JETRO
Japan External Trade Organization

イスラエル・マンスリー・トレンド

Israel Monthly Trends

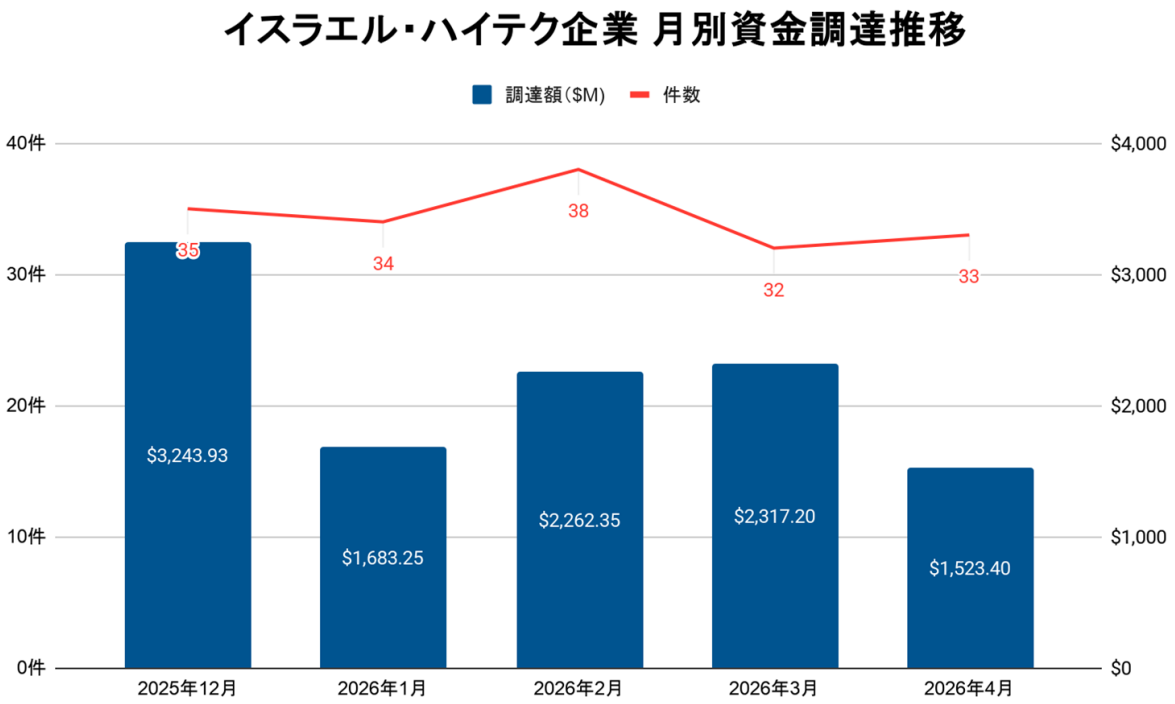
2026年5月

目次

本レポートは、「スタートアップエコシステムが発達しているイスラエルで、どのようなイノベーションが起こっているかを伝える情報提供を目的として作成されています。本レポートが日系企業の戦略策定の一助になれば幸いです。

1．イスラエルの現在の状況_5月

2026年3月16日から4月15日におけるスタートアップへの資金調達動向は、案件数が33件で、調達額の合計は15億2,340万ドルであった。前期（2026年2月16日から3月15日）の資金調達（32件・23億1,720万ドル）に比べて、案件数は微増したが、調達総額は34.3%減少した。



出典：IVC Data（2026年4月16日アクセス）を基にJakore作成

本レポートの毎月のデータ収集期間は、前々月16日から前月15日までとなる。

2026年3月中旬から2026年4月中旬にかけては、エンタープライズソフトウェア・インフラ分野が市場を牽引した。Pagayaがデットファイナンスで5億ドル、Oasis Securityがセカンドラウンドで1億2,000万ドル、ScaleOps社がサードラウンドおよびセカンダリーディールで計1億3,000万ドルを調達し、同分野における大型案件が市場全体の資金流入を押し上げた。加えて、ネットワークインフラ分野ではNoTrafficがサードラウンドで9,000万ドルを調達し、分野横断的にも大型資金調達が目立つ期間となった。

2．今月の注目テーマ：サイバーセキュリティ分野のエージェント型AI

サイバーセキュリティ分野のエージェント型AIとは、観測（Observe）、状況把握（Orient）、判断（Decide）、実行（Act）から成るOODAループを継続的に回しながら、自律的に脅威調査や対応を行う人工知能である。従来の人間支援型AIとは異なり、API連携による遮断・隔離・スキャンなどを自律実行できる点に特徴がある。日本では人材不足や重要インフラ防御への対応策として期待されている。

主要な取り組みと成果

イスラエルでは、エージェント型AIを「自律型サイバーセキュリティ基盤」として提示している。従来のコパイロット型AIから、自律的に調査・分析・対応を行うエージェント型システムへの転換が進んでおり、人材不足や高度化するサイバー攻撃への対応策として位置付けられている。また、自律型SOC、Non-Human Identity管理、IoT・OT防御などを統合した「エージェント型プラットフォーム」への移行も進んでいる。

