Akamai

eブック

セグメンテーションの現状

セグメンテーションの導入障壁を克服することが変革につながる

eコマースセクター

目次

はじめに 2

辛抱強くセグメンテーションを導入すればリスクが大幅に減る 3

セグメンテーションはゼロトラストの重要な一部であると広く認識されている 5

導入には時間がかかるが、辛抱強く取り組めば必ず結果がついてくる 6

重要ポイント：6 つの重要なビジネス領域をセグメント化した組織は、リスクを大幅に軽減できる 7

ソフトウェアベースのマイクロセグメンテーションソリューションによって課題を解決する方法 8

適切なソリューションとサポートで辛抱強くセキュリティ体制を変革する 9

調査対象 10

はじめに

IT セキュリティチーム、とりわけ e コマース組織を守るチームの仕事は決して楽なものではありません。従来から予算もセキュリティリソースも限られているため、エンタープライズの防御担当者は少ないリソースで多くのことをこなさなければなりませんでした。しかし現在では、攻撃意欲が高く巧妙な手口を使う攻撃者と、ますます複雑化するインフラの管理が相まって、セキュリティチームにはこれまで以上に大きなリスク緩和のプレッシャーにさらされています。e コマース組織は、パフォーマンスの高いオンラインプレゼンスに頼った運営を行なっているため、ランサムウェア攻撃のような攻撃に一度でも侵害されると、ブランドの評判や収益に、修復不能とまでは言わないまでも、甚大な被害を受ける可能性があります。大量暗号化だけでなく、データ窃取による二重の脅迫を受ける可能性があるため、重要なサーバーやシステムが利用できなくなり、オンライン業務、注文処理、生産ラインが停止した場合に損害がどのくらいなるか想像してみてください。

e コマースを対象としたこの「セグメンテーションの現状」レポートの調査結果が示すように、これらの攻撃の影響がさらに大きくなっており、パフォーマンスを犠牲にしたり、運用上のオーバーヘッドを増やしたりすることなく、重要なデータを安全に保つための適切なツールとソリューションを選択する必要性が高まっています。本レポートによると、e コマースはすべての調査回答者の中で最も標的となっている業界セクターであり、被害を食い止めるために、ランサムウェア攻撃をできるだけ早く予防、検知、対応することが緊急の課題であることが明確になっています。

e コマースセクターに属する組織の回答者（米国、LATAM、EMEA、APAC など、全地域の回答者）は、IT 資産を保護し続けるためにはセグメンテーションが有効であるとの意見に圧倒的な同意を示していますが、重要なビジネスアプリケーション、サーバー、システムに対するセグメンテーションの導入状況は、全体的に予想よりも進んでいませんでした。e コマース組織にとっての大きな障害は、セグメンテーションを効果的に導入するための専門知識が不足していることと、データコンプライアンス要件が負担になっていることです。これは、チームがその業界に必要な人材を採用し維持することに苦労しているだけでなく、貴重な時間が法規制遵守に費やされており、すでにひっ迫しているリソースをさらに消費している可能性があることを示しています。

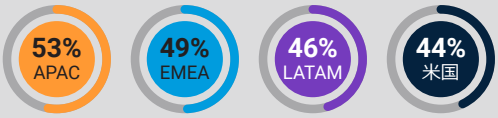
幸い、辛抱強く続け、適切な解決策を選択すれば、道は開けます。重要な資産のほとんどを 6 つの主要な領域にうまくセグメント化できた組織では、セグメンテーションが防御能力を大きく強化することが実証されており、資産を 1 つだけセグメント化した組織よりも 11 時間早くランサムウェアを緩和して封じ込めることができます。この 11 時間という差が、インシデント対応の担当者だけでなく、顧客やブランドの評判におよぼす影響の大きさを想像してみてください。

