SecuAvail
NEWS RELEASE

関係者各位

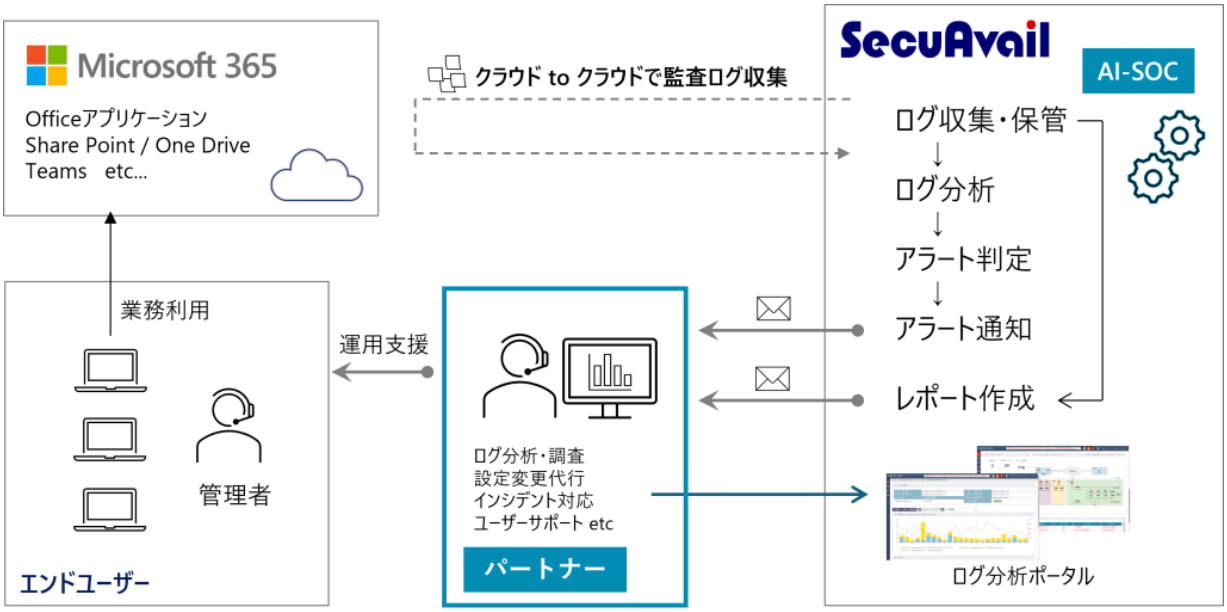
令和 8 年 4 月 27 日
株式会社セキュアヴェイル
東証スタンダード/札証本則 証券コード 3042
代表取締役社長　米今政臣

セキュアヴェイルが提供する『AI-SOC for Microsoft 365』のソリューションパートナーにスノーピークビジネスソリューションズが参画

IT セキュリティの専業企業、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、証券コード：3042、以下セキュアヴェイル）が提供する次世代 SOC（Security Operation Center）サービス「AI-SOC for Microsoftt365」のソリューションパートナーに、株式会社スノーピークビジネスソリューションズ（本社：愛知県岡崎市、代表取締役社長：坂田真也、以下 Snow Peak BS）が参画しました。マイクロソフト認定パートナーとして Microsoft 365 の導入から運用定着まで 350 社を超える実績を持つ SnowPeak BS の参画により、AI-SOC のサービス内容の拡充を図ります。

「AI-SOC」は、セキュアヴェイルが創業期から 25 年にわたって蓄積したセキュリティ運用のノウハウ AI に継承し、SOC の無人化と低価格化を実現した次世代の SOC サービスです。
FortiGate の通信ログを分析して不正アクセスや内部からの不正通信よる情報流失の可能性などを検知する「AI-SOC for FortiGate」、Microsoft 365 の監査ログを分析してセキュリティリスクの高い事象を検知する「AI-SOC for Microsoft 365」をラインアップし、セキュリティ対策がサイロ化し負担が増大する IT 運用担当者の業務を支援します

この度ソリューションパートナーとなった SnowPeak BS はマイクロソフト認定パートナーとして Microsoft 365 の導入から運用定着までのトータルサポートを 350 社以上のユーザー企業に提供しています。この経験を元にユーザー企業の実務視点でのログ分析やアラートを AI-SOC for Microsoft 365 に反映するなど、セキュアヴェイルと共同で AI-SOC のサービス内容の拡充を図るとともに、ソリューションパートナーオリジナルの運用サービスやサポートサービスなどのビジネスを推進します。



ソリューションパートナーによる AI-SOC 提供イメージ

110.　日付別ログ件数サマリ(サービス名 SharePoint)	
期間	2025-12-01 00:00:00 - 2025-12-31 23:59:59
デバイス名	Microsoft 365 監査ログ収集
利用監視・収集項目	Office365監査ログ (60)
レポート作成条件	サービス名(Workload)
	'SharePoint'

【ログ分析結果】

「110.　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月のほとんどの日でログ件数は10件前後で安定しています。
- 例外的に12月4日に150件と大幅に増加しており、通常の約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28件、29件と他の日より多めのログ件数を示しています。

2. ユーザーID（UserId）Distinct件数の傾向
- 大半の日でユーザーIDは1名のみがログを生成しています。
- 12月4日のみ2名のユーザーがログを生成しており、この日が最も多様なユーザーによるアクセスがあったことを示しています。

