次世代のZero-Trust、Zero-Knowledge パスワード管理プラットフォームのご紹介

～サイバー攻撃脅威からの組織保護強化と
運用効率向上でITセキュリティ投資対効果の最大化を～

Keeper Security , Inc. について

- 2011年設立
  日本法人を2022年設立　APAC本社を2023年5月に開設
- IDおよびアクセス管理 (IAM)における専門家
  - 法人パスワード管理
  - 機密情報管理
  - 特権アクセス管理
- 25,000社、1800万のユーザー
  （YE 2022）
- IAM、パスワードセキュリティ、2FA、ダークウェブ保護、SSO統合を対象とする特許を保有
- 業界最高位の受賞歴とユーザー評価
- 米国、カナダ、ヨーロッパ、日本、オーストラリアにクラウドデータセンターを配備

Keeper Securityが取得した認定書

ISO 27001

SOC 2

FedRAMP

StateRAMP

HIPAA

GDPR

PCI DSS Level 1

TRUSTe

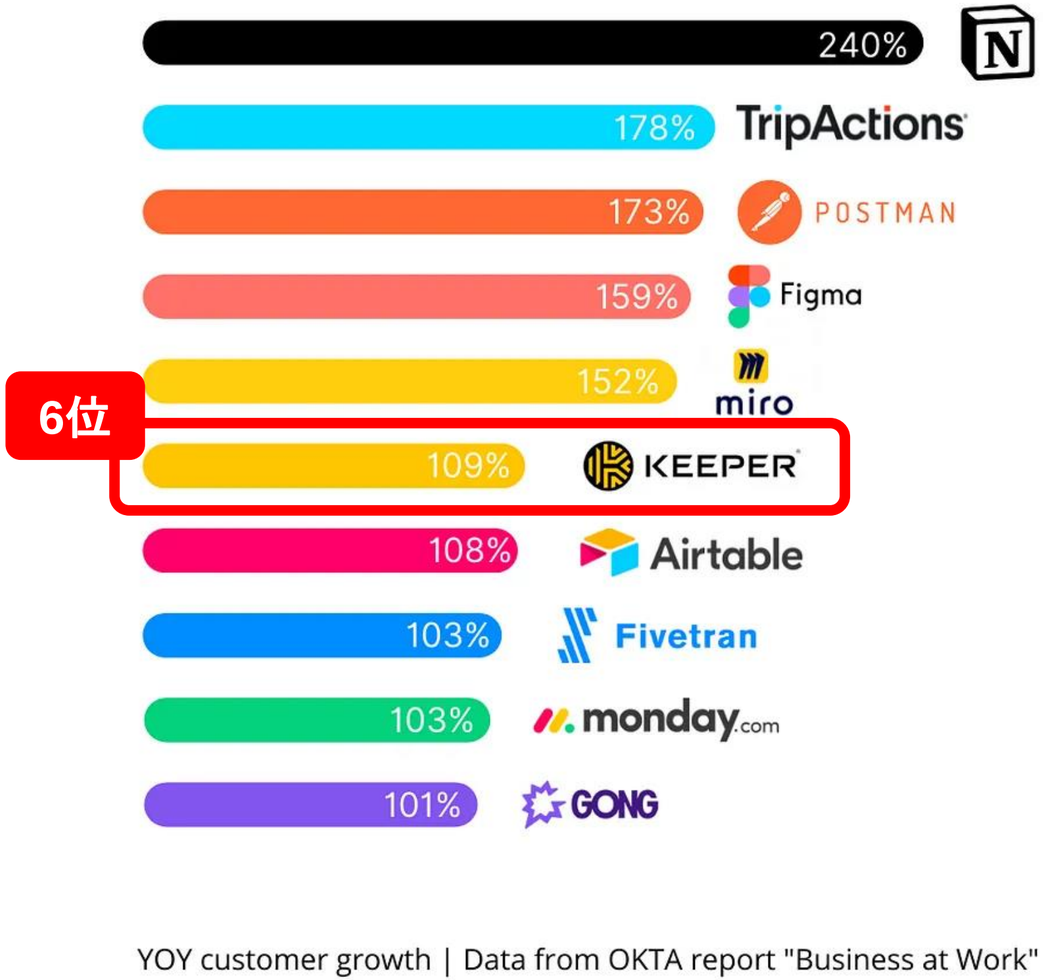
Level 1

FIPS-140-2

EU-US Privacy Shield

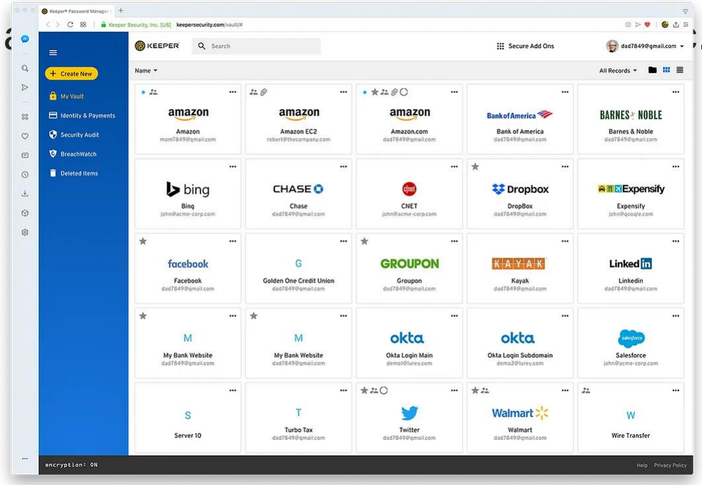
ISO27001,SOC2、FedRAMPの認定を取得しているのは、弊社だけ！！
FedRAMP：グローバルでも３５０社程しか取得できていない認定。