こうした分野では、投資と技術開発が継続的に拡大している。2024～2025年には、イスラエルのサイバーセキュリティ系スタートアップが高水準の資金調達を維持したとされ、多くの企業は研究開発拠点をイスラエル国内に置きつつ、営業・事業開発拠点を米国に配置する「スプリット・シード」戦略を採用している。CyeraやArmisへの大型投資は、個別機能型ではなく、包括的かつ拡張性の高い基盤型アーキテクチャへの市場期待の高まりを示している。

具体的な取り組みとして、Huntersはセキュリティデータ相関分析を自動化する自律型脅威ハンティングを展開し、Torqはマルチエージェント型SOC運用による自律対応を推進している。Oasis SecurityはAIエージェント向けアクセス管理を提供し、Cyeraは生成AIを活用したデータ文脈理解によって機微情報の保護を行っている。また、SternumはIoT機器内部へのランタイム保護実装を進めているほか、Cylusは鉄道向け異常検知、Upstream Securityはコネクテッドカー向け脅威検知を展開している。これらの企業は、重要インフラやモビリティ分野を含む実運用環境への導入を見据えた技術開発を進めている。

今後の展望

今後は、サイバーセキュリティ市場が個別機能型ソリューションから「エージェント型プラットフォーム」へ移行する見込みが示されている。CyeraやArmisへの大型投資は、包括的かつ拡張性の高い基盤型アーキテクチャへの市場期待の高まりを示している。また、Tier-1およびTier-2のセキュリティ運用業務を自動化可能なプラットフォームへの投資が拡大している。さらに、多くの企業は研究開発拠点をイスラエル国内に維持しつつ、営業・事業開発を米国市場へ展開する「スプリット・シード」戦略を採用している。今後は、OT（Operational Technology）、IoT、モビリティ、重要インフラ分野を含む実運用環境への導入がさらに進み、イスラエル企業によるエージェント型AIは、次世代サイバーセキュリティ基盤の中核技術として存在感を高めつつある。

出典：https://www.prnewswire.com/news-releases/oasis-security-launches-agentic-access-management-the-first-identity-solution-built-for-ai-agents-302619375.html

3．サイバーセキュリティ分野のエージェント型AIの協業事例紹介

●Cyera × Microsoft（2025年11月）

CyeraはMicrosoftと連携し、「Microsoft Copilot Studio」向けAIエージェントのデータセキュリティ強化を進めている。CyeraのAI Security技術を活用し、AIエージェントによる機密情報アクセスやデータ再出力をリアルタイムで可視化・制御することで、安全な生成AI運用を支援している。また、AIガバナンスやデータ保護の強化にも活用されている。

参考：https://www.cyera.com/blog/securing-ai-agents-with-cyera-and-microsoft-copilot-studio

Cyera（https://www.cyera.com/）
クラウド、SaaS、オンプレミス、生成AI環境にまたがるデータセキュリティ基盤を提供するイスラエル企業である。AIを活用したデータ文脈理解、DSPM、機密情報保護を行うAI Securityプラットフォームを展開している。

●C2A Security × Daimler Truck Holding（2024年3月 ）

Daimler Truckは、C2A Securityの「EVSec」を採用し、車両開発・運用におけるサイバーセキュリティ運用を強化している。EVSecは、AIと自動化を活用し、TARA、自動リスク分析、脅威インテリジェンス、UN R155対応を効率化する。Daimler Truck社は、同プラットフォームを全8ブランドへ展開し、SDV向けサイバーセキュリティ管理を進めている。

参考：https://c2a-sec.com/c2a-securitys-evsec-risk-management-and-automation-platform-gains-traction/

C2A Security（https://c2a-sec.com/）
ソフトウェア定義車両（SDV）やコネクテッドカー向けのサイバーセキュリティ基盤を提供するイスラエル企業である。AIや自動化を活用した脅威分析、TARA、規制対応を行う「EVSec」を展開している。

●Cylus × Alstom（2020年12月）

Alstomは、Cylusの鉄道向けサイバーセキュリティ基盤を活用し、鉄道インフラ向けサイバーセキュリティ運用を強化している。Cylusの「CylusOne」は、AIやMachine Learningを活用し、鉄道通信ネットワークや信号システムをリアルタイムで監視しながら、異常検知、脅威分析、SOC統合を行う。

参考：https://www.alstom.com/press-releases-news/2020/12/alstom-invests-railway-cybersecurity-specialist-cylus-and-signs

Cylus（https://www.cylus.com/）
鉄道インフラ向けのサイバーセキュリティ基盤を提供するイスラエル企業である。AIやMachine Learningを活用した異常検知、脅威分析、鉄道OT環境向けSOC運用を行う「CylusOne」を展開している。