# ALog EVA × Microsoft 365

ファイル共有やメール機能の操作履歴を自動レポート

# Microsoft 365のログ管理 実践ガイド

# 目次


- はじめに 3p
  ニューノーマルな働き方を支える「記録の自動化」
- 記録と分析は SIEM で自動化できる 4p
- ログの長期保管は
  ハイエンドのライセンスが必要？ 5p
- SIEM を選ぶなら海外製か？国産か？ 6p
- なぜ ALog が選ばれるのか 7p
- ALog EVA ×Microsoft 365 8p
- ALog EVA × Microsoft 365 で取得できるログ 9P
- ログのサンプル / 活用例 10p
- おわりに 11p
  もう運用に悩む必要はない

# はじめに

## ニューノーマルな働き方を支える「記録の自動化」

世界中でテレワークが浸透し、システムのクラウド化が進む中、
様々な不正を監視し、盗難防止を徹底する上で、
「アクセス記録」が重要となっています。

**記録**
運転には、万一のために
ドライブレコーダー（記録動画）が必要

▶

**保管**
デジタルデータにも
まさかのためにログの記録保管が大事

▶

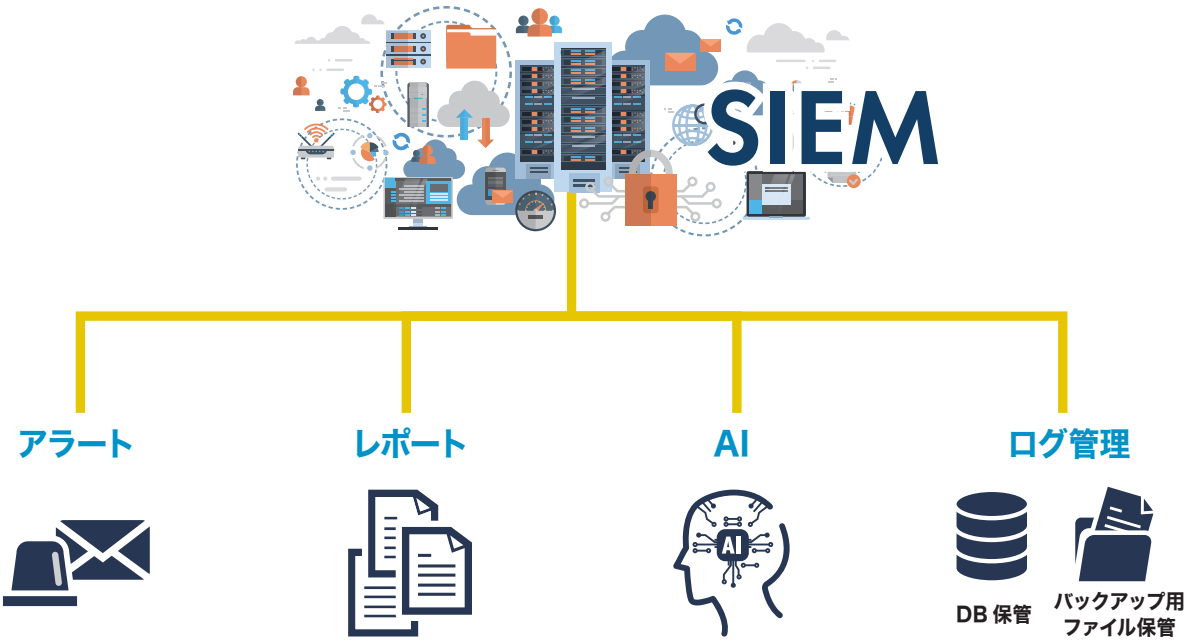
**レビュー**
記録がないと、
あとで原因特定ができない

新型コロナウィルスの蔓延は、多くの企業にとって、仕事の在り方を考えさせられるきっかけとなりました。いまだ予断の許されぬ状況下、世間では、オフィスワークに代わってテレワークを標準化する「ニューノーマルな働き方」が注目されています。

