Akamai

ホワイトペーパー

2023 年の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

目次

はじめに

IT セキュリティ部門の仕事はこれまでも決して楽ではありませんでした。しかし現在では、ますます巧妙になった攻撃者が技術を組み合わせて、より大規模で頻繁な脅威を引き起こすようになっており、セキュリティチームは以前にも増して大きなプレッシャーにさらされています。どのようなビジネスもオンラインプレゼンスなくして運営することはできず、たった一度の侵害が、評判や収益に深刻な（場合によっては取り返しのつかない）ダメージを与える可能性があります。

このレポートの調査結果からも分かるように、こうした攻撃の影響も大きくなっており、全体的なパフォーマンスやイノベーションを損なわずに適切なソリューションを選択し、環境全体の安全を確保しなければならないというプレッシャーが、セキュリティリーダーにのしかかっています。

2021 年以来、このレポートの調査結果を更新するにあたり、私たちはセグメンテーションがソリューションとして適しているのか、また、セグメンテーションは効果的なのかを明らかにすることを目的としました。回答した 1,200 社は、資産の保護を維持す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ましたが、重要なビジネスアプリケーションや資産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低いものでした。地域を問わず、最大の障壁は、セグメンテーションを導入するための専門知識が不足していることでした。特に IT 環境が複雑化しているため、パフォーマンスを阻害する可能性のあるセグメンテーションプロジェクトに着手することを多くの組織がためらっています。

朗報としては、この障壁を打破して、セグメンテーションを導入すれば必ず報われます。セグメンテーションは防御面で革新的な効果をもたらします。主要資産のほとんどをセグメント化した企業は、1 つの資産のみをセグメント化した企業よりも 11 時間早くランサムウェアを緩和し、封じ込めることができます。この 11 時間が、貴社のチーム、顧客、ブランドの評判、収益に及ぼす違いを想像してみてください。

ランサムウェア攻撃は増加の一途をたどり、その影響も深刻化

（成功か失敗かを問わず）ランサムウェア攻撃の件数は、2021 年の平均 43 件から 2023 年には 86 件と、過去 2 年間で倍増しています。2022 年第 1 四半期から 2023 年第 1 四半期にかけて、約 90 の異なるランサムウェアグループのリークサイトから収集したデータでは、さらに大幅な増加が計測されました。2023 年 8 月にリリースされた、「猛威を振るうランサムウェア：進化する悪用手法と執拗なゼロデイの利用」では、ゼロデイおよびワンデイ脆弱性の悪用によりランサムウェアの被害総数が 143% 増加したと報告されています。

米国企業が依然として最も多くのランサムウェアの脅威に直面していることは、言うまでもありません（図 1）：米国の IT セキュリティチームおよび意思決定者は、過去 12 か月間に平均 115 件のランサムウェア攻撃を受けたと報告しています。

過去 12 か月間のランサムウェア攻撃の国別平均件数

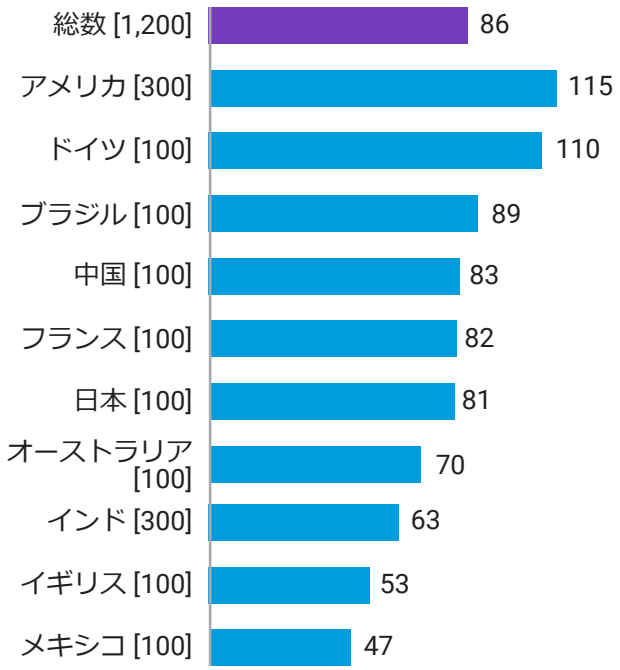

図 .1：過去 12 か月間に、あなたの組織は何件のランサムウェア攻撃を受けましたか（成功したかどうかは問いません）？ [1,200]、過去 12 か月間の平均攻撃回数のみを国別に分けて表示。

