

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)	(31.6)	39.7	(52.5)
<i>Operating Margin</i>	(13.8%)	12.6%	(20.2%)
Ordinary Profit (Loss)	(31.6)	39.8	(51.9)
<i>Ordinary Profit Margin</i>	(13.8%)	12.6%	(20.0%)
Profit (Loss) Attributable to Owners of Parent	(32.9)	28.6	(53.7)
<i>Net Profit Margin</i>	(14.4%)	9.1%	(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

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

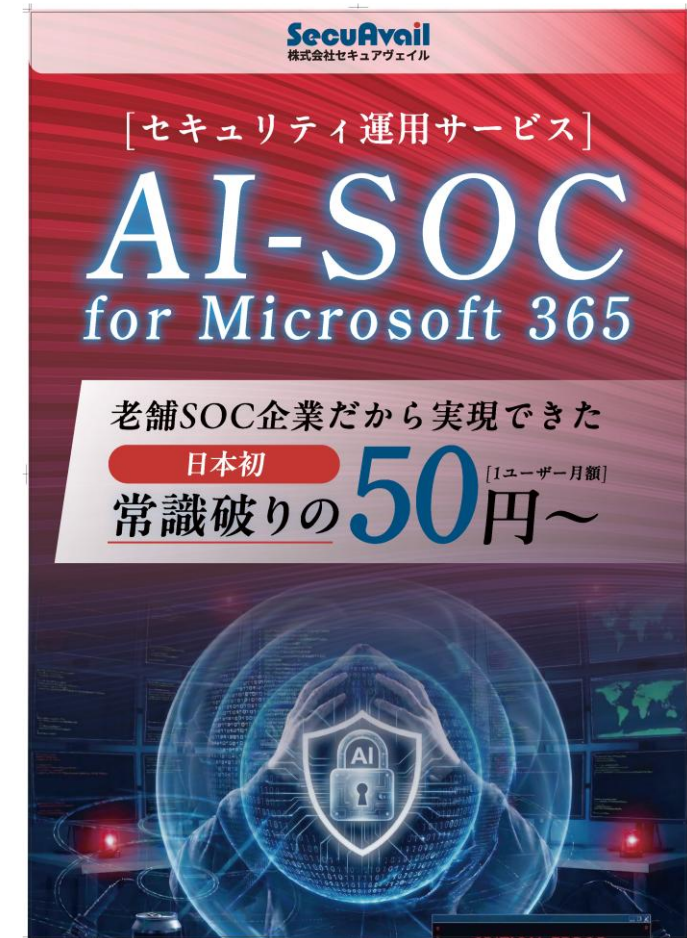
- Received high practical evaluations at Interop Tokyo 2026
- Number of business leads increased significantly after Interop Tokyo 2026