セグメンテーションの導入は全体的に緩やかなペースで進んできましたが、辛抱強く導入に取り組んできた組織はリスクの大幅な削減に成功しています。

セグメンテーションは効果的。マイクロセグメンテーションはさらに効果的。

セグメンテーションとは、セキュリティを向上させること、そしてフラットなネットワークに付き物のリスクを軽減することを目的とした、ネットワークをより小さなセグメントに分割するアーキテクチャ上のアプローチです。このアプローチは、e コマース主体の組織で PCI コンプライアンスの達成と維持の範囲、コスト、難易度を軽減するためにも使用されています。

マイクロセグメンテーションとは、ネットワークを個別のワークロードやプロセスレベル（レイヤー 7）までの明確なセキュリティセグメントに論理的に分割する、ソフトウェア定義のセキュリティ手法です。VLAN、ACL、内部ファイアウォールなどの従来のセグメンテーション方式がレイヤー 4 しか制御できないのに比べて、各セグメントに対してよりきめ細かいレベルでセキュリティ制御とサービス提供を定義することができます。そのため、e コマース回答者の 94% が、従来の方法よりもソフトウェアベースのセグメンテーションソリューションが良いと回答しています。



APAC のセキュリティに関する意思決定者は、EMEA、LATAM、米国の意思決定者よりも、ネットワークのセグメンテーションが組織のセキュリティを確保するうえで非常に重要であると回答する傾向があります。また、LATAM の意思決定者は、APAC（35%）、米国（34%）、EMEA（26%）の意思決定者よりも、マイクロセグメンテーションが最優先事項（42%）であると回答する傾向があります。

e コマースは最も標的にされている業界であり、ランサムウェア攻撃は増加の一途をたどっている

e コマース組織で発生したランサムウェア攻撃の件数（成功したものも失敗したものも含む）は、過去 12 か月間で平均 167 件に上ります。これは、e コマースがランサムウェア攻撃の平均件数のトップに位置するだけでなく、最も件数の低いセクター（建築業の平均 89 件）の約 2 倍になります。

サイバー攻撃者は米国の e コマース組織を標的にする傾向が強くあります。米国でのランサムウェア攻撃の件数は、過去 12 か月間で平均 312 件と全地域の中で最多であり、APAC では 119 件、EMEA では 91 件、LATAM では 68 件でした（図 1）。

e コマース組織における過去 12 か月間の平均ランサムウェア攻撃件数（地域別）

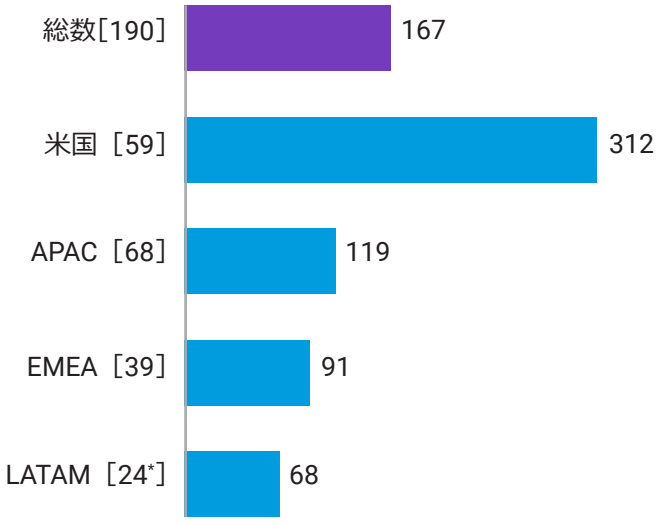


図 1：過去 12 か月間に、組織は何件のランサムウェア攻撃を受けましたか（成功したかどうかは問いません）？過去 12 か月間の平均攻撃件数を地域別に示しています。e コマースセクターのデータのみ表示。