米国が、2 つ以上のミッションクリティカルなビジネス領域にわたってセグメンテーションを実装している可能性が最も低い 2 か国のうちの 1 つであることを考慮すると（図 2）、ランサムウェア攻撃で上位にランクインしていることと、セグメンテーションの導入で下位にランクインしていることは関連があるものと考えられます。

もちろん、米国におけるランサムウェア攻撃の多さは、ロシアのサイバー犯罪グループが連邦政府機関に対して行った 2023 年の大規模な侵害のニュース性の高さや、米国の IoT デバイスの普及率（2 位の中国より 20 億台多い）など、さまざまな要因に起因すると考えられます。IoT 向けランサムウェア（R4IoT）は、IP カメラなどの脆弱な IoT デバイスを悪用して最初の足掛かりを得ると、IT ネットワーク内でラテラルムーブメントを図り、貧弱なセキュリティ慣行を利用してミッションクリティカルなプロセスを占拠してしまいます。

ランサムウェア攻撃は、2023 年と 2021 年を比較すると、世界的に頻度が高くなっただけでなく、その影響も大きくなっています（図 3）。回答者は、ネットワークのダウンタイム、データ損失、評判の失墜が増加していると回答しており、こうしたことがすべて、セキュリティチームへの負担を大きくしています。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組織の数は、2021 年の 5% から 2023 年には 13% に増加しています。セキュリティ戦略に日々影響を与える要因は、従業員の分散とアプリケーション／データのクラウド移行だけではありません。

2 つ以上の資産／領域をセグメント化している回答者（国別）

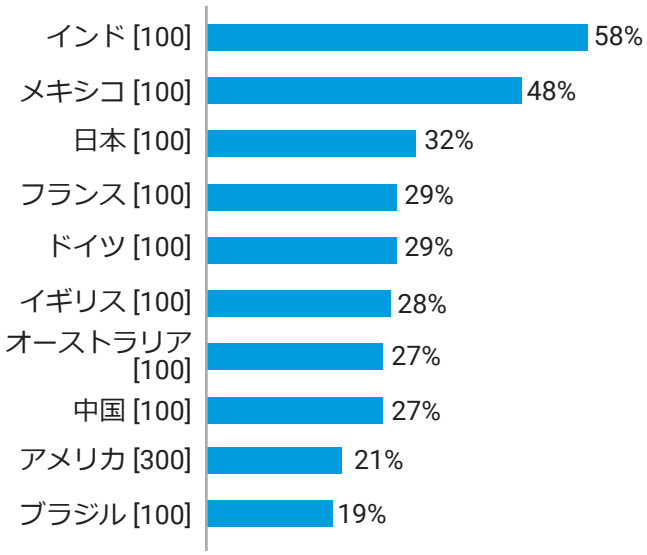

図 2：以下の IT セキュリティ対策について、どの資産を対象としていますか？ [1,200] 、セグメンテーションのセキュリティ対策のみに関する回答と、重要資産の保護にセグメンテーションを使用している割合を国別に表示。

ランサムウェア／サイバー攻撃の影響

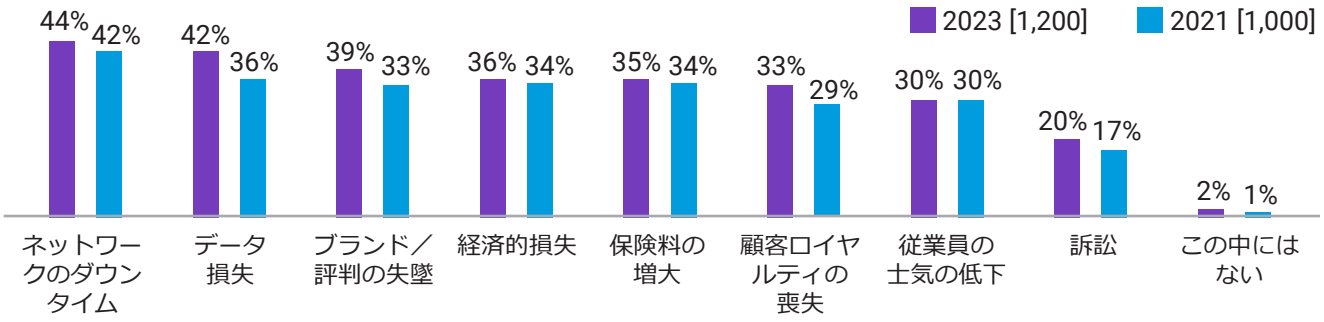

図 3：過去にランサムウェアやその他のサイバー攻撃を検知した際に、組織に及んだ影響は次のうちどれですか？［チャートのベースサイズ］、回答の選択肢の一部について、過去のデータと比較して表示。

