

2027年3月期 第1四半期 決算説明サマリー

株式会社セキュアヴェイル
2026年4月1日-2026年6月30日

お客様に最適かつ高品質のセキュリティサポートサービスと安全なセキュリティ環境を提供することで、「ネットワーク社会」におけるインフラの担い手として、社会の要請に応える。

連結業績ハイライト

■ 売上高：260.5百万円（前年同期比▲17.5%）

- ・ストック型サービスは前年並み
- ・前年同期の大型ソフトウェア販売案件が非発生
- ・通期見込み通りに業績推移

（商談案件は順調。例年、期末時等に棚卸資産ゼロの公共向けソフトウェア販売が急増、収益向上）

■ 営業損失：52.5百万円（前年同期は39.7百万円の利益）

- ・既存ソフトウェアの先行費用：20百万円
- ・販促強化の広告宣伝費：+4.8百万円
- ・人件費：+12.7百万円

■ 四半期純損失：53.7百万円

単位：百万円（%）	前々第1四半期	前第1四半期	当第1四半期
売上高	229.1	315.7	260.5
営業利益 (利益率)	△31.6 (△13.8%)	39.7 (12.6%)	△52.5 (△20.2%)
経常利益 (利益率)	△31.6 (△13.8%)	39.8 (12.6%)	△51.9 (△20.0%)
当期純利益 (利益率)	△32.9 (△14.4%)	28.6 (9.1%)	△53.7 (△20.6%)

セグメント別状況

■情報セキュリティ事業

- ・売上高：194.7百万円（▲23.9% 前期大型ソフトウェア販売案件）
- ・セグメント損失：22.0百万円
- ・「AI-SOC」広告宣伝を強化
- ・既存ソフトウェアの先行費用

■人材サービス事業

- ・売上高：65.7百万円（+10.2%）
- ・セグメント利益：7.6百万円
- ・派遣案件が順調に推移

セグメント別状況			
<情報セキュリティ事業>			
	前々第1四半期	前第1四半期	当第1四半期
単位：百万円			
売上高	182.1	256.1	194.7
セグメント利益	14.0	74.9	△22
<人材サービス事業>			
	前々第1四半期	前第1四半期	当第1四半期
単位：百万円			
売上高	47.0	59.6	65.7
セグメント利益	1.1	8.8	7.6

