



NEWS RELEASE

October 20, 2026

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

SecuAvail Offers Free Microsoft 365 Audit Log Analysis Reports Powered by AI-SOC Amid Rising Unauthorized Access Incidents (Limited to the First 100 Companies)

SecuAvail Inc. (Headquarters: Kita-ku, Osaka; President and CEO: Masaomi Yoneima; TSE Standard: 3042), a company specializing in IT security, provides its "AI-SOC Service." This service leverages the operational expertise gained from 25 years of delivering SOC (Security Operations Center) services since its founding, combined with the AI log analysis capabilities developed by its group company, LogStare Inc.

To help mitigate the recent surge in unauthorized access and assist with current status investigations, the company will utilize its "AI-SOC Service" technology to provide security investigation and analysis reports on Microsoft 365 (hereafter "M365") audit logs free of charge to the first 100 companies.

The primary causes of unauthorized access and data breach incidents targeting corporate and local government infrastructure are believed to be the illicit acquisition of user IDs and passwords through cyberattacks exploiting sophisticated AI technologies, attacks exploiting misconfigurations or system vulnerabilities, and malware infections such as ransomware.

Regardless of their size, many companies using M365 manage not only their Office applications but also their business systems and various cloud services by utilizing M365's user management and sign-in authentication features. By analyzing M365 audit logs using AI-SOC capabilities, the service identifies potential account takeover attacks, external intrusions, and risks of data leakage due to misconfigured access rights. Furthermore, the report provides a general assessment of usage status broken down by time period, service, user, and file, along with comprehensive security condition reporting and analysis metrics for each item.

For interested client companies, we will analyze the current state of vulnerabilities based on the audit logs collected and stored up to the point when we complete the initial setup, and then provide a report (delivery within 7 to 15 days).

Service Overview Image



Sample Report

【報告コメント】

本報告レポートはMicrosoft 365のログデータとして、Microsoft 365環境における2023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利用状況】

- ログ件数はExchangeの増加に多く（11,250件）、次いでAzureActiveDirectory（2,000件）が増加しています。これら2サービスが全体の大半を占めており、監視・監視の対象です。
- Exchangeではログ件数増加により約4%減少しましたが、特定ユーザー（11~6人）による大量アクセスが確認されています。特にメールアイテムアクセス（MailItemAccessed）が9,400件と増加し、監視・監視の対象です。ユーザーごとのアクセス状況により監視・監視の対象となります。
- AzureActiveDirectoryはログ件数増加（約15%増）かつユーザー数減少（11~6人）という特徴的な変化があり、一部ユーザーによる集中アクセスや特定のサービス利用が増えています。特に「Updates service principal」の操作の集中とログイン失敗の増加（13%増）がセキュリティリスクとして監視されます。
- SharePointではログ件数増加であり、特定サイト「DemoSoftware」へのアクセス・ファイル操作・共有権限の変更が顕著です。一部ユーザーによる多数回のリンク作成や共有リンク作成（各11件）が確認されており、共有権限の適正化が必要です。
- OneDriveは全体的にログ件数減少傾向ですが、匿名リンク更新や共有リンク更新は増加しており、共有権限に注意すべき状況です。利用者は定期的にユーザーごとの確認が必要です。
- Microsoft Teamsは利用状況による増加した活動であり、大きな変更や異常は見られません。
- 監視サービスとしてPlannerが監視対象に追加されており、今後の利用状況の監視が求められます。

【関係者・対応依頼】

- ExchangeおよびAzureActiveDirectoryでは環境関係者と各関係者2~3名にアクセス権があります。特にExchangeのログはログ収集により増加し、一部パッチ処理や監視処理の可能性があります。
- SharePointでは半日程度にアクセス集中（13件）が確認され、監視・監視の自動化やパッチ処理が確認されています。また2件程度にもアクセス集中（13件）が確認され、監視・監視の自動化やパッチ処理が確認されています。
- ログイン増加は10%と10%に増加しており、この関係者で多数ユーザーによるログイン増加・失敗も確認されています。特に10%に増加したログイン失敗は監視されており、不正アクセスの監視・監視の自動化やパッチ処理が確認されています。
- 監視関係（22件~64件）のファイル操作やアクセスは大幅減少しましたが、年明け以降には一部ユーザーによる62件のファイル操作が確認されています。監視・監視の自動化やパッチ処理が確認されています。
- 監視では12月4日を境に監視サービスでログ件数・ユーザー数増加が見られます。この日はExchange、AzureAD、SharePointなど監視サービスで監視対象の増加に伴って増加している可能性があります。