各地域の調査結果

サイバー攻撃者は南北アメリカの組織を標的にする傾向が強い：ランサムウェア攻撃の総数は南北アメリカで最も多く、過去 12 か月の平均攻撃数は EMEA の 83 件、APAC の 75 件に対して 96 件でした。

セグメンテーションとマイクロセグメンテーションは、EMEA よりも APAC と南北アメリカで重要視されている：APAC（62%）および南北アメリカ地域（60%）の IT セキュリティチームおよび意思決定者は、EMEA（53%）に比べて、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上で非常に重要であると回答する傾向が高くなっています。

マイクロセグメンテーションが最優先事項であると回答した割合は、APAC（35%）および EMEA（23%）の回答者よりも南北アメリカの回答者の方が高くなっています（41%）。

EMEA では、セグメンテーションを行わない傾向が強い：ビジネスクリティカルな資産をセグメント化していないと回答した組織は、EMEA（10%）が APAC（4%）や南北アメリカ（1%）よりもはるかに多くなっています。

最も導入が遅れているのは英国で、23% の組織が**まったくセグメント化していないと回答しています。**セグメント化を妨げる主な障壁となっているのが、旧式の機器（46%）でした。

APAC の組織は最もセグメント化している：APAC の組織は、EMEA（29%）や南北アメリカ（26%）よりも、2 つ以上のビジネスクリティカルな資産をセグメント化している傾向が高くなっています（36%）。

どの地域でも、組織は困難に直面している：南北アメリカの 97% 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、EMEA（94%）と APAC（97%）でも同程度の回答でした。

EMEA と APAC の回答者は、セグメンテーションの最大の障壁として、スキル／専門知識の不足（EMEA は 38%、APAC は 43%）を挙げています。南北アメリカでは、最大の障壁として、パフォーマンスのボトルネックの増加と回答しています（41%）。

南北アメリカでは、自社のゼロトラストセキュリティの枠組みが成熟していると考える企業が増えている：南北アメリカの回答者は、APAC（35%）や EMEA（33%）よりも、ゼロトラストの展開が完全に完了し、定義されていると回答する割合が高くなっています（49%）。

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。業種を問わず、93% がセグメンテーションは有害な攻撃を阻止する上で重要だと考えており、中でも製造／生産業では 99% に上っています。これは、これらの業界ではサプライチェーンが複数のサードパーティーに大きく依存しており、混乱が発生するとビジネスに大規模な連鎖的影響を及ぼす可能性があるためと考えられます。

また、セグメンテーションはゼロトラストのフレームワークにも大きく貢献します。セグメンテーションプロジェクトを開始した理由を尋ねると、「ゼロトラストを推進するため」という回答が 3 番目に多く寄せられました。セグメンテーションを実施したほぼすべての企業が、ゼロトラストのセキュリティフレームワークを導入中または導入済み（99%）だと回答しています。ただし、ゼロトラストのフレームワークが完全に定義され、完成していると回答した企業は 5 社に 2 社（40%）にとどまりました。

世界全体では、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。89% がマイクロセグメンテーションを優先度は高いと回答し、34% が最優先事項だと回答しています。さらに、IT セキュリティチームと意思決定者の 97% 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。この数字は、公共部門（ヘルスケア部門を除く）では 80% にまで低下します。この差は、マイクロセグメンテーションによるワークロードレベルの保護を導入する上で、厳しい予算と古いインフラが大きな障壁となっていると考えられます。

マイクロセグメンテーション

自分の業界の一部の組織がマイクロセグメンテーションを導入していると回答した IT セキュリティチームと意思決定者の割合

しかし、公共部門がマイクロセグメンテーションのような高度なセキュリティ技術を実装すれば、大きなメリットが得られます。公共部門のシステムは必ずしも連携するように設計されていないため、相互運用性がなく、人為的ミスの可能性とサイバー攻撃が成功する可能性の両方が高まります。

公共部門の回答者の 93% がセグメンテーションの重要性を認識しているにもかかわらず、15% がセグメンテーションを行っていないと回答しています。公共部門はセグメンテーションの導入率が最も低い業界であり、最大の障壁はコンプライアンス要件（52%）です。

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、パフォーマンスとセキュリティを強化する目的で、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アプローチです。

マイクロセグメンテーションは、ネットワークを個々のワークロードレベルのセグメントに分割し、セキュリティ制御とサービス提供をセグメントごとに定義します。

導入には時間がかかるが、粘り強く取り組めば革新的な結果が得られる

セグメンテーションが攻撃を阻止する鍵であ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。2023 年時点で 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組織はわずか 30%（2021 年は 25%）にとどまっています。44% 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。

重要なビジネス領域

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（39%）、パフォーマンスのボトルネックの増加（39%）、コンプライアンス要件（38%、図 4）です。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、同じ障壁を報告しています。スキルや専門知識の不足がセグメンテーションプロジェクト遅延の最大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。

