SecuAvail

NEWS RELEASE

April 27, 2026

SecuAvail Inc.
Masaomi Yoneima,
President & Representative Director
Securities Code: 3042
Tokyo Stock Exchange (Standard Market)
/ Sapporo Securities Exchange
https://www.secuavail.com/

Snow Peak Business Solutions Joins as a Solution Partner for SecuAvail's "AI-SOC for Microsoft 365"

SecuAvail Inc. (Head Office: Kita-ku, Osaka; President & Representative Director: Masaomi Yoneima; Securities Code: 3042; hereinafter "SecuAvail"), a specialized IT security company, is pleased to announce that Snow Peak Business Solutions Inc. (Head Office: Okazaki City, Aichi; President & Representative Director: Shinya Sakata; hereinafter "Snow Peak BS") has joined as a solution partner for "AI-SOC for Microsoft 365," a next-generation Security Operation Center (SOC) service provided by SecuAvail.

Snow Peak BS is a certified Microsoft partner with a proven track record of supporting more than 350 companies in the implementation and operational adoption of Microsoft 365. Its participation will further enhance and expand the capabilities of the AI-SOC service lineup.

"AI-SOC" is a next-generation SOC service that incorporates SecuAvail's approximately 25 years of accumulated security operations expertise into AI, enabling highly automated SOC operations and improved cost efficiency.

The AI-SOC lineup includes "AI-SOC for FortiGate," which analyzes FortiGate communication logs to detect unauthorized access and potential data exfiltration caused by malicious internal activities, and "AI-SOC for Microsoft 365," which analyzes Microsoft 365 audit logs to identify security-critical events. These services help reduce the operational burden on IT personnel amid increasingly siloed security environments.

Snow Peak BS will collaborate with SecuAvail to enhance "AI-SOC for Microsoft 365" by incorporating practical, user-oriented log analysis and alerting perspectives based on its extensive experience supporting Microsoft 365 adoption. In addition, Snow Peak BS will promote its own value-added offerings, including partner-specific operational and support services.

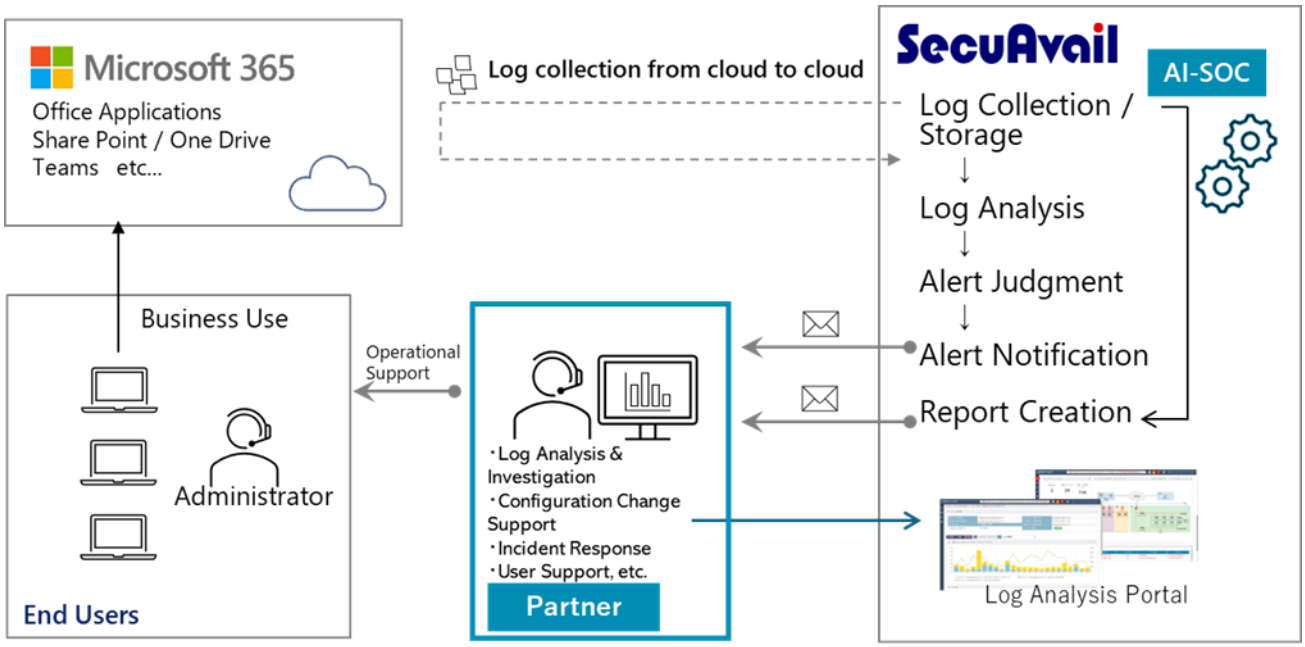
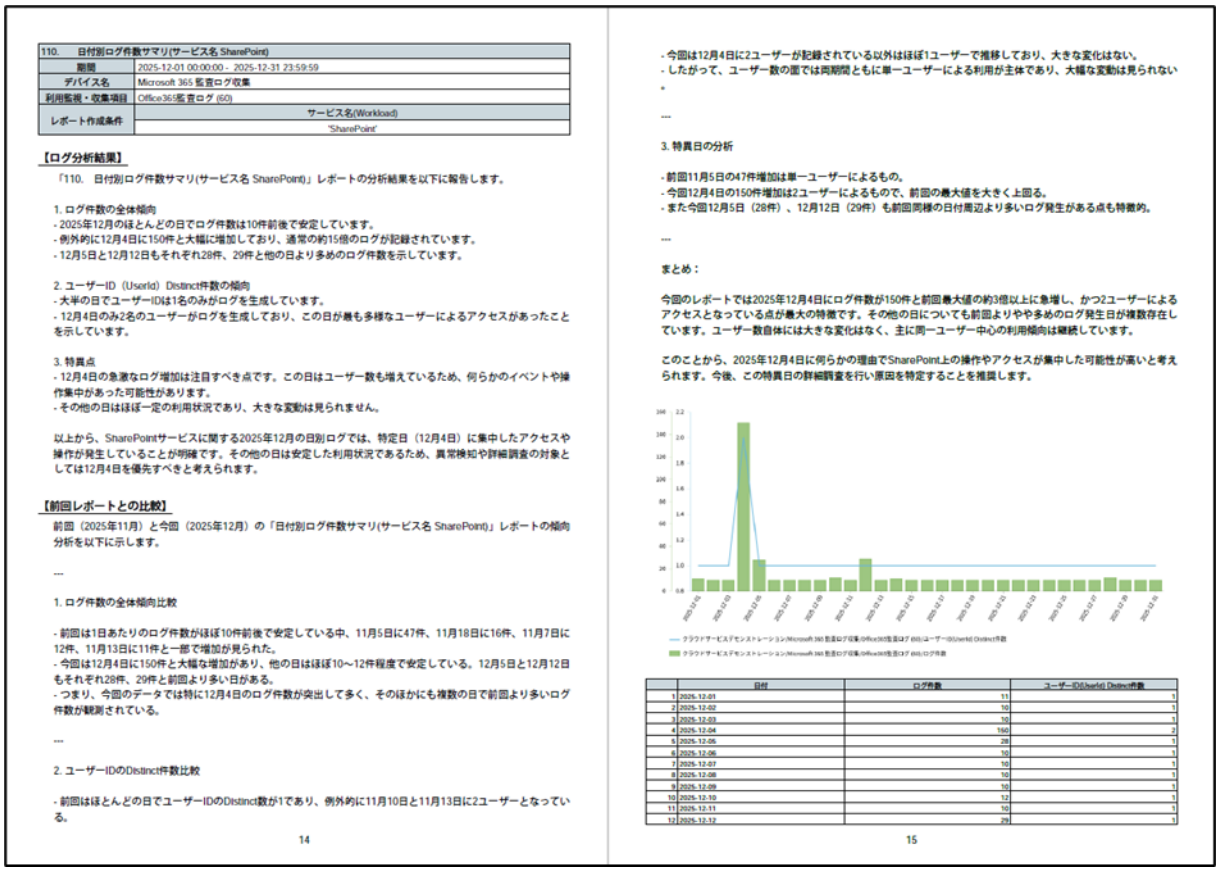


