

Akamai 脅威レポート： 過去 2 年間でランサムウェア攻撃が倍増したことが明らかに 攻撃の増加に伴い、ゼロトラストとマイクロセグメンテーションの導入が増加

※本リリースは 2023 年 10 月 30 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。

オンラインライフの力となり、守るクラウド企業の [Akamai Technologies, Inc.](#)（NASDAQ：AKAM）は、ランサムウェアの増加、ゼロトラストの導入、マイクロセグメンテーションの利点について取り上げた新しいレポート「[インターネットの現状 | 猛威を振るランサムウェア](#)」を発表しました。本レポートでは、調査に回答した企業が過去 12 か月間で平均 86 回のランサムウェア攻撃を受けており、年間平均攻撃数が 2 年前の 43 回から増加していることが明らかになりました。セキュリティ部門は、ゼロトラスト戦略やマイクロセグメンテーション戦略を導入することで、最近の攻撃の増加に対応してきました。いずれかの形態のセグメンテーションを導入したと答えた回答者のほぼ全員（99%）が、ゼロトラスト・セキュリティ・フレームワークも導入しており、このことからセグメンテーションがゼロトラスト戦略において必要な要素であることが分かります。

このレポートは、世界中の約 1,200 人の IT 意思決定者とセキュリティ意思決定者から得た情報に基づいています。回答者は、マイクロセグメンテーションが資産の保護に効果的なツールであることに大いに同意していますが、導入率は予想よりも低く、2 つ以上のビジネスクリティカルな領域においてセグメント化を実施している組織の割合は 30% でした。世界的に見て、マイクロセグメンテーションを導入する上での最大の障壁はスキル／専門知識の不足（39%）であり、続いてパフォーマンスのボトルネックの増大（39%）、コンプライアンス要件（38%）があげられています。調査回答者のほとんどは、セクター、業界、国を問わず、程度は若干異なるものの、共通の障壁を認識しています。

マイクロセグメンテーションの導入は遅れているものの、ミッションクリティカルな 6 つの領域で粘り強くマイクロセグメンテーション戦略を実施した組織は、平均わずか 4 時間で攻撃から復旧したと述べています。これは 1 つの重要な領域でのみセグメント化を行った組織よりも 11 時間早く、マイクロセグメンテーションを利用したゼロトラスト戦略の効果を如実に示しています。

「サイバーセキュリティの情勢は、サイバー犯罪者が開発した最新の脅威手法に応じて常に進化し、変化しています。阻止するのがランサムウェアでも、新しいゼロデイ攻撃でも、洗練されたフィッシング攻撃でも、企業は重要な資産を保護するためにリスクを再評価することが重要です」と Akamai の Advisory CISO を務める Steve Winterfeld は述べています。「そのための重要な方法の 1 つが、ゼロトラスト・アーキテクチャです。つまり、ゼロ

トラスト・ネットワーク・アクセス（ZTNA）とマイクロセグメンテーションを組み合わせ、必要なスキルを持つスタッフやパートナーへのアクセスによって支えられている明確なセキュリティ戦略の一部として統合することです」

レポートではその他に以下のような調査結果を示しています。

- 回答者の 93% が、ランサムウェア攻撃を阻止するためにはマイクロセグメンテーションが不可欠であると回答
- ランサムウェア攻撃を受けた組織が被る影響は、ネットワークのダウンタイム（44%）、データ損失（42%）、ブランド／評判の低下（39%）
- 過去 1 年間でランサムウェア攻撃の報告数が多かった国の上位は米国（115 件）とドイツ（110 件）
- セグメンテーションに関して先行しているのはインドで、58% の組織が 2 つ以上の資産／領域でセグメント化を実施しています。続いて、メキシコが 48%、日本が 32% でした。

レポート全文はこちらでご覧いただけます。

[インターネットの現状 猛威を振るうランサムウェア](#)

手法

Akamai は Vanson Bourne 社と提携して、10 か国の IT 意思決定者とセキュリティ決定者 1,200 人にインタビューを行い、セグメンテーションの役割にフォーカスしながら、組織による環境保護の進捗状況を測定しました。

調査参加者には、IT セキュリティのアプローチとセグメンテーション戦略、および 2023 年に組織が直面した脅威に関する質問をしました。この調査結果から、2021 年以降にセキュリティ戦略がどのように変更されたか、また、今後どのような発展が必要なのかに関する知見を得ることができます。

インタビューを受けたのは、米国、メキシコ、ブラジル、英国、フランス、ドイツ、中国、インド、日本、オーストラリアのセキュリティ担当者および意思決定者です。回答者は全員、従業員数 1,000 人超の組織に勤めており、さまざまな業界やセクターからバランスよく選ばれています。

Akamai Technologies 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。世界中の先進企業が 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、世界中の人々の生活、仕事、娯楽をサポートしています。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 をご覧いただくか、[X](#) (旧 Twitter) と [LinkedIn](https://www.linkedin.com/company/akamai) で Akamai Technologies をフォローしてください。

※Akamai と Akamai ロゴは、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