2022年 顧客数ベースで最も急速に成長しているアプリ



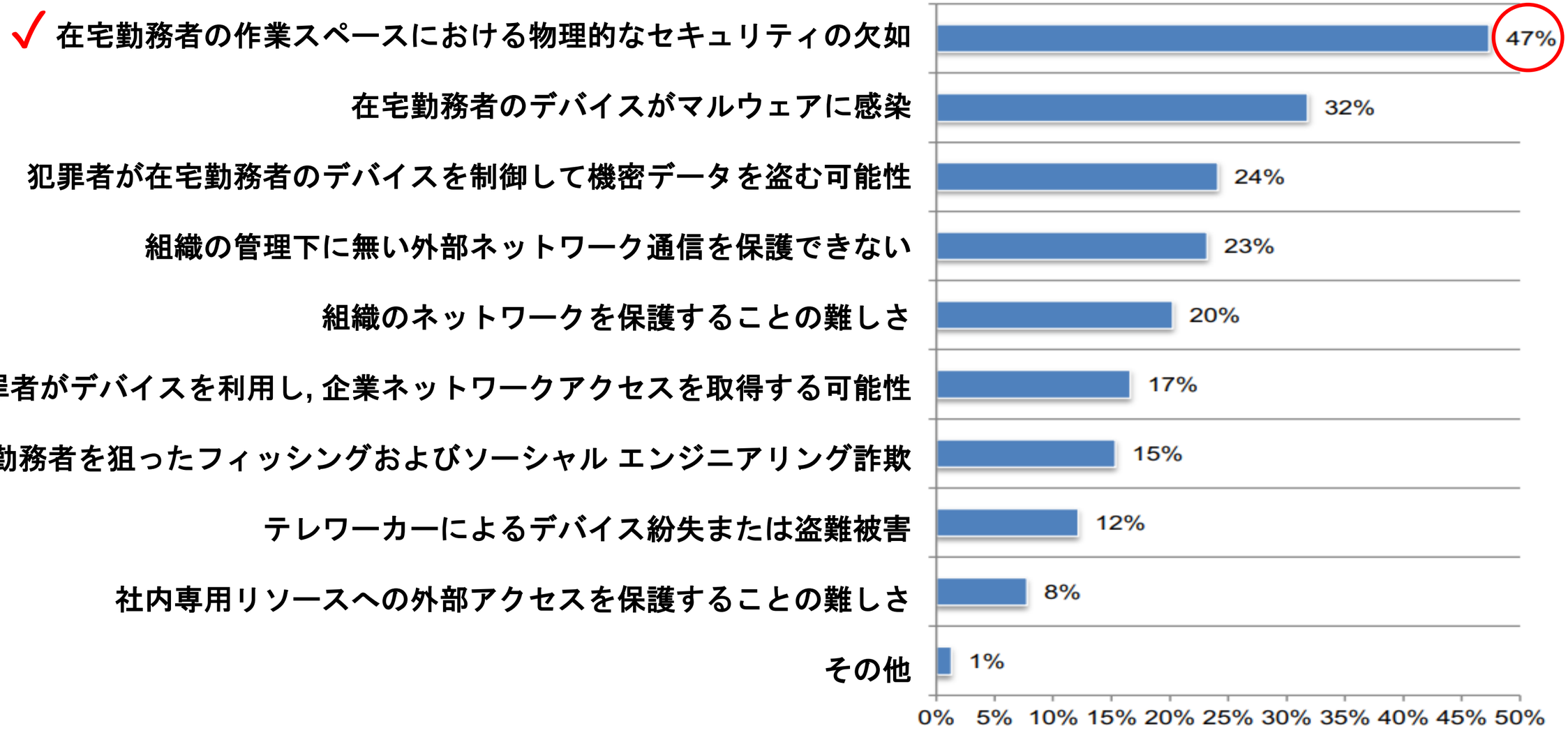
Keeper

Keeper is a suite focused on IT and data security. At its core is a password-manager where you can you safely store passwords, logins and passwords, and financial data. It also includes a password generator