* 注意 – 回答者数は 30 人未満

米国以外の地域の平均値が低いとは言えませんが、米国に標的を絞った攻撃の数に比べれば大した数ではありません。米国は、世界最大の経済大国であり、ランサムウェア集団が最も標的とする国ですが、攻撃者は他の英語圏や西洋諸国に狙いを定めることもよくあります。どの国やセクターが最も被害を受けるかどうかには、地政学的な動機も関係しています。 e コマース組織は、金融サービス業のような他の業界と比較して、従来からセキュリティの成熟度が低いため、 攻撃対象になりやすいのです。その他にもプレッシャーの要因となることがあります。ランサムウェア攻撃が成功したとします。とりわけ休日、祭典、スポーツイベント、新学期、ピーク時のショッピングイベントのような収益を生み出す重要な時期に攻撃が成功し、営業停止するような事態になったとしたら、攻撃者も金銭を得るチャンスが増えたと感じるでしょう。

e コマース組織を標的にしているランサムウェア攻撃の件数が多いにもかかわらず、実際に導入されているセグメンテーションのレベルは想像以下です。これらの組織のうち、2 つ以上の領域をセグメント化しているのはわずか 11% で、この数字は、全地域でほぼ一貫しています。これは、これらの組織の多くが、問題や攻撃の発生時の対処に必要なリソースを確保できていないことを示しています。

e コマースセクターでのランサムウェア攻撃は、ビジネスに甚大かつ直接的な影響を及ぼしかねません（図 2）。回答者は、経済的な損失と評判の低下を言及していますが、どちらも e コマース組織のセキュリティチームにとって深刻な問題となります。また、保険料が増大したと述べる回答者の割合も増えています。これは、e コマース組織が抱えているリスクの大きさを示しています。というのも、e コマース組織は、多くの場合、在庫や倉庫保管に関する物流上の問題に関連するリスクに加えて、個人とその購買習慣に関する個人情報を保持しているからです。

影響に対する捉え方は地域によって異なります。APAC における回答者は、金銭的損失を重視する傾向が特に高く、全体の平均が 42% であるのに対して、半数以上（51%）にその傾向が見られました。その一方で、米国の回答者は、ネットワークのダウンタイムを報告する傾向が最も高く、全体の平均である 39% に比べてほぼ半数（49%）にその傾向が見られました。EU の回答者は、従業員の士気の低下を影響として報告する傾向が高くなっています（全体の 36% と比較して 41%）。

このプレッシャーは各組織の戦略にも影響を及ぼしています。ランサムウェアへの対応だけでなく、絶えず変化するアタックサーフェスへの対応として、サイバーセキュリティ戦略やポリシーを継続的に更新している e コマース組織の数は、2021 年の 3% から 2023 年には 13% に増加しています。ワークロードがクラウドに移行するにつれ、インフラの複雑さが増していますが、これは、セキュリティ戦略やセキュリティチームに常に影響を与えているリスク要因のほんの一部にすぎません。

ランサムウェア／サイバー攻撃が e コマース組織に与える影響

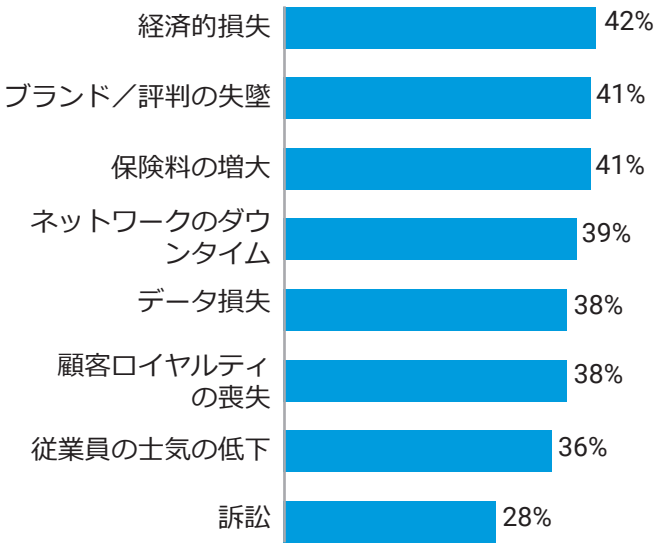


図 2：過去にランサムウェアやその他のサイバー攻撃を検知した際に、組織に及んだ影響は次のうちどれですか？グラフには、e コマースセクターのデータのみ掲載しており、すべての回答の選択肢を掲載しているわけではありません。

