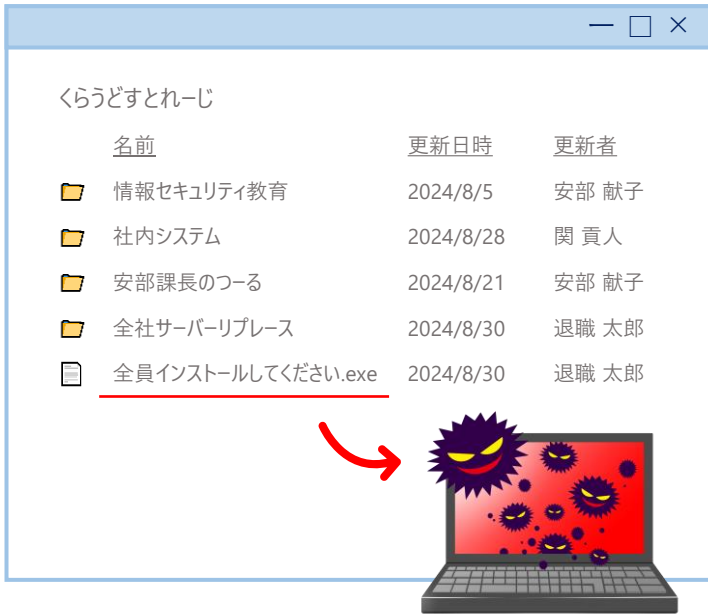


クラウドストレージのファイルが原因で・・・

# 社内がランサムウェア感染 !!



セキュリティツールでは検知されなかった!?  
なぜファイルサーバーにマルウェアがあったのか

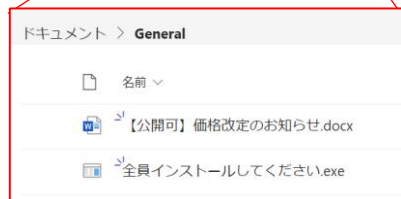
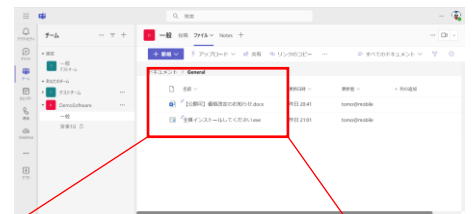
例えば

攻撃者が従業員のアカウントを不正利用したかも・・・



情シスのフォルダーに社員の名前で保存してあったからセキュリティパッチだと思ったわ！  
マルウェアと気づかずインストールしてしまう人がいるかもしれないわね。

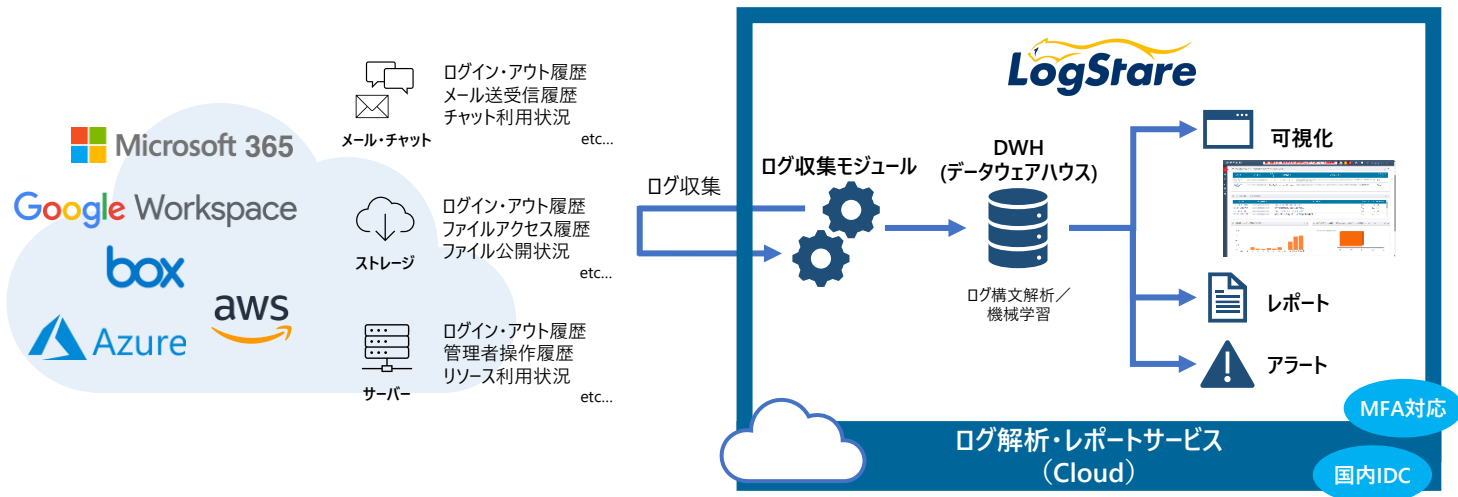
正規のアカウントでログインしているのでセキュリティツールでの検知が難しく、発見が遅くなってしまう。  
対策を強化しないと・・・



LogStareなら  
不審なログインとその後の行動がわかります

## 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。

