識して警戒する必要がある。
- システムとソフトウェアを常に最新の状態に保ち、強力で評判の良いアンチウイルスプログラムをインストールする。
- 公共のWi-Fiネットワークに接続する際は注意し、公共のネットワーク上では購入を含む機密性の高い取引を行わないこと。
- 各オンラインアカウントに強力でユニークなパスフレーズを作成し、定期的にパスフレーズを変更する。
- 多要素認証を許可しているすべてのアカウントで多要素認証を設定する。
- メッセージに返信したり、サイトを訪問したりする前に、すべての通信に含まれる電子メール・アドレスを調べ、ウェブサイトのURLを精査する。
- 迷惑メールやテキスト・メッセージはクリックしないこと。
- オンラインプロフィールやソーシャルメディアのアカウントで共有する情報には慎重になること。ペットの名前、学校名、家族構成などを共有すると、詐欺師があなたのパスワードやアカウントのセキュリティ質問の答えを推測するためのヒントを与えてしまう可能性があります。
- 金銭的な支援を求めている見知らぬ人物や組織には支払いを送らず、早急な行動を促すこと。
- 参考

インターネット上の詐欺と安全

代理店のアドバイス

- **ファイアウォールをオンにしておく**

  ファイアウォールは、コンピュータをクラッシュさせたり、情報を削除したり、
  あるいはパスワードやその他の機密情報を盗もうとするハッカーからコンピュータを保護するのに役立ちます。ソフトウェア・
  ファイアウォールは、1台のコンピュータに広く推奨されている。このソフトウェアは、
  いくつかのオペレーティングシステムにあらかじめパッケージされているか、個々のコンピュータ用に購入することができる。
  複数のネットワーク・コンピュータの場合、ハードウェア・ルーターがファイアウォール・プロテクションを提供するのが一般的だ。

- **ウイルス対策ソフトウェアのインストールまたは更新**

  アンチウイルス・ソフトウェアは、悪意のあるソフトウェア・
  プログラムがコンピュータに埋め込まれるのを防ぐように設計されています。
  ウイルスやワームのような悪意のあるコードを検出した場合、それを解除または除去するために働く。
  ウイルスはユーザーの知らないうちにコンピュータに感染する。ほとんどのウイルス対策ソフトは、
  自動的にアップデートするように設定できる。

- **スパイウェア対策技術のインストールまたはアップデート**

  スパイウェアとはその名の通り、あなたのコンピューターに密かにインストールされ、
  コンピューター上でのあなたの行動を他人が覗き見できるようにするソフトウェアのことです。スパイウェアの中には、
  同意なしにあなたに関する情報を収集したり、ウェブブラウザに不要なポップアップ広告を表示したりするものもあります。
  オペレーティングシステムによっては、スパイウェア対策を無料で提供しているものもありますし、
  安価なソフトウェアはインターネットやお近くのコンピューターショップで簡単にダウンロードできます。
  ダウンロード可能なスパイウェア対策製品を提供するインターネット上の広告には注意が必要です。これらの製品は偽物の場合があり、
  実際にはスパイウェアやその他の悪質なコードが含まれている可能性があります。食料品を買うのと同じで、
  信頼できるところで買い物をする。

- **オペレーティングシステムを最新の状態に保つ**

  コンピュータのオペレーティング・システムは、技術的な要求に対応し、セキュリティ・ホールを修正するために定期的に更新される。
  必ずアップデートをインストールし、コンピュータが最新の保護機能を備えていることを確認してください。

- **ダウンロードにご注意ください**

  電子メールの添付ファイルを不用意にダウンロードすると、どんなに用心深いアンチウイルス・ソフトウェアでも回避することができる。
  知らない人からの電子メールの添付ファイルは決して開かないこと。また、
  知っている人からの転送された添付ファイルにも注意すること。知らず知らずのうちに悪意のあるコードを進めていたのかもしれない。

