2021年度 職場における パスワード過誤レポート

Keeper Securirty提供独占調査レポート

Pollfish

はじめに

職場におけるパスワード衛生が不十分だったことは、COVID-19が大流行する以前から組織のサイバーセキュリティへの脅威となっていました。COVID-19によって世界中の組織がリモートワークの迅速な展開と安全確保を余儀なくされると、チームはリモートで組織のリソースに接続するようになりましたが、雇用主が管理しない環境下で、多くの場合自分のデバイスを使用して行われました。

Keeper Securityが2020年にPonemon社に委託した調査「**Cybersecurity in the Remote Work Era: A Global Risk Report**（リモートワーク時代のサイバーセキュリティ：グローバルリスクレポート）」の回答者は、組織におけるパスワードセキュリティに対して深刻な懸念を表明しています。

- 回答者の60%は、過去12ヶ月間に自分の組織がサイバー攻撃を受けたと回答しています。
- これらの攻撃の50%以上は、盗まれた認証情報を利用したものでした。
- IT資産の盗難により、企業の25%が500万ドル以上の損害を被りました。

パンデミックにより、企業はリモートで働く従業員をつなげて共同作業を行い、仕事を継続させるために、多数の新しい技術を急速に展開する必要に迫られました。ZoomからGoogle Workspace、Slackに至るまで、従業員はさらに多くのオンラインアカウントにサインアップする必要がありました。そして、数多くのパスワードを管理しなければならなくなったのです。

Keeperは、企業がリモートワーク環境に移行して以来、パスワードセキュリティがどれほど変化してきたのかについて疑問に思っていました。リモートの従業員は、パスワードを保護するための簡単なベストプラクティスに従っていたのでしょうか。あるいは「パスワード疲れ」に襲われて、重大なサイバーセキュリティリスクにつながる悪習慣に陥ってしまったのでしょうか。そこで、KeeperはPollfish社と共同で「職場のパスワード過誤に関する調査」を実施しました。

Ponemon社は組織のリーダーを対象に調査を実施したのに対し、Keeperは従業員を対象に直接調査を実施し、米国のフルタイムで働く従業員1,000人にパスワード習慣についての質問をしました。調査は仕事関連のオンラインアカウントにログインする際にパスワードを使用している個人のみを対象とし、2021年2月に完了しました。

調査結果のうち最も重要な発見を以下に示します。調査の全データは5ページでも閲覧できます。

調査結果1：米国の従業員は、ログイン認証情報を安全に管理および保存していない

当社の調査によると、米国の従業員は、仕事関連のパスワードを保存し管理する際にベストプラクティスに従っていないため、雇用主に重大なサイバーセキュリティのリスクを呈していることがわかりました。

- 回答者の半数以上（57%）が仕事関連のオンラインパスワードを「付箋」に書き留めたことを認めており、3分の2（67%）はそうしたメモを紛失したことがあると告白しています。これは、会社の極秘情報が従業員の自宅に住む人物や訪問者の目に触れるところに放置されるだけではなく、組織の効率も損なわれてしまいます。付箋の紛失はパスワードの紛失を意味し、結果としてヘルプデスクチケットでパスワードをリセットすることになります。
- 回答者の62%がログイン認証情報をノートや日誌に保存しており、圧倒的多数（82%）がこのようなノートを仕事用デバイスの横もしくは近くに保管しているため、自宅の住人や訪問者がアクセスできる環境にあると回答しています。

紙とペンを使用してパスワードを管理することは、リモートワークの世界において深刻な問題となっています。リモートで働く人の大半（66%）が、オフィス勤務の時よりも自宅勤務の時の方が仕事関連のパスワードを書き留める傾向が高いと回答しています。

パスワードの管理や保存にデジタルの手法を使用している場合でも、米国の従業員によるパスワードセキュリティ対策は脆弱なものとなっています。

- 回答者の半数近く（49%）が仕事関連のパスワードをクラウド上の文書に保存していると回答しています。
- 回答者の半数以上（51%）が、現在このようなパスワードをパソコンに保存された文書に保存していると回答しています。
- 55%は、仕事関連のパスワードを携帯電話に保存していると回答しています。

暗号化されていないファイルにパスワードを保存することは非常に危険です。サイバー犯罪者はクラウドストレージやコンピューター、モバイル機器に侵入するだけで、従業員のパスワードすべてにアクセスできてしまうのです。