3. 特異点
- 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あった可能性があります。
- 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。

【前回レポートとの比較】

前回（2025年11月）と今回（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

- 前回は1日あたりのログ件数がほぼ10件前後で安定している中、11月5日に47件、11月18日に16件、11月7日に12件、11月13日に11件と一部で増加が見られた。
- 今回は12月4日に150件と大幅な増加があり、他の日はほぼ10〜12件程度で安定している。12月5日と12月12日もそれぞれ28件、29件と前回より多い日がある。
- つまり、今回のデータでは特に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回より多いログ件数が観測されている。

---

2. ユーザーIDのDistinct件数比較

- 前回はほとんどの日でユーザーIDのDistinct数が1であり、例外的に11月10日と11月13日に2ユーザーとなっている。

- 今回は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、大きな変化はない。
- したがって、ユーザー数の面では両期間ともに単一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。

---

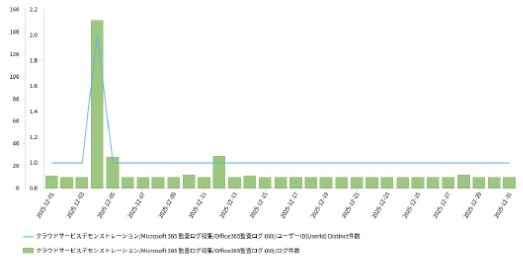
3. 特異日の分析

- 前回11月5日の47件増加は単一ユーザーによるもの。
- 今回12月4日の150件増加は2ユーザーによるもので、前回の最大値を大きく上回る。
- また今回12月5日（28件）、12月12日（29件）も前回同様の日付周辺より多いログ発生がある点も特徴的。

まとめ：

今回のレポートでは2025年12月4日にログ件数が150件と前回最大値の約3倍以上に急増し、かつ2ユーザーによるアクセスとなっている点が最大の特徴です。その他の日についても前回よりやや多めのログ発生日が複数存在しています。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は継続しています。

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。



	日付	ログ件数	ユーザーID(UserId) Distinct件数
1	2025-12-01	11	1
2	2025-12-02	10	1
3	2025-12-03	10	1
4	2025-12-04	150	2
5	2025-12-05	28	1
6	2025-12-06	10	1
7	2025-12-07	10	1
8	2025-12-08	10	1
9	2025-12-09	10	1
10	2025-12-10	12	1
11	2025-12-11	10	1
12	2025-12-12	29	1

AI-SOC for Microsoft 365　レポートサンプル（一部抜粋）

【概要】
アラート名：xx.　同一ユーザに対する複数IPアドレスログイン施行
ログソース：Microsoft 365 監査ログ収集

【AIによるアドバイザリー】
※アラート条件の設定変更やしきい値の変更は文末の連絡先までお問い合わせください。

1. 状況サマリー

ユーザーID「mob[@]ad[.]hits-net[.]com」が2026年1月7日に日本（東京都）とアメリカ（バージニア州）の異なる2つのIPアドレスからMicrosoft 365へログインを試みています。特にアメリカのIPアドレスからは複数回のログイン失敗後に成功しているログが確認されました。

2. 詳細分析

- **脅威の性質**
  同一ユーザーIDに対し、地理的に離れた2か所（日本：152.165.112.75、アメリカ：104.208.243.191）からのアクセスが検出されており、不正アクセスまたはアカウント乗っ取りの可能性がある。
- **影響範囲**
  対象はMicrosoft 365環境で、このユーザーの権限範囲に依存するが、情報漏洩や業務妨害など重大なリスクがある。
- **攻撃パターン**
  アメリカ側IPからは連続した6回のログイン失敗（UserLoginFailed）があり、その後3回連続でログイン成功（UserLoggedIn）が発生している。これはブルートフォース攻撃やパスワード推測攻撃の典型的な兆候。
- **緊急性**
  ログイン成功が複数回確認されているため、即時対応が必要。特に不正利用を防ぐため迅速な調査と対策が求められる。

3. 推奨調査・対応

- **対象ユーザー**
  mob[@]ad[.]hits-net[.]com のMicrosoft 365アカウント全般
- **調査観点**

AI-SOC for Microsoft 365　アラートメールサンプル（一部抜粋）

株式会社スノーピークビジネスソリューションズ概要

アウトドア総合メーカーである株式会社スノーピークの子会社として、2016 年 7 月に設立。
「自然の壮大なエネルギーと、テクノロジーの無限の可能性を健全に融合して、人間らしく働く人を増やすことで真に豊かな世界を創る」をミッションとしています。
ワークバリュー創造事業部では、Microsoft 365 を基盤としたクラウド活用支援、セキュリティ・ガバナンス設計、運用定着支援を通じて、時代に合った働き方の実現を支援しています。単なる IT 導入や効率化に留まらず、現場の創造性や主体性が発揮されることを重視し、ツール・制度・運用を一体で捉えた伴走型の支援を強みとしています。

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 セキュリティ専業企業。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
大阪市北区東天満 1-1-19
アーバンエース東天満ビル
経営企画本部　IR 担当
TEL：06-6136-0026　Email: ir@secuavail.com