2025 年 12 月 11 日

Press Release

アカマイ・テクノロジーズ合同会社

Akamai、クラウドとセキュリティにおける 2026 年の予測を発表

AI がクラウドの変革とリスクを再定義、
APAC における企業のデジタルインフラの構築とセキュリティ確保のあり方が大きく変わると予想

※本リリースは 2025 年 12 月 3 日(現地時間) シンガポールで発表されたプレスリリースの抄訳版です。

オンラインライフの力となり、守るクラウド企業、Akamai Technologies, Inc.（NASDAQ：AKAM）は、アジア太平洋地域における 2026 年のクラウドおよびセキュリティに関する予測を発表しました。Akamai は、AI によって引き起こされるサイバー脅威、デジタル主権関連の規制の強化、分散型 AI の運用要件が、APAC 地域におけるデジタルインフラの構築、保護、管理のあり方に多大な影響を与えると予想しています。

セキュリティ：AI が APAC 全域でサイバー脅威を強化

- **自律型 AI により攻撃のスピードが加速：** 2026 年には 攻撃者が AI を活用して、攻撃コードの生成や展開の高速化と自動化を進める一方、AI が自ら判断して行動することによる脅威が、APAC 地域におけるサイバー攻撃に根本的な変化を起こすと Akamai は予想しています。攻撃者は、生成 AI と自律型 AI の両方の機能を活用することで、脆弱性をスキャンして、攻撃のエントリーポイントをテストし、人間の関与を最小限に抑えて攻撃コードを実行できるようになるでしょう。こうしたマシン駆動型モデルによって、かつては数週間とされていたデータ侵害の所要時間が数時間以内にまで短縮されることから、シンガポールや韓国、日本などの価値の高いデジタル市場全体でのリスクは高まっています。
- **API がアプリケーションレイヤー侵害の主な経路に：**デジタルバンキング、公共サービス、および小売アプリケーションが API エコシステムへの依存を強めるなか、API 主導の攻撃が Web ベースの攻撃を上回ることが予想されます。APAC 地域の 80% 以上の組織が、過去 1 年間に少なくとも 1 回の API セキュリティインシデントを経験しています。さらに約 3 分の 2 の組織は、自社のどの API が機微な情報を送信しているのかを把握できていません。このような可視性の欠如と AI による攻撃の自動化が組み合わさることで、攻撃者が脆弱な API を迅速に調査、特定、悪用できる環境が生まれています。
- **ランサムウェア攻撃がより手軽に：**ランサムウェアは 2026 年には完全に商品化され、大規模なサイバー犯罪経済へと変貌するでしょう。市販型の「Ransomware as a Service（RaaS: サービスとしてのランサムウェア）」のサブスクリプション、AI を利用して人々の感情や心理を操作する「バイブハッキング」、さらにサイバー犯罪者、ハクティビスト、国家主体の攻撃者らの連携の拡大により、脅迫型攻撃を仕掛けるために必要な専門知識はこれまでよりもはるかに少なくなることが見込まれます。金融、ヘルスケア、小売、メディアなどの機微な情報を多く扱う業界は、より集中的な攻撃の標的となるでしょう。一

方で、マネージド・サービス・プロバイダーやサプライ・チェーン・ベンダーは価値の高いエントリーポイントとて狙われると考えられます。半導体などのハイテク産業は、今後も特に脆弱な業界であり続けるでしょう。

Akamai の Director of Security Technology & Strategy である Reuben Koh は「AI は、APAC におけるサイバー攻撃の経済構造を根本的に変えようとしています。攻撃者らは、もはや人の手ではなく、自動化によって攻撃を拡大しているのです。マシンの速度で変化する脅威の環境において、リーダーたちは、人間の速度に依存した防御に頼ることはできません。2026 年、セキュリティチームは、攻撃者と同じスピードで対応し、リアルタイムでの脅威の検知、分析、封じ込めを行う必要があります。その第一歩となるのは、API ガバナンスの最新化、脅威封じ込めの自動化への投資、サプライチェーン全体のレジリエンスの強化です。このような変革を早期に実現する組織は、AI 主導の脅威環境の中でも、顧客の信頼を確保し、事業の継続性を維持できることでしょう」と述べています。

