Keeper Security APAC株式会社
トークセッションパネル

Keeper Security APAC 株式会社
アジアパシフィック地域　営業統括本部
統括本部長
黒田　和国

KEEPER

ユーザーボルトでのご利用

パスワードは、
覚える必要はありません！！

１）強固なパスワードを自動生成も可能
２）「記録」でパスワード群を管理
３）ID、パスワードの自動入力
（ブラウザの拡張機能keeper Fill)
４）デスクトップアプリ、webブラウザ、keeper fill、モバイル対応など、複数デバイス、プラットフォームで対応。

管理コンソールでのご利用

今すぐに！
組織全体の可視化と制御が可能！！

１）管理者がユーザーに対して強制policyなどを設定できる。
２）SSOとの連携可能
３）組織毎にロール権限やフォルダ共有が可能。（ユーザー、ロール、チームのツリー構造管理が可能）
４）プロビジョニングが可能。

効率性

安全性

１）漏洩パスワードの可視化
２）脆弱なパスワードの可視化
３）生成されたパスワードは暗号化されている。
４）ゼロナレッジ→ユーザーだけが暗号化、複合化が可能。
５）二要素認証の設定が可能。

１）従業員の漏洩パスワードの有無を可視化
２）従業員の脆弱なパスワードの有無を可視化
３）レポート&アラートの設定が可能。
４）社内報告用に、コンプライアンスレポート機能も充実。
５）SSO Connect によるSAML2.0の連携が可能。

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/

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。）

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

KEEPER

Thank you!!!