- **コンピュータの電源を切る**

  高速インターネット接続の普及に伴い、多くの人がパソコンの電源を入れっぱなしにしておくことを選ぶようになった。欠点は、"常時オン"であるためにコンピュータが影響を受けやすいことだ。コンピュータの電源を切ることは、
  不要な攻撃を防ぐために設計されたファイアウォールプロテクションにとどまらず、スパイウェアやボットネットなど、
  攻撃者の接続を効果的に遮断することができる。

- 参考

Good

bitwarden

連邦捜査局（FBI）
ビットワルデンの総合評価良い

- パスワードマネージャーの使用は推奨しない
- 強固なパスワードの重要性を訴える
- パスワード・セキュリティをさらにサポートする2FA/MFAの必要性を指摘
- 全体的なセキュリティに関する助言が最新ではなく、NIST のガイドラインに準拠していない。
- パスワード・セキュリティに関する推奨事項を、わかりやすく、消化しやすく、見つけやすく説明していない。

"Be careful with what information you share online or on social media. By openly sharing things like pet names, schools you attended, links to family members, and your birthday, you can give a scammer all the information they need to guess your password or answer your security questions."

FBI

連邦取引委員会（FTC）

強力なパスワードの作成とアカウントを保護するその他の方法

代理店のアドバイス

- もうひとつの方法は、サードパーティのパスワード・マネージャーを使って強力なパスワードを作成し、それを覚えておくことだ。評判の良いパスワード・マネージャーを見つけるには、専門家のレビューを読んでみよう。パスワード・マネージャーで使用しているパスワードが強固で安全であることを確認してください。ウェブ・ブラウザ、モバイル・ブラウザ、パスワード・マネージャーはすべて、パスワードを保存してくれる。

- 強固なパスワードは、あなたのアカウントをハッカーから守るための重要な第一歩です。しかし、強力なパスワードでもサイバー攻撃には弱い。多要素認証を使用することは、パスワードを盗んだハッカーが、別の認証要素なしにアカウントにログインできないことを意味します。

- 多要素認証の最も一般的なタイプは、テキストメッセージや電子メールで受け取る認証パスコードである。このワンタイムパスコードは通常6桁以上で、自動的に失効する。しかし、これは二要素認証の中で最も安全性の低いタイプなので、オプションがあれば、認証アプリや セキュリティキーのような、より安全性の高い方法を選びましょう。

- 参考

パスワードチェックリスト

代理店のアドバイス

- **パスワードは長くて強固なものにしてください。**つまり最低でも12文字。一般的に、パスワードを長くすることは、パスワードをより強固なものにする最も簡単な方法である。パスワードがより覚えやすいように、ランダムな単語からなるパスフレーズを使用することを検討するが、一般的な単語やフレーズを使用することは避ける。使用しているサービスが長いパスワードを許可していない場合は、大文字と小文字、数字、記号を混ぜることで、より強力なパスワードを作ることができます。

- **他のアカウントで使ったパスワードを再利用しないこと。**アカウントごとにパスワードを使い分ける。そうすれば、ハッカーが1つのアカウントのパスワードを入手しても、それを使って他のアカウントに侵入することはできない。

- **多要素認証が利用可能な場合は利用する。**アカウントによっては、ログインにパスワード以外の何かを要求することで、さらに安全性を高めているものもある。これは多要素認証と呼ばれる。アカウントにログインするために必要な「何か特別なもの」は、2つのカテゴリーに分けられる：

  - あなたが持っているもの–認証アプリやセキュリティ・キーで取得したパスコードなど。

  - 指紋、網膜、顔のスキャンのように。

- **パスワードマネージャーを検討する。**ほとんどの人は、すべてのパスワードを管理するのが大変だ。パスワードは長ければ長いほど、複雑であればあるほど強力ですが、長ければ長いほど覚えるのが難しくなります。パスワードとセキュリティ質問は、信頼できるパスワード・マネージャーに保存することを検討しましょう。評判の良いパスワード・マネージャーを見つけるには、独立系のレビュー・サイトを検索したり、友人や家族が使っているものについて話を聞いたりすることだ。パスワード・マネージャー内の情報を保護するために、必ず強力なパスワードを使用してください。

