

**Akamai 脅威レポート :**  
**サイバーセキュリティチームを支援する Defenders' Guide 2025 を発表**  
新しいレポートでは、セキュリティ専門家がサイバー犯罪者の先手を打ち、  
攻撃を阻止するための新たな調査結果と知見を提供

※本リリースは 2025 年 2 月 11 日 (現地時間) 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。

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、[Akamai Technologies](#) (NASDAQ : AKAM) は、「[Defenders' Guide 2025 : より堅牢な防御の未来へ](#)」の公開を発表しました。Akamai が刊行するセキュリティレポート「インターネットの現状 (SOTI) 」は、リスクスコアリング、VPN の不正利用、高度なマルウェア技術に関する新たな発見などの実践的な調査結果を提供し、組織のサイバーセキュリティポスチャの強化に活用されています。最高情報セキュリティ責任者 (CISO) 向けに、詳細なセキュリティフレームワークとプロアクティブな対策が統合されているので、調査に基づくサイバーセキュリティ戦略の基盤を強固にする際に役立ちます。

Akamai の Senior Vice President 兼 Chief Security Officer である Boaz Gelbord は、「このガイドは、調査結果をサイバー戦略全体に組み込むことの重要性を CISO が再確認していただける内容となっています。攻撃に関する最先端の技術分析を活用して、人、プロセス、テクノロジーに情報を提供することで、組織は、ますます複雑になるデジタル環境においてリスクを緩和できます。十分な情報に基づいて戦略を立てることで、セキュリティ投資の最適化やコストのかかるインシデントリスクの低減を通じて、最終的にコスト削減を実現できるのです。本質的に、調査に基づく戦略は、セキュリティチームがプログラムを最新の開発状況に即して調整し、脅威の状況に合わせて実用的で関連性の高いプログラムの構築を可能にします」と述べています。

このレポートでは、脅威に対抗するために日々最前線で闘うサイバーセキュリティの専門家やデータサイエンティストによる、セキュリティ担当者としての知見が得られます。Defenders' Guide は、従来のレポートとは異なるアプローチを採用しており、抽象的なトレンドではなくアクション可能なインテリジェンスを提供します。

Akamai の Head of Cybersecurity Research である Mitch Mayne は「これまでサイバーセキュリティ業界が公開してきた主要な脅威に関するレポートは、CISO やサイバーセキュリティのリーダーが活用してきました。これは重要なものです。同様に重要なのが、最前線のセキュリティ担当者向けの年次レポートです。Defenders' Guide はまさにそれに該当し、業界初の試みを文書化したレポートとなります。セキュリティ担当者が新たな脅威に先手を打てるよう、新しい発見とベストプラクティスを統合した、包括的かつ一元化されたリソースを提供します。トップレベルの調査結果を総合することで、サイバーセキュリティ担当者に重要な知見を提供するだけでなく、彼らが限られた時間とリソースをより効率的に、最も効果のある現場での進歩に割り当てられるようサポートします」と述べました。

Defenders' Guide 2025 の主なポイントは次のとおりです。

### リスク管理

- **新しいリスクスコアリングモデル**は、アプリケーションの重要性、ネットワークの複雑性、および侵害の可能性を評価することで、組織の脆弱性を定量化します。推奨事項には、エンドポイントの影響分析、セグメンテーション戦略、社内外のリスク緩和方法が含まれます。
- **マルウェアの変容**は、ピアツーピアアーキテクチャやファイルレスマルウェアのような高度な戦術に焦点を当て、NoaBot や RedTail などのボットネットファミリーに関する知見を提供します。本レポートでは、パッチ管理や従業員トレーニングなど、こうした脅威を緩和するための現実的な対応策を紹介しています。

### ネットワークアーキテクチャ

- **新たな VPN の不正利用**に関する調査では、高度な脅威アクターが不正利用する VPN 機器の脆弱性を明らかにしています。ソリューションには、安全な LDAP プロトコル、カスタム暗号化、ファームウェアのアップデートの採用が含まれます。
- **クロスサイトスクリプティング (XSS)**に関する調査では、ユーザー入力処理の脆弱性に対処するための多層防御に対する重要なニーズを示しています。

### ホストのセキュリティ

- 2023～2024 年に発生した 6 つの **Kubernetes** の脆弱性に関する分析では、コマンドインジェクション攻撃のリスクについて解説しています。本レポートでは、コンテナ化された環境における新たな脅威に対するプロアクティブなパッチ適用と警戒に着目しています。

**レポートの全文をご覧ください。** Defenders' Guide 2025 は、ますます複雑になるデジタル環境で常に最新情報を把握したいと考える組織にとって、非常に重要なリソースです。詳細な調査結果と戦略を確認するには、[レポートの全文をダウンロード](#)してください。

### Akamai について

Akamai はオンラインライフの力となり、守っています。世界中のトップ企業が Akamai を選び、安全なデジタル体験を構築して提供することで、毎日、いつでもどこでも、世界中の人々の人生をより豊かにしています。超分散型のエッジおよびクラウドプラットフォームである [Akamai Connected Cloud](#) は、アプリと体験をユーザーに近づけ、脅威を遠ざけます。Akamai のクラウドコンピューティング、セキュリティ、コンテンツデリバリーの各ソリューションの詳細については、[akamai.com](#) および [akamai.com/blog](#) をご覧くださいか、[X](#) (旧 Twitter) と [LinkedIn](#) で Akamai Technologies をフォローしてください。

※Akamai と Akamai □□ は、Akamai Technologies Inc. の商標または登録商標です

※その他、記載されている会社名ならびに組織名、ロゴ、サービス名は、各社の商標または登録商標です

※本プレスリリースの内容は、個別の事例に基づくものであり、個々の状況により変動しうるものです