セキュリティ体制とCOVID-19

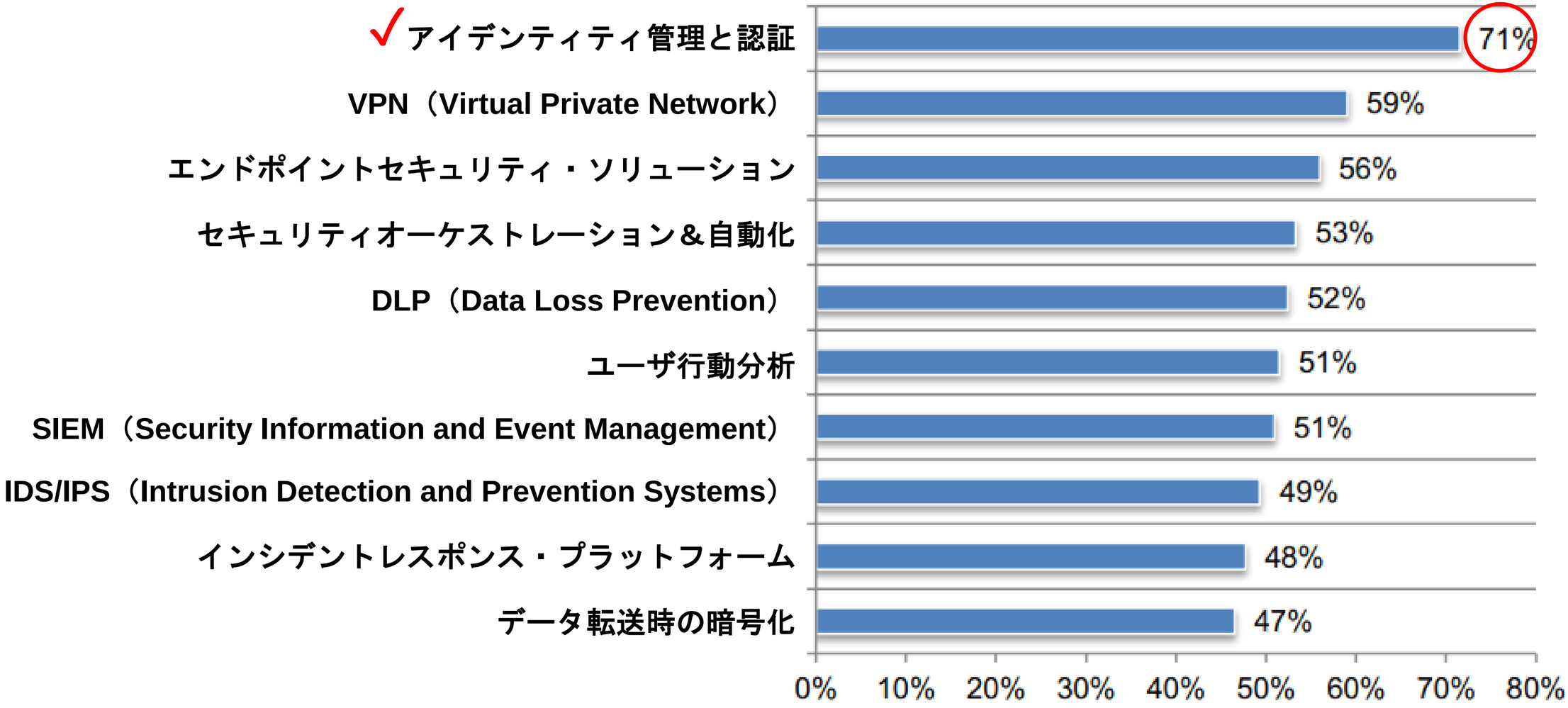
組織が最も懸念しているセキュリティ リスク



Ponemon Institute, Cybersecurity in the Remote Work Era: A Global Risk Report, October 2020