セグメンテーションはゼロトラストの重要な一部であると広く認識されている

回答者は、特にマルウェアへの対策をはじめ、組織の安全性を確保するためにセグメンテーションが重要であることに同意しています。

ほぼ半数（48%）がセグメンテーションの重要性の高さを認めており、89% が被害をもたらす攻撃を阻止するためには不可欠であると回答しています。

セグメンテーションはゼロトラスト・セキュリティ・フレームワークの基盤として認識されており、この分野ですでに進展が見られていることは e コマース組織にとって朗報です。すべての組織がゼロトラスト・セキュリティ・フレームワークを導入しているか、すでに導入済みです（100%）。しかし、ゼロトラスト・フレームワークが完全に完成して定義されており、成熟しているとみなされる組織は 5 分の 2 程度（42%）にすぎません。つまり、セグメンテーションによって e コマース組織がゼロトラストへの移行を進めることができる領域がそれだけあるということです。データによると、ゼロトラスト・セキュリティ・フレームワークの導入に関しては、米国の組織の方がはるかに成熟度が高くなっています。ゼロトラストの導入が完全に完了し、定義されていると回答した割合は、米国（63%）の方が、LATAM（46%）、APAC（32%）、EMEA（23%）よりもはるかに高くなっています。

ネットワークのセグメンテーションプロジェクトを開始した理由は地域によって大きく異なり、行政機関がサイバーセキュリティを重視していることが 41% とトップになっているところもあります。LATAM と EU 諸国はどちらも、セグメンテーションイニシアチブを推進する上で最も重要な要因として、注目されているゼロデイ脆弱性を挙げています（それぞれ 44% と 42%）。しかし、EU の回答者は、それがベストプラクティスであるためにプロジェクトを開始したと回答する割合がはるかに高くなっています（全体の 22% と比較して 41%）。それに対して、米国と APJ の回答者は、政府がサイバーセキュリティに重点を置いているために開始したと回答する割合が高くなっています（全体の 35% と比較して、それぞれ 41% と 39%）。また、APJ の回答者は、重要なアプリケーションをクラウドに移行することがプロジェクト開始のきっかけとなったと回答する割合が高くなっています（全体の 32% と比較して 39%）。

e コマース組織の回答者の大多数が、アプリケーションのワークロードをさらに細かいレベルで保護するマイクロセグメンテーションの実装を進めたいと考えています。回答者の 92% がマイクロセグメンテーションは優先度が高いと回答し、34% が最優先事項だと回答しています。さらに、この業界の IT およびセキュリティの意思決定者の全員（100%）が、自分の業界では、少なくとも一部の組織がマイクロセグメンテーションを導入済みだと回答しています。このことは、マイクロセグメンテーションの普及が今のところ限定的であるとしても、少なくともすべての企業から広く認識されたソリューションであることを示しています。

また、回答者は、組織の IT 環境全体の可視性を高める必要があったと回答しています。リスクを軽減するために、ネットワーク通信や資産の場所などに「はるかに高い」可視性が必要とする地域は、LATAM（63%）が最も高く、その後に APAC（56%）、米国（46%）、EMEA（44%）と続きます。

導入には時間がかかるが、辛抱強く取り組めば必ず結果がついてくる

セグメンテーションで IT 資産を保護することで攻撃を阻止できることがこれほど広く認識されているにもかかわらず、セグメンテーションの導入が遅々として進まないという厳しい現実があります。

2 つ以上の重要なビジネス領域にわたってセグメンテーションを行っている e コマース組織はわずか 11% にとどまっています。48% は 2 年以上前にネットワーク・セグメンテーション・プロジェクトを開始しており、取り組みが停滞していることを示唆しています。