■ 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

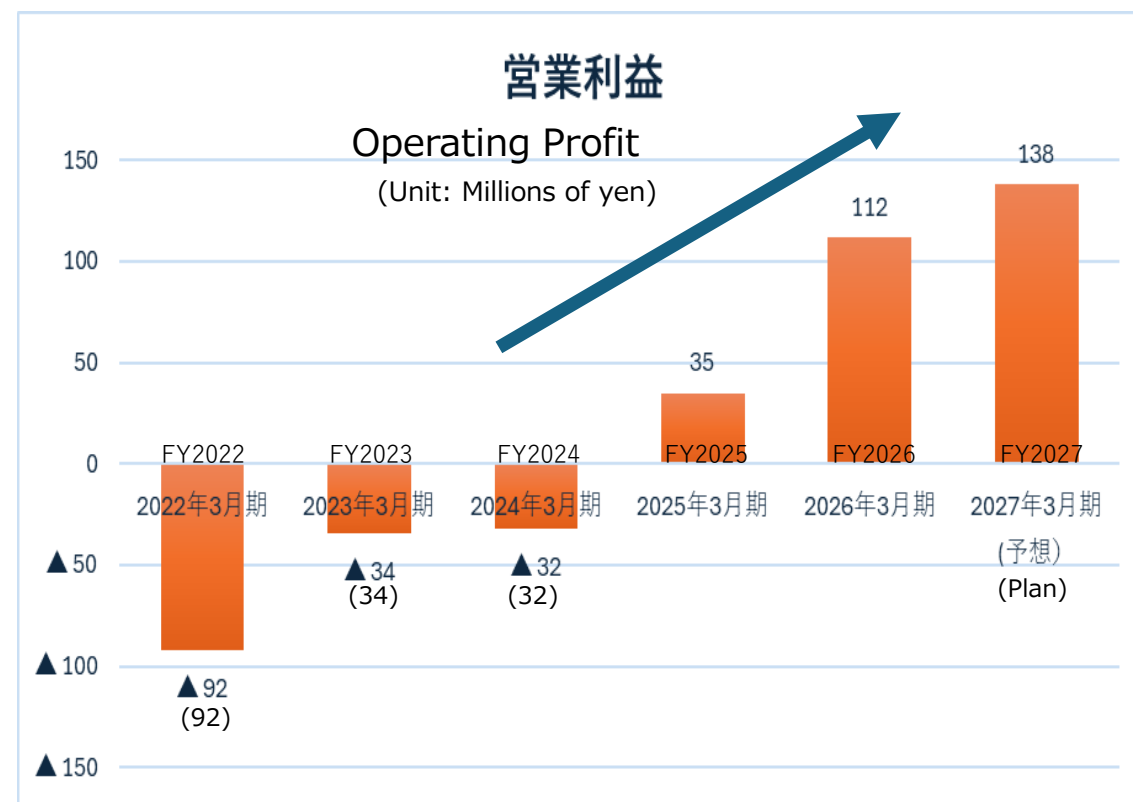
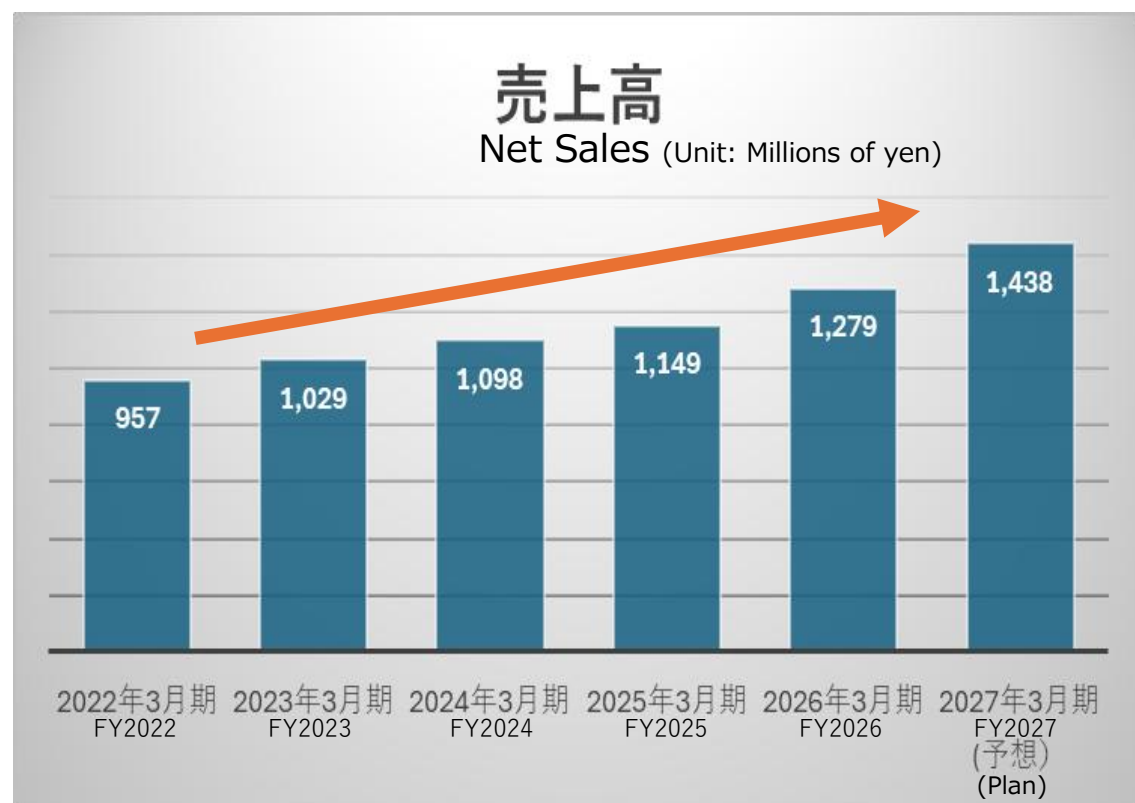
The Government Cloud is a shared IT infrastructure (cloud platform) developed under the leadership of the Digital Agency for use by national and local government entities. By standardizing systems that were previously managed individually by municipalities and organizations across Japan, it aims to reduce 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)