調査結果2：米国の従業員は脆弱で推測されやすいパスワードを作成している

強力なパスワードは、大文字と小文字、数字、特殊文字をランダムに組み合わせた文字列で構成されています。しかし、回答者の多くは、サイバー犯罪者がSNSなどで簡単に見つけることができる個人情報が含まれたパスワードを使用していることを認めています。

- 回答者の3分の1以上（37%）が、仕事関連のパスワードに雇用主の名前を使用したことがあると回答しています。
- 回答者の3分の1以上（34%）が、自分にとって大切な人の名前や誕生日を使用したことがあると回答しています。
- 回答者の3分の1近く（31%）が、自分の子供の名前や誕生日を使用したことがあると回答しています。

個人アカウントと仕事関連のアカウント間でパスワードを使い回すことは、企業にとってサイバーセキュリティの重大なリスクとなっています。回答者の44%は個人アカウントと仕事関連のアカウントでパスワードを使い回していることを認めており、53%はパスワードで保護された個人アカウントを仕事用デバイスに保存していることを認めています。

調査結果3：米国の従業員は、許可されていない相手と仕事関連のパスワードを共有している

米国の従業員の多くは、仕事関連のパスワードを共有する相手について注意を払っていません。このため、そのようなパスワードが不注意な人物や悪意のある人物の手に渡った場合、組織は侵害のリスクに晒されることになります。

- 回答者の14%は、過去1年間に仕事関連のパスワードを自分にとって大切な人や配偶者と共有したことがあると回答しています。
- 回答者の11%が、仕事関連のパスワードを家族と共有したことがあると回答しています。

データ侵害が発生しない場合でも、許可されていない人物がコンプライアンスで保護されたデータを閲覧したことが判明した場合、雇用主はコンプライアンス違反を指摘されて甚大な罰則を科される可能性があるのです。

調査結果4：米国の雇用主は、パスワードの安全な共有および許可された関係者とのみの共有を保証する対策を講じていない

当社の調査では、職場でのパスワードの共有は一般的に行われていることがわかりました。

- 回答者の半数近く（46%）が、複数のユーザーが使用するアカウントのパスワードを会社で共有していると回答しています。
- 回答者の3分の1以上（34%）が、仕事関連のパスワードを同じチームの同僚と共有したことがあると回答しています。
- 回答者の3分の1近く（32%）が、仕事関連のパスワードを上司と共有したことがあると回答しています。
- 回答者の19%が、パスワードを経営陣と共有したことがあると回答しています。

最善策は、すべてのユーザーに対し、仕事関連のアカウントやアプリケーションごとに独自のパスワードを与えることです。これは、企業向けのパスワード管理（EPM）プラットフォームを使用することで実際に可能です。パスワードを安全に共有し、許可された関係者とのみパスワードを共有するならば、職場でのパスワード共有は安全なものとなります。今回の調査結果では、米国の雇用主の多くがパスワードを安全に共有するためのリスク軽減策を実施していないことがわかりました。

- 回答者の大半（62%）が仕事関連のパスワードをSMSやメールで共有していると回答していますが、こうすることで送信中サイバー犯罪者に傍受される可能性があるのです。
- 回答者の3分の1近く（32%）が以前勤めていた会社のオンラインアカウントにアクセスしたことを認めています。これは、多くの雇用主が従業員の退職時にアカウントを無効化していないことを示すものです。

結論

企業向けKeeper パスワードマネージャーのようなパスワード管理プラットフォームを採用し導入することで、この調査で明らかになったパスワード過誤を正すことができるはずです。Keeperのゼロ知識パスワード暗号化とゼロトラストフレームワークは、高度なパスワード管理、安全な共有などのセキュリティ機能を提供します。IT管理者やリーダーは、従業員のパスワード慣行を完全に可視化し、制御することができます。これには以下のような方法が挙げられます。