事業環境の変化

ビジネスチャンス増大

■ 経済安全保障の強化が急務（純国産の重要度↗）

- ・ 国際的な決済ネットワーク障害を契機に、重要インフラのレジリエンス向上が加速

■ ガバメントクラウド移行の進展（純国産の重要度↗）

- ・ 期限は延長も、特定事業者への集中が進行
- ・ デジタル主権・通信ログ統合管理が課題

■ SOC運用支援の需要増加

- ・ 高度化するクラウドセキュリティ
- ・ 対応可能な人材不足が深刻化

「AI-SOC」シリーズの成長ポテンシャル

■ 集中的なプロモーションにより認知度が急速に向上

- ・ Interop Tokyoで実用面で高評価
- ・ 展示会後の商談リードが大幅増加

■ 商談パイプラインの“確実な刈り取り”で収益飛躍の可能性

- ・ AI-SOCは高収益案件が多く、裾野も広い
- ・ 成約に至れば 収益が大きく飛躍する可能性

■ ガバメントクラウド・SCS評価制度という追い風（純国産独自開発の強み）

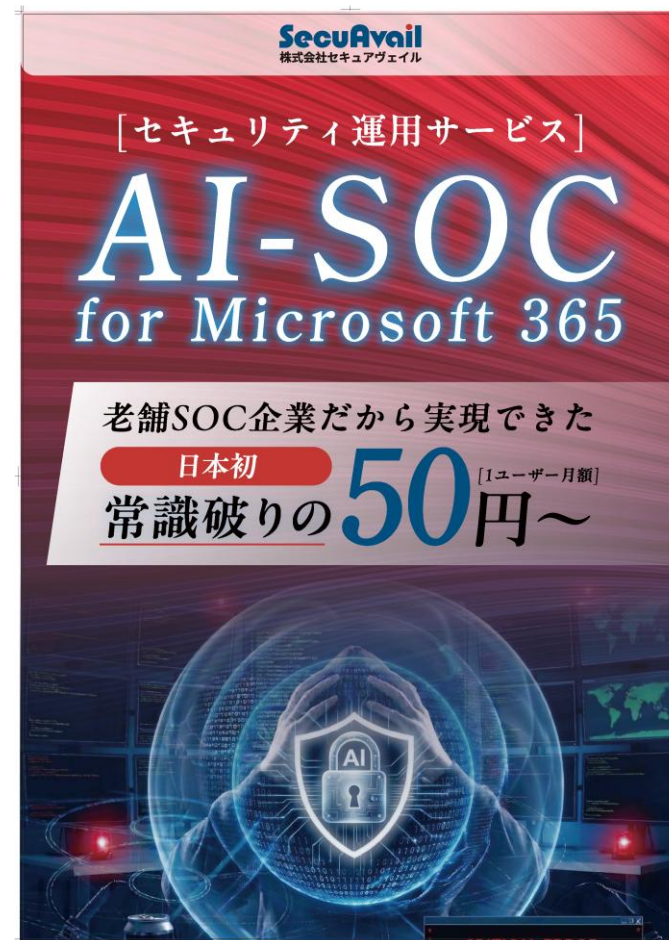
- ・ ログ管理・監視の標準化が進む
- ・ 当社サービスとの親和性が高く、導入ニーズ拡大の可能性

ガバメントクラウド

デジタル庁が主導して整備する、国や地方自治体が共同で利用する共通のITインフラ（クラウド基盤）。これまで全国の自治体、組織が個別管理していたシステムを共通化することで、コスト削減、セキュリティ向上、行政手続きのオンライン化、自治体間のスムーズなデータ連携を推進する仕組み。政府は2026年度末に全体の9割完了を目指している。初期に選定されたガバメントクラウドは米国IT大手（Amazon, Google, Microsoft, Oracle）に占められていたため、安全保障や円安等のリスクがある。最近純国産のさくらインターネットがガバメントクラウドに選定された。各自治体及び組織は、システム操作の「ログ管理」を行い、監視・証明（監査）の必要がある。

SCS評価制度

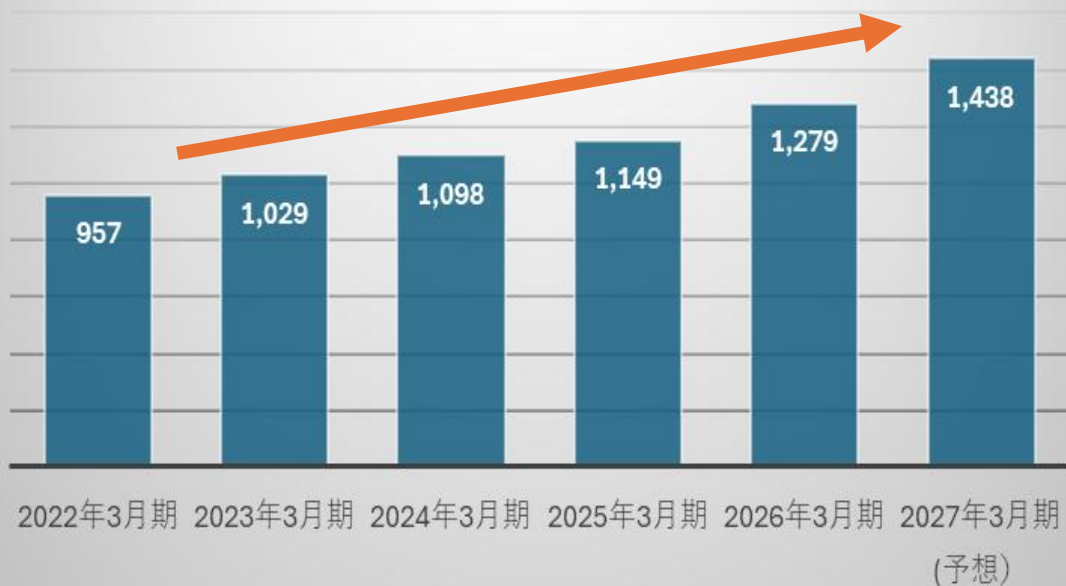
経済産業省が主導する、自動車産業等で原材料調達から販売までの一連のつながりであるサプライチェーン強化に向けたセキュリティ対策評価制度で、企業のサイバーセキュリティ対策の強さを「星の数」でわかりやすく格付けする。法規制はないものの取引先から☆3以上の評価を要求される状況が推定される。2026年度末の運用開始が示されている。2025年後半からアスクル、アサヒグループホールディングスや冷蔵物流のニチレイでは、ランサムウェア（身代金ウィルス）等の攻撃で経済活動が止まる大打撃を受けている。