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

Microsoft365 運用上のセキュリティリスク、AIが検知から対応方法まで導く

新登場

AI-SOC for Microsoft 365

老舗SOC企業だから実現できた“常識破り”の月額50円～[1ユーザー]

代理店も
募集中！

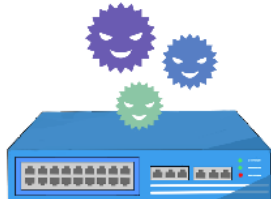
“AI-SOC” Series

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ウェイルの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場合がございます

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ウェイルの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異なります

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

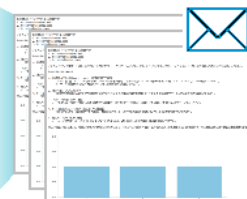
『AI-SOC for Microsoft 365』はMicrosoft 365の利用状況をAIが監視し、セキュリティリスクの高い事象を検知してアラートする次世代のSOC (Security Operation Center) サービスです。SOC黎明期から25年にわたって培ったセキュアウェイルのログ分析のノウハウをAIに継承し、Microsoft 365の監査ログからアカウント乗っ取りの可能性、外部からの不正アクセスによる侵入、アクセス権の不備による情報漏失のリスクなどを検知してアラート通知します。

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

製造業・中堅企業向け

経済産業省 情報セキュリティサービス基準 登録事業者

NetStore

SCS認証に必要なセキュリティ監視・運用を、SOCが24時間担います。

経済産業省が推進するSCS評価制度。★3・★4取得に求められるセキュリティ監視・ログ管理・インシデント対応を、NetStore SOCサービスが24時間365日代行します。

NetStore UTM 境界防御 SOCサービス

ネットワークの境界を、SOCが24時間守ります。

▶ ネットワークの脅威から保護するセキュリティマネジメント、
▶ 安定したシステム稼働を継続するシステムマネジメントを提供

NetStore EDR エンドポイント SOCサービス

エンドポイントへの侵入を、SOCが検知・封じ込めます。

▶ EDR監視・脅威ハンティング・インシデント対応をSOCが代行（MDR）
▶ 初期チューニングから自動隔離まで、SOCが一気通貫でサポート

SCS評価制度とは

経済産業省が推進する、サプライチェーン全体のセキュリティ強化を目的とした評価・認証制度。★3は基礎的対策、★4は高度な対策の実施が求められます。今後は、製造業を中心に、大手メーカーや発注元から取引先への認証取得要求が急速に広がり、認証の有無がビジネス継続に直結する可能性があります。

SCS評価制度の目的と期待される効果

出典：経済産業省

受注企業への効果	発注企業への効果	社会全体への効果
- リスク低減・費用対効果の可視化 - 対策実施の説明責任・信頼性向上 - セキュリティサービス選択肢の拡大	- 取引先のセキュリティ状況の把握・適正化 - サプライチェーンに起因するリスク低減	- サイバーレジリエンスの強化 - 取引コストの効率的な低減 - セキュリティ市場の拡大・競争力向上

