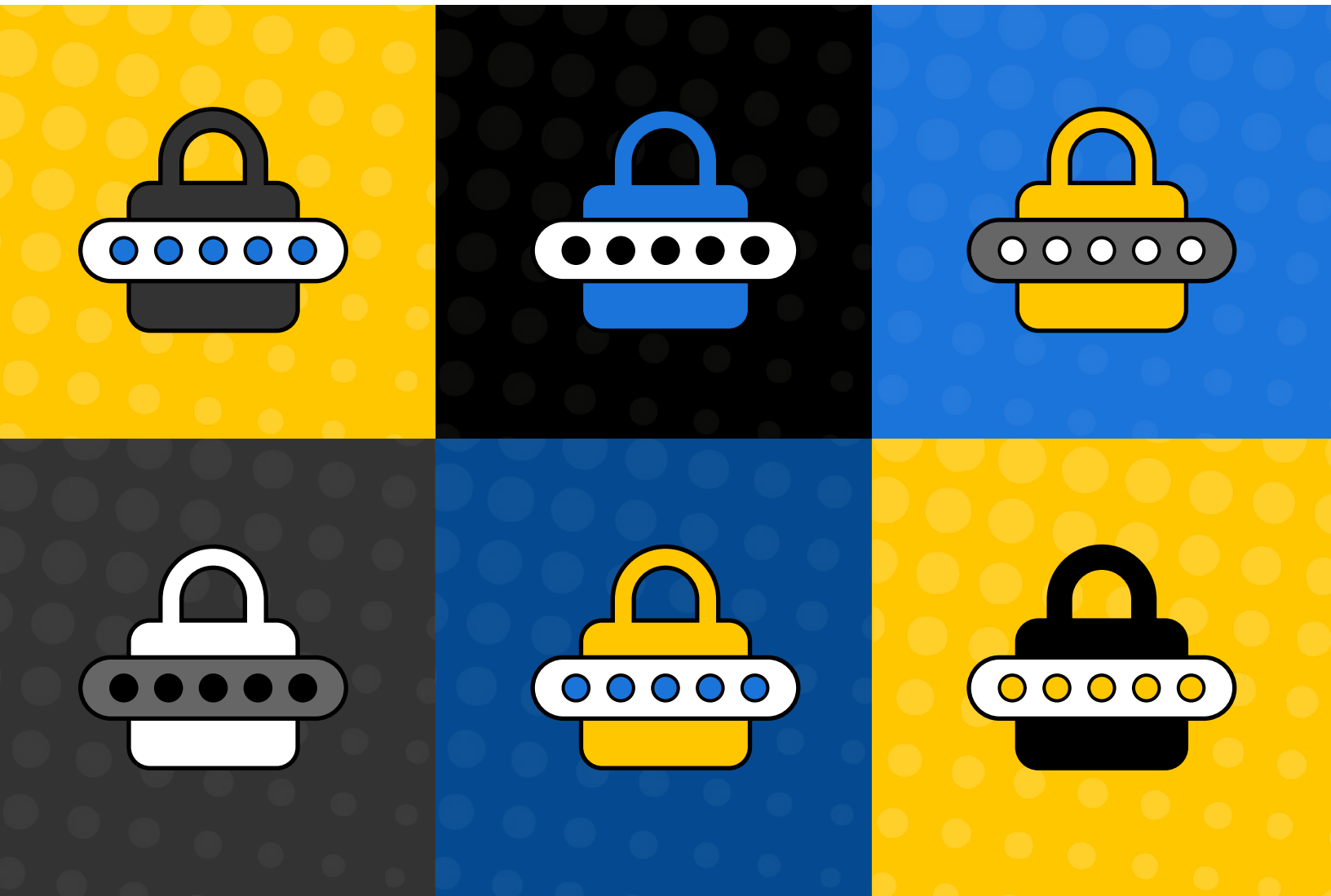
KEEPER
Cybersecurity Starts Here®

2022年
米国パスワード慣行レポート



序文

オンラインパスワードは、私たちの生活における数多くの重要な側面で使われています。コミュニケーションや仕事、取引、旅行において、パスワードは必要不可欠です。銀行口座から健康に関する記録まで、非常に機密性の高いデータにアクセスする際にパスワードを使用しています。デジタル化が進む中、パスワードは私たちの生活に欠かせないものです。

しかし、パスワードの選択からパスワードを覚える手段、そして厄介なことには機密性の高いパスワードを他の人と共有しても構わないという意思に至るまで、私たちはパスワード保護に関して驚くほど無頓着です。