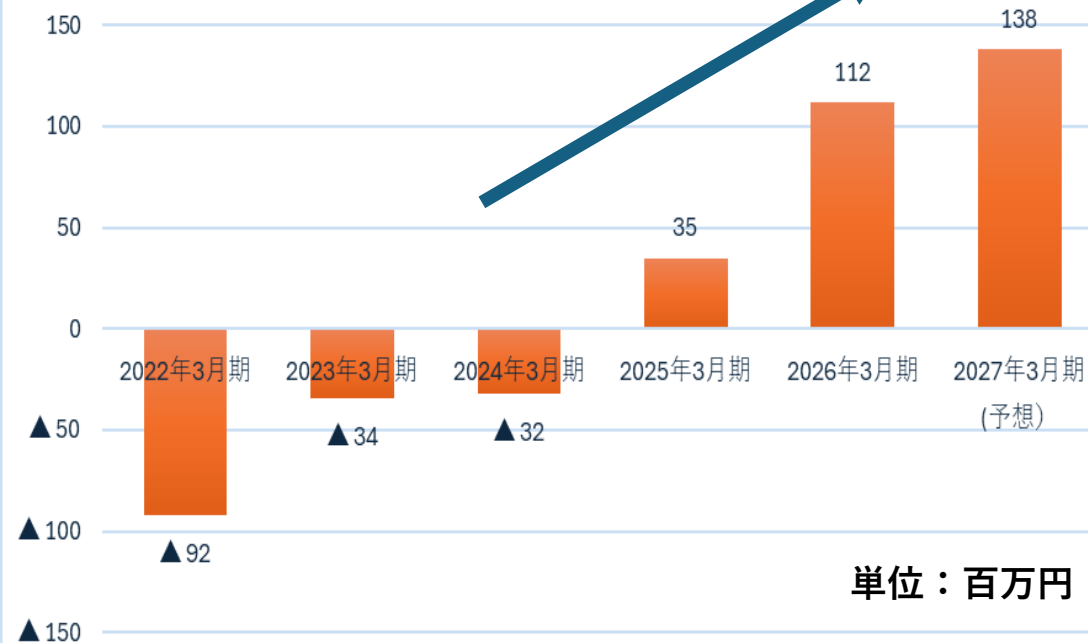
連結業績推移

通期見通し（計画通りに推移）

売上高 単位：百万円



営業利益



重点施策

- 「AI-SOC」シリーズを軸としたパートナー開拓
- 既存パートナーの活性化
- 既存顧客への関与度向上
- LogStare製品の販売強化
- 「AI-SOC」シリーズの広告マーケティング戦略を継続展開

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シリーズ

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

SCS評価制度への対応

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 境界防衛 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。

② 運用・対応の遅れ

UTMのアラートや脆弱性情報が出てから内容を確認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。

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

EPP/EDR サービス基盤

Log

Log収集

Log転送

Log分析基盤

24×365

緊急連絡

脅威検知アラート

レポート配信

マネージドサービス

セキュアウェルSOC

24×365監視

セキュリティアラート通知

インシデント対応支援

UTMの障害支援/設定変更/ファームウェアバージョンアップ

ヘルプデスク

運用報告会

SOCレポート/最終レポート

お客様への提供

24×365監視

セキュリティアラート通知

インシデント対応支援

UTMの障害支援/設定変更/ファームウェアバージョンアップ

ヘルプデスク

運用報告会

SOCレポート/最終レポート

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。何から手をつければいいのか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

- クラウドSaaS: M365/Box/Google Workspace
- セキュリティ製品: FW・UTM・IDS/IPS, WAF/Proxy/EDR
- 認証サーバ: CASB/SWG
- 業務サーバ・端末

LogStare Collector

ログ収集モジュール

対象デバイス

セキュリティ製品

認証サーバなど

ログ収集・保管サーバ (Linux/Windows)

ログ暗号化/圧縮保管

LogStare Reporter

データ連携

DWH (データウェアハウス)

ログ解析・機械学習

レポート

アラート

LogStare M365

クラウド特化監査

連携

OpenAI API

- ① AI分析検知アラート
- ② AI分析傾向レポート
- ③ ボーカルレポートAI分析機能

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。

20260805