そうした背景を受け、今加速しているのがビジネスの「クラウド化」です。
しかし、Microsoft365 をはじめとするクラウドサービスは、働く場所を問わない点で利便性が高い反面、手軽に重要データを持ち出せてしまうというセキュリティ上の懸念があります。

有効なセキュリティ対策としては、重要ファイルに対して、いつ誰が操作したかなどの「アクセスの記録＝ログ」を管理することですが、あらゆるシステムの難解なログを、逐一人の目で管理するのは現実的ではありません。
そこで本資料は、そのセキュリティ運用を**「簡単に自動化」**する方法についてご紹介します。

# 記録と分析は SIEM で自動化できる




SIEM（Security Information and Event Management）とは、「データを統合管理・長期保管・分析するツール」です。
SIEM ひとつあれば、クラウド、オンプレミス環境に混在する様々なシステムのログを統合的に管理し、システムをまたがった横串の相関性の理解が可能になります。ログデータを自動で集約するだけでなく、既成のアラート機能やレポート機能を使って簡単に不正や問題の発見を自動化します。更に、過去データを蓄積すれば、AI 機能で未来の不正予兆を導き出す先進的なツールにも飛躍します。

例えば最近では、Apple や楽天カード等に扮するなりすましメールの他、新型コロナウィルスに端を欲した給付金や雇用調整助成金の案内などの標的型メールが増加傾向にあります。たとえアンチウイルス対策を施した PC でも、いとも簡単に侵入・感染してしまい、企業はそのことに気づくことすらできないというのが実情です。
このような脅威・不正を検知する仕組みとして、システム全体を監視・統合管理できる SIEM が、今後不可欠となります。

# ログの長期保管は
# ハイエンドのライセンスが必要？

Microsoft 365 には複数のライセンスタイプがありますが、ログを1年間保持するためにはハイエンドのライセンスを購入する必要があります。
しかし、多くの従業員を抱える大企業にとっては、中長期かかる販売管理費として、重いコスト負担となってしまいます。

ログ保管だけのために、ハイエンドのライセンスを契約するくらいなら、別の場所で保管したいと思うのは当然の流れでしょう。その際にかかる、ログの管理・運用の負担を、SIEM の利用によって解決するというのが、今ではスタンダードになりつつあります。

# SIEM を選ぶなら海外製か？国産か？

ここまでで、SIEM の利便性についてはご理解いただけたと思います。
しかし、海外製の SIEM は導入に専門的なノウハウを要するため、プロの Sier に委託せざるを得なくなり、結果、多額の出費となってしまうケースが多くあります。せっかく Microsoft 365 のライセンス費用を抑えても、SIEM の運用がコスト高になっては本末転倒です。
また委託を受ける Sier 側も、ツールの技術的理解に加えて、製品専門の技術者を育成する手間と費用が発生するため、前向きではないのが実態です。

では国産の SIEM 製品はどうか？
残念ながらこれまでの国産製品は、ユーザー側でプログラミングをする SDK 製品が多く、簡単に実装できるパッケージツールを探すのは困難でした。

その概念を根本から覆すのが、ALog です。
ALog といえば、データアクセス管理のスタンダードとして、サーバアクセス市場シェア No.1 を独走する国産のログ製品。数あるシリーズラインナップの中で、SIEM 製品としての特長を持つのが ALog EVA です。ALog シリーズ共通コンセプトである、圧倒的な簡便性と価格の妥当性を引き継ぎ、多くの導入実績を誇っております。