Keeper Securityが米国と英国で4,000人以上を対象に行った調査では、パスワード保護に対する認識の甘さが浮き彫りになりました。つまり、パスワードを配偶者と共有したり、紙切れに書き留めたり、頻繁に変更したり、さらには年に50回以上もパスワードを忘れてしまったりといったことです。

その結果、米国での調査に対する回答者2,000人の半数近くが、少なくとも一度はハッキングされた経験があり、サイバー攻撃1件につき平均して378ドル盗まれたことがあると回答しています。

パスワードが適切に保護されてないせいで、オンライン犯罪や身元情報盗難が増加している時代に大きな打撃を受ける可能性があるのです。ハッキングされたパスワードのせいで、銀行口座に不正行為が起きたり、信用が下がったり、私生活に支障が出たり、ビジネス上の関係が断絶したりといった事態が生じる可能性があります。

私たちはこれまで以上にデジタルに依存しているため、パスワード保護が不十分であることは、サイバー攻撃の脅威を拡大させる原因となってしまいます。2020年の調査では、平均的なアメリカ人は **10台以上の接続された状態にあるデバイス** を家庭で所有しており、85%はスマートフォンを持っていると答えています。その結果、特に毎日 **2,000件以上のサイバー攻撃** がFBIに報告され、無数の事例が報告されずにいる状況下では、危機的な個人データ漏洩が発生する可能性は極めて高いものと言えるでしょう。

脆弱なパスワードの問題に対する意識を高めるために、ゼロトラストおよびゼロ知識サイバーセキュリティソフトウェアの大手プロバイダーである **Keeper Security**は、アメリカ人のパスワード習慣や慣行についての知見をここに共有いたします。当社は、脆弱なパスワードや重複したパスワード、共有されたパスワードによって日々危険にさらされている個人の財政情報やデータに対する意識を高めることで、サイバー犯罪のリスクを軽減し、より優れたパスワード慣行をアメリカ人に促進したいと考えております。

要約

当社の調査は、独立系市場調査コンサルティング会社であるCensuswide社によって、2022年8月11日から15日まで実施されました。調査は、英国と米国の全国を代表する回答者4,007人（18歳以上）を対象とし、オンラインリンクを介して行われました。Censuswide社は英国世論調査協議会（British Polling Council）のメンバーであり、ESOMARの原則に基づいた市場調査協会（Market Research Society）に準拠し、そのメンバーを雇用しています。

アメリカ人は、サイバー犯罪に対する意識は高まっているものの基本的なパスワード衛生を無視し続けているため、知らず知らずのうちにサイバー犯罪者や詐欺師に情報を差し出してしまい、結果として個人情報の漏洩や資金の損失につながっていることがこのデータを通してわかりました。

回答者の約56%がパスワードを使い回していることは、調査で明らかになった憂慮すべき結果です。あるアカウントのパスワードが漏洩すると、被害者は自分の他のアカウントも漏洩のリスクに晒していることになるのです。

Keeperの調査によると、サイバー攻撃の主な原因は、パスワード保護に対する憂慮すべき軽率な態度であることが判明しました。回答者10人中7人近くが、サイバー攻撃に見舞われたらどうなるかと懸念していますが、回答者の5分の1ほどは通知を受けた場合にのみパスワードを変更すると答えています。一方、回答者の15%が、自分のパスワードが既にダークウェブ上で侵害されていることを認識していると認めています。

米国内で人々がパスワードと結びつけて考える重要度を測るため、調査では回答者に対し、パスワードをすべて失うことと比較してむしろ何が起こった方が良いと考えているのかを尋ねました。

回答者の3分の1以上が、デートをすっぽかされることやテレビを1週間見られないことの方が良いと回答したのです！それについてよく考えてみると、私たちの日常生活における多くのことはパスワードで保護されています。パスワードで保護されたアカウントごとに全く新しいパスワードを再設定したり作成したりすることは、骨の折れる作業となるでしょう。

調査で現れた態度や行動を考慮すると、米国の消費者がパスワード衛生について見て見ぬふりをしていることは憂慮すべき事態です。これは、一般の人々が信頼できるパスワード管理システムを使用し、より優れたサイバーセキュリティを採用することへの切迫したニーズを示しています。

調査結果

不十分なパスワード管理とその影響

不十分なパスワード保護

45～54歳の回答者の3分の1以上（34%）が、パートナーや配偶者を信じてパスワードを委ねていると答えているのに対し、同様の回答をした18～24歳の回答者は5分の1以上（22%）でした。