【ログ件数】

サービス	2023-12-01 00:00:00 - 2023-12-31 23:59:59
ログ件数	11,250件
ユーザー数	11~6人

【ログ件数】

1. ログ件数の全体傾向

2. ユーザーごとの傾向

3. 特異点

4. 特異点

5. 特異点

6. 特異点

7. 特異点

8. 特異点

9. 特異点

10. 特異点

11. 特異点

12. 特異点

13. 特異点

14. 特異点

15. 特異点

16. 特異点

17. 特異点

18. 特異点

19. 特異点

20. 特異点

21. 特異点

22. 特異点

23. 特異点

24. 特異点

25. 特異点

26. 特異点

27. 特異点

28. 特異点

29. 特異点

30. 特異点

31. 特異点

32. 特異点

33. 特異点

34. 特異点

35. 特異点

36. 特異点

37. 特異点

38. 特異点

39. 特異点

40. 特異点

41. 特異点

42. 特異点

43. 特異点

44. 特異点

45. 特異点

46. 特異点

47. 特異点

48. 特異点

49. 特異点

50. 特異点

51. 特異点

52. 特異点

53. 特異点

54. 特異点

55. 特異点

56. 特異点

57. 特異点

58. 特異点

59. 特異点

60. 特異点

61. 特異点

62. 特異点

63. 特異点

64. 特異点

65. 特異点

66. 特異点

67. 特異点

68. 特異点

69. 特異点

70. 特異点

71. 特異点

72. 特異点

73. 特異点

74. 特異点

75. 特異点

76. 特異点

77. 特異点

78. 特異点

79. 特異点

80. 特異点

81. 特異点

82. 特異点

83. 特異点

84. 特異点

85. 特異点

86. 特異点

87. 特異点

88. 特異点

89. 特異点

90. 特異点

91. 特異点

92. 特異点

93. 特異点

94. 特異点

95. 特異点

96. 特異点

97. 特異点

98. 特異点

99. 特異点

100. 特異点

【関係者・対応依頼】

1. ExchangeおよびAzureActiveDirectoryでは環境関係者と各関係者2~3名にアクセス権があります。特にExchangeのログはログ収集により増加し、一部パッチ処理や監視処理の可能性があります。

2. SharePointでは半日程度にアクセス集中（13件）が確認され、監視・監視の自動化やパッチ処理が確認されています。また2件程度にもアクセス集中（13件）が確認され、監視・監視の自動化やパッチ処理が確認されています。

3. ログイン増加は10%と10%に増加しており、この関係者で多数ユーザーによるログイン増加・失敗も確認されています。特に10%に増加したログイン失敗は監視されており、不正アクセスの監視・監視の自動化やパッチ処理が確認されています。

4. 監視関係（22件~64件）のファイル操作やアクセスは大幅減少しましたが、年明け以降には一部ユーザーによる62件のファイル操作が確認されています。監視・監視の自動化やパッチ処理が確認されています。

5. 監視では12月4日を境に監視サービスでログ件数・ユーザー数増加が見られます。この日はExchange、AzureAD、SharePointなど監視サービスで監視対象の増加に伴って増加している可能性があります。

About AI-SOC for Microsoft 365

- Initial Setup Fee: ¥50,000
- Monthly Fee: ¥50 / month per user (Annual contract, minimum 20 users, with add-ons available in increments of 10 users)

Options:

- Log Analysis Portal
- Log Storage
- Log Analysis & Investigation (Advisory Services)

Related Article

How to Retrieve Microsoft 365 Audit Logs | An Explanation of Crucial Reasons to Keep Logs and Their Retention Periods

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

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>

Trademarks

Company names and product names mentioned herein are trademarks or registered trademarks of their respective owners.

For inquiries regarding this press release:
SecuAvail Inc. – Customer Support Center
TEL: +81-3-4405-6128 Email: contact@gr.secuavail.com

For IR inquiries (excluding those related to the products and services described in this press release)
SecuAvail Inc. – Corporate Planning Division, IR
TEL: +81-6-6136-0026 Email: ir@secuavail.com

【Explanation of Terms】

• **Log**

In a nutshell, a log is a "history or record" of system communications and operations. When computers, servers, or cloud services run, a digital footprint of "who, when, from where, and what they did" is automatically and continuously recorded as text data. It is much like a "flight recorder" on an airplane. In particular, an audit log refers to "critical operation records used for security checks and fraud prevention (auditing)."

• **SecuAvail's "AI-SOC"**

SecuAvail leverages its 25 years of experience as a security service provider, utilizing its extensive know-how in log analysis and alerting alongside the AI capabilities of LogStare, a proprietary product developed within its corporate group. Through this synergy, the company offers SecuAvail's "AI-SOC" series at an affordable price point, specifically designed for companies and organizations that are unable to appoint a dedicated IT system security administrator.

"AI-SOC for Microsoft 365"

Office applications have transitioned from traditional on-premises models—where software is installed directly onto owned hardware—to Microsoft 365, a cloud-based service. Organizations are leveraging features like Teams and the latest versions of Office apps to share files via cloud storage, thereby enhancing business productivity.

On the flip side, this shift introduces unique risks, such as unauthorized internal or external users gaining access to confidential information. Consequently, companies now require security measures and troubleshooting protocols that differ significantly from traditional on-premises environments.

In response to these challenges, SecuAvail launched "AI-SOC for Microsoft 365" late last year. This specialized SOC service leverages AI technology to analyze Microsoft 365 audit logs, detecting high-security-risk events and providing proactive alert notifications.

End