

Gigamon 2026 調査 : AI がセキュリティ侵害の 83%に関与 攻撃者のスピードが防御側を凌駕する

セキュリティ投資の増加にもかかわらず、侵害件数は年間 18%増加。AI が防御側の監視範囲を超えて攻撃を加速させるにつれ、両者のギャップは拡大している

カリフォルニア州サンタクララ – 2026 年 5 月 6 日 –ディープオブザーバビリティのリーダーである Gigamon は本日、「2026 年 ハイブリッドクラウドセキュリティ調査」を発表し、サイバー脅威の状況に根本的な変化が生じていることを明らかにしました。報告された**セキュリティ侵害の 83%に AI が関与**しており、攻撃者は多くの組織が防御できる以上のスピードと規模で攻撃を実行できるようになっています。

2026 年ハイブリッドクラウドセキュリティ調査 :

<https://www.gigamon.com/campaigns/hybrid-cloud-security-survey.html>

ツールやガバナンスポリシーへの投資を拡大しているにもかかわらず、過去 1 年間に **65%の組織が情報漏洩を経験**しており、これは**過去 3 年間で 40%の増加**を示しています*。この調査結果は、攻撃者が AI を活用してサイバー攻撃を加速させる一方で、防御側はネットワーク全体で何が起きているかについて断片的な可視性しか得られず、制約を受けているという、拡大する不均衡を浮き彫りにしています。

「AI は攻撃チェーンのほぼすべての段階に組み込まれており、攻撃者は検知と対応のスピードを凌駕しています」と、Gigamon の社長兼 CEO であるシェーン・バックリー氏は述べています。「**組織の 93%が新しいセキュリティツールに投資**している一方で、多くの組織は依然として自社の環境におけるデータの流れを把握できておらず、誤った安心感を得ている状況です。このギャップを埋めるには、ディープオブザーバビリティが必要であり、セキュリティチームが脅威をより早期に検知し、的確に対応するために必要な明確さを得ることが重要です。」

今年で 4 年目となるこの年次調査は、オーストラリア、フランス、ドイツ、シンガポール、英国、米国など世界各国のセキュリティおよび IT リーダー1,000 名以上を対象に実施されました。調査報告書「現実検証 : AI セキュリティの幻想を暴く」は、自信と現実の乖離を探り、組織が AI 関連リスクを評価する際の重大な盲点を明らかにしています。

主な調査結果 : AI は攻撃と防御の両方を変革している

- 自信が能力を上回っています。組織の約 3 分の 2 (64%) は、新しい AI 技術を保護する能力が「明確」または「統合済み」だと考えていますが、過去 1 年間に 65%が情報漏洩を経験し、3 分の 1 が複数回の情報漏洩を経験しています。
- AI は、この構図の双方を変革しつつあります。現在、AI はセキュリティ運用全体に組み込まれており、94%が人間の介入なしにセキュリティ機能を自律的に実行していると報告しています。最も一般的なのは、アラートのトリアージ（選別）

と優先順位付け（53％）です。同時に、AI セキュリティインシデントは、以下のような複数のリスクカテゴリに及んでいます。

- 外部からの AI 攻撃（41％）
- 内部からの情報漏えい（30％）
- 許可されていない AI の使用（30％）
- LLM システムへの直接攻撃（33％）
- クラウド AI 導入に対する信頼は低下の一途を辿っています。リスクの増大に伴い、データ戦略も変化しています。現在、リーダーの大多数（72％）は、データレイクの方が AI ワークロードにとってより安全だと考えている一方、パブリッククラウド環境での AI 導入に消極的なリーダーは 70％に上り、前年の 54％から増加しています。
- 量子コンピューティングに伴うリスクが、対応を急ぐべき状況を加速させています。将来を見据えると、87％が「Harvest Now, Decrypt Later（今収集し、後で復号する）」攻撃を懸念しています。こうした攻撃は、現在の暗号化データを将来的なリスクにさらすものであり、現状の可視性の欠如がもたらす長期的な影響を浮き彫りにしています。