調査対象者は、推測しやすいパスワードを使っているためにサイバー犯罪に対して無防備な状態にあります。回答者の18%がペットの名前を使用、13%が家族の名前を使用、12%が自分の誕生日を使用、11%が自分の名前を使用、9%が連続した数字（例：123）を使用しているのです。

18～24歳の回答者の4分の1（24%）が、パスワードを作成する際に自分の誕生日を使用すると答えたのに対し、55～64歳の回答者の14人に1人（7%）が同様の回答をしています。これは、パスワード衛生に対する若者の悠長な態度を指摘するものです。

また、これらの調査結果は、推測されやすいパスワードが他の家族や親しい友人に利用される可能性も示しています。

パスワードの重複

回答者の56%が、複数のサイトやアプリで同じパスワードを使用しており、回答者は平均して4つの異なるサイトやアプリで同じパスワードを使用しています。

年齢別の平均を見てみると、25～34歳の回答者は5つの異なるサイトやアプリで同じパスワードを使用しており、65歳以上の回答者は3つの異なるサイトやアプリで同じパスワードを使用しています。

結果として、複数のアカウントがサイバー攻撃の影響を受ける可能性は、米国では現実に起こり得ることなのです。

ハッキングによる影響

当社の調査回答者の55%が、少なくとも1回はサイバー攻撃の被害に遭った経験があり、回答者の約5分の1（18%）が、結果として金銭を盗まれたと答えています。回答者の平均損失額は 378 ドルでした。

回答者の3分の1近く（32%）が、SNSアカウントのログイン情報が盗まれたと回答しており、18〜24歳の回答者の場合はさらに高い割合を示しています。若者グループの回答者の5人に2人以上が、漏洩のせいで自分のSNSのログイン情報が盗まれたことがあると回答しています。

一方、調査対象者の15%が、自分のパスワードが漏洩した、あるいはダークウェブで売られていることを認識していると回答しています。

パスワードをどれだけ大切にしているのか？

25〜34歳の回答者の3分の1以上（34%）が、パスワードをすべて失うくらいなら、デートにすっぽかされた方がいいと回答しています。

回答者の約3分の1以上が、パスワードをすべて失うくらいなら、テレビを1週間見ない方がいいと回答しています。

回答者の19%が、パスワードをすべて失うよりも飛行機に乗り遅れる方がいいと答え、17%はパスワードをすべて失うよりも歯の根管治療を受ける方がいいと回答しています。

65歳以上の回答者の4分の3以上（77%）が、パスワードについて考える際にセキュリティが最も重要だと回答しており、18〜24歳の回答者の場合は66%が同様の回答をしています。