ミッションクリティカルな領域

- 重要アプリケーション
- 公開アプリケーション
- ドメインコントローラー
- エンドポイント
- サーバー
- ビジネス上重要な資産／データ

導入の遅れの原因は、 回答者が遭遇した上位の障壁が端的に示しています。 それは、 セグメンテーションのスキルや専門知識の不足 (40%)、コンプライアンス要件 (40%)、パフォーマンスのボトルネックの増加 (38%) であり 、いずれも従来のセグメンテーション手法にまつわるものです。 リソースや専門知識の不足がセグメンテーションプロジェクトの遅延のトップの原因である一方で 、サイバーセキュリティ全体にわたって人材不足が存在し 、さらにこの分野の変化が非常に速いことから 、スキルギャップの発生は避けられません。

どの地域でも、e コマース組織は困難に直面しており、米国と LATAM の組織の 100% が 、ネットワークのセグメント化にあたって問題があると回答しています。また、APAC(99%) と EMEA(97%) でも同程度の回答でした。

しかし、最も遭遇しやすい障壁は地域によって異なります (図 3)。これは、特定の問題 (スキルの不足、コンプライアンスなど) が、グローバルな問題と同じか、それ以上に、その地域の問題によって生じた可能性があることを示しています。

EMEA と LATAM の回答者は、セグメンテーションの最大の課題として、スキル／専門知識の不足（ともに 54%）を挙げています。米国の場合、最大の課題はパフォーマンスのボトルネックの増加 (44%) であり、APAC の場合、コンプライアンス要件 (43%) が問題になる傾向が強く出ています。

	発生する可能性が最も高い問題	2 番目、3 番目に発生する可能性が高い問題	
米国［59］	パフォーマンスのボトルネックの増加（44%）	コンプライアンス要件／適切なツールの不足（ともに 41%）	
LATAM［24*］	セグメンテーションのスキル／専門知識の不足（54%）	複雑性が非常に高い（46%）	使用している機器の一部／すべてが私有物、使用している機器の一部／すべてが古い（ともに 38%）
EMEA［39］	セグメンテーションのスキル／専門知識の不足（54%）	適切なツールの不足（41%）	コンプライアンス要件、使用している機器の一部／すべてが古い、非常に高価（いずれも 36%）
APAC［67］	コンプライアンス要件（43%）	適切なツールの不足、使用している機器の一部／すべてが私有物、パフォーマンスのボトルネックの増加（すべて 37%）	

図 3：ネットワークをセグメント化する際に、どのような問題が発生しましたか？グラフは、ある時点でネットワークをセグメント化したと回答した組織について、その上位 3 位までの回答を地域別で示したものです。なお、対象データは e コマースセクターのみです。

* 注意 – 回答者数は 30 人未満

重要ポイント：6 つの重要なビジネス領域をセグメント化した組織は、リスクを大幅に軽減できる

e コマース環境全体でより多くの資産を保護し、セグメント化することができれば、組織は即座により安全になります。適切なソリューションにより、セキュリティチームは攻撃を迅速に特定できるため、インシデントの平均検知時間 (MTTD) と平均応答時間 (MTTR) が向上します。しかし、資産のセグメンテーションが不十分な場合（通常はレガシーなセグメンテーションテクノロジーを使用した結果）、セキュリティギャップや盲点が生じ、組織の脆弱性が高まることもあれば、事後対応に追われることもあり得ます。しかし、ソフトウェア定義のアプローチによるセグメンテーションを適切に実行すれば、組織はアタックサーフェスをより適切に管理し、重要な資産をより効率的でコスト効率の高い方法で保護し続けることができます。

当社の調査によると、セグメンテーションを行うことで、セキュリティ侵害後の復旧が 11 時間早くなります。つまりこういうことです。6 つのミッションクリティカルな領域にセグメンテーションを実装した場合、ランサムウェア攻撃を完全に阻止するのにかかる時間は平均 3 時間です。1 つの資産に対してのみセグメンテーションを行っている場合は、14 時間かかります。