- 独自のゼロ知識セキュリティモデルとゼロトラストフレームワークシステム。転送中のデータや保存データはすべて暗号化されており、Keeper Securityの従業員や外部のいかなる人物もそれを閲覧することはできません。
- あらゆるデバイスへの迅速な展開が可能で、新たな設備の設定やインストール費用は必要ありません。
- カスタマイズされたオンボーディング、および専用サポートスペシャリストによるトレーニングを24時間年中無休で提供。
- RBAC、2FA、監査、イベントレポート作成、HIPAA、DPA、FINRA、GDPRなど多数のコンプライアンス基準に対応。
- 安全な共有フォルダ、サブフォルダ、パスワードをチームにプロビジョニング。
- シングルシングルオン（SAML 2.0）認証。
- SSOが利用できない場合、オフラインでボルト(安全なデジタル保管庫)へのアクセスが可能。
- SCIMを介してボルトへの動的プロビジョニング。
- 高可用性（HA）の設定。
- 高度な二要素認証/多要素認証。
- アクティブディレクトリおよびLDP同期。
- SCIMおよびAzure ADプロビジョニング。
- パスワードローテーションとバックエンド統合のための開発者API。

調査結果

単一回答
SQ1. 現在正社員として雇用されていますか？

#	回答	回答(%)	回答数
A1	はい	100.00%	1000
A2	いいえ	0.00%	0

単一回答
SQ2. 現在、仕事関連のオンラインアカウントにログインする際にパスワードを使用していますか？

#	回答	回答 (%)	回答数
A1	はい	100.00%	1000
A2	いいえ	0.00%	0

単一回答
Q1. 現在、付箋や紙切れなどに書き留めている仕事関連のオンラインパスワードはありますか？

#	回答	回答 (%)	回答数
A1	はい	57.30%	573
A2	いいえ	42.70%	427

単一回答
Q2. 「はい」と答えた方は、その付箋や紙切れなどを紛失したことはありますか？

#	回答	回答 (%)	回答数
A1	はい	66.55%	382
A2	いいえ	33.45%	192

単一回答
Q3. 在宅勤務中に仕事関連のオンラインパスワードを書き留めることが多いですか？

#	回答	回答 (%)	回答数
A1	はい	66.00%	660
A2	いいえ	34.00%	340

単一回答
Q4. 現在、ログイン情報やパスワードをノートや日誌などに保存していますか？

#	回答	回答 (%)	回答数
A1	はい	62.10%	621
A2	いいえ	37.90%	379

単一回答
Q5. 「はい」と答えた方は、そのノートは仕事で利用するデバイスの横または近くにありますか？

#	回答	回答 (%)	回答数
A1	はい	81.79%	512
A2	いいえ	18.21%	114

単一回答
Q6. 現在、仕事関連のパスワードをクラウド上の文書に保存していますか？

#	回答	回答 (%)	回答数
A1	はい	48.90%	489
A2	いいえ	51.10%	511

単一回答
Q7. 現在、仕事関連のパスワードをコンピューターやパソコンに保存していますか？

#	回答	回答 (%)	回答数
A1	はい	50.60%	506
A2	いいえ	49.40%	494

単一回答

Q8. 現在、仕事関連のパスワードを携帯電話に保存していますか？

#	回答	回答 (%)	回答数
A1	はい	54.70%	547
A2	いいえ	45.30%	453

単一回答

Q9. 仕事関連のパスワードをSMSやメールで共有したことはありますか？

#	回答	回答 (%)	回答数
A1	はい	38.10%	381
A2	いいえ	61.90%	619

複数回答

Q10. 過去1年間に、仕事関連のパスワードを誰と共有しましたか？当てはまるものをすべて選択してください。

ⓘ 回答者の割合は、各回答の数をこの設問に対する回答者数の合計で割って計算したものです。回答の割合は、各回答数を集計された回答数の合計で割って計算したものです。

#	回答	回答者 (%)	回答 (%	回答数
A1	同じチームの同僚	34.40%	18.86%	344
A2	別部門の同僚	13.10%	7.18%	131
A3	上司	31.70%	17.38%	317
A4	経営陣	18.50%	10.14%	185
A5	元同僚	6.90%	3.78%	69
A6	自分にとって大切な人や配偶者	14.40%	7.89%	144
A7	子供	7.90%	4.33%	79
A8	他の家族	10.60%	5.81%	106
A9	仕事仲間ではない友人	4.70%	2.58%	47
A10	いずれにも該当しない	37.60%	20.61%	376
A11	その他	2.60%	1.43%	26