パスワードをすべて失うことは、〇〇よりも嫌！

34% デートにすっぽかされる

34% テレビを1週間見ない

19% 飛行機に乗り遅れる

17% 歯の根管治療を受ける

良好な衛生環境を維持し、パスワードの負担を減少させる

パスワードを覚えること、変更すること

調査では、回答者は平均してパスワードを年に51回忘れることがわかりました。

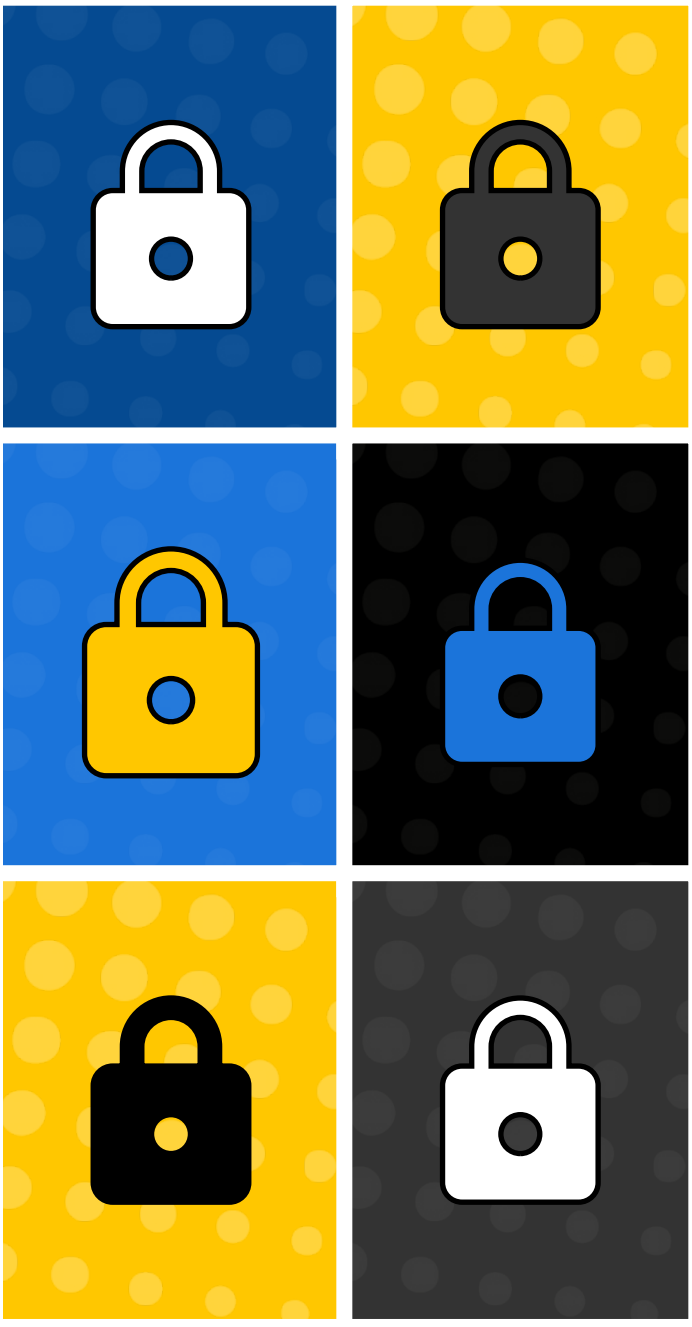
18～24歳の回答者は、パスワードを年に50回近く忘れると回答しているのに対し、65歳以上の回答者は年に62回忘れると回答しています。

平均して、調査の回答者はパスワードを年に10回変更しており、回答者の約9人に1人（11%）がパスワードを月に1回変更しています。パスワードを覚えたり変更したりすることは明らかに問題であり、セキュリティの抜け穴が広がっていることを示しています。

回答者の22%が、パスワードを「ただ覚える」と答えていますが、その結果は、忘れっぽい人たちにとって課題でした。

パスワードを覚えるために最もよく使われる方法、特に年齢の高いグループの場合は、パスワードを何かに書き留めることでした。65歳以上の回答者の半数以上（53%）が、パスワードを付箋や日記、メモ帳に書き留めていると回答しています。35～44歳の回答者の24%が同じ回答をしており、調査対象者の16%がパスワード管理ソフトウェアを使用していますが、12%はパスワードをウェブブラウザに保存することを選んでいます。

このような事例は、サイバー犯罪者が最も機密性の高いデバイスやデータにすぐにアクセスできる可能性を示すものです。



パスワードで保護されたアカウントやアプリをいくつ持っていますか？

回答者は、平均してパスワードで保護されたアカウントやアプリを20個持っていると報告しています。65歳以上の回答者は、パスワードで保護されたアカウントやアプリの数は平均して22種類だと答えています。

私たちが毎日使用するアカウントやアプリはパスワードで保護されているため、数多くのデバイスでパスワードを確実に保護することには差し迫った必要性があります

パスワードロックを使用する

多くの個人は、デバイスを全く保護していません。自分の携帯電話へのアクセスを保護するためにパスコードを使用している回答者は、わずか5人に3人（64%）です。

回答者の約半数（53%）が、パスコードを使用してコンピュータのロックを解除しています

多要素認証または二要素認証（MFA/2FA）を使用する

回答者の約6人に1人は多要素認証または二要素認証と呼ばれる2つ目のステップを使用して自分のアカウントを保護したことがありますが、使いづらかったと答えています。

同様に、回答者の5分の1（20%）が、多要素認証が難しすぎるのではないかという懸念だけで、多要素認証を使用したことがないと回答しています。

リスクを認識し、警戒する

サイバー攻撃の検知と識別

回答者の62%が、フィッシングメールを自信を持って特定できると回答しています。

回答者の60%は、実際の発信者ではない友人から送られた偽のSNSメッセージを見抜くことができると確信していました。

回答者の57%が、ポップアップをサイバー攻撃の兆候として認識することに自信があると回答していますが、18%は自信がないと答えています。

回答者の54%が、自分のオンラインパスワードが突然使えなくなったら、それはサイバー攻撃の兆候かもしれないと認識できると回答していますが、18%は見分けることに自信がないと回答しています。

