

関係各位

令和 8 年 10 月 20 日
株式会社セキュアヴェイル
東証スタンダード 3042/札証本則 証券コード 3042
代表取締役社長 米今政臣

緊急対応 Microsoft 365 監査ログの調査分析レポート無償提供 不正アクセス急増に『AI-SOC』を活用(先着 100 社)

IT セキュリティの専門企業、株式会社セキュアヴェイル（本社：大阪市北区、代表取締役社長：米今政臣、東証スタンダード：3042、以下セキュアヴェイル）は、創業より 25 年にわたって提供する SOC サービス（セキュリティ運用サービス）の運用経験とグループ会社である株式会社 LogStare が開発した AI ログ分析機能を活用した『AI-SOC サービス』を提供しています。

昨今の増大する不正アクセスへの対策や現状調査の一助になれるよう『AI-SOC サービス』の技術を活用することでユーザー企業の Microsoft 365（以降：M365）の監査ログに対するセキュリティ調査分析レポートを先着 100 社に無償で提供します。

企業や自治体のインフラを狙った不正アクセスと情報漏えい事故の要因は、巧妙化した AI 技術を用いたサイバー攻撃などによるユーザーID・パスワードの不正取得、設定ミスやシステムの脆弱性を悪用した攻撃、ランサムウェアなどのマルウェア感染などと考えられます。

企業の大小に関わらず M365 を利用するユーザーは Office アプリだけではなく業務システムや様々なクラウドサービスなどを M365 のユーザー管理機能やサインイン認証の機能などを利用し管理しているケースが多々見受けられます。M365 の監査ログを AI-SOC 機能で分析することによりアカウント乗っ取りの可能性がある攻撃、外部からの侵入、アクセス権の設定不備による流出可能性などを分析し使用状況の総評・時間帯やサービス別・ユーザー別・ファイル別セキュリティ状況の報告・各項目の分析単位をレポートします。

今回、ご依頼いただきましたユーザー様には、弊社にて設定を完了した時点で収集保管されている監査ログから脆弱性の現状を分析し、レポートします。（7 日～15 日）

【サービスイメージ】



【レポート例】

【監査コメント】

本監査レポートの範囲として、Microsoft 365環境における2025年12月の利用状況とセキュリティ上の注意点を以下に報告します。

—

【全体傾向とサービス別傾向】

1. ログ件数はExchangeが圧倒的に多く（1,200件）、次いでAzureActiveDirectory（2,000件）が顕著です。これら7サービスが全体の大半を占めており、監査・監視の重点対象です。

2. Exchangeではログ件数が増加傾向にありますが、特定ユーザー（3名）による大量アクセスが確認されています。特にメールシステムアクセス（MailboxAccessed）が40,000件と突出し、管理者権限を持つユーザーや特定の機能利用による集中傾向が疑われます。

3. AzureActiveDirectoryはログ件数増加（前12月比）がユーザー数減少（11→8人）という特異的な変化があり、一部ユーザーによる集中アクセスや特権アカウントの使用が考えられます。特に（Updateserviceprincipal）操作の集中とログイン失敗の顕著な増加（11件）がセキュリティリスクとして顕著です。

4. SharePointはログ件数増加傾向であり、特定サイト「DemoSoftware-1G」へのアクセス・ファイル操作・共有権設定変更が顕著です。非ユーザーによる多数回の匿名リンク作成や共有リンク作成（各31件）が確認されており、共有権設定の悪用が懸念されます。

5. OneDriveは全体的にログ件数が減少ですが、匿名リンク共有や共有リンク更新は増加しており、共有管理に注意すべきと見做されます。利用者は既定通り非ユーザー中心です。

6. Microsoft Teamsは利用量1名による安定した活動であり、大きな変動や異常は見られません。

7. 監視サービスとしてPlannerが監視対象に追加されており、今後の利用状況の把握が求められます。

—

【期間等・日付情報】

1. ExchangeおよびAzureActiveDirectoryでは既述の傾向と合わせて10～13間台にアクセス集中があります。特にExchangeの間台は全体的にログ増加傾向にあり、一部イベント監視や権限取得の可能性が示されています。

2. SharePointでは年終整理にアクセス集中（31件）が確認され、業務時間外の自動処理やバックアップ処理が推定されます。また12月台にも集中的なアクセス傾向が確認されています。

3. ログ生成間隔は20秒と15秒にピークがあり、この間隔等で稼働ユーザーによるログイン成功・失敗も多数発生しています。特に15秒間隔には90秒未満のログイン失敗が頻発されており、不正アクセス試行や権限取得への対応強化を推奨します。