SCS評価制度対応で多くの企業が直面する課題

① 専門人材不足

24時間のセキュリティ監視体制を自社で構築・維持するのは、現実的ではありません。脅威の高度化に対し、社内リソースだけでは対応には限界があります。

NetStore がこの課題を解決します →

② 運用・対応の遅れ

UTMのアラートや脆弱性情報が出ていても内容を判断できる担当者がおらず、ファームウェア更新・設定変更の対応が後手に回るケースが多くあります。

NetStore がこの課題を解決します →

③ エンドポイント脅威の高度化

エンドポイントへの攻撃は巧妙化しており、EPP・EDRを導入し、正しく運用する必要があります。継続的な監視と、インシデント発生時の迅速な対応・封じ込めが不可欠です。

NetStore がこの課題を解決します →

NetStore SOCサービス ご提供イメージ

お客様 監視対象

セキュアウェルSOC

お客様への提供

お客様 監視対象

セキュアウェルSOC

お客様への提供

製造業・中堅企業向け

LogStare

SCS★3・★4認証取得を、ログ監視から支援します。

経済産業省が推進するSCS評価制度（サプライチェーン強化に向けたセキュリティ対策評価制度）★3・★4取得に求められるログ収集・継続監視・証跡管理を、LogStareがひとつの基盤でカバーします。

SCS評価制度とは

経済産業省が推進する、サプライチェーン全体のセキュリティ強化を目的とした評価・認証制度。★3は基礎的対策、★4は高度な対策の実施が求められます。今後は、製造業を中心に、大手メーカーや発注元から取引先への認証取得要求が急速に広がり、認証の有無がビジネス継続に直結する可能性があります。

SCS評価制度の目的と期待される効果

出典：経済産業省

受注企業への効果	発注企業への効果	社会全体への効果
- リスク低減・費用対効果の可視化 - 対策実施の説明責任・信頼性向上 - セキュリティサービス選択肢の拡大	- 取引先のセキュリティ状況の把握・適正化 - サプライチェーンに起因するリスク低減	- サイバーレジリエンスの強化 - 取引コストの効率的な低減 - セキュリティ市場の拡大・競争力向上

SCS評価制度対応で多くの企業が直面する課題

① 対策の実施・記録・経営報告、すべてがセットで求められる

SCS評価では、ログの取得に加え、定期的な分析・モニタリング、記録の保管、年1回以上の経営層への報告まで継続的な運用が義務付けられています（要求事項 1-4-1-1、4-4-3-3 等）。証跡を伴う運用体制の整備が評価の前提となります。

② 情シス・セキュリティ担当者の人手が、そもそも足りない

クラウド・SaaSの普及でICT環境が複雑化する一方、情報システム部門の人員は慢性的に不足しています。SCS対応に求められるログの監視・分析・レポートには、業務効率化と専門知見を備えた体制が不可欠です。

③ 取引先からの認証要求は、待てない

「SCS認証を取得してほしい」という大手からの要求が急増しています。何から手をつけ、いかに分からないまま対応が後手に回れば、ビジネス機会の損失に直結します。

LogStareが描く、SCS対応ログ管理の全体像

監視対象 → LogStare Collector で収集・保管 → LogStare Reporter で分析 + LogStare M365 でクラウド特化監査

監視対象

LogStare Collector

LogStare Reporter

LogStare M365

LogStare M365

あらゆるセキュリティ製品のログ解析に対応

Palo Alto Networks / FORTINET / F5 / SONICWALL / WatchGuard / AWS / A10 / CISCO / I-FILTER / CrowdStrike / Falcon / LANSCOPE on-premises / LANSCOPE Endpoint Manager / yara / Windows Server(Eventlog) / Soliton OneGate / Microsoft 365 / Box / Google Workspace ほか、対応製品についてはお問い合わせください。

▼ SCS要求事項対応の詳細は裏面をご覧ください。