FileAudit

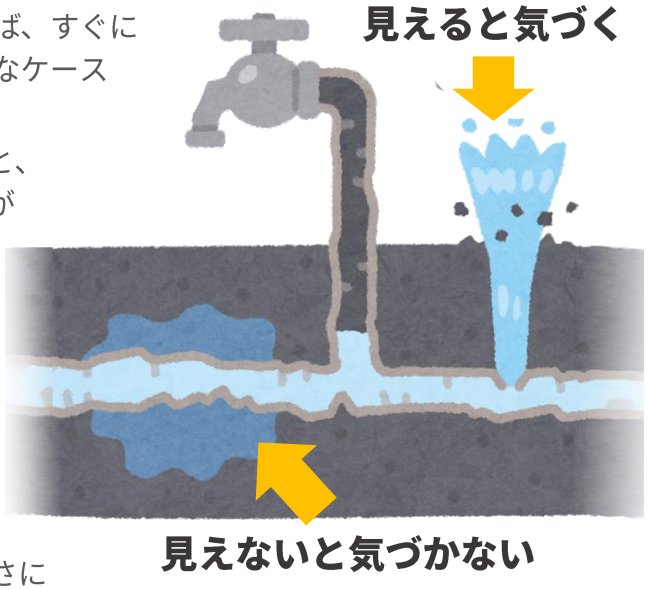
内部不正やなりすましには「異常検知」が重要

水漏れとデータ漏えい

例えば、水道管からの“水漏れ”は、見える箇所で浸水被害があれば、すぐに気づけますが、見えない箇所で少量の水がじわじわ染み出すようなケースだと分からないことが多いそうです。

この水漏れを、企業や組織におけるデータ漏えいに置き換えると、マルウェアやランサムウェア、インターネット上などにデータが流出した場合、被害が確認できるため、インシデントにいち早く気づけるかもしれません。

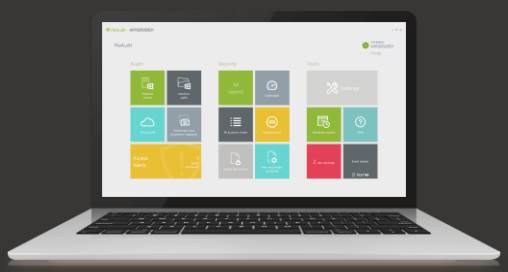
しかし、内部不正やなりすましによる被害は、正規ユーザーのアクセスと変わらないため、インシデントに気づくことが難しく、数年単位でようやく被害に気づくということも珍しくありません。しかも、最新の調査では情報漏えいのルートとして最も多いのが中途退職者による**内部不正**なのです。



水漏れでもデータ漏えいでも被害の大きさは放置された期間の長さに比例します。水漏れ対策で**「湿度センサー」**や**「漏水センサー」**を設置するように、データ漏えいには**「ファイルアクセス管理」**や**「ログ管理」**がポイントです。

「ファイル監査」や「ログ管理」だけでなく、「異常検知アラート」も実現

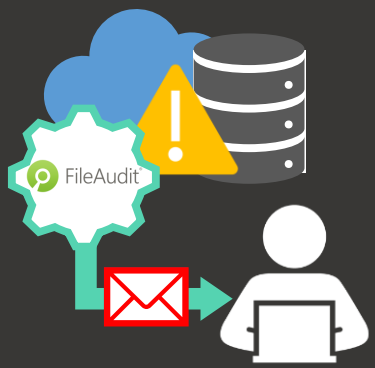
水漏れ対策の「湿度センサー」や「漏水センサー」のような役目を、機密ファイルなどのデジタルデータに対して行ってくれるのが**ファイル監査・セキュリティ強化ツール「FileAudit」**です。



シンプルかつエージェントレスで、手間と時間をかけずに導入が可能、オンプレのファイルサーバーだけでなく、クラウドストレージにも対応し、一元的なファイル監査/ログ管理を実現します。

しかも、FileAuditはログとデータだけの一般的な監査ツールではありません。不正アクセスなどのデータ侵害から大切な情報を守るさまざまな機能を搭載しています。

自社のセキュリティポリシーに沿わないアクティビティ、疑わしいアクセス方法などを管理画面で設定することで、例えば、大量のファイル削除や書き換え、深夜帯などの時間外アクセス、特定のIPアドレスやアカウントからのアクセスなど、不審なアクセスやアクティビティを検知するとメールでアラート通知します。さらにスクリプトによるアラート後の自動一次対応（アクセス遮断など）の実行も設定可能です。



ファイルとフォルダへの異常検知アラートとは

リアルタイムで検知

シングルアクセスイベント

ファイルの削除、アクセスの拒否、特定のユーザー、端末、IPアドレスからのイベントに対してリアルタイムでの異常検知、自動化された一次対応を可能にします。

マスアクセスイベント

同じユーザーによって実行されるアクセスイベントの頻度を監視、ファイルの一括コピー、ファイルの一括削除または移動等に対してアラートのしきい値を設定することが可能です。

アラートは次のような基準に基づいてカスタマイズが可能です

- ファイルとフォルダ
- ユーザーとグループ
- アクセスとオブジェクトタイプ
- アクセス時間
- アクセス頻度
- 端末名とIPアドレス
- プロセス名
- 受信者

クラウドデータへの異常検知アラート

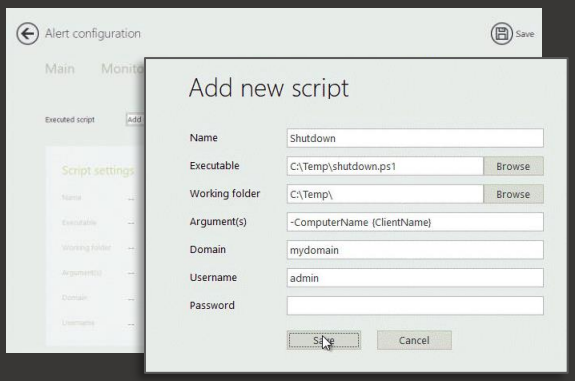
FileAuditは主要なクラウドプラットフォームに対応しており、クラウドストレージ内のファイルとフォルダへのすべてのアクセスに関する監査、レポートを行うことができます。また不審なアクティビティによるアラート機能はクラウドストレージにも適用されます。

対応クラウドストレージ

OneDrive / SharePoint Online /Box
Google Drive / Dropbox Business

異常検知アラートに対する自動対応

リアルタイム監視と異常検知アラートに加えて、FileAuditはアラートに対して設定していたアクションを自動的に実行でき、管理者の介入を待たずに一次対応をとることが可能です。特定のアラートがトリガーされると、カスタマイズしたスクリプトを実行します。マシンのシャットダウンや、ユーザーのログオフ等を実行できるため、損害が発生する前に、潜在的な脅威に対処が可能です。



OCEANBRIDGE

株式会社オーシャンブリッジ

〒107-0051 東京都港区元赤坂1-5-12 住友不動産元赤坂ビル7F
https://www.isdecisions.jp/
fileaudit@oceanbridge.jp