

退職者が情報を持ち出し!?

名前	更新日時	更新者
総務課	2024/8/5	安部 献子
情報システム関連	2024/8/28	関 貢人
安部課長のひみつ	2024/8/21	安部 献子
新商品開発PJ	2024/8/30	退職 太郎
新商品開発リリース計画.xlsx	2024/8/30	退職 太郎
従業員名簿_コピー.xlsx	2024/8/30	退職 太郎
【重要】予算関連.xlsx	2024/8/30	退職 太郎
社外秘_新素材サンプル.png	2024/8/30	退職 太郎
社外秘_研究室.png	2024/8/30	退職 太郎



アカウントの削除申請はきちんとしたはずなのに
なぜ退職者がアクセスできてしまったのか？

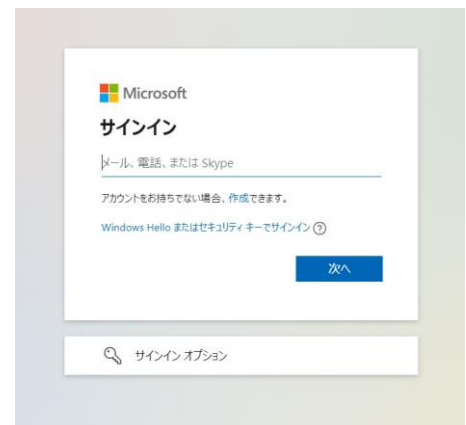
例えば

退職後 1 ヶ月経過でアカウントを削除する運用だと・・・



退職した人の個人フォルダーにある
ファイルやメールの履歴が必要になる
かもしれないし、管理職としては暫く
残しておいて欲しいわ。

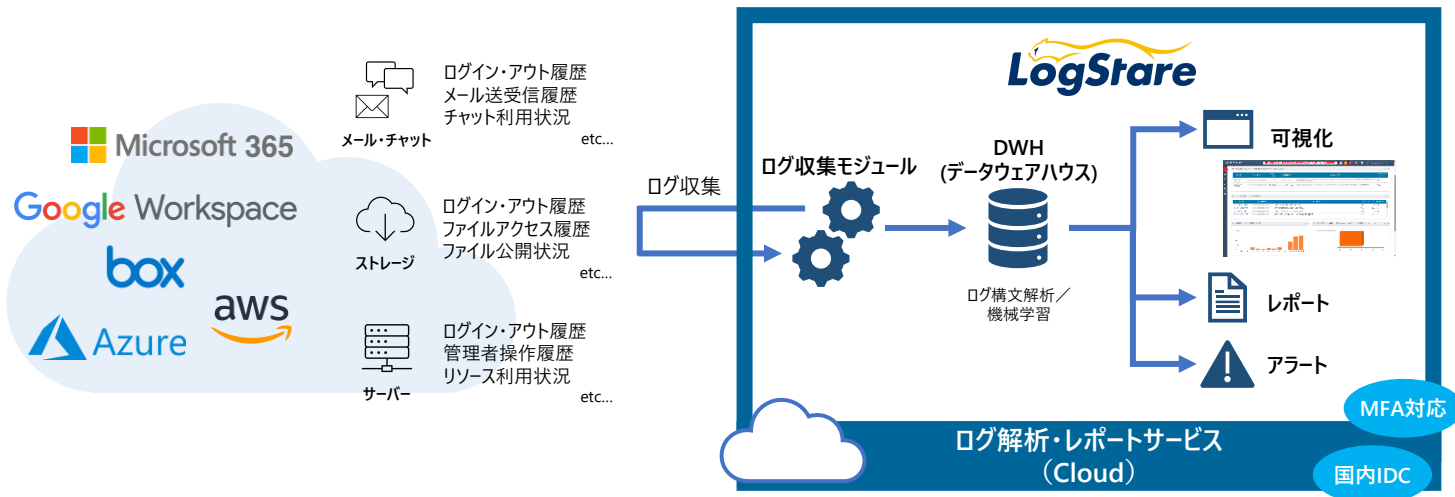
クラウドサービスは世界中のどこから
でもブラウザ経由で簡単にログインで
きてしまいます。
退職者のアカウントをそのまま残して
おくと悪用されるリスクが！



LogStareなら
誰がどのファイルにアクセスしたか分かります

クラウドサービスのログを可視化してリスクを把握

LogStare（ログステア）は、Microsoft 365やBoxなど様々なクラウドサービスのログをクラウド to クラウドで収集し、ユーザーの利用実態の可視化やセキュリティリスクの発見に役立てることができるセキュリティ運用ソフトです。



CHECK!

不正アクセスの予兆を発見

世界中の攻撃者がログイン試行できるクラウドツールは特に注意が必要。LogStareは日々のログイン状況を可視化し不審なログインを発見できます。万が一侵入されていた場合の被害範囲（アクセスされたデータ）の特定も簡単です。



CHECK!

情報流出の可能性を発見

クラウドストレージからファイルを過剰にダウンロードしているユーザーは外部に情報を持ち出している可能性があります。ユーザーごとの日々のダウンロード状況を可視化すれば不審な動きが一目瞭然。さらにログを追跡すれば、どのファイルがどこでダウンロードされたか特定できます。