4. 業務時間外（22時～04時）のファイル操作系アクセスは大幅減少しましたが、年終4時台には非ユーザーによる62件のファイル操作集中があります。既述傾向との詳細調査を推奨します。

5. 日別では12月4日を中心に稼働サービスでログ急増・ユーザー数増加が見られます。この日はExchange、AzureAD、SharePointなど複数サービスで異常なアクセス増加傾向となっており、今後の調査対象です。

【10. 日付別ログ件数サマリサービス名 (SharePoint)】

期間	件数
2025-12-01 00:00:00 - 2025-12-31 23:59:59	1,200

サービス名: Microsoft 365 監査ログ対象

利用環境: 本環境

レポート作成者: サービス監視/監査

SharePoint

【ログ分析結果】

「10. 日付別ログ件数サマリサービス名 (SharePoint)」レポートの分析結果を以下に報告します。

1. ログ件数の全体傾向

- 2025年12月の全日平均ではログ件数は10件前後で推移しています。
- 全体的に12月4日15:00時と大幅な増加傾向があり、通常の15倍のログが記録されています。
- 12月5日と12月12日もそれぞれ20件、20件と他の日より多くのログ件数を示しています。

2. ユーザーID (User) 別件数傾向

- 12月4日の急激なログ増加は注目すべき点です。この日はユーザー数も増えているため、何らかのイベントや操作集中が考えられます。
- 12月5日の急激なログ増加は注目すべき点です。この日はユーザー数も増えているため、何らかのイベントや操作集中が考えられます。
- その他の日はほぼ一定の利用状況であり、大きな変動は見られません。

以上から、SharePointサービスに関する2025年12月の日別ログでは、特定日（12月4日）に集中したアクセスや操作が発生していることが明確です。その他の日は安定した利用状況であるため、異常検知や詳細調査の対象としては12月4日を優先すべきと考えられます。

【期間レポートとの比較】

前日（2025年11月）と今日（2025年12月）の「日付別ログ件数サマリサービス名 (SharePoint)」レポートの傾向分析を以下に示します。

—

1. ログ件数の全体傾向比較

前日は1日あたり10件程度のログ件数でほぼ10件前後で推移していたが、11月5日に47件、11月18日に16件、11月21日に11件、11月22日に11件と一部で増加が見られた。

→ 今日は12月4日に150件と大幅な増加があり、他の日はほぼ10～12件程度で推移している。12月5日と12月12日もそれぞれ20件、20件と前日より多いログ件数がある。

つまり、今日のデータでは特に12月4日のログ件数が突出して多く、そのほかにも複数の日で前日より多いログ件数が確認されている。

—

2. ユーザーIDの別件数比較

前日はほとんどの日でユーザーIDが10件以下であり、例外的に11月10日と11月13日にユーザーとなっている。

→ 今日は12月4日に2ユーザーが記録されている以外はほぼ1ユーザーで推移しており、未だ未だ変化はない。

→ したがって、ユーザー数の面では前日よりもユーザーによる利用が主体であり、大幅な変動は見られない。

—

3. 特異日の分析

前日（11月5日）の47件増加は非ユーザーによるもので、前日の最大値を大きく上回る。

→ 今日は12月4日の150件増加はユーザーによるもので、前日の最大値を大きく上回る。

→ また今日は12月5日（20件）、12月12日（20件）も前日の増加より多いログ件数がある点も特異的。

—

まとめ：

今日のレポートでは2025年12月4日にログ件数が150件と前日の最大値の約15倍に急増し、かつ2ユーザーによるアクセスとなっている点が顕著な特徴です。その他の日についても前日よりやや多めのログ発生日が複数発生しています。ユーザー数自体には大きな変化はなく、主に同一ユーザー中心の利用傾向が確認されています。