同様に、セグメンテーションにより、ラテラルムーブメントの阻止にかかる時間を 11 時間短縮できます。6 つのミッションクリティカルな領域すべてにセグメンテーションを実装した場合、ランサムウェア攻撃のラテラルムーブメントの動きを有意に制限するのにかかる時間は平均 3 時間です。1 つの資産に対してのみセグメンテーションを行っている場合は、平均 14 時間かかります。

どちらのシナリオにしても、この 11 時間の違いが貴社のチーム、評判、コストに及ぼす影響を考えてみてください。

攻撃の抑止にかかる時間

3 時間

6 つのビジネス資産すべてをセグメント化した場合に、ランサムウェア攻撃を完全に阻止するのにかかる平均時間。1 つの資産しかセグメント化していない場合：**14 時間**

ラテラルムーブメントの抑止にかかる時間

3 時間

6 つのビジネス資産すべてをセグメント化した場合に、ランサムウェア攻撃のラテラルムーブメント（横方向の移動）を有意に制限するのにかかる平均時間。1 つの資産しかセグメント化していない場合：**14 時間**

ソフトウェアベースのマイクロセグメンテーションソリューションによって課題を解決する方法

マイクロセグメンテーションは、より高度できめ細かなセグメンテーションを可能にするだけでなく、実装も容易にします。

Akamai Guardicore Segmentation のようなソフトウェアベースのソリューションは、ネットワークに物理的な変更を加えることなく、迅速に導入できます。新しいセグメントの IP 再設定も、サーバーやデバイスの物理的な配置場所の考慮も、必要ありません。そのため、ファイアウォールや VLAN のようなインフラベースのアプローチよりも、はるかに迅速かつ容易にソリューションを導入することができます。また、このソリューションはポリシーの適用を基盤となるオペレーティングシステムに依存しないため、ベアメタルサーバーからマルチクラウドの展開まで、あるいは Windows Server 2003、Windows XP のような旧来の技術から最新の POS システム、IoT ／ OT デバイス、コンテナ化技術まで、マシンやオペレーティングシステムを問わずシームレスに動作します。つまり、物理的な場所を問わず、1 つのインターフェースを備えた 1 つのソリューションを管理するだけで、環境全体を通して異なるオペレーティングシステムやデバイスによって行われる接続を可視化し、制御できるということです。

導入の容易さ

Akamai Guardicore Segmentation はまず、環境内で行われているすべての接続をインタラクティブに視覚化します。これは、主な導入障壁を克服するための重要な要素です。さらに Akamai は、パフォーマンスのボトルネックやコンプライアンス要件に対処するための能動的な方法をソリューションに組み込んでいます。

パフォーマンスのボトルネックは、セグメンテーションソリューションによるシステムへの技術的な負荷から必ずしも発生するわけではなく、人手がかかるというボトルネックから発生します。手作業でビジネス領域をセグメント化し、その領域が壊れたときに手作業でトラブルシューティングする場合にかかる時間と労力は、非常に大きなものになるでしょう。Akamai は、手作業によるセグメント化の必要性を減らすとともに、トップクラスのテクニカルサポートとプロフェッショナルサービスを提供することで、この問題、そして最大の導入障壁である専門知識の不足を解決しています。当社のセグメンテーションのエキスパートは、導入プロセスを通じてお客様とパートナーシップを組み、お客様固有の IT 環境におけるセグメンテーションの目標を確実に達成します。

ソリューション自体もセグメンテーションの導入をサポートしています。AI を活用したラベリングとポリシーの推奨と、一般的なユースケースに対応したすぐに使えるポリシーテンプレートにより、時間とクリック数を節約し、ワークフローをシンプル化し、ポリシー設定までの全体的な時間を短縮し、ヒューマンエラーによる設定ミスを防止します。あるお客様では、所要期間 2 年、総費用 100 万米ドル以上と見積もられていた緻密なセグメンテーションのプロジェクトを、たった 1 人のエンジニアでわずか 6 週間で実現し、プロジェクト全体のコストを 85% 削減しました。これは、ボトルネックに悩まされることなく、緻密なセグメンテーションを迅速かつ容易に導入できることを証明するものです。