ハッキングされるのを心配していますか？

回答者の約10人に7人（68%）が、万が一ハッキングされたらどうなるかを心配している一方で、非常に心配していると答えたのは3分の1（33%）にとどまり、サイバー漏洩の影響に対する軽率な態度を表しています。

回答者の3分の1近く（32%）が、自分はハッキングされる可能性が高いと考えており、12人に1人以上がハッキングされる可能性が非常に高いと答えています。これは、2020年10月から11月にかけて世界31カ国で実施された別の調査と併せたものです。その調査では、回答者の3分の1が、自分のオンラインアカウント（メールやSNS、銀行など）の少なくとも1つは翌年ハッキングされるだろうと予想していたことが明らかになりました。

62%
フィッシングメールを確実に特定できるとした回答者の割合

60%
偽のSNSメッセージを見抜く自信があるとした回答者の割合

57%
ポップアップをサイバー攻撃の兆候として特定できるとした回答者の割合

結論

私たちの調査結果は、人々がパスワードに結びつける価値と、パスワードを保護するために使用する手段との間に、憂慮すべき断絶があることを示しています。米国では、人々はパスワードを失うくらいなら歯医者に診てもらうほうが良い（それほど絶望的なもの）と言いますが、この調査では、パスワードの安全な選択や保存、管理が著しく欠けていることがわかりました。

パスワードが複数のプラットフォームで共有され、重複していることは、大きな懸念事項です。同様に、名前や誕生日など公的に入手可能なデータに依存するような、あまりにも単純なパスワードの使用を目にするのも憂慮すべきことです。これは、私たちがインターネットにアクセスするためにさまざまなデバイスやプラットフォームを引き続き使用していくため、依然として深刻な課題となります。

パスワードの保護が不十分であることによる影響は、この調査で何人もの回答者が自らサイバー攻撃の被害に遭ったことがあり、その結果として発生した金銭的な損失やSNSプロフィールの漏洩を報告していることから裏付けられています。

何よりも、このレポートは、サイバーセキュリティがそれに向き合う姿勢に左右されることを示しています。サイバー犯罪に対する意識が高いことは実証されていますが、多要素認証の回避から、サイバー漏洩の発生を知りながら対策を怠るといったことなど、サイバー犯罪に対処する策を講じるのに消極的であることが指摘されました。したがって、私たちが目にしているのは非常に無関心な状態が続いている、つまり、サイバー攻撃は日常的に発生する不便なことで、現代生活の一部だと見なされているというものです。

しかし、放っておけばサイバー犯罪は更に悪化していくでしょう。連邦捜査局による2021年インターネット犯罪レポートによると、サイバー犯罪による損失額は、米国民に対して69億ドルもの被害に達するとされています。また、FBIは、2021年に発生したサイバー犯罪のトップ2は、個人データの漏洩とフィッシング攻撃だったと報告しています。

私たちは、パスワード衛生を怠ってしまいがちですが、サイバー犯罪の脅威は常態化しています。サイバー攻撃問題を未然に防ぐことが可能な、予防に役立つシンプルなソリューションへの意識を高めることが重要です。個人データの保護は、パスワードマネージャーの導入や多要素認証の使用で簡単に実行できるのです。

Keeper Securityについて

Keeper Security, Inc.（Keeper）は、組織と個人が認証情報やシークレット、接続、および機密性の高いデジタルアセットを保護する方法を変革し、可視性と制御を向上しながら、個人情報のセキュリティに関するサイバー攻撃のリスクを大幅に削減します。Keeperは、パスワード管理、機密情報管理、特権アクセス、安全なリモートインフラストラクチャアクセスと暗号化されたメッセージングにおいて、何百万人もの人々と何千もの組織から信頼されているゼロトラストとゼロ知識のセキュリティクラウドサービスの主要なプロバイダです。

Keeperの製品は、G2、Trustpilot、PCMag、およびU.S. News & World Reportにおいて、業界で最も高い評価を受けています。過去数年間、Keeperはサイバーセキュリティ・エンタープライズソフトウェア部門で、Cyber Defense MagazineからInfoSec賞を複数回受賞しています。Keeperは、SOC 2およびISO 27001認証、FIPS 140-2検証、FedRAMPおよびStateRAMP認証を取得しています。Keeperは、900億ドルのAUMを持つ大手ベンチャーキャピタルと未公開株式投資会社であるInsight Partnersの支援を受けています。