組織がサイバーセキュリティリスクを管理するために取っている, または取るべき手順

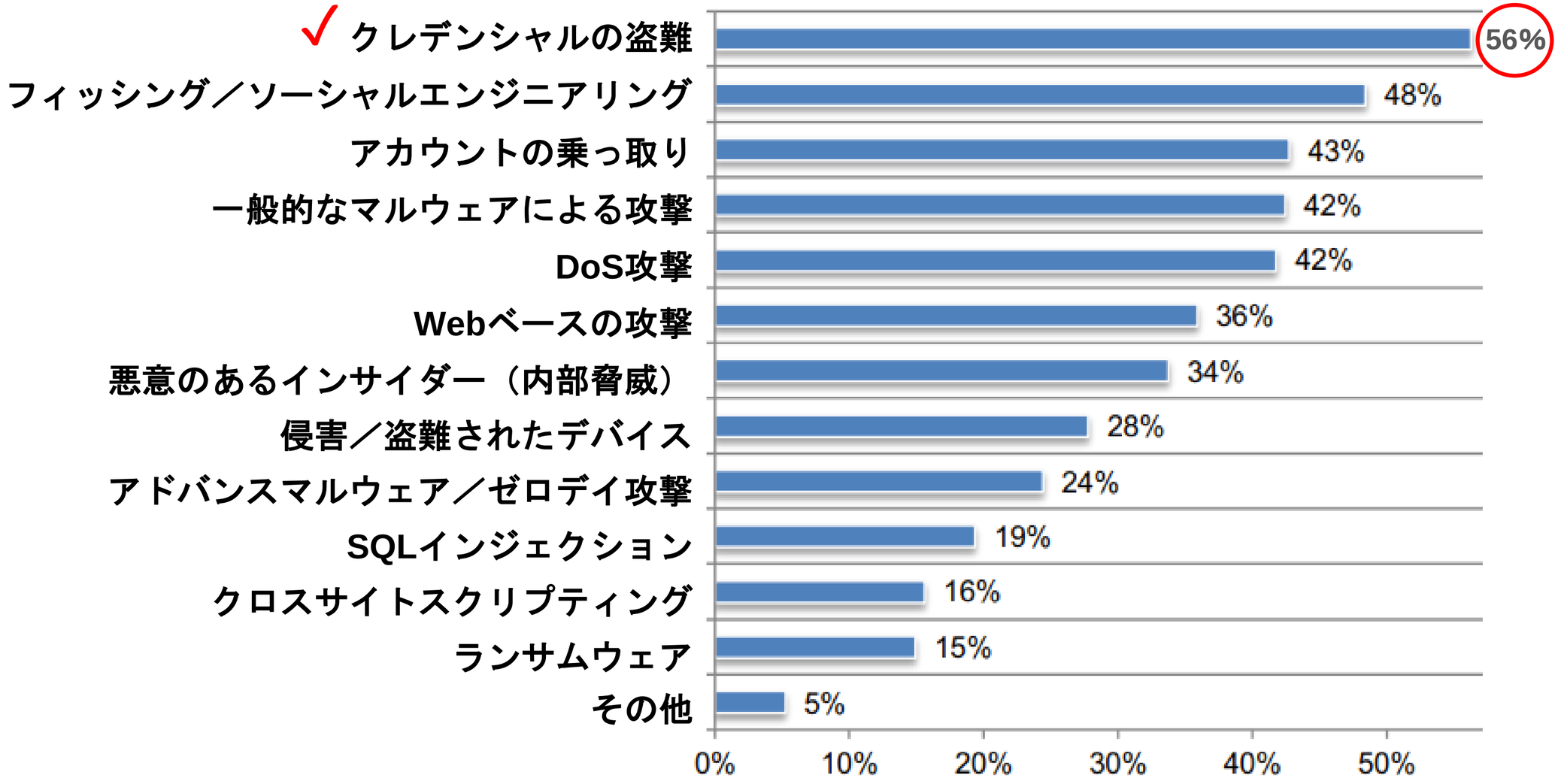
組織のサイバーセキュリティ体制を改善するトップ 10のテクノロジー



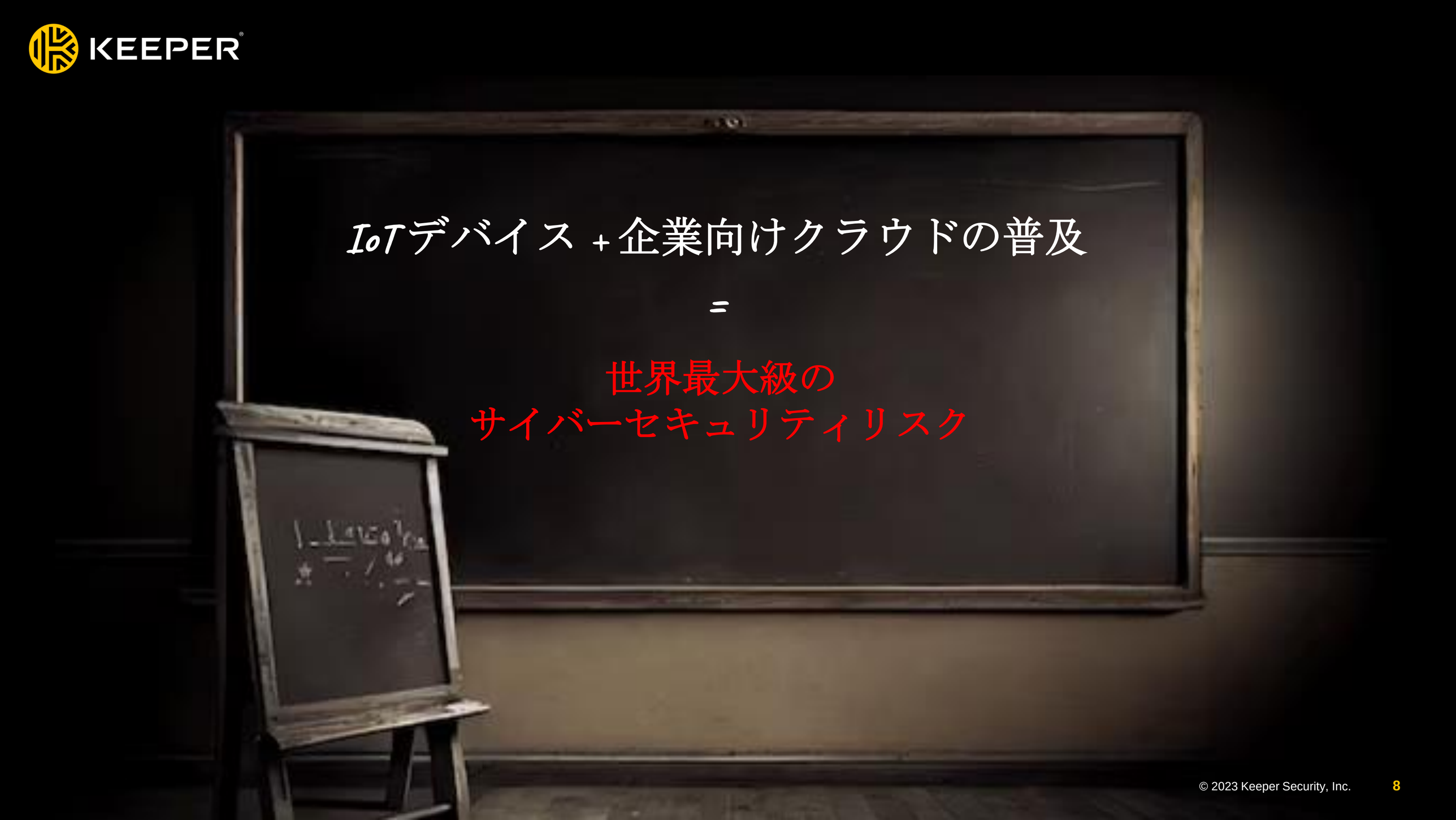
Ponemon Institute, Cybersecurity in the Remote Work Era: A Global Risk Report, October 2020

COVID-19パンデミックの経験を通したサイバーセキュリティリスク

組織が経験した攻撃の種類を最もよく表しているのはどれですか?