単一回答
Q11. 以前の職場を退職した後、その職場のオンラインアカウントにログインしたことはありますか？

#	回答	回答 (%)	回答数
A1	はい	32.40%	324
A2	いいえ	67.60%	676

単一回答
Q12. 仕事関連のアカウントで新しいパスワードを作成する際に、自分の会社名を使用したことはありますか？

#	回答	回答 (%)	回答数
A1	はい	36.70%	367
A2	いいえ	63.30%	633

単一回答
Q13. 複数のユーザーが使用するアカウントのパスワードを会社で共有していますか？

#	回答	回答 (%)	回答数
A1	はい	46.10%	461
A2	いいえ	53.90%	539

単一回答
Q14. 同僚同士で共有する仕事関連のパスワードに会社名が含まれていますか？

#	回答	回答 (%)	回答数
A1	はい	33.80%	338
A2	いいえ	47.20%	472
A3	自分には当てはまらない	19.00%	190

単一回答
Q15. 現在、個人アカウントと仕事関連のアカウントで同じパスワードを使用していますか？

#	回答	回答 (%)	回答数
A1	はい	43.70%	437
A2	いいえ	56.30%	563

単一回答
Q16. 仕事関連のパスワードの中に、自分の大切な人の名前や誕生日が含まれているものはありますか？

#	回答	回答 (%)	回答数
A1	はい	34.20%	342
A2	いいえ	65.80%	658

単一回答
Q17. 仕事関連のパスワードの中に、子供の名前や誕生日が含まれたものはありますか？

#	回答	回答 (%)	回答数
A1	はい	31.40%	314
A2	いいえ	52.00%	520
A3	子供はいない	16.60%	166

単一回答
Q18. 現在、個人アカウントと仕事関連のアカウントで同じパスワードを使用していますか？

#	回答	回答 (%)	回答数
A1	はい	20.60%	206
A2	いいえ	59.40%	594
A3	子供はいない	20.00%	200

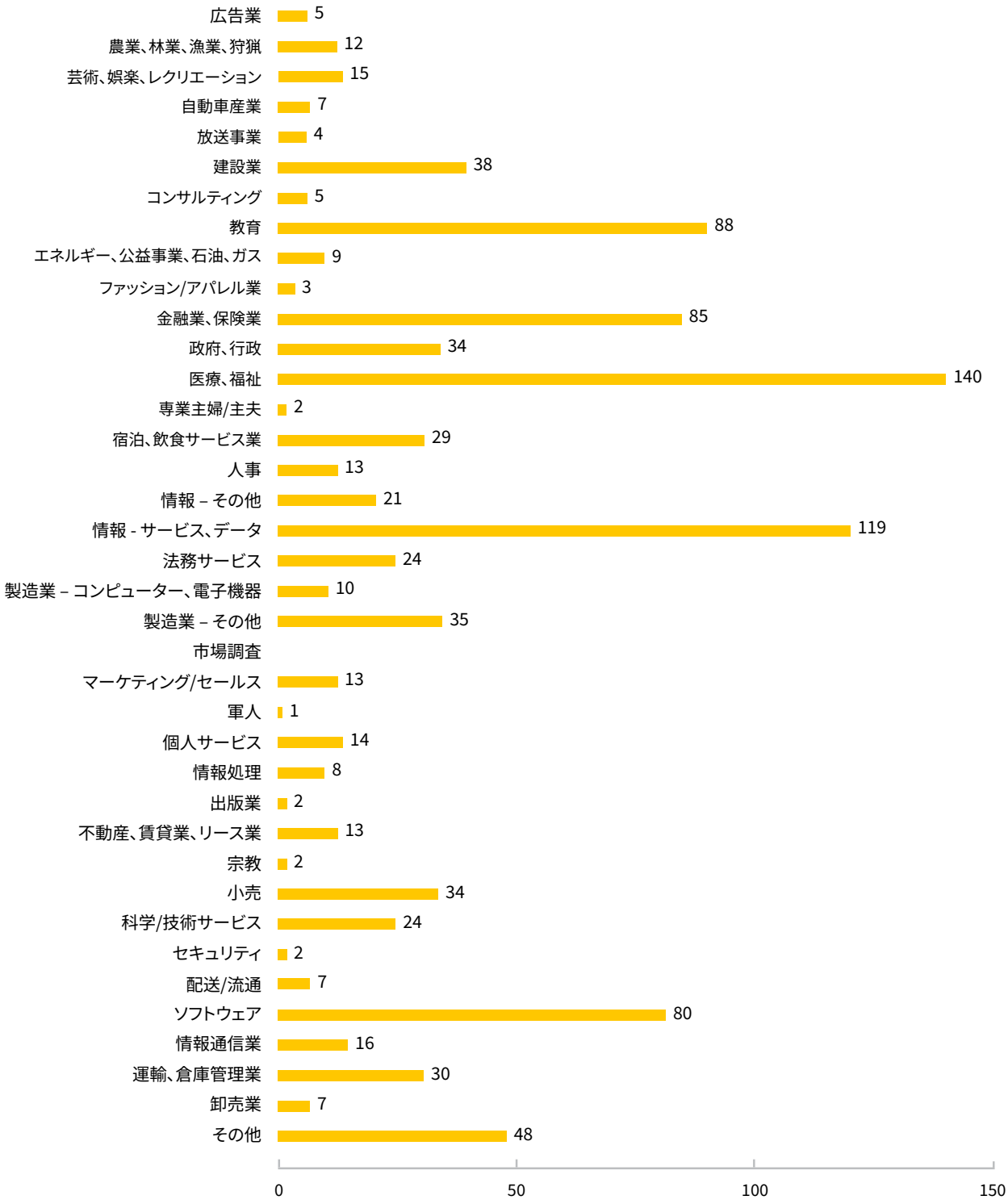
単一回答
Q15. 現在、個人アカウントと仕事関連のアカウントで同じパスワードを使用していますか？