- **自分だけが答えを知っているセキュリティ上の質問を選ぶ。**サイトがセキュリティ上の質問に答えるよう求めてきた場合、郵便番号、出生地、母親の旧姓など、公的記録で入手可能な答えや、オンラインで簡単に検索できる答えを答えるのは避けましょう。また、攻撃者が簡単に推測できるような、回答数が限られている質問（初めて買った車の色など）は使わないこと。推測を難しくするために、無意味な答えを使うこともできる。

- **パスワードが破られた場合は、速やかに変更すること。**
  ハッカーがあなたのパスワードを入手した可能性のあるデータ流出があったと企業から聞かされたら、その企業で使っているパスワードをすぐに変更し、同じようなパスワードを使っているアカウントもすべて変更すること。

- 参考

Excellent

bitwarden

連邦取引委員会（FTC）
ビットワルデンの総合評価素晴らしい

- パスワード・マネージャーの使用を推奨
- 強固なパスワードの重要性を訴える
- パスワードの安全性をさらに高める2FA/MFAの必要性を指摘
- 全体的なセキュリティに関する助言が最新で、NIST のガイドラインに準拠している。
- パスワード・セキュリティに関する推奨事項を、わかりやすく、消化しやすく、見つけやすく説明する。

"Use a password manager. A third-party password manager also can create a strong password. To find a reputable password manager, read expert reviews. Make sure the password for your password manager is strong. And protect it like you do your other passwords."

FTC

商務省

全国サイバーセキュリティ月間オンラインで身を守る

代理店のアドバイス

- 以前は、特殊文字、大文字、数字、アルファベットを使ってパスワードを作成し、年に何度もパスワードを変更させるなど、さまざまな任意のルールを設けるのが常識だった。調査によると、私たち一人一人が同じようなことをしたようだ。パスワードを使いまわしたり、同じパスワードのバリエーションを作ったりしたのは、サイトやログイン、アプリケーションごとに何十個ものユニークなパスワードを記憶するよう求められたからだ。

- 私たちの自然な本能がオンライン・セキュリティの弱点を作り出し、サイバー犯罪者がそれを利用したのだ。パスワードの使用に関する研究は、ユーザーが任意に複雑なパスワードを記憶することを期待することの本質的な弱点と、個人情報を保護するために多要素認証（MFA）を使用することの重要性を実証している。重要なのは、私たちの考え方がこのトピックをめぐって発展してきたことであり、私たち自身をよりよく守るために以下のような実践を行なっている：
  - パスワードを使用しなければならない場合は、より長いパスワード（15文字以上）、あるいはパスフレーズを使用してください。パスフレーズは覚えやすいという利点もある。
  - MFA（電子メールで送信されるワンタイムコードや、携帯電話の認証アプリなど）を採用することで、漏洩したパスワードから保護するための第二の重要なレイヤーが追加される。MFAはいつでも設定できるはずだ。ほんの2、3分かかるだけだが、安心感を与えてくれる。
  - パスワード・マネージャーは、MFAを有効にした1つの非常に強力で長いパスワードで保護されているため、すべてを記憶する必要がなく、サイトごとに固有のパスワードを作成することができる。

- 参考

NISTは商務省の管轄下にある。

代理店のアドバイス

- 相互接続されたグローバル・ネットワーク、そしてそれらのネットワークに接続された機器やデータのセキュリティを確保することは、この時代を象徴する課題のひとつである。
- 商務省の任務は、サイバーセキュリティに対する認識と保護を強化し、プライバシーを保護し、公共の安全を維持し、経済的および国家的安全保障を支援し、アメリカ人がオンラインで安全管理を向上できるようにすることである。
  - NIST、プライバシー・フレームワークのバージョン1.0をリリース
  - NIST、セキュリティとプライバシーのセーフガードカタログの「クイックスタート」ガイドを提供
  - 中小企業のサイバーセキュリティ・コーナー
- 参考

