SecuAvail

Financial Results Summary

for the Three Months Ended June 30, 2026

(FY2027 First Quarter)

SecuAvail Inc. (Securities Code: 3042)

By delivering advanced, high-quality security services and a safe digital environment, we fulfill society's expectations as a core infrastructure provider in the increasingly networked world.

Consolidated Financial Highlights

■ **Net sales: ¥260.5 million (down 17.5% year on year)**

・Revenue from stock-type services remained at approximately the same level as in the corresponding period of the previous fiscal year.
・No large-scale software sales project was recorded this quarter, unlike in the first quarter of the previous fiscal year.
・Performance is progressing in line with the full-year forecast.
Business negotiations are proceeding smoothly, and as in past years, sales of public-sector software—typically recorded toward the fiscal year-end and recognized with zero inventories—are expected to increase significantly, contributing to improved profitability.

■ **Operating loss: ¥52.5 million (compared with operating profit of ¥39.7 million in the same period of the previous fiscal year)**)

・¥20 million in upfront expenses related to existing software
・¥4.8 million increase in advertising and promotion expenses to strengthen marketing activities
・¥12.7 million increase in personnel expenses

■ **Loss attributable to owners of parent: ¥53.7 million**

Figures in Millions of Yen / %	1Q FY2025 Two Years Ago	1Q FY2026 Previous Year	1Q FY 2027 Current Year
Net Sales	**229.1**	**315.7**	**260.5**
Operating Profit (Loss) *Operating Margin*	**(31.6)** *(13.8%)*	**39.7** *12.6%*	**(52.5)** ***(20.2%)***
Ordinary Profit (Loss) *Ordinary Profit Margin*	**(31.6)** *(13.8%)*	**39.8** *12. 6 %*	**(51.9)** *(20.0%)*
Profit (Loss) Attributable to Owners of Parent *Net Profit Margin*	**(32.9)** *(14.4%)*	**28.6** *9.1%*	**(53.7)** *(20.6%)*

Segment Overview

■Information Security Business

- Net sales: ¥194.7 million (down 23.9% year on year)
- Large-scale software sales occurred in the previous fiscal year.
- Segment loss: ¥22.0 million
- Strengthened advertising and promotional activities for the AI-SOC series
- Upfront expenses incurred for existing software

■Human Resource Services Business

- Net sales: ¥65.7 million (up 10.2% year on year)
- Segment profit: ¥7.6 million
- Staffing assignments progressed smoothly

Segment Overview			
＜Information Security Business＞			
Figures in Millions of Yen	1Q FY2025 Two Years Ago	1Q FY2026 Previous Year	1Q FY 2027 Current Year
Net sales	182.1	256.1	194.7
Segment Profit(loss)	14.0	74.9	(22.0)
＜Human Resource Services Business＞			
Figures in Millions of Yen	前々第1四半期	前第1四半期	当第1四半期
Net sales	47.0	59.6	65.7
Segment Profit	1.1	8.8	7.6

SecuAvail

Changes in the Business Environment

Expansion of Business Opportunities

■ **Strengthening of Economic Security (Growing importance of domestic solutions)**

- The international payment network outage has accelerated efforts to enhance the resilience of critical infrastructure.

■ **Progress in Government Cloud Migration (Growing importance of domestic solutions)**

- Although the deadline has been extended, concentration of workloads among specific service providers continues.
- Digital sovereignty and integrated management of communication logs have become major challenges.

■ **Increasing Demand for SOC Operation Support**

- Cloud security is becoming increasingly sophisticated.
- The shortage of personnel capable of handling these advanced requirements is becoming more severe.

Growth Potential of the “AI-SOC” Series

■ **Rapid increase in brand recognition driven by intensive promotion**

・Received high practical evaluations at Interop Tokyo 2026

・Number of business leads increased significantly after Interop Tokyo 2026

■ **Strong potential for a major earnings uplift through solid conversion of the business pipeline**