#	回答	回答 (%)	回答数
A1	はい	53.35%	534
A2	いいえ	46.65%	467

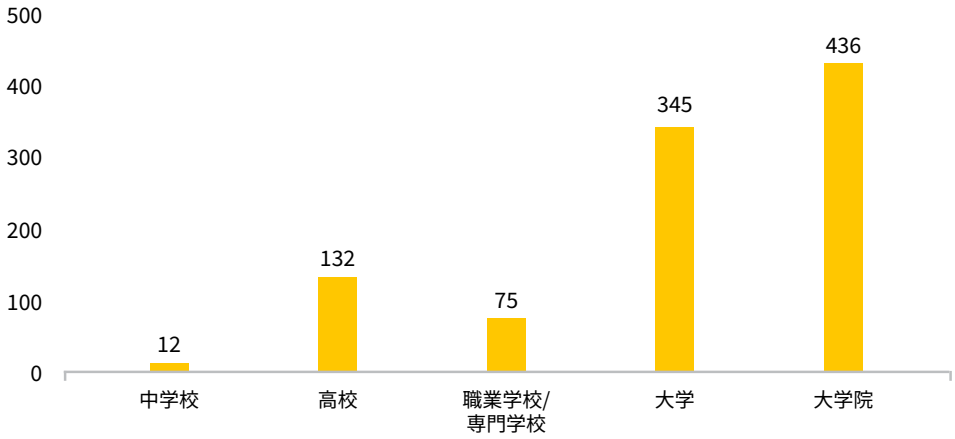
アンケート回答者の属性

サンプルサイズ 1000