セグメンテーションによるコンプライアンスの合理化

当社のお客様の多くは、PCI DSS、SWIFT、サーベンスオクスリー法（SOX 法）、HIPAA、GDPR など、多くの国固有のコンプライアンス要件や国際的なコンプライアンス要件の遵守を保証および証明するために当社のソリューションを導入しています。これらのコンプライアンス義務では、通常、PCI DSS 対応のカード所有者データ環境（CDE）のように、対象範囲内のデータを環境内の他のシステムから分離して保護することが求められます。ファイアウォールや VLAN でこのような分離を行うことは容易ではありませんが、当社のソフトウェアベースのソリューションであれば、対象データ専用のセグメントを作成し、そのデータにアクセスできるものとできないものに関する通信ルールを適用することができます。ほぼリアルタイムで履歴を表示できる当社のビジュアルマップを使用すれば、対象範囲内のデータが不正なユーザーやシステム、マシンによってアクセスされていないことを物理的に示すことで、コンプライアンス義務に準拠していることを証明できます。

適切なソリューションとサポートで辛抱強くセキュリティ体制を変革する

セグメンテーションを実施するのは非常に困難な場合があります。しかし、この報告書が示すように、効果的な実装に成功した企業は、サイバーリスクの大幅な低減を実現しています。適切なセグメンテーションを行うことで、ラテラルムーブメントを制限し、アクティブな攻撃を受けたときにインシデント対応の担当者が迅速に対応することができます。また、侵害が発生した後でも、復旧作業は確実に行われ、作業時間も短くなります。

従来のセグメンテーションの導入に伴う一般的な課題を克服するように設計されたソフトウェア定義のソリューションを選択し、エキスパートとパートナーシップを組みながら、セグメンテーションの導入を進めることで、セキュリティ体制を効果的に変革することができます。さらに、ビジネス領域をセグメント化すればするほど、現在のリスクを低減し、ゼロトラスト・アーキテクチャを強化できます。

調査対象

本レポートは、e コマースセクターに従事する 190 人の回答者（米国 59 人、EMEA 39 人、APAC 68 人、LATAM 24 人）を対象に分析したものです。

本調査全文では、10 か国の IT／セキュリティ意思決定者 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、各組織の環境セキュリティ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。

この調査は、米国、インド、メキシコ、ブラジル、英国、フランス、ドイツ、中国、日本、オーストラリアなど、世界各国にある、1,000 人以上の従業員を抱える、さまざまな業界およびセクターの組織を対象に実施しました。

注：このサンプルは、2021 年とは若干異なっています。サンプルサイズ：2023：全 1,200 件、2021 年：全 1,000 件。2023 年は、オーストラリア、日本、中国の回答者にもインタビューを実施。セクターは 2021 年とは若干異なります。2023 年は、デジタルコマースを独自のセクターとして特に焦点をあてました。

Akamai Guardicore Segmentation の詳細はこちら

Akamai は、お客様が生み出すものすべてにセキュリティを組み込む取り組みを支援することで、どこで構築しどこへ提供しようとも、顧客体験、従業員、システム、データを守ります。グローバルな脅威に対する可視性を備えた Akamai のプラットフォームは、セキュリティ体制の適応と進化を後押しして、ゼロトラストの実現、ランサムウェアの阻止、アプリケーションと API のセキュリティの確保、DDoS 攻撃の撃退を支援します。これにより、お客様は自信を持って、継続して、イノベーションを起こし、可能性を広げ、新たな可能性を生み出すことができます。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 で Akamai Technologies をフォローしてください。公開日：2024 年 5 月。

VansonBourne

Vanson Bourne 社は、テクノロジー分野の市場調査を専門とする独立系企業です。徹底したリサーチ原則と、あらゆる事業部門、あらゆる主要市場において、技術部門とビジネス部門の垣根を越えて上級意思決定者の意見を求める能力に基づく、堅実で信頼性の高いリサーチベースの分析で高い評価を得ています。詳しくは、www.vansonbourne.com をご覧ください。