# なぜ ALog が選ばれるのか

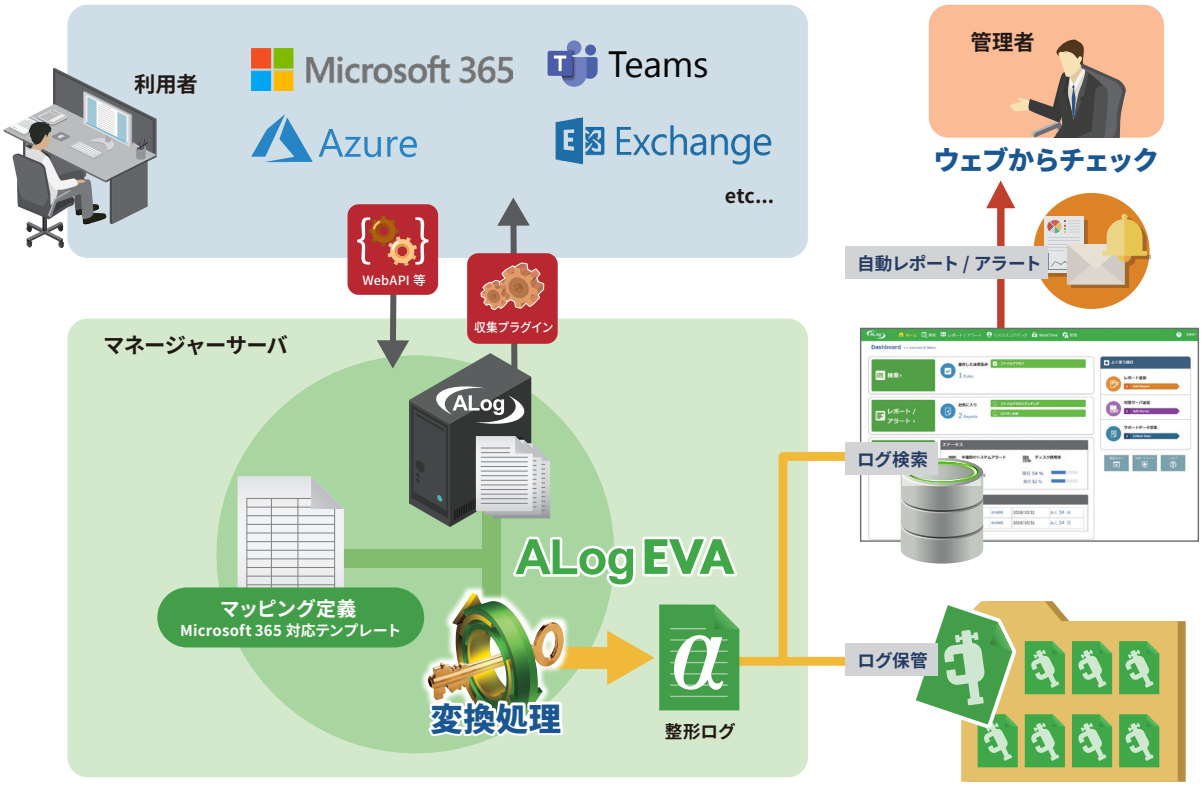
その導入障壁とコストの低さもさることながら、ALog が選ばれる理由としてもっとも重要なポイントが「設定 / 運用の手軽さ」です。
一度設定してしまえば、アラートもレポートも日々自動で出力されます。また設定自体も、すでにあるテンプレートに項目を設定するだけなので、専門知識がなくても、誰でも簡単に使いこなすことができます。

また、他製品にはないユニークポイントが「AI 機能による予兆検知」です。
ユーザー毎の「普段」との差異を AI が分析し、閾値の設定だけでは漏れてしまう内部不正の可能性を自動検知します。

その他、ログの長期保管や高速検索、改ざん防止など、SIEM に求められる機能を標準装備。SIEM 製品にありがちな、追加のオプション費用は必要ありません。

# ALog EVA ×Microsoft 365

ALog EVA と Microsoft 365 を連携させることで、Microsoft のアプリケーションやサービスの操作履歴を簡単に統合管理することができます。
例えば、ファイル共有やメール機能、グループウェアに対し、**「いつ」「誰が」「なにをしたのか」を可視化**することができるのです。
また、Microsoft 365 を利用するエンタープライズ企業は、既存のオンプレシステムとのハイブリッド運用を行うことが多いことでしょう。このようなハイブリッド環境でも ALog であれば、既にあるファイルサーバやストレージサーバ、AD などのログも合わせて包括管理できるので、管理の一貫性と網羅性、どちらの観点からも利便性が高いのです。




