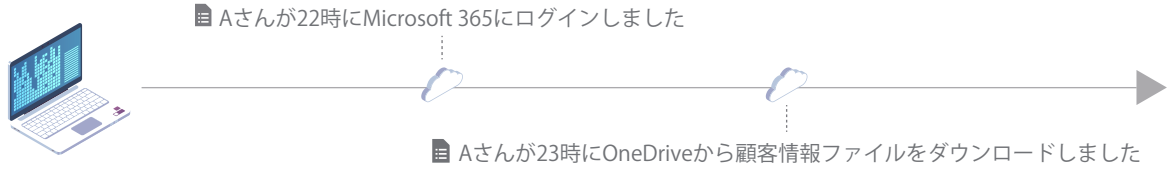
企業活動のあらゆるログを統合管理

Logstorage

ログってなに？

ログはサーバやネットワーク機器、クラウドなどシステムの稼働状況や操作履歴を記録したものです。

Microsoft 365ログイメージ



ログには「いつ、だれが、どうした」などを示す情報が含まれています。
ログを確認することで、情報システムの状況を把握できます。

PC操作ログ

AさんがX時にファイルにアクセスしました
AさんがY時にファイルを印刷しました

▶ ⚠ エンジニアのAさんが
セールスチームの顧客名簿を印刷している。
もしかして、個人情報を持ちだしている？

ネットワーク通信ログ（F/W）

X時に外部からの通信を遮断しました
Y時に外部からの通信を遮断しました

▶ ⚠ ある時間帯で100件も
外部からの通信を遮断している。
もしかして攻撃されている？

サーバログ

Cさんが22時にログイン失敗しました
Cさんが23時にログイン失敗しました

▶ ⚠ 深夜帯に大量にログイン失敗している。
もしかして、不正アクセス？

ログを活用することで、多様なセキュリティ課題を解決

ログはコンプライアンス対応、脅威対策、システム運用に活用されています。

コンプライアンス

各種法令、業界／団体ガイドラインの準拠

- PCI DSS
- ISMS（ISO27001）
- 医療情報システムの安全管理に関するガイドライン
- 自工会/部工会・サイバーセキュリティガイドライン
- 金融機関等コンピュータシステムの安全対策基準・解説書
- 地方公共団体における情報セキュリティポリシーに関するガイドライン
- 重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針

…他多数

共通で書かれている

ログを
1. 収集
2. 整理・安全保管
3. 定期監視・分析
しなさい

脅威対策

脅威の検出（標的型攻撃／内部情報漏えい）
フォレンジック（攻撃を受けた際の証拠保全）

システム運用

システムの状態把握
障害時の調査、解析

取得に時間がかかる。すぐに消える。読めない。

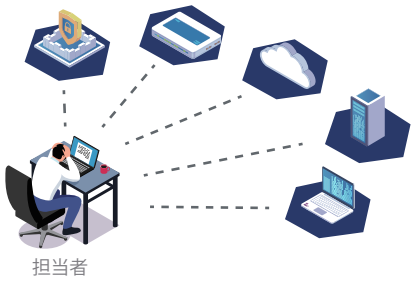
ログを活用するのって大変...

課題

SIEM・統合ログ管理システム
Logstorage で解決

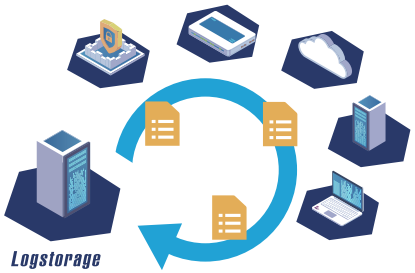
01 ログの収集

取得が大変



散らばるログを手作業で取得する場合、
コストがかかる上に、抜け漏れリスクも増加。

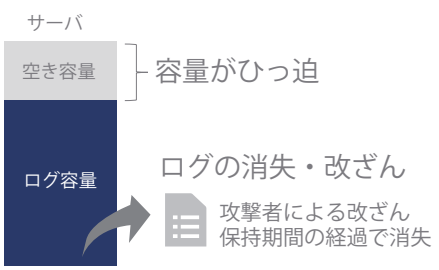
自動で収集



ログを自動で漏れなく収集し、
担当者の手間とコストを大幅削減。

02 ログの保管

適切な長期保管が困難



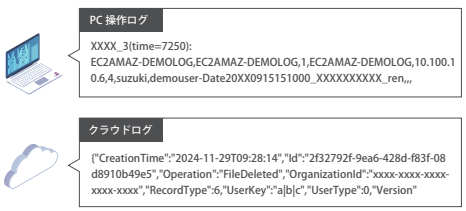
ログの長期保管には、サーバのひっ迫や
ログの消失・改ざんなど課題が山積み。

圧縮して長期保全

ログを高圧縮・暗号化することで
コストを抑えながら、安全に長期保管。

03 ログの分析

分析が困難



ログを読むのは難しく、
膨大なログを常に監視するのは非現実的。
調査・分析には、専門知識と労力が必要。

直感的に分析

怪しい動きに対して検知アラートを発報。
成形されたログを表やグラフで可視化。
分析結果のレポートをメール送信。

■ 開発元・お問合せ先
Infoscience インフォサイエンス株式会社
〒108-0023 東京都港区芝浦2-4-1 インフォサイエンスビル https://www.infoscience.co.jp/
TEL.03-5427-3503 FAX.03-5427-3889 E-mail: info@logstorage.com

Logstorage
製品紹介パンフレットはこちら
https://logstorage.com/download/