2026 年 8 月 7 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：企業における AI 利用のほぼ半数が 社内のセキュリティ管理を回避、大規模な「シャドーAI」の可視性ギャップを招く

※本リリースは 2026 年 8 月 5 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。

- **「AI パワーユーザー」の台頭：**AI の利用があらゆる業務部門に広がる一方で、そのリスクは一部の特定のユーザーに集中。企業 AI に関するリスクの大部分は、利用頻度が非常に高いパワーユーザー群によって引き起こされている
- **「シャドーAI」の蔓延：**セキュリティチームは深刻な可視性ギャップに直面。承認済みのわずかなプラットフォームに監視が偏る一方で、その水面下では、管理されていないアプリケーションが膨大な「ロングテール」を形成し、密かに稼働している
- **AI ネイティブな攻撃ベクトルの出現：**本レポートでは、2026 年に研究者が発見した、従来の境界防御を完全に回避する 3 つの新たな脅威の手法を詳しく解説

Akamai（NASDAQ：AKAM）は本日、新たな「インターネットの現状（SOTI）」セキュリティレポート「2026 年エンタープライズ AI の利用に関するリスクレポート」を公開しました。本レポートでは、不正なブラウザー拡張機能や脆弱な自律型エージェントによって、企業のアタックサーフェスが実際にどのように拡大しているのかを詳しく説明しています。また、分散型シャドーAI、利用頻度が非常に高い AI パワーユーザー、密かに動作するブラウザー拡張機能によって、企業の重要資産がまったく新しい種類のサイバーリスクにさらされている実態を明らかにしています。

本レポートは、企業における AI 導入の大きな変化を捉えています。2025 年初頭に慎重な試行錯誤として始まった AI の利用は、今や組織全体の必須要件として定着しています。しかし、この急速な導入に、従来のセキュリティ対策は追いついていません。

Akamai の Enterprise Security Product and Engineering 担当 Vice President である Or Eshed は「AI はもはや単なる生産性向上ツールではありません。企業の最重要資産に直接アクセスし、協働する同僚のような存在になっています」「従来のデータ漏えい防止（DLP）ツールは、ファイル転送やメールが中心だった時代を前提に設計されています。現在、企業の機微な情報は、絶えず生成される膨大な数のプロンプト、管理されていない個人アカウント、そして自律型 AI エージェントにわたって、組織的に断片化されています。セキュリティ責任者は、AI を阻止する発想から脱却し、AI の運用をインタラクションレベルで継続的に制御する方針への転換が求められます」と述べています。

AI ネイティブな攻撃ベクトルの台頭

本レポートでは、2026 年に研究者が発見した、従来の境界防御を完全にすり抜ける新たな脅威の 3 つの手法について詳しく解説しています。

- **バイブハッキング：**攻撃者が開発環境内にあるローカルのマークダウン指示ファイルを密かに改変する手法。この巧みな改変により、最先端のコーディングアシスタントに、安全でないコードを生成させたり、許可されていないアクションを実行させたりします。開発者の通常のワークフローを巧妙に装うのが特徴です。
- **カーソルジャッキング：**不正なブラウザー拡張機能が広範な権限を悪用し、ブラウザー環境から API キー、専有コードベース、対話履歴を密かに収集する手法。これは、Cursor など広く利用されている AI コーディングアシスタントを標的とする、影響度の大きいエクスプロイトです。
- **コメットジャッキング：**攻撃者が公開 Web ページに悪性の命令を埋め込み、間接型プロンプトインジェクションによってユーザーのローカル AI エージェントを操作する手法。乗っ取られたエージェントは、ユーザーに気付かれることなく、ローカルファイル、メール、セッション認証情報を外部へ流出させることができます。この脅威は、Perplexity の Comet AI のようなエージェント型ブラウザーを標的としています。

AI のセキュリティを確保するための CISO 向けロードマップ（2026 年版）

AI による経済的なメリットを享受しながら重要データをリスクにさらさないために、Akamai のレポートでは、今日の CISO に向けた 5 つの中核的な緩和戦略を提示しています。

- **AI パワーユーザーへの対策強化：**対話型 AI へのプロンプトの大部分を生み出している高リスクな従業員（全体の約 5%）を対象に、テレメトリの収集、モニタリング、個別のコーチングを重点的に実施します。
- **シャドーAI の排除：**すべてのプラットフォームにシングルサインオン（SSO）による連携を徹底し、ニッチな AI サービス型ソフトウェア（SaaS）ツールのロングテールを継続的に発見します。
- **インタラクションレイヤーの検査：**静的な DLP から脱却し、プロンプト、コピー＆ペースト用バッファ、文書アップロードを対象とするリアルタイムかつコンテキストに応じた解析へと移行します。
- **ブラウザー拡張機能と IDE 拡張機能の精査：**拡張機能を、高い特権を持つソフトウェアとして厳格に扱います。AI 拡張機能の 75%近くが高レベルまたはクリティカルレベルの権限を要求しており、16.3%には既知の CVE が存在します。
- **AI エージェントのセキュリティ確保：**従業員に代わって動作する自律型 AI エージェントに対し、最小権限の原則に基づく厳格な権限境界を設定し、そのふるまいを監視します。

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。