Illustration of AI-SOC Service Delivery by Solution Partners



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	Office 365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周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

Sample AI-SOC for Microsoft 365 Report (Excerpt)


【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

Sample AI-SOC for Microsoft 365 Alert Email (Excerpt)

■About Snow Peak Business Solutions Inc.

Snow Peak Business Solutions Inc. was established in July 2016 as a subsidiary of Snow Peak, Inc., a comprehensive outdoor products manufacturer. The company's mission is "to create a truly enriched world by harmoniously integrating the immense energy of nature with the limitless potential of technology, thereby increasing the number of people who can work in a more human-centric way."

Through its Work Value Creation Division, the company supports the realization of modern workstyles by providing cloud utilization support based on Microsoft 365, as well as security and governance design and operational adoption services. Beyond simple IT implementation and efficiency improvements, Snow Peak Business Solutions emphasizes enabling creativity and autonomy in the workplace, offering hands-on support that integrates tools, frameworks, and operations.

■About SecuAvail Inc.

Founded in 2001, SecuAvail Inc. is one of the few Japan-based companies exclusively dedicated to network security, offering long-term operational support for corporate and organizational information systems. To ensure robust system security and uninterrupted business continuity, the company provides services that are both highly secure and practically applicable.

For over two decades, SecuAvail has offered NetStare, an integrated security operations service that uniquely combines the capabilities of both a Security Operation Center (SOC) and a Network Operation Center (NOC).

Through NetStare, the company monitors more than 11,000 client network devices in real time, collecting approximately 2.5 billion log entries per day. This enables rapid detection of equipment failures, communication outages, and cyberattacks—24 hours a day, 365 days a year.

To learn more, please visit: https://www.secuavail.com

For inquiries regarding this press release:
SecuAvail Inc. – Marketing Grp.
TEL: +81-3-6264-7180
Email: marketing@secuavail.com

For IR inquiries (excluding product/service inquiries):
SecuAvail Inc. – Corporate Planning Division, IR
Urban Ace Higashi-Tenma Building, 1-1-19 Higashitenma, Kita-ku, Osaka
TEL: +81-6-6136-0026
Email: ir@secuavail.com