しかし、遅々として進んではいないものの、セグメンテーションの割合は全体として徐々に増加しています。2021 年から 2023 年にかけて、ビジネス上重要なアプリケーション／データをセグメント化している組織の割合は 12% 増加し、サーバーをセグメント化している組織の割合は 8% 増加しました。

ネットワークセグメンテーションを妨げる障壁

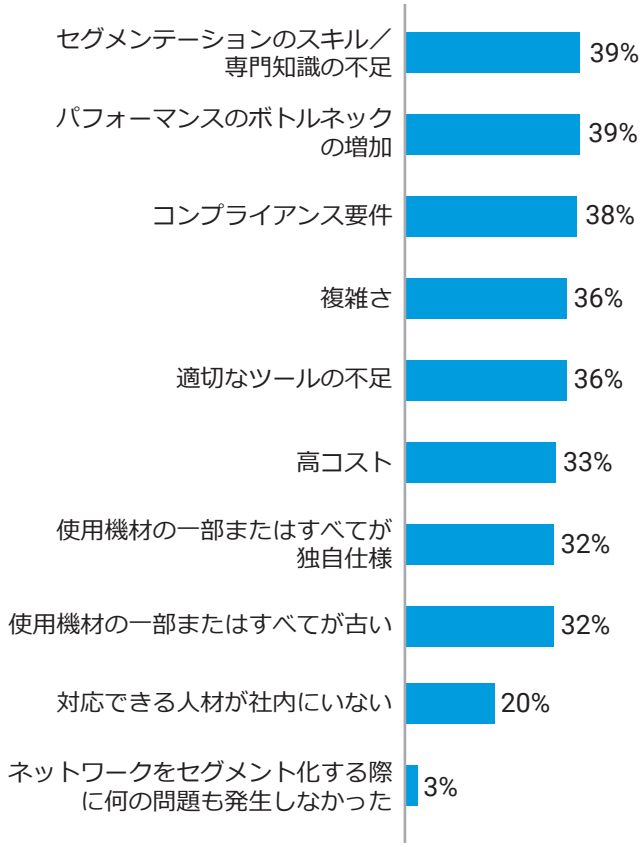

図 4：ネットワークをセグメント化する際に、どのような問題が発生しましたか？ [1,187]、いずれかの時点でネットワークをセグメント化した組織にのみ表示。回答の選択肢は一部のみ表示。

結論：6 つの重要なビジネス領域をセグメント化すれば、リスクを大幅に軽減できる

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、組織はより安全になります。セキュリティチームは攻撃を特定しやすくなり、はるかに効果的に対応できるようになります。セグメンテーション戦略が未熟であったり、定義が不十分であったりすると、組織のリスクは高まるばかりです。しかし、正しく行うのであれば、セグメンテーションに障壁を克服して実装する価値があることは明らかです。

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ている場合、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 4 時間です。一方、1 つの資産に対してのみセグメンテーションを実施している場合は、15 時間です。

同様に、セグメンテーションでラテラルムーブメントを制限すると 11 時間短縮されます。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。

どちらのシナリオでも、11 時間の違いがチームに与える影響や、コストやブランドへのダメージの抑制に与える影響を考えてみてください。

攻撃の抑止にかかる時間

4 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：
15 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 を再設定したり、サーバーやデバイスの物理的な配置場所を考慮したりする必要はありません。このため、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、ポリシーの適用に独自のドライバーを使用しているため、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 のような旧来の技術から最新の IoT/OT デバイスや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

マイクロセグメンテーションはまず、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、必ずしもセグメンテーションソリューションによるシステムの技術的な負担から生じるとは限りません。手作業でビジネス領域をセグメント化し、その領域が破損したときに手作業でトラブルシューティングを行うことによって生じる従業員のボトルネックが原因となることもあります。Akamai は、手作業によるセグメント化の必要性を減らし、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。

コンプライアンスの緩和

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、国内外の数多くの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展開しています。このようなコンプライアンス遵守の要求に対しては、通常、対象範囲内のデータを環境内の他のシステムから分離する必要があります。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、これらの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、脅威のラテラルムーブメントを制限し、アクティブな侵害時に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、時間もかかりません。

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、将来の脅威ベクトルに対する第一線の防御を確保することで、ゼロトラスト・アーキテクチャを強化できます。

調査対象

Akamai 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にフォーカスしながら、各組織の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。

調査対象者は、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。

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 年：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、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、アプリケーションと API のセキュリティの保護、インフラの保全を支援します。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 のセキュリティ、コンピューティング、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：2023 年 10 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。