Very Good

bitwarden

商務省

ビットワルデンの総合評価非常に良い

- パスワード・マネージャーの使用を推奨
- 強固なパスワードの重要性を訴える
- パスワードの安全性をさらに高める2FA/MFAの必要性を指摘
- 全体的なセキュリティに関する助言が最新で、NIST のガイドラインに準拠している。
- パスワード・セキュリティに関する推奨事項を、わかりやすく、消化しやすく、見つけやすく説明していない。

連邦通信委員会（FCC）

中小企業向けサイバーセキュリティ・チップシート

- 従業員にセキュリティ原則を教育する。強力なパスワードの義務付け、適切なインターネット利用ガイドラインの策定など、
  従業員に対する基本的なセキュリティ慣行とポリシーを確立し、
  会社のサイバーセキュリティポリシーに違反した場合の罰則について詳述する。顧客情報やその他の重要なデータをどのように扱い、
  保護するかを記述した行動規範を確立する。

- 従業員には一意のパスワードを使用し、3カ月ごとにパスワードを変更することを義務付ける。
  パスワード以外の追加情報を必要とする多要素認証の導入を検討する。機密データを扱う業者、特に金融機関が、
  あなたのアカウントに多要素認証を提供しているかどうかを確認してください。

- 参考

10. Passwords and authentication

Require employees to use unique passwords and change passwords every three months. Consider implementing multi-factor authentication that requires additional information beyond a password to gain entry. Check with your vendors that handle sensitive data, especially financial institutions, to see if they offer multi-factor authentication for your account.

Fair

bitwarden

連邦通信委員会（FCC）

ビットワルデンの総合評価まあまあ

- パスワードマネージャーの使用は推奨しない
- 強固なパスワードの重要性を訴える
  - パスワード・セキュリティに焦点を当てたコンテンツへのリンク
  - しかし、内容は明らかに古く、もっと整理する必要がある。
- パスワードのセキュリティをさらにサポートする2FA/MFAの必要性を一貫して挙げていない。
- 全体的なセキュリティに関する助言が最新ではなく、NIST のガイドラインに準拠していない。
  - NISTのガイドラインに反し、パスワードは3カ月ごとに変更することを推奨
- パスワード・セキュリティに関する推奨事項を、わかりやすく、消化しやすく、見つけやすく説明していない。

中小企業庁（SBA）

サイバー攻撃を防ぐためのベストプラクティス

代理店のアドバイス

- 従業員とその業務上のコミュニケーションは、御社のシステムへの直接の侵入経路であるため、
  中小企業にとってデータ漏洩の主要な原因となっています。
  基本的なインターネット利用のベストプラクティスについて従業員を訓練することは、サイバー攻撃を防ぐ上で大いに役立つ。
  - その他のトレーニング・トピックは以下の通り：
    - フィッシングメールを見破る
    - インターネットを上手に利用する
    - 不審なダウンロードを避ける
    - 認証ツールの有効化（強力なパスワード、多要素認証など）
    - ベンダーと顧客の機密情報の保護
- 参考

Enable Multi-Factor Authentication

Multi-Factor Authentication (MFA) is a mechanism to verify an individual's identity by requiring them to provide more than just a typical username and password. MFA commonly requires users to provide two or more of the following: something the user knows (password, phrase, PIN), something the user has (physical token, phone), and/or something that physically represents the user (fingerprint, facial recognition). Check with your vendors to see if they offer MFA for your various types of accounts (e.g., financial, accounting, payroll).