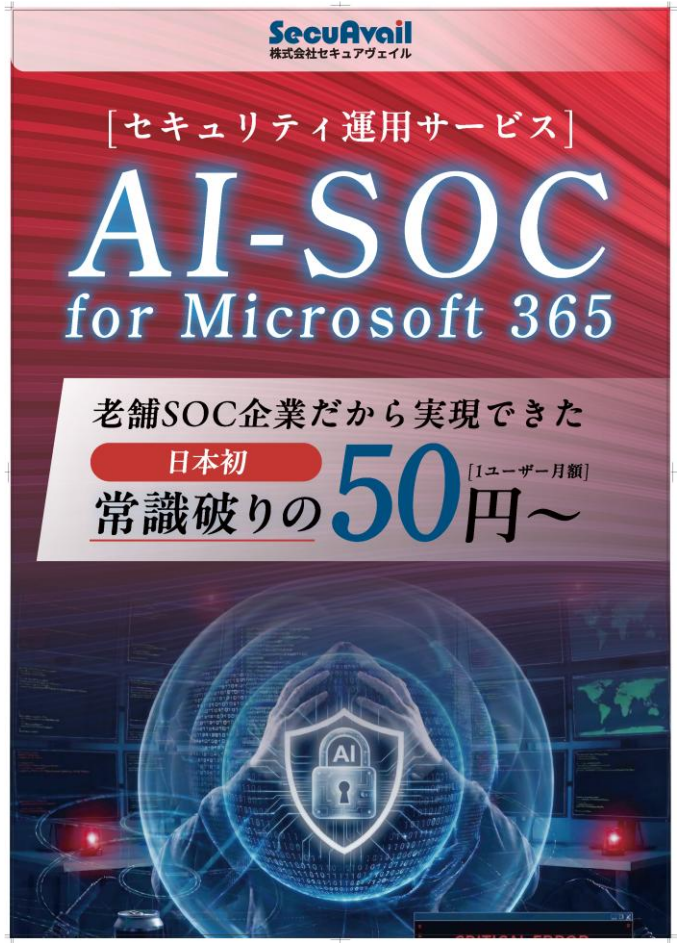
・AI-SOC projects tend to be highly profitable and have a broad market reach

・Successful conversion of these opportunities could lead to a substantial increase in earnings

■ **Favorable tailwinds from Government Cloud migration and the SCS evaluation framework (strength of fully domestic, proprietary development)**

・Standardization of log management and monitoring is progressing

・High compatibility with our services, creating potential for further expansion in adoption needs



Glossary of Terms

Government Cloud

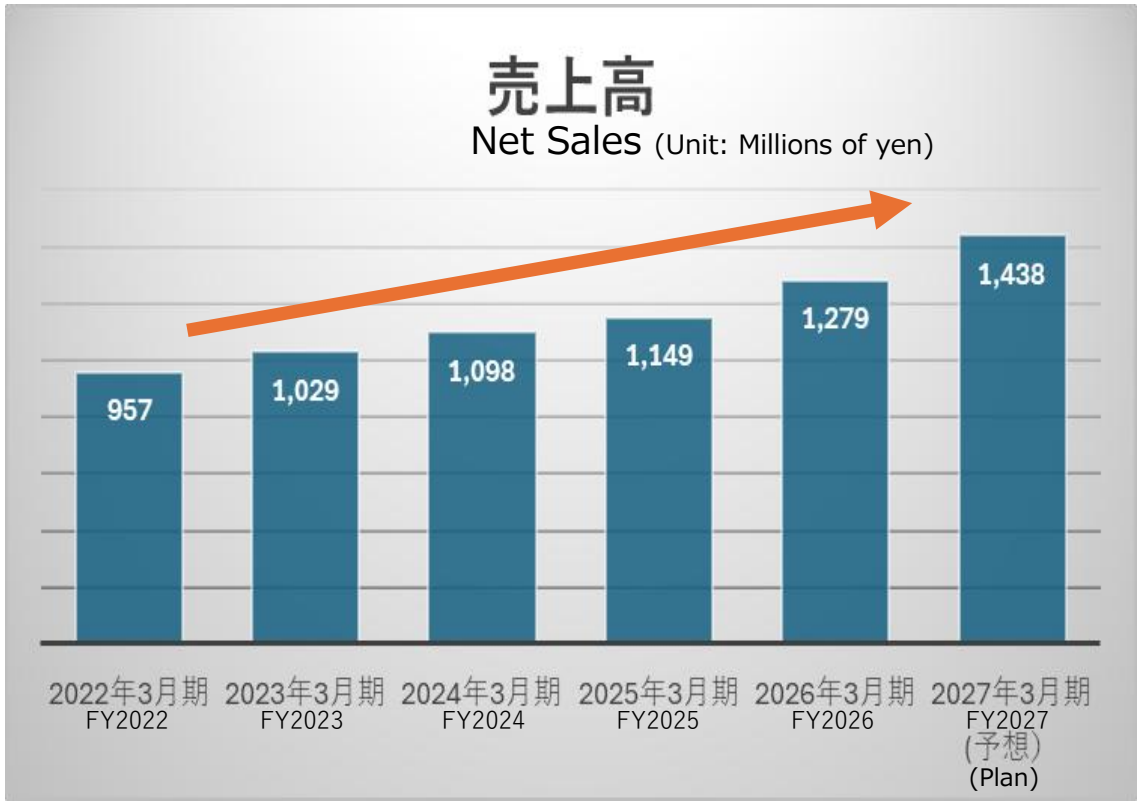
The Government Cloud is a shared IT infrastructure (cloud platform) developed under the leadership of the Digital Agency for use by national and local government entities. By standardizing systems that were previously managed individually by municipalities and organizations across Japan, it aims to reduce costs, enhance security, promote the digitalization of administrative procedures, and facilitate smooth data collaboration among local governments.The government aims to complete approximately 90% of the overall migration by the end of fiscal year 2026.In the initial phase, Government Cloud providers were dominated by major U.S. IT companies (Amazon, Google, Microsoft, and Oracle), raising concerns related to economic security and foreign-exchange risks. Recently, the fully domestic provider Sakura Internet has been selected as a Government Cloud vendor.Municipalities and organizations are required to perform log management for system operations, including monitoring and verification for audit purposes.