Ponemon Institute, Cybersecurity in the Remote Work Era: A Global Risk Report, October 2020



AWSなど40万超える企業のアカウント情報、マルウェアにより盗まれる

2023/07/27の記事

AWS、Salesforce、Hubspot、Quickbooks、Google Cloud、Okta、DocuSign の認証情報を含むログが発見

→インフォスティーラと呼ばれる種類のマルウェアは**Webブラウザ**、電子メールクライアント、インスタントメッセンジャー、暗号資産ウォレット、FTPクライアント、ゲームサービスなどのアプリケーションが保存したデータを窃取

https://news.mynavi.jp/techplus/article/20230727-2735487/

最新のセキュリティ脅威トレンド

順位	組織	前年順位
1位	ランサムウェアによる被害	1位
2位	サプライチェーンの弱点を悪用した攻撃	3位
3位	標的型攻撃による機密情報の窃取	2位
4位	内部不正による情報漏えい	5位
5位	テレワーク等の ニューノーマルな働き方を狙った攻撃	4位

※出典　独立行政法人　情報処理推進機構　https://www.ipa.go.jp/security/10threats/10threats2023.html

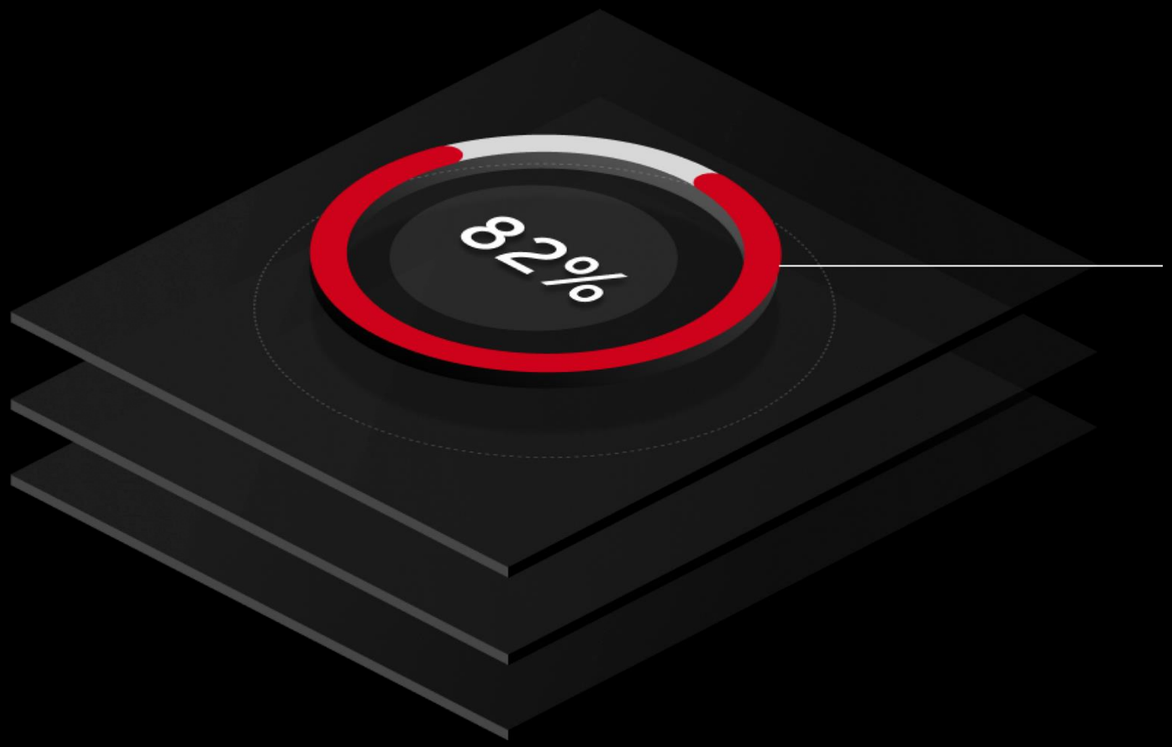
最新のセキュリティ脅威トレンド

順位	組織	前年順位
1位	ランサムウェアによる被害	1位
2位		3位
3位		2位
4位		5位
5位	テレワーク等の ニューノーマルな働き方を狙った攻撃	4位

多くの脅威はパスワードを含む
認証情報の侵害から始まります。

※出典　独立行政法人　情報処理推進機構　https://www.ipa.go.jp/security/10threats/10threats2023.html

パスワード, 認証情報の保護は,
世界で最も課題となっているサイバーセキュリティ問題です。



データ漏えいの82%は人的要因であり, 脆弱なパスワード, 認証情報, 機密情報などの盗難による被害が大部分を占めています。*

Verizon Data Breach Report 2022

数字で見る脅威と被害想定

240億以上

ダークウェブへ流出していると言われているパスワードの総数。
ハッカー（クラッカー）がいつでも悪用できる状態になっている。

出典　Digital Shadows White Paper

約3億円

日本における情報漏洩等による
セキュリティインシデントの
年間平均被害額。

出典　法人組織のセキュリティ成熟度調査 | トレンドマイクロ

約2万8千円

日本における情報漏洩した場合の
1名あたりの平均想定賠償額。

出典　JNSA インシデント損害額調査レポート

パスワードが侵害される要因

- **パスワードの使いまわし**

※日本で働く方の4割はパスワードを使いまわしているといわれています。

- **パスワードの強度が弱い**
- **メモ紙等に残してしまっている**

パスワードの管理を個人に任せることにより、

任せられた個人は”パスワード忘れ”を危惧してしまうため。

ブラウザとの比較

機能	ブラウザ	企業向けパスワードマネージャー
パスワード保管・保持	△	◉
パスワードの暗号化	○	◉
パスワード自動生成・入力	○	◉
パスワードの共有	×	◉
マルチ環境対応	×	◉
パスワードの使い回し検知	△	◉
弱いパスワードの利用検知	△	◉
パスワード漏洩検知	△	◉
シークレット管理	×	◉