このことから、2025年12月4日に何らかの理由でSharePoint上の操作やアクセスが集中した可能性が高いと考えられます。今後、この特異日の詳細調査を行い原因を特定することを推奨します。

件数

2025-12-01

2025-12-02

2025-12-03

2025-12-04

2025-12-05

2025-12-06

2025-12-07

2025-12-08

2025-12-09

2025-12-10

2025-12-11

2025-12-12

2025-12-13

2025-12-14

2025-12-15

2025-12-16

2025-12-17

2025-12-18

2025-12-19

2025-12-20

2025-12-21

2025-12-22

2025-12-23

2025-12-24

2025-12-25

2025-12-26

2025-12-27

2025-12-28

2025-12-29

2025-12-30

2025-12-31

10

20

30

40

50

60

70

80

90

100

110

120

130

140

150

160

170

180

190

200

1

14

15

【AI-SOC for Microsoft 365 について】

- ・ 初期費用 ￥50,000
 - ・ 月額料金 **¥50**／月 （20USER～10USER 追加単位での年間契約）
- オプション：ログ分析ポータル
- ：ログ保管
 - ：ログ分析調査（アドバイザリー）

【関連記事】

Microsoft 365 監査ログの取得方法 | 絶対にとっておくべき理由や保存期間も解説

<https://www.secuavail.com/kb/microsoft-365/audit-log/>

株式会社セキュアヴェイル概要

2001 年設立。創業以来ネットワークセキュリティに特化して企業や組織の情報システムの運用をサポートする国内では数少ない IT セキュリティ 専門企業。企業のシステムセキュリティを確保し、事業運営を安心して継続させるために「安全」で「役立つ」サービスを提供します。

創業期から 20 年以上提供し続ける統合セキュリティ運用サービス「NetStare」は SOC（Security Operation Center）と NOC（Network Operation Center）双方を提供する業界でも数少ない統合セキュリティ運用サービスです。クライアント企業のネットワーク機器を常時 1.1 万台以上監視し、1 日 25 億件の膨大なログを収集し、機器故障、通信障害、サイバー攻撃などを 24 時間 365 日体制でいち早く発見します。

※記載されている会社名および商品名は、各社の登録商標または商標です。

※本プレスリリースに関するお問い合わせは下記までお願いします。

株式会社セキュアヴェイル カスタマーサポートセンター

TEL: 03-4405-6128 Email: contact@gr.secuavail.com

※本プレスリリース含む製品・サービス以外の IR 窓口

株式会社セキュアヴェイル 経営企画本部 IR 担当

TEL：06-6136-0026 Email: ir@secuavail.com

【語句解説】

・ログ

一言でいうと、「システムの通信や操作の『履歴・記録』」のことです。

パソコンやサーバー、クラウドサービスなどが動く際、「誰が、いつ、どこから、何をしたか」という足跡が自動的にテキストデータとして刻々と記録されていきます。飛行機の「フライトレコーダー（飛行記録装置）」のようなイメージです。特に、監査ログは「セキュリティや不正防止のチェック（監査）を目的とした重要な操作記録」を指します。

セキュアヴェイルの『AI-SOC』について

セキュアヴェイルはセキュリティサービス事業者としての 25 年にわたって培ったログ分析やアラートのノウハウと、自社グループのプロダクトである LogStare の AI 機能を活用し、IT システムのセキュリティ運用管理者を専任で置けない企業、組織に向け、『AI-SOC』シリーズを安価に提供しています。

『AI-SOC for Microsoft 365』について

Office アプリケーションも従来のオンプレ型（所有する機器へのアプリケーションのインストール）の製品からクラウドサービスである Microsoft 365 に移行し、Teams や最新版の Office アプリケーションをクラウドストレージでファイル共有などを活用し業務の生産性を高めています。

その反面、本来はアクセスすべきでない社内外のユーザーが機密情報にアクセスできてしまうなどのリスクがあり、オンプレとは異なるセキュリティ対策、トラブル対応が必要となっています。

セキュアヴェイルは Microsoft 365 の監査ログを AI が分析し、セキュリティリスクの高い事象を検知してアラート通知する SOC サービス『AI-SOC for Microsoft 365』を昨年末より開始しました。