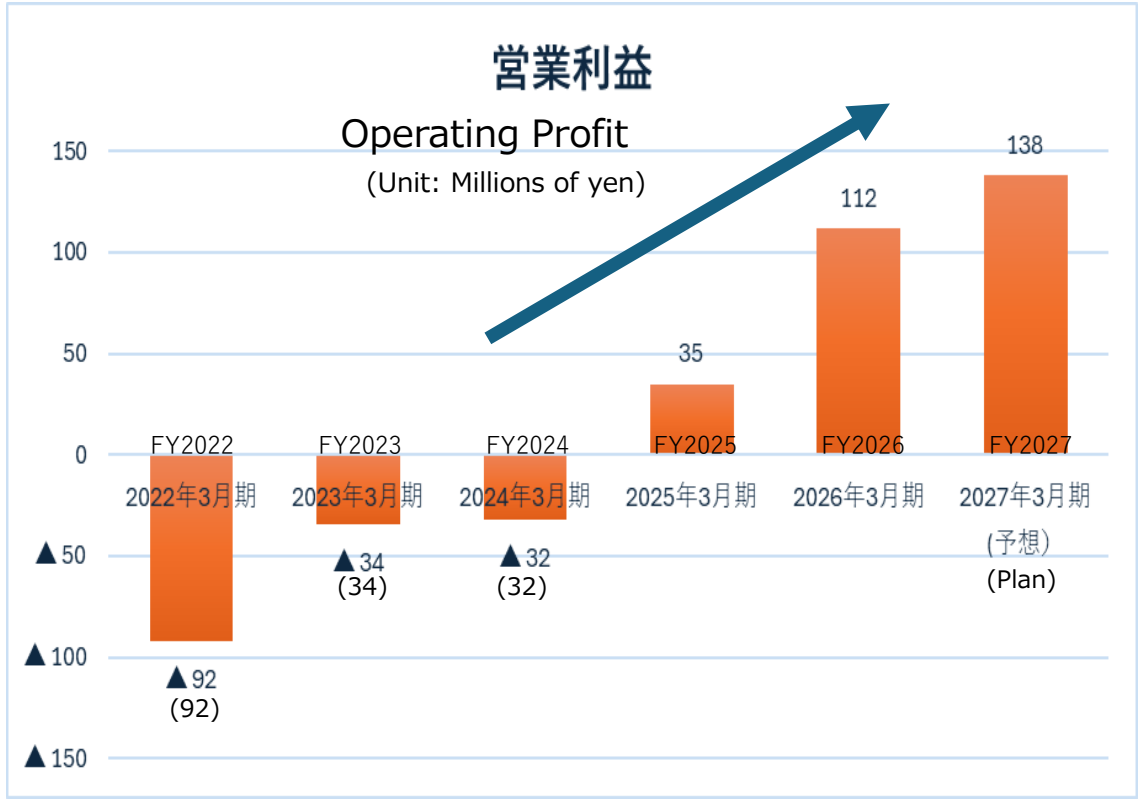
SCS Evaluation System

The SCS Evaluation System is a security assessment framework led by the Ministry of Economy, Trade and Industry (METI) designed to strengthen supply chains across industries such as the automotive sector—from raw material procurement to final sales.It provides an easy-to-understand rating of a company’s cybersecurity measures using a “star-based” scale.Although not legally mandated, it is expected that business partners will increasingly require companies to achieve a rating of three stars or higher.Operation of the system is scheduled to begin by the end of fiscal year 2026.In the latter half of 2025, companies such as Askul, Asahi Group Holdings, and Nichirei’s refrigerated logistics division suffered major disruptions to economic activity due to ransomware and other cyberattacks, highlighting the urgency of strengthening supply-chain security.