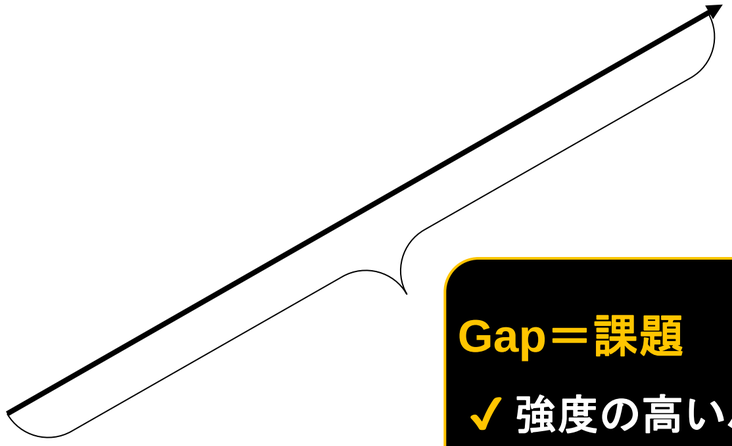
【ブラウザでのパスワード管理の注意点】

- 非ブラウザ環境下での利用ができない
- マルチブラウザ対応ができない
- パスワードの使い回しを管理者が検知することができない
- 弱いパスワードの利用を管理者が検知することができない
- パスワードの漏洩を管理者が検知することができない
- パスワードを他人に安全に共有することができない
  （共有アカウントのパスワード安全に利用できない）
- フィッシングやキーロガー、マルウェア等の攻撃にさらされる可能性が高い。（サイバー攻撃例：Cross-Site Scripting (XSS)攻撃、Cross-Site Request Forgery (CSRF) 攻撃など。）

パスワード管理における企業の課題

・システムそれぞれに、強度の高い
別々のパスワードを設定
・パスワードを安全に管理・運用

あるべき姿



・パスワードの使いまわし
・弱いパスワード
・メモ紙に残してしまう

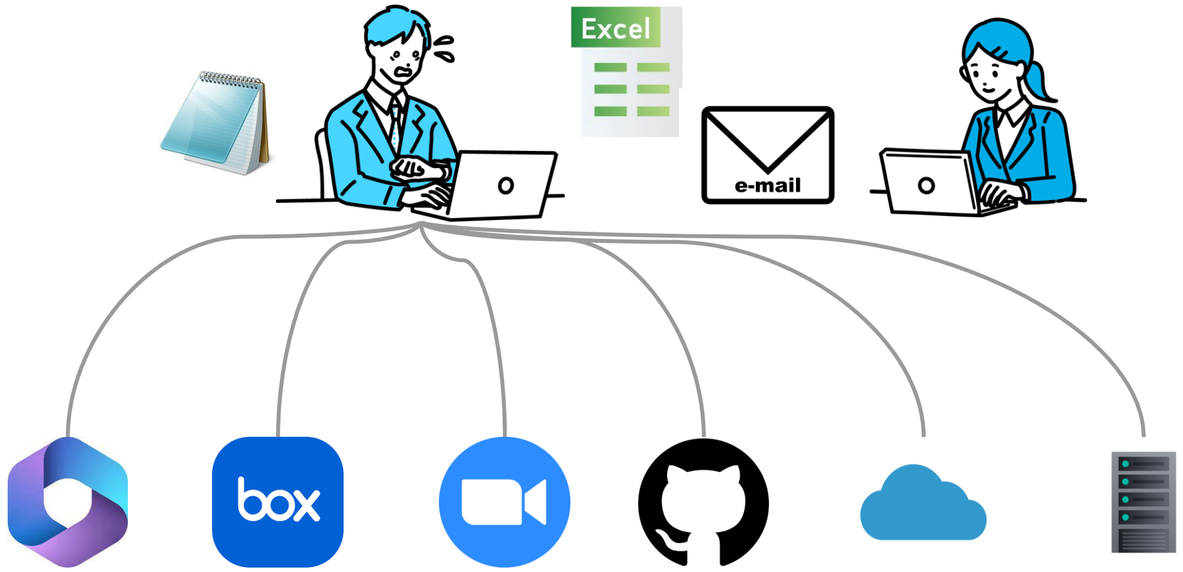
現状

Gap＝課題

✓ 強度の高いパスワードを自動で生成できるようにしたい。
✓ 安全な場所へパスワードを保管し、必要な時に
すぐに呼び出せる（使える）ようにしたい。
✓ 個人任せではなく、組織全体のパスワードの状態を
管理・監査できる仕組みづくりを行いたい。