クラウド：デジタル主権が APAC 地域におけるクラウド戦略を再定義

- **デジタル主権が経済的主権となる：**2025 年、ハイパースケーラーへの依存度を下げる EU の取り組みを受け、APAC 全体でも同様の動きが広がっています。企業は現在、クラウドのポータビリティをコスト最適化の手段ではなく、地政学的な不確実性やベンダーに関する懸念に対する重要なリスク緩和策と捉えています。インドはこの変革に先進的に取り組んでおり、オーストラリアは大規模な概念実証を実施しています。真のデジタル主権を実現するためには、インフラの独立性が必要です。つまり、技術的または経済的な制約を受けることなく、プロバイダー、地域、アーキテクチャ間でワークロードを移動できる必要があります。当初、この柔軟性はリスク管理の観点から求められていましたが、コンピューティング環境のポータビリティを必要とする次世代 AI アプリケーションにも不可欠です。
- **AI アーキテクチャの高度化と分散化：**企業がレイテンシーとパフォーマンスを向上させるために推論処理をユーザーや運用システムに近い場所に移行させることに伴い、分散型 AI アーキテクチャの採用はさらに加速すると見込んでいます。このことは、モビリティ、公共サービス、産業オートメーションなどのセクターが次のデジタルイニシアチブをどのように拡張するかに影響を与えるでしょう。
- **AI のセキュリティはエンドポイントのセキュリティより重要：**セキュリティとコスト面の課題がより複雑になるなか、企業は AI ガバナンスを強化することを求められるでしょう。エンドポイントを保護するだけでは不十分となり、リーダーたちはトレーニングデータセットから推論トラフィックやモデル出力まで、AI データサプライチェーン全体を保護する必要があります。これにより、プロンプトや応答をリアルタイムで検査する「AI ファイアウォール」の導入が加速し、中央集中型の環境ではなく、分散型の AI ワークロードと並行してエッジでリスクを検知できるようになります。同時に、AI ガバナンスが急速に成熟し、来歴の管理が可能になります。
- **FinOps のシフトレフトがついに実現：**AI コンピューティングの変動性が高まることで、FinOps のあり方に大幅な転換が必要になります。2026 年には、導入後にコストを探索するのではなく、エンジニアリングチームとプロダクトチームが、モデル設計の財務的な影響に対するリアルタイムのコストに可視性を組み込み、モデルバージョン、導入地域、推論パターンなどの選択がもたらす財務的な影響を把握できるようになるでしょう。シフトレフトに対応する FinOps を採用している組織は、決定的なメリットを得ることができます。導入初日からアーキテクチャ上のあらゆる決定にコスト効率を組み込むことで、そのような企業は、競合他社が追随できない経済的優位性を獲得し、AI アプリケーションを展開できるのです。

Akamai の Cloud Computing Services Chief Technology Officer である Jay Jenkins は「APAC のクラウド戦略は自律化の道を進んでいます。リーダーたちは、ワークロードを容易に移動し、強力なデータ管理を実施して、コアでもエッジでも、最も理にかなった場所で AI を実行する能力を求めています。IDC によると、APAC の CIO の 80% が、2027 年までに AI のパフォーマンスとコンプライアンス確保のためにエッジサービスに依存するようになると予測しています。この地域はすでに、分散型の未来に向けて準備を進めていることは明らかです。2026 年には、ポータビリティと分散型 AI を追求する設計が、レジリエンス を備え、将来に対応するデジタルサービスを構築するうえで不可欠になります」と述べています。

Akamai について：

Akamai はサイバーセキュリティとクラウドコンピューティングを提供することで、オンラインビジネスの力となり、守っています。市場をリードするセキュリティソリューション、優れた脅威インテリジェンス、そして世界中の運用チームが、あらゆるところで企業のデータとアプリケーションを多層防御で守ります。Akamai のフルスタック・クラウドコンピューティング・ソリューションは、世界で最も分散されたプラットフォーム上で、パフォーマンスと手頃な価格を両立します。安心してビジネスを展開できる業界トップクラスの信頼性、スケール、専門知識の提供により、Akamai は、グローバル企業の信頼を獲得しています。詳細については、akamai.com および akamai.com/blog をご覧いただくか、X と LinkedIn で Akamai Technologies をフォローしてください。