Good

bitwarden

中小企業庁（SBA）
ビットワルデンの総合評価良い

- パスワードマネージャーの使用は推奨しない
- 強固なパスワードの重要性を訴える
- パスワードの安全性をさらに高める2FA/MFAの必要性を指摘
- 全体的なセキュリティに関する助言が最新ではなく、NIST のガイドラインに準拠していない。
- パスワード・セキュリティに関する推奨事項を、明確で、消化しやすく、見つけやすい方法で説明していない。

証券取引委員会（SEC）

2023年7月、SECは「上場企業が経験した重要なサイバーセキュリティ事件と、サイバーセキュリティのリスク管理、戦略、ガバナンスに関する重要な情報の両方を年次で開示することを義務付ける最終規則を採択した」。サイバーセキュリティ・コンプライアンスを実施するSECの役割を考えると、SEC自身のパスワード・セキュリティに関する助言を評価することは賢明であると思われる。

SEC.govのウェブサイトで "password security "を検索すると、12件の文書がヒットするが、いずれも数年前のものと思われる。サイバーセキュリティに特化したページもあるが、CISAから再利用したかなり一般的な推奨事項を提供している。2020年からのサイバーセキュリティ・リスクアラート「サイバーセキュリティ：クレデンシャルの危殆化から顧客アカウントを保護する」と題された2020年からのサイバーセキュリティ・リスク警告は、クレデンシャル・スタッフィングについて論じたPDFにつながる。パスワード」という言葉は随所で使われているが、「パスワードの安全性」については明確に言及されていない。「強力なパスワード」は、以下の文脈で言及されている：

サイバーセキュリティクレデンシャル漏洩から顧客アカウントを守る

代理店のアドバイス

- 会社がクレデンシャル・スタッフィング攻撃に備えるにあたり、OCIEスタッフは、会社に対し、現在のプラクティス（例えば、上記のMFAやその他のプラクティス）と、それらのプラクティスの潜在的な限界を検討し、会社の顧客やスタッフが、アカウントをより安全に保護する方法について適切な情報を得ているかどうかを検討するよう促している。情報提供された顧客ほとんどの企業は、顧客やスタッフに強力なパスワードを作成し、使用するよう求めている。しかし、パスワードの使用は、顧客やスタッフが他のサイトからのパスワードを再利用する場合、あまり効果的ではありません。より効果的なものにするため、一部の企業は顧客や従業員に対し、強固でユニークなパスワードを作成し、パスワードが漏洩した兆候がある場合はパスワードを変更するよう通知・奨励している。

The Commission has noted that cybersecurity risks have increased alongside the ever-increasing share of economic activity that depends on electronic systems, the growth of remote work, the ability of criminals to monetize cybersecurity incidents, the use of digital payments, and the increasing reliance on third party service providers for information technology services, including cloud computing technology. In my view, artificial intelligence and other technologies may enhance both the ability of public companies to defend against cybersecurity threats but also the capacity of threat actors to launch sophisticated attacks. The Commission also observed that the cost to companies and their investors of cybersecurity incidents is rising at an increasing rate. All of these trends highlight investors' need for improved disclosure.

Fair

bitwarden

証券取引委員会（SEC）

ビットワルデンの総合評価まあまあ

- パスワードマネージャーの使用は推奨しない
- 強固なパスワードの重要性を訴える
  - 強力なパスワードの存在を認めつつも、もっと明確な表現が可能な日付のコンテンツへのリンク
- パスワードのセキュリティをさらにサポートする2FA/MFAの必要性を一貫して挙げていない。
  - 2FA/MFAは上記のリンク先のPDFで言及されているが、多くのアドバイスがあるわけではないので、見つけるには検索が必要である。
- 全体的なセキュリティに関する助言が最新ではなく、NIST のガイドラインに準拠していない。
- パスワード・セキュリティに関する推奨事項を、わかりやすく、消化しやすく、見つけやすく説明していない。