KEEPER バリュー：利便性向上とセキュリティ対策を実現

Before



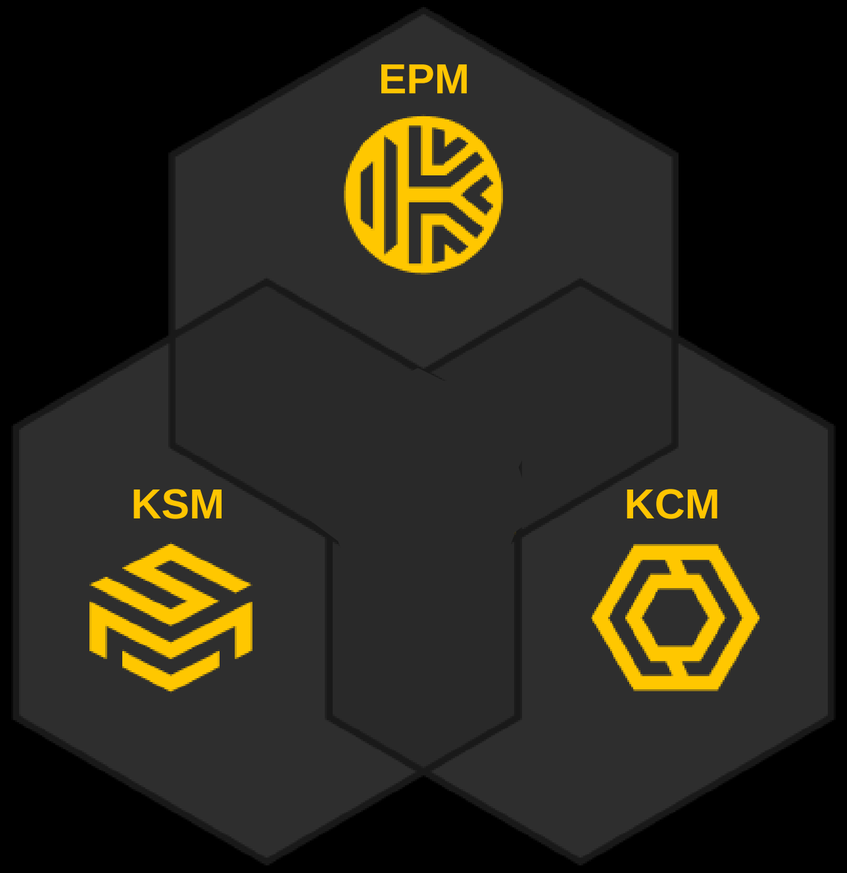
☑パスワードをメモ帳・Excelに保管している
☑パスワードをメール・チャットで送付
☑ログイン用パスワードを使いまわしている
☑漏洩しているパスワードかどうかわからない
☑パスワードを忘れてITヘルプデスクへ問合せ
☑ソースコード内にDB読出用パスワードが記載

After

☑ログイン用アカウントはすべて安全に保管
☑共有アカウントのパスワードを非表示で共有
☑パスワードの使いまわしを防止
☑漏洩しているパスワードをリアルタイムで確認
☑各種アプリ・システムへシームレスにログイン
☑ソースコード内はパスワード非表示でも運用可

Keeper 統合プラットフォームの主要コンポーネント

クレデンシャル（≒パスワード）管理を中心に、
セキュアデータ共有、セキュアアクセスを実現する統合プラットフォーム



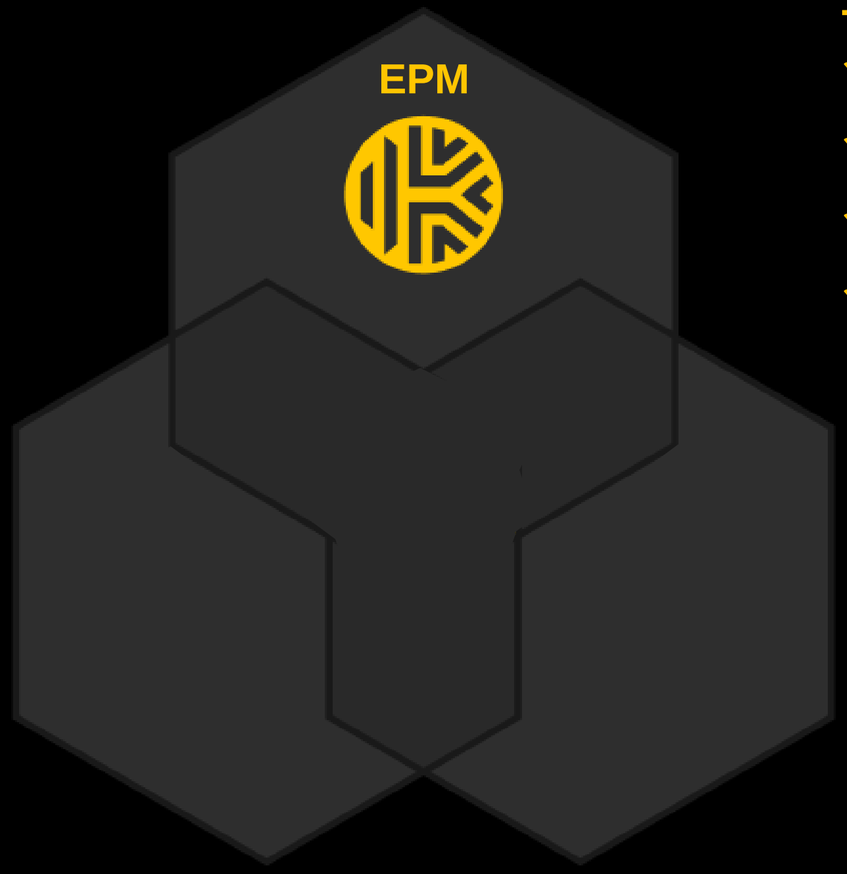
Keeper Enterprise Password Manager（EPM）
組織全体のパスワード利用状況の可視化と適切な管理、パスワード利用の効率性向上等、パスワードのライフサイクル全体を通じて、安全性と効率性を提供します。