Consolidated Performance Trends

Full-Year Outlook (Progressing as Planned)





SecuAvail

Key Strategic Initiatives

- Partner Expansion Centered on the “AI-SOC” Series
- Revitalization of Existing Partners
- Enhancement of Engagement with Existing Customers
- Strengthening Sales of LogStare Products
- Continued Deployment of Advertising and Marketing Strategies for the “AI-SOC” Series

“AI-SOC” Series

25年にわたるPAシリーズのSOCノウハウをAI化
リスクの高い通信を迅速に検知・通知します

AI-SOC for PaloAlto

powered by NetStare

『AI-SOC for PaloAlto』はPA-400シリーズの通信のログを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する次世代のSOC（Security Operation Center）サービスです。
SOC黎明期から25年にわたって培ったセキュアヴェイルのSOCノウハウをAIに継承し、不正アクセスや不審な通信による情報漏えいの可能性を検知してアラートします。

こんな異常をアラートします
- ✓ ウィルス感染の疑いがある端末
- ✓ フィッシングサイトへのアクセス
- ✓ VPNアカウントの不正利用の予兆
- ✓ 管理者アカウントの不正利用の予兆

※サービス提供対象は、PA-410, 415, 440, 445, 450となります
※アラート内容はご利用中のライセンスやポリシーにより異なることがございます

24時間365日ネットワークを監視
リスク兆候をＡＩが継続的に分析し
必要なタイミングで通知します

- 通過するすべての通信のログを分析しリスクを可視化
- いざという時は24/365の有人窓口への質問もOK
- より高度なマネージドサービス(SOCサービス)への拡張も可

歴25年の豊富なSOCノウハウでFortiGateを監視
不審な通信をいち早くアラートします

AI-SOC for FortiGate

powered by NetStare

『AI-SOC for FortiGate』はFortiGateの通信のログを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する次世代のSOC（Security Operation Center）サービスです。
SOC黎明期から25年にわたって培ったセキュアヴェイルのSOCノウハウをAIに継承し、不正アクセスや不審な通信による情報漏えいの可能性を検知してアラートします。

こんな異常をアラートします
- ✓ ウィルス感染の疑いがある端末
- ✓ フィッシングサイトへのアクセス
- ✓ VPNアカウントの不正利用の予兆
- ✓ ブロックされていない不正アクセス

※FortiGate 30, 40, 50の各シリーズを対象としたサービスです
※アラート内容はご利用中のFortiGateのライセンスやポリシーによります

人の目より速く、広く、深く
ＡＩ－ＳＯＣがネットワーク通信の
セキュリティリスクを即キャッチ

- 月額9,800円、AI-SOCだから実現できるサービス価格
- いざという時は24/365の有人窓口への質問もOK
- より高度なFortiGateマネージドサービスへの拡張も可

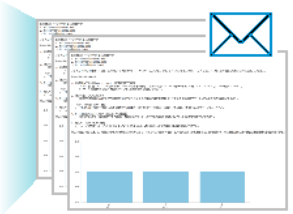
Microsoft 365の“運用上のリスク”をAIが監視
クラウド時代の新しいSOCサービス

AI-SOC for Microsoft 365

powered by NetStare

『AI-SOC for Microsoft 365』はMicrosoft 365の利用状況をAIが監視し、セキュリティリスクの高い事象を検知してアラートする次世代のSOC（Security Operation Center）サービスです。
SOC黎明期から25年にわたって培ったセキュアヴェイルのログ分析のノウハウをAIに継承し、Microsoft 365の監査ログからアカウント乗っ取りの可能性、外部からの不正アクセスによる侵入、アクセス権の不備による情報流失のリスクなどを検知してアラート通知します。

- 従業員のアカウントが不正使用された!?
- 重要ファイルが世界中に公開された!?
- 退職者が重要ファイルをダウンロードした!?
- 管理者権限を悪用された!?



人手では見逃しがちなリスクを
ＡＩ－ＳＯＣが代わりに監視
クラウド活用の安心と効率が向上します

- 1ユーザー月額50円、AI-SOCだから実現できるサービス価格
- いざという時は24/365の有人窓口への質問もOK
- より高度なSOCやログ分析サービスに柔軟に拡張できる

Measures to Comply with the SCS Evaluation System