2026 年 9 月 24 日

Press Release

アカマイ・テクノロジーズ合同会社

Akamai 脅威レポート：AI エージェントのセキュリティ確保には ふるまい制御のガバナンスへの移行が不可欠

※本リリースは 2026 年 9 月 22 日(現地時間) 米国マサチューセッツ州ケンブリッジで発表されたプレスリリースの抄訳版です。

- **非人間アイデンティティ（ノンヒューマンアイデンティティ）：**企業が抱えるリスクは、人間主体のヒューマンアイデンティティの管理から、自律的な非人間エンティティのガバナンスへと変化している。
- **保護されていないワークスペースとしてのブラウザー：** 企業のユーザーの 40%以上が AI を活用したブラウザー拡張機能をインストールしており、そのうち 25%の拡張機能は 12 か月以内に権限を変更している。
- **チャットボットとの会話：**チャットボットとの会話の 6%以上に機微な情報が含まれている。

組織が API やシステムを横断するタスクを実行するためにエージェント型 AI を展開する中、企業はリスクの根本的な変化に直面しています。Akamai（NASDAQ：AKAM）は本日、新たな AI の課題に焦点を当てた最新の「インターネットの現状（SOTI）セキュリティ」レポートを公開しました。CISO を読者に想定した本レポート、「エージェント型脅威の現状：スピード、規模、ノンヒューマンアイデンティティ」では、現代のビジネスのセキュリティ確保が、アイデンティティ管理やユーザーのアクセス管理に限らず、非人間エンティティのふるまいを制御するためのガバナンスの課題へと進化していることについて解説しています。

本レポートで取り上げる重要な課題は 2 つあります。1 つは、自律型エージェントのガードレールを設定することの難しさ、もう 1 つは、AI モデルがしばしば人間によるパッチ適用のサイクルを上回る速度で脆弱性を発見していることです。

SOTI レポートの主な調査結果

- **Model Context Protocol（MCP）の可視性のギャップ：**MCP（AI エージェントが複数のソフトウェアシステムと連携できるようにするプロトコル）は、AI モデルが複数システム間で自律的なアクションの実行を可能にするしくみですが、MCP のリスクへの対応は、現在の CISO が挙げるセキュリティ上の優先事項の中で最も優先度が低い項目となっています。セキュリティリーダーが 2030 年までに不正な AI エージェントがサイバー脅威の最上位に躍り出ると予想しているにもかかわらず、この現状は、重大な可視性のギャップを浮き彫りにしています。
- **チャットボットのデータ漏えい：**企業が利用する AI チャットボットとの会話の 6%以上が、主に個人を特定できる情報などの機微な情報を含む内容であり、その 47%は監視されていない個人アカウントを介して実行されています。

- **エクスプロイトの加速：**フロンティア AI の開発によって、モデルがシステムの脆弱性を迅速に発見し、それらを組み合わせて悪用できることが実証されています。そのため、事後対応型のパッチ適用では不十分であり、エッジでのリアルタイムな緩和策が必要になっています。
- **保護されていないワークスペースとしてのブラウザー：**企業のユーザーの 40%以上が AI を活用したブラウザー拡張機能をインストールしており、そのうち 25%の拡張機能は 12 か月以内に権限を変更しています。これらのツールは、標準的な拡張機能よりも既知の脆弱性（CVE）を含んでいる可能性が 60%高いことが判明しています。
- **合成顧客（シンセティックカスタマー）の台頭：**ブランド認知の向上において、AI エージェントが従来の Web トラフィックに置き換わるなか、CISO にはマルウェア対策にとどまらず、サイテーション（引用）、正確性、センチメント、ボット管理といった生成エンジン最適化（GEO）指標まで包含する形で、保護の範囲を拡張することが求められています。

Akamai の Chief Security Officer である Boaz Gelbord は「AI は、セキュリティエコシステム全体にとって、『Everything Everywhere All at Once（同時にあらゆるできごとが、あらゆる場所で起こる）』ような状況をもたらしています。これには 3 つの脅威があります。1 つ目は、組織全体における AI の利用です。これには、AI によって生成されたコードや、AI 生産性ツールの利用も含まれます。2 つ目は、AI を顧客向け製品やクラウドワークロードに直接組み込むことです。これにより、運用リスクのプロファイルが変容します。3 つ目が、企業を標的とした AI 駆動型の攻撃です。急速に進化するこの現実に、セキュリティプログラムを適応させる必要があります。また、このような変化がかつてないほどのスピードで起こっているため、システムには大きな負荷がかかっています。これらの脅威は、近い将来、取締役会、お客様、規制当局にとって中心的なテーマとなるでしょう」と述べています。

さらに、Akamai の Advisory CISO を務める Steve Winterfeld は「エージェント型 Web の台頭により、ビジネス価値と運用ロジックの構築方法は根本的に変わります。自律型 AI が、単純なクエリーへの応答から複数ステップのビジネス戦略の実行へと進化していることに伴い、セキュリティリーダーシップにも進化が求められているのです」と述べています。

セキュリティリーダー向けの戦略的推奨事項

エージェント型 AI 時代に対応するため、Akamai は本レポートで、CISO に向けた 4 つの中核的な柱を提示しています。

1. **適応型エッジガバナンスへの移行：**エッジネイティブのランタイム保護、API フィルター、分離（アイソレーション）メカニズムを導入して、バックエンドでのパッチ適用の間でも即座に脆弱性を無効化します。
2. **ブラウザーエッジのロックダウン：**管理対象外の AI 拡張機能や Web ホスト型モデルを従業員が安全に利用できるよう、ブラウザー内で可視性とふるまいの制御を確立してセキュアなワークフォースを確立します。
3. **ゼロクリックエコノミーにおけるブランド権威の保護：**ネットワークエッジに GEO 戦略と機械可読データ層を実装することで、AI クローラーや AI が生み出す「シンセティックカスタマー」による企業のブランド情報のハルシネーションや誤表現を防止します。
4. **自律性と検証可能性の整合：**AI エージェントに自律的な運用を認める際に、アクションをどの程度容易に検証可能か、潜在的な障害はどの程度復旧可能であるかといったことに基づいて判断することで、重要なアクションには人を介在させる（ヒューマン・イン・ザ・ループ）制御を維持できます。

今年で 12 年目を迎える Akamai の SOTI レポートでは、全世界の Web トラフィックの大部分を処理している Akamai のサイバーセキュリティインフラから獲得したデータを基に、サイバーセキュリティのトレンドと Web パフォーマンスに関する重要な知見を引き続き提供していきます。

Akamai について

Akamai は、オンラインビジネスの力となり、守るサイバーセキュリティおよびクラウドコンピューティング企業です。当社の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、グローバル運用チームによって、あらゆる場所でエンタープライズデータとアプリケーションを保護する多層防御を利用いただけます。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、世界で最も分散化されたプラットフォームで高いパフォーマンスとコストを実現しています。多くのグローバル企業が、ビジネスの成長に必要な業界最高レベルの信頼性、拡張性、専門知識を提供できる Akamai に信頼を寄せています。詳細については、akamai.com および akamai.com/blog をご覧いただくか、X や LinkedIn で Akamai Technologies をフォローしてください。

Akamai では、AI・クラウド・セキュリティの最新トピックや最新情報を 3 分で解説するポッドキャスト「Akamai Tech Insight」を配信しています。ぜひあわせてお聴きください。
URL：https://x.gd/G0bb1m