Keeper Secrets Manager (KSM)
パスワードのみならず、APIキー、データベースクレデンシャル、アクセスキー等、様々なクレデンシャルを統合的に管理可能なプラットフォームを提供します。

Keeper Connection Manager (KCM)
エージェントレスのセキュアゲートウェイにより、安全かつ高速なリモートデスクトップ(RDP,SSH等)作業、データベースへのアクセスを実現致します。

Keeper Enterprise Password Manager（EPM）

あなた専用のパスワードコンシェルジュとして、パスワード管理に効率性と安全性を提供



こんな時にオススメ

- ✓ パスワードを覚えるのが大変
- ✓ 「パスワード忘れ」によりスムーズに業務ができなかった経験がある
- ✓ 正直、パスワードを使いまわしてしまっている
- ✓ 組織全体のパスワード利用状況が不安（脆弱なパスワード利用、漏洩有無等）

特徴

- ゼロ知識証明による保護
- マルチデバイス対応
- FIPS 140-2 対応

機能

- 安全なパスワードの自動生成
- パスワード自動入力
- パスワード共有
- パスワードの強度評価
- 生体認証、二要素認証対応
- IdP連携、シングルサインオン対応
- パスワードの漏洩モニタリング（BreachWatch）
- 全ユーザーのパスワード利用状況の確認（管理者向け）

Keeper Secrets Manager (KSM)

多種多様なクレデンシャルを効率的かつ安全に管理、利用する環境を提供

こんな時にオススメ

✓ パスワード以外の、クレデンシャル（APIキー、SSHキー、アクセストークン等）を効率的かつ安全に使いたい

✓ アプリケーション、システムにクレデンシャルを利用させたい

✓ コンフィグファイルにクレデンシャル情報を含みたくない

特徴

- ゼロ知識証明による保護
- マルチデバイス対応
- FIPS 140-2 対応

機能

- クレデンシャル共有
- ワンタイムトークンによるクレデンシャルへのアクセス管理
- クレデンシャルに対する権限管理（編集可or読取のみ）
- 全ユーザーのKSM利用状況の確認（管理者向け）

※KSMはEnterprise Password Managerの一部となります。

Keeper Connection Manager (KCM)

開発, テスト, 運用環境に, 高速かつ高い安全性のリモートアクセス環境を提供

こんな時にオススメ

- ✓ VPNアクセスが不安定で効率的に作業ができない
- ✓ 環境やOSに依存せず、安全かつ高速なリモートアクセスを実現したい
- ✓ データベースへのアクセス状況を可視化し、管理したい
- ✓ リモートアクセスの際、ID基盤と連携して認証をしたい

特徴

- 非OS依存（ブラウザ動作）
- 高速アクセス
- シンプルなアクセス管理
- オンプレ、クラウド対応

機能

- RDP、SSH、VNC、K8 プロトコル対応
- MySQL、PostgreSQL、SQL Server プロトコル対応
- セッションレコーディング
- 特権セッション管理
- マルチユーザー セッション共有
- 役割ベースのアクセス制御、二要素認証対応
- SSO、OpenID Connect、Active Directory、LDAP 連携

クレデンシャル（≒パスワード）管理の主な課題

効率性

Excelやメモ紙によるパスワード管理　サービス/システムを利用する際、多くのパスワードを記憶、管理する必要がある

パスワードを都度入力する作業　サービス/システムを利用する度にパスワードを入力する行為は業務効率を低下させている可能性がある

パスワード忘れ等への対応

ある調査*ではIT担当部門への問合せの20~50%がパスワード忘れ/リセット依頼となっており多くの工数が割かれている

安全性

ハッカーによるクレデンシャルの悪用

多くのサイバー攻撃で、パスワード等のクレデンシャルが悪用されており、サイバー攻撃における常套手段となっている

脆弱なパスワード, 使いまわし

脆弱なパスワード使用、使いまわし行為は、サイバー攻撃成功のハードルを大幅に下げ、セキュリティリスクを上げる

ソーシャルエンジニアリングと不正アクセス

ランサムウェアグループ等、多くのハッカーがメールやSNSを活用し、不正にパスワード等のクレデンシャルを入手することで、サイバー攻撃を成功させている。また、自社だけでなく、サプライチェーンリスクやSaaS側設備からの漏洩対策考慮も必要

*リサーチ会社：ガートナー社による調査

Keeper Security による問題解決

ビジネスの最適化

パスワードは「覚えないもの」へ
パスワード等、様々なクレデンシャルはKeeper Vaultで管理/保管されるためパスワードを覚える必要がなくなります

「パスワード手入力」からの卒業
KeeperFillの自動入力により、ログイン時に複雑なパスワードやID, その他必要情報自体を入力する手間がなくなります

「忘れるパスワード」は無くなります
パスワードを覚える必要がないため、忘れるパスワードそのものが存在しません

サイバー攻撃からの脅威削減

ダークウェブモニタリング
あなたのパスワードがダークウェブ(闇サイト等)に漏洩していないかBreachWatchがリアルタイムに監視。万一、漏洩が確認された際は即時アラート

組織全体のパスワード強度評価
Keeper管理者コンソールで、組織全体のパスワード利用状況を確認可能。弱いパスワードの利用、使いまわしの等の状況を可視化

多層暗号化システム＆フィッシング対策の強化
パスワード管理/保管/入力が機械化されるため、従業員が誤って、なりすましサイト等にID/PWを入力してしまうリスクを低減。サードパーティ設備からの万が一の情報漏洩時でも暗号化技術により解読を不可能に。

Thank You