AI による脅威に対抗する上で、可視性が決定的な要素として浮上

今年の調査では、AI の脅威に対する防御において「可視性（Visibility）」が最優先のセキュリティ課題として浮上しましたが、同時に、防御側がこの分野で遅れをとっていることも明らかになりました。攻撃者は AI を活用してより迅速に、より大規模に攻撃を仕掛けていますが、組織は暗号化されたトラフィックや East-West トラフィック（ネットワーク内部の通信）、AI ワークロード、クラウド環境など、あらゆる場所で移動するデータの全体像を把握できていません。侵害を経験した組織のうち、効果的に対応するために必要なツールを備えていたと回答したのはわずか 30％に過ぎず、投資と成果の間に重大なギャップが存在することが浮き彫りになりました。

このギャップを埋めるため、組織はディープオブザーバビリティに注目しています。メタデータ、パケット、フローなどのネットワーク由来のテレメトリを使用し、それをセキュリティ、オブザーバビリティ（可観測性）、クラウドツールに取り込むことで、組織はあらゆるデータの流れを完全に可視化できます。ほぼ全員（93％）がこれに同意し、パケットレベルのデータと豊富なアプリケーションメタデータへのアクセスは、従来の MELT データ（メトリクス、イベント、ログ、トレース）が提供する可視性を超えて、現代の脅威を検出および理解するために不可欠であると報告しています。

こうした変化は経営陣にも及んでおり、リーダーの 90％が、取締役会がディープオブザーバビリティの取り組みを支持していると回答しています。これは、今日の AI 主導の脅威から身を守ることができる最新のアプローチへの継続的な取り組みを示しています。

詳細については

- 「2026 年ハイブリッドクラウドセキュリティレポート：現実検証：AI セキュリティの幻想を暴く」をダウンロードしてください。
<https://www.gigamon.com/campaigns/hybrid-cloud-security-survey.html>
- 300 人以上のグローバル CISO からのデータに基づいたレポート「CISO インサイト：AI 時代の CISO の権限強化」をお読みください。
<https://www.gigamon.com/content/dam/resource-library/english/executive-summary/es-gigamon-hybrid-cloud-security-2026.pdf>
- ブログ記事「AI セキュリティの幻想：自信が証拠を上回る時」をお読みください。
<https://blog.gigamon.com/2026/05/05/the-ai-security-illusion-when-confidence-outpaces-proof/>

調査について

2026 年ハイブリッドクラウドセキュリティ調査は、Gigamon の委託を受け、Vitreous World との共同で実施されました。このデータは、2026 年 2 月 16 日から 17 日にかけて実施された、世界中の 1,023 名の回答者を対象としたオンライン調査の結果に基づいています。

*出典：2024 年、2025 年、2026 年 Gigamon ハイブリッドクラウドセキュリティレポート

Gigamon について

Gigamon は、世界で最も複雑な組織のハイブリッドクラウドネットワークとデータを保護します。AI を搭載した Gigamon Deep Observability Pipeline は、信頼性の高いネットワーク由来のテレメトリをクラウド、セキュリティ、およびオペレービリティツールに直接提供することで、あらゆるデータフローを完全に可視化します。パケット、フロー、およびアプリケーションメタデータ全体にわたる AI 駆動型のインサイトにより、組織は暗号化されたトラフィックやラテラルムーブメントに潜む脅威を検出し、ネットワークおよびアプリケーションのパフォーマンスボトルネックを解消し、コンプライアンスを検証しながら、コストと複雑さを削減できます。Gigamon は、Fortune 100 企業の 83 社、主要なモバイルネットワーク事業者、あらゆるレベルの公共機関など、世界中の 4,000 以上の組織から信頼されています。

詳細は <https://www.gigamon.com/> をご覧ください。

© 2026 Gigamon. All rights reserved. Gigamon および Gigamon ロゴは、米国およびその他の国における Gigamon の商標です。Gigamon の商標については、<https://www.gigamon.com/legal%20-trademarks> をご覧ください。その他のすべての商標は、それぞれの所有者の財産です。

【本プレスリリースに関するお問合せ】

Gigamon Inc. APAC Headquarters

6 Temasek Boulevard, Suntec City, Tower Four #24-01

Singapore 038986

Email: sales-japan@gigamon.com

URL: <https://www.gigamon.com/jp/>