**インターフェイスの一元化**

**セキュリティリスクの軽減**

**システム横断的なログ管理**

**ログ消失リスクの軽減**

# ALog EVA × Microsoft 365 で取得できるログ

SharePoint
OneDrive for Business

## ファイルアクセスログ

- ●ファイルアクセス
- ●ファイルとフォルダー操作
  （移動 / コピー / 削除 / 復元）
- ●ファイルアップロード / ダウンロード
- ●ファイルとフォルダーの共有

Azure

## AD 管理操作ログ

- ●ユーザの作成 / 変更 / 削除
- ●ユーザのパスワード変更 / 再設定
- ●ユーザのライセンス変更
- ●管理者の役割（権限）変更 / 削除
- ●電子情報開示検索（監査）の操作

Exchange

## メールログ

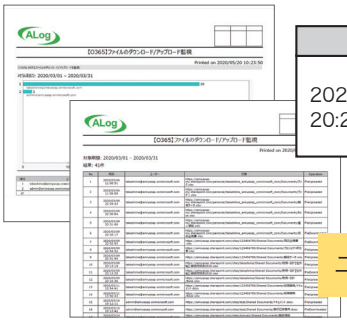
- ●メールボックスへのサインイン
- ●メールの作成 / コピー / 移動 / 削除

ALog EVA なら sharepoint のファイルアクセスログや AD の管理操作、Exchange のメールログをまとめて取れるようになります。
以降のページでは、実際にそれぞれのログを取ることでどんな効果があるのかを具体的に紹介します。

# ログのサンプル / 活用例

## 不正アップロード / ダウンロードの監視

重要ファイルのアップロード / ダウンロードや、外部共有の履歴を一覧化

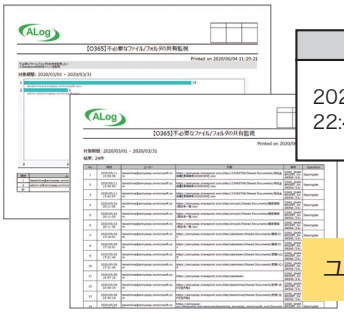


| 時刻 | ユーザー | 対象 | Operation |
|---|---|---|---|
| 2020/3/24 20:24:47 | takashima@amiyasap.onmicrosoft.com | https://amiyasap.sharepoint.com/sites/AmiyaX/Lists/List/ 顧客リスト .xlsx | FileUploaded |

ユーザー「**takashima**」さんが「**顧客リスト .xlsx**」を**アップロード**している

## 外部共有の監視

機密情報が不正に持ち出されていないか、内部不正対策に



| 時刻 | ユーザー | 対象 | Operation |
|---|---|---|---|
| 2020/03/26 22:40:14 | watanabe@amiyasap.onmicrosoft.com | https://amiyasap.sharepoint.com/sites/Shared Documents/ 財務・会計【社外秘】.xlsx | SharingSet |

ユーザー「**watanabe**」さんが「**財務・会計【社外秘】.xlsx**」を**共有**している

## Microsoft365 自動監視パックの項目

上記の他にも、監視すべき要所への監視項目は全てテンプレートとして
ご用意があります。ログ管理に深い知見がない方でも、1 日あれば導入と実装が
できます。

| 対象サービス | リスク分類 | 検知内容 |
|---|---|---|
| OneDrive/Sharepoint | アクセス監視 | ファイルアクセス監視（作成/参照/更新/コピー/削除など） |
| | 情報漏洩 | ファイル/フォルダの共有監視 |
| | | ファイルのダウンロード/アップロード監視 |
| Azure Active Directory | アクセス監視 | ADへのアクセス監視（サインインログ、サインイン失敗ログ） |
| | | 職場以外からのMS365アクセス監視 |
| Exchange | 内部不正/乗っ取り | 管理者操作の監視 |
| | 内部不正/乗っ取り | メールボックスへのアクセス監視（サインイン） |
| | | メールの作成/ コピー/ 移動/ 削除 |