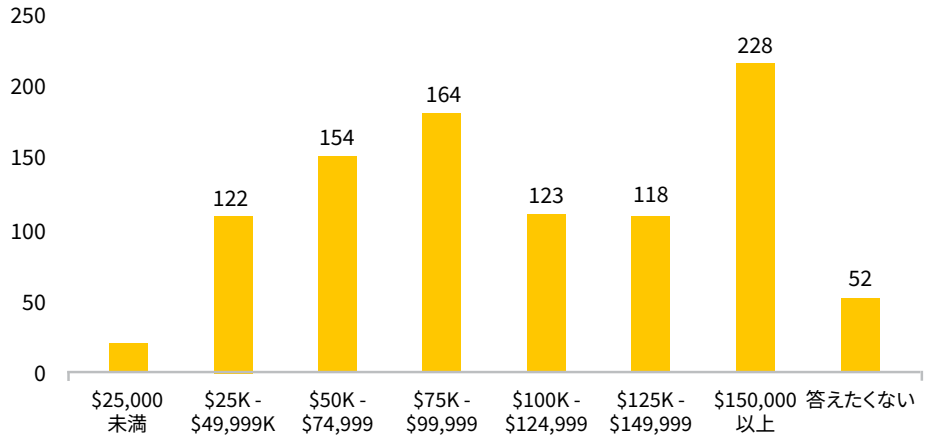
職種



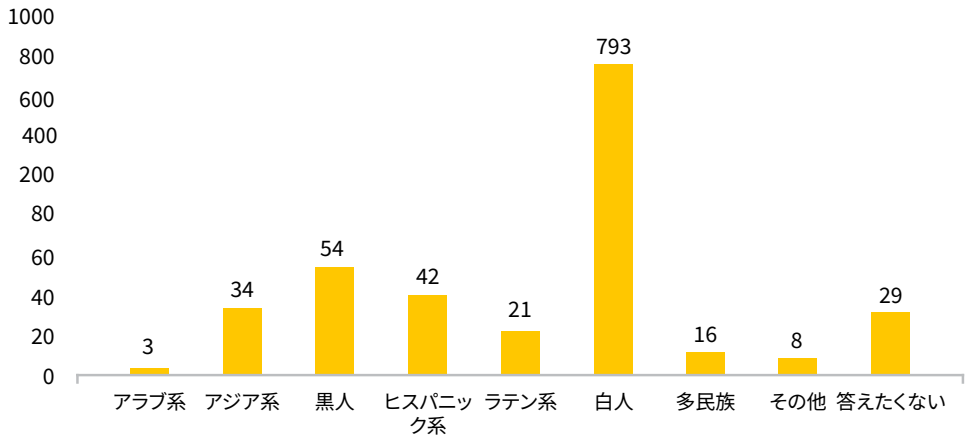
教育



収入

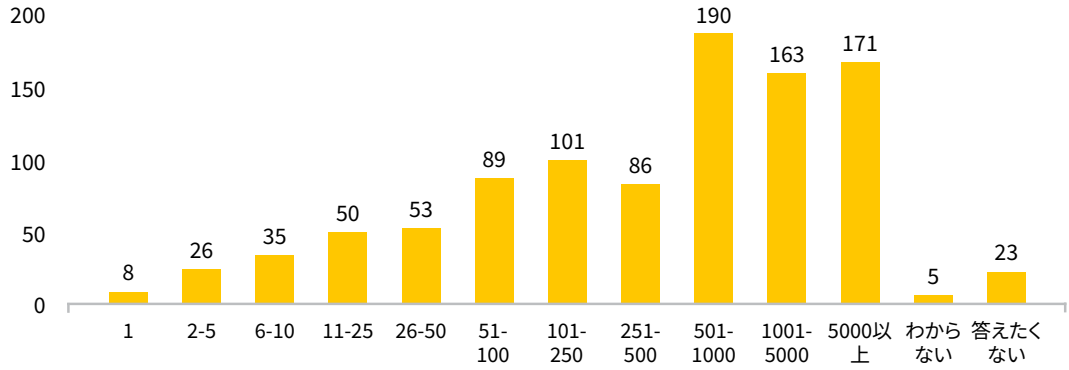