ホワイトハウス

2023年「サイバーセキュリティ啓発月間」宣言

代理店のアドバイス

- 「私は、米国の国民、企業、機関に対し、サイバーセキュリティの重要性を認識し、行動するよう呼びかけるとともに、国家の安全保障と回復力を支援するため、サイバーセキュリティ啓発月間を実施する。私はまた、企業や機関に対し、サイバー脅威から米国民をよりよく守り、米労働者が高賃金のサイバー職に就く新たな機会を創出するための行動を起こすよう求める。アメリカ人はまた、多要素認証を有効にする、コンピューターやデバイスのソフトウェアをアップデートする、強固なパスワードを使用する、不審なリンクのクリックに注意を払うなど、自分自身をよりよく守るためにすぐに行動を起こすことができる。
- 参考

デジタル・ファーストのパブリック・エクスペリエンスを提供

代理店のアドバイス

- また、パスワードの「貼り付け」やその他の自動化されたクライアント側の支援メカニズムを妨げてはならない。
- 参考

ホワイトハウス多要素認証近代化シンポジウム報告書

代理店のアドバイス

- 「CISA事務局長のブランドン・ウェールズは、「オンラインを安全に利用するためには、パスワード以上のものが必要であり、悪意のあるサイバー行為者からデータをより確実に保護するために、多要素認証が必要なのです。「CISAは一貫して、重要なデータにアクセスしにくくするため、すべてのユーザーにMFAを導入するよう組織に求めてきた。今日のシンポジウムは、私たち全員が現実のものにするために努力しているビジョンを描くために集まるものです」。
- 参考

バイデン-ハリス政権、米国消費者保護のためのスマートデバイス向けサイバーセキュリティ表示プログラムを発表
代理店のアドバイス

- FCCは、無線通信機器を規制する権限に基づき、サイバーセキュリティに関する自主的な表示プログラムを2024年に開始する予定で、その展開についてパブリックコメントを求める見込みである。提案されているように、このプログラムは、例えば、ユニークで強力なデフォルトパスワード、データ保護、ソフトウェアアップデート、インシデント検出機能などを要求する米国標準技術局（NIST）が公表した特定のサイバーセキュリティ基準に基づいて、製品の認証とラベル付けを行う関係者主導の取り組みを活用するものである。

- 参考

ホワイトハウス

ビットワルデンの総合評価良い

- パスワードマネージャーの使用は推奨しない
  - ホワイトハウスは、2022年のサイバーセキュリティ啓発月間で、パスワード・マネージャーの使用を推奨した。
    ホワイトハウスは、2023年サイバーセキュリティ啓発ブログで同じことをする機会を得た。彼らはそうしなかった。
    ブログでは「強力なパスワードの使用」を推奨しているが、パスワード・マネージャーについての言及はない。
- 強固なパスワードの重要性を訴える
- パスワードの安全性をさらに高める2FA/MFAの必要性を指摘
- 全体的なセキュリティに関する助言が最新ではなく、NIST のガイドラインに準拠していない。
  - ホワイトハウスは、これまでのコミュニケーションで、NISTのアドバイスに反してパスワードの変更を推奨してきた。
    パスワードは、脆弱であったり、再利用されていたり、漏洩していたりする場合にのみ変更すべきである。
    強固でユニークなパスワードは、漏洩の疑いがない限り、変更する必要はないかもしれない。
- パスワード・セキュリティに関する推奨事項を、わかりやすく、消化しやすく、見つけやすく説明していない。
  - サイバーセキュリティの専門ページがない

概要

オンラインを安全に保つためにできることはたくさんあるが、最も簡単で、セキュリティに即座に大きな影響を与えるのは、パスワード・マネージャーを使うことだ。無制限にユニークで強力なパスワードを生成・保存できる、知識ゼロのエンド・ツー・エンド暗号化を備えたクロスプラットフォームのパスワード・マネージャーを選ぼう。無料アカウントでBitwardenを始めることもできるし、年間10ドル以下のプレミアムを選んで高度な機能を手に入れることもできる。

その他のリソース

- パスワードセキュリティの現状プレゼンテーションを見る