# おわりに

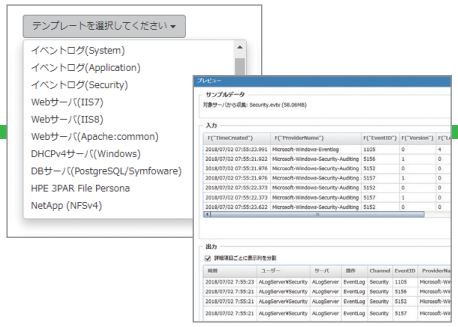
## もう運用に悩む必要はない

ALog であれば、SIEM 製品でにありがちな運用の難しさと高度な知識は不要となります。
自動でセットされたテンプレートを活用することで、高度専門の SIEM 分析ノウハウを伴わずに使用できます。

更に、追加費用なく AI 機能も利用でき、これまで気づけなかった不正の潜伏傾向が迅速に察知できるようにもなります。
詳しくは、『標的型攻撃に対応するセキュリティ運用自動化メソッド』のホワイトペーパーをご覧ください。

## 設計 / 設定がカンタン

ログ取込用のテンプレートを多数装備
オリジナルのテンプレート作成もカンタン

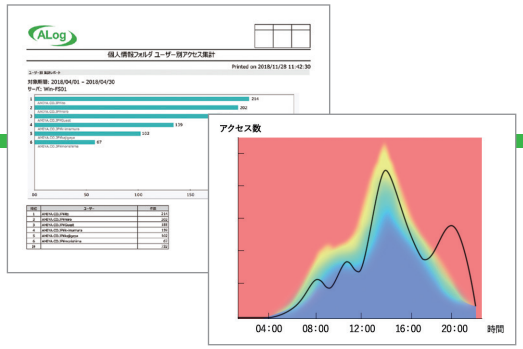



## 直感的に使える GUI

分かりやすいビジュアルと用語で
構成しているので、誰でも簡単に操作可能

## 理解できる！活用できる！

ただ蓄積するだけではなく、
統計分析や危険予知に活用可能



サーバアクセスログ
## ALog ConVerter®

ALog ConVerter は、重要データへのアクセス記録をエージェントレスで取得する製品です。重要データが格納されるサーバ側からログを取得することにより、ストレスのない効率的なログ管理を実現します。

統合ログ
## ALog EVA

ALog EVA は、ALog シリーズの守備範囲を飛躍的に拡張します。
高度な専門技術を要求する従来の統合ログ製品から一線を画した手軽さと柔軟さを備えた新しい統合データマネジメントツールです。

詳しい製品のご紹介、評価版のご依頼は以下にお問い合わせください。

お問い合わせ先

株式会社網屋
データセキュリティ事業部
TEL：03-6822-9996　E-mail bv-sales@amiya.co.jp

**詳しい製品概要資料はこちら ＞**

**開発元**

AMIYA 株式会社 網屋

〒103-0007 東京都中央区日本橋浜町3-3-2 トルナーレ日本橋浜町 11F
TEL: 03-6822-9999 FAX: 03-6822-9998
https://www.amiya.co.jp/

**販売元**

ALog ConVerterは株式会社網屋の登録商標です。
記載された製品の仕様・機能等は改良のため予告なく変更される場合があります。
このパンフレットの内容の一部またはすべての複写・転用・転載等を株式会社網屋に無断で行った場合、著作権の侵害になります。