人種・民族

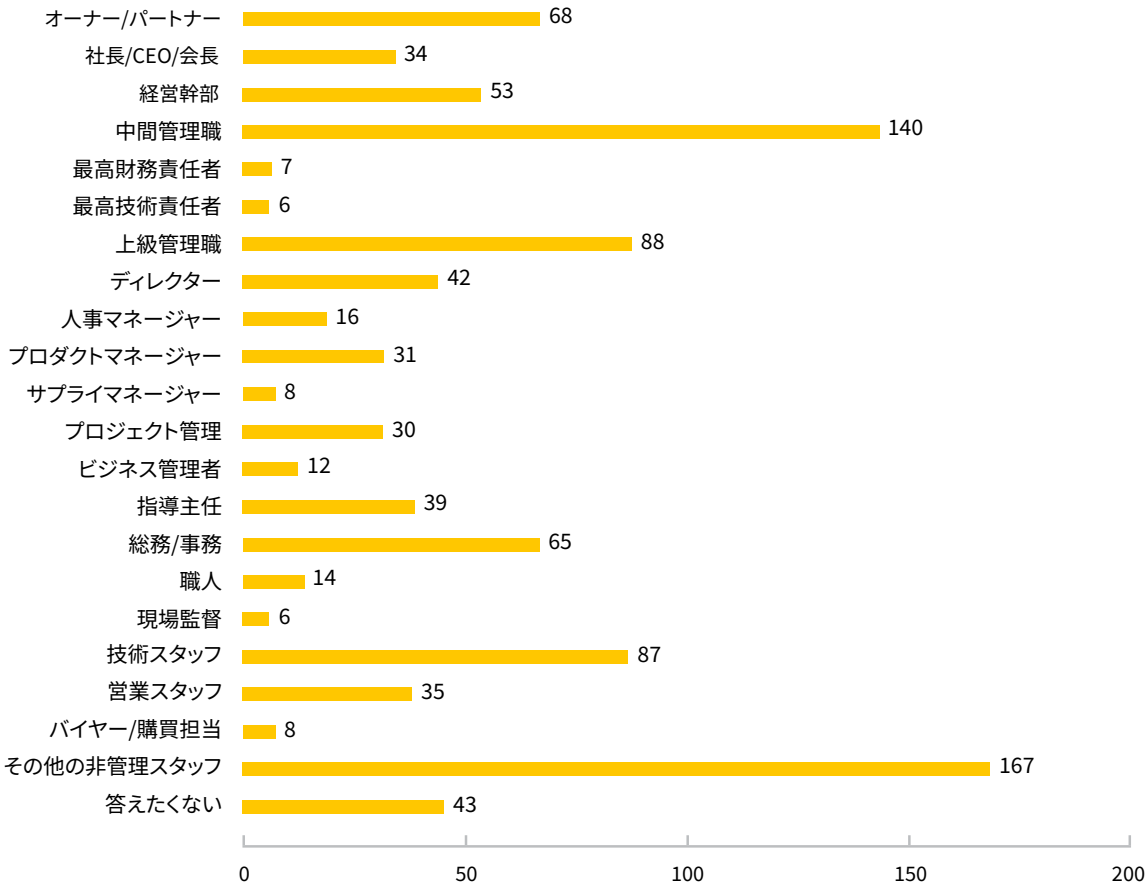


雇用状況

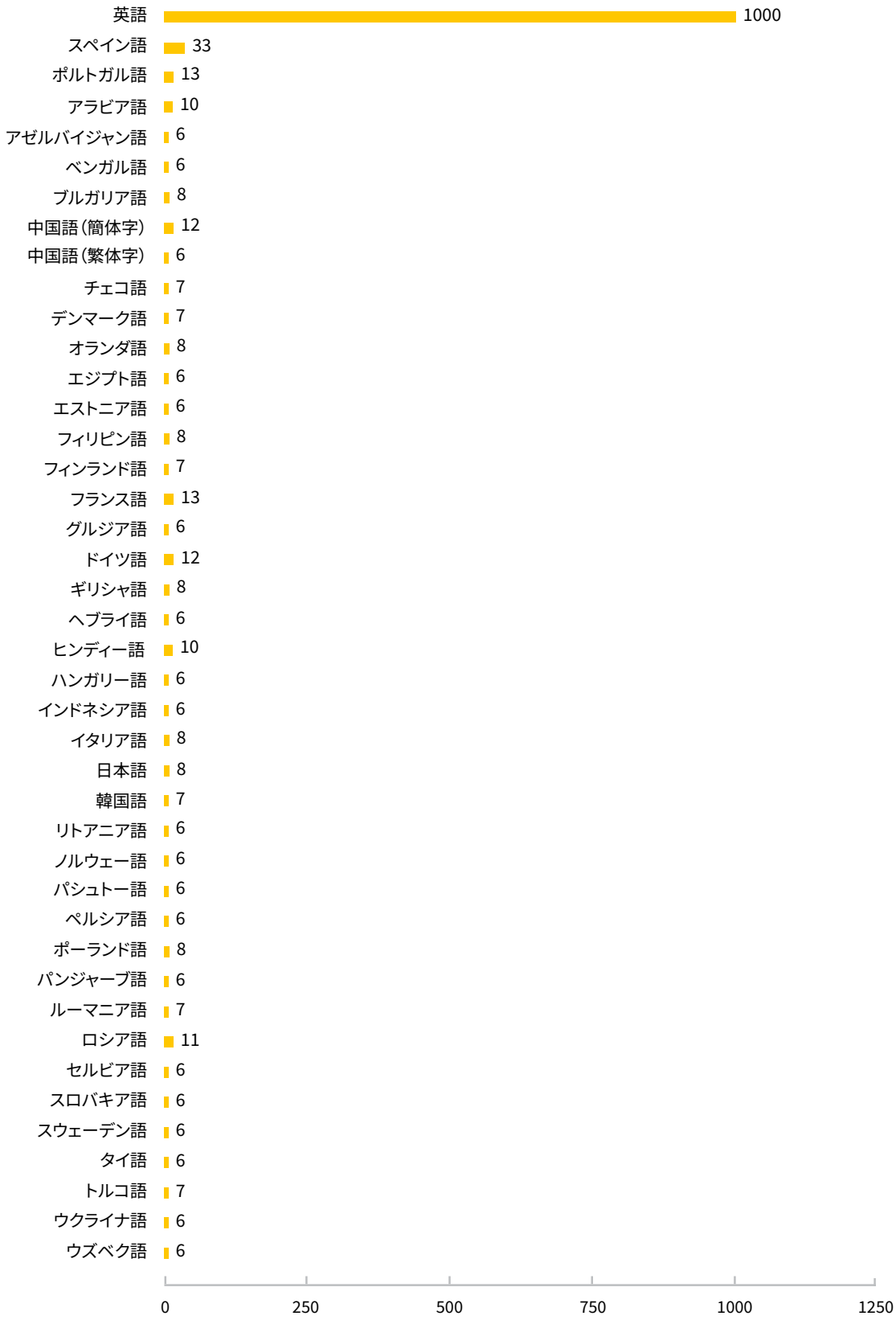
企業規模(従業員数)



社内役職


オーナー/パートナー 68
社長/CEO/会長 34
経営幹部 53
中間管理職 140
最高財務責任者 7
最高技術責任者 6
上級管理職 88
ディレクター 42
人事マネージャー 16
プロダクトマネージャー 31
サプライマネージャー 8
プロジェクト管理 30
ビジネス管理者 12
指導主任 39
総務/事務 65
職人 14
現場監督 6
技術スタッフ 87
営業スタッフ 35
バイヤー/購買担当 8
その他の非管理スタッフ 167
答えたくない 43
0
50
100
150
200

使用言語



評価および受賞

Keeperは、PCマガジンの年間最優秀パスワードマネージャー賞ならびにエディターズチョイス賞、PCWorldのエディターズチョイス賞に2年連続で選定されました。また、G2賞のベストソフトウェア部門で4賞を獲得し、中小企業向けパスワード管理および中小企業向けサイバーセキュリティのベストプロダクト部門で4つのInfoSec賞を獲得しています。KeeperはSOC-2およびISO 27001認証を取得しており、米国連邦政府による賞管理システム (SAM) 使用に指定されています。

ガートナー・ピア・インサイト
5つ星のうち4.9

スパイスワークス
5つ星のうち5

エディターズチョイス
5つ星のうち4.5

2020年度エンタープライズ・リーダー
5つ星のうち4.7

- **パブリッシャーズ・チョイス賞（サイバーセキュリティパスワード管理）**
- **年間で最も最先端を行く最高経営責任者**

- **パスワード管理部門における最優秀製品**
- **中小企業サイバーセキュリティ部門で最優秀製品**
- **パブリッシャーズ・チョイス賞（年間最高経営責任者）**
- **年間最も革新的なCTO**

年間最優秀パスワードマネージャー、2019年および2020年度エディターズチョイス

2018年および2019年度エディターズチョイス

職場でのパスワード過誤レポートやインフォグラフィックなどをダウンロードするには、専用のリソースハブをご覧ください。Keeper Securityについての詳しい情報や、パスワード関連のデータ漏洩から組織を保護する方法については、keepersecurity.com にアクセスしてください。

調査方法

Keeper SecurityはPollfishと提携し、米国内のフルタイム従業員1,000人を対象とした調査を実施しました。仕事関連のオンラインアカウントにログインする際にパスワードを使用する個人のみを対象としています。調査は2021年2月に完了しました。

Keeper Security, Inc.について

Keeper Security, Inc. (Keeper) は、パスワード関連のデータ漏洩やサイバー脅威を防ぐサイバーセキュリティプラットフォームとして高い評価を受けており、特許を取得しています。Keeperのゼロ知識セキュリティおよび暗号化ソフトウェアは、サイバー窃盗のリスクを軽減し、従業員の生産性を向上させ、コンプライアンス基準を満たすために、世界中の何百万人ものユーザーや数千もの企業から信頼されています。Keeperは、2020年にPCMagの年間最優秀パスワードマネージャー賞を獲得し、エディターズチョイスに3度目の受賞を果たしました。Keeperは、PCWorldのエディターズチョイスにも選定され、G2ベストソフトウェア賞4部門、中小企業サイバーセキュリティパスワード管理のベストプロダクト部門でInfoSec賞を獲得しています。KeeperはSOC-2およびISO 27001認証を取得しており、米国連邦政府による賞管理システム (SAM) の使用にも指定されています。