Akamai

e ブック

重要な銀行システムの保護における導入障壁の克服

世界のセグメンテーションの現状に関するレポート

目次

はじめに

金融サービス業界の IT セキュリティチームは、かねてより、重大かつ固有の課題に直面していました。しかし現在では、ますます巧妙になった攻撃者がさまざまな手法を組み合わせて、より大規模で頻繁な脅威を引き起こすようになっているため、金融サービス機関の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。金融サービス機関はデジタルプレゼンスなくして運営することはできません。そのため、一度でも侵害を許してしまうと、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）ダメージを受け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は大きくなっています。全体的なパフォーマンスを低下させたり、大量の機微な情報を危険にさらすことなく、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。

金融サービス機関の回答者（米国、LATAM、EMEA、APAC など、全地域の回答者）は、資産を保護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ていますが、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。金融サービス機関にとって最大の障壁となっているのが、ボトルネックの増加です。これは、セグメンテーションの導入がパフォーマンスに及ぼす影響を十分に理解して緩和するための時間やサポートがない状態で、セキュリティチームが脅威に対応してきたことを示唆しています。

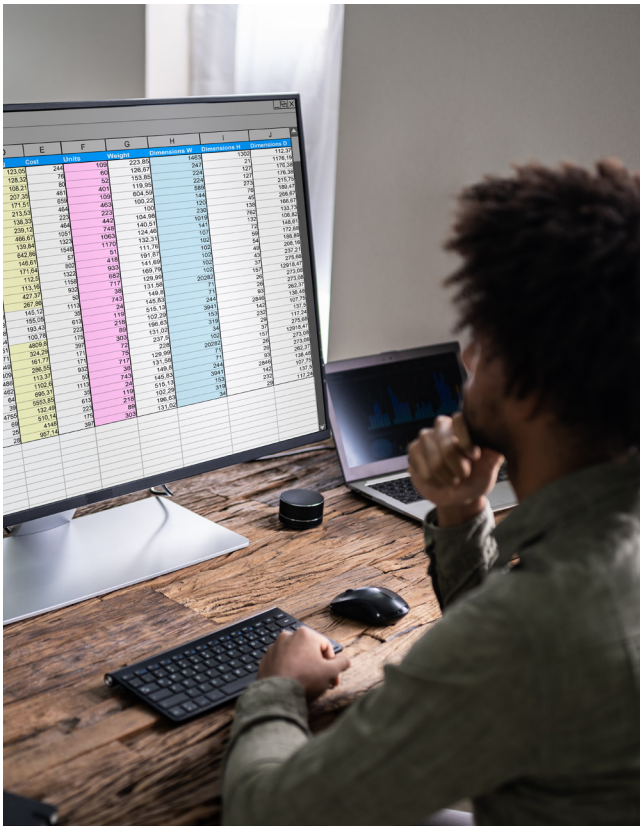
幸い、この障壁を打破して、セグメンテーションを導入すれば必ず報われます。セグメンテーションは防御面で革新的な効果をもたらします。主要資産のほとんどをセグメント化した企業は、1 つの資産のみをセグメント化した企業よりも 13 時間早くランサムウェアを緩和し、封じ込めることができます。この 13 時間が、貴社のチーム、顧客、ブランドの評判に及ぼす違いを想像してみてください。

調査結果：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、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とは、個々のワークロードのレベルまで、ネットワークを細かいセキュリティセグメントに論理的に分割するセキュリティ手法です。これにより、分割したセグメントごとにセキュリティ制御やサービスデリバリーを定義できます。



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

金融サービス機関に対するランサムウェア攻撃の件数（成功か失敗かを問わず）は、2021 年の平均 43 件から 2023 年には 62 件と、過去 2 年間で 50% 近く増えています。金融サービス業界は堅牢なセキュリティ対策を導入していることで有名です。しかし上記の数字は、この業界が決して無視できない重大な脆弱性を抱えていることを示しています。金融サービス業界がランサムウェア攻撃と無縁ではないことは明らかです。油断は許されません。

ランサムウェア攻撃の件数が最も多かったのは APAC 地域の金融サービス機関（73）で、最も少なかったのは LATAM（48、図 1）でした。

金融サービス業界における過去 12 か月間の平均ランサムウェア攻撃件数（地域別）

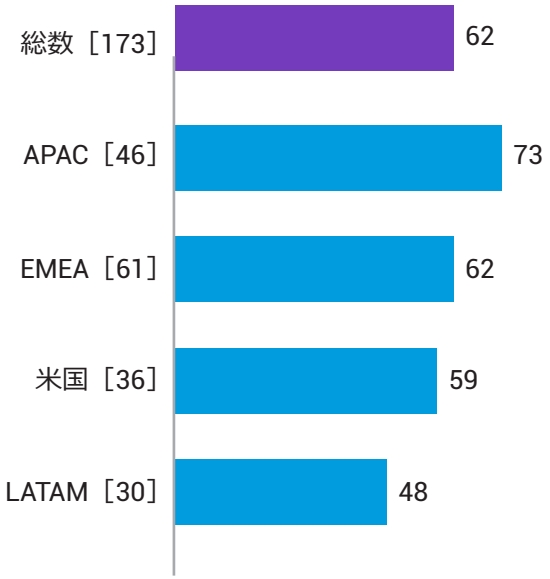


図 1：過去 12 か月間に、組織は何件のランサムウェア攻撃を受けましたか（成功したかどうかは問いません）？過去 12 か月間の平均攻撃件数を地域別に示しています（カッコ内は回答者数）。金融サービス機関の回答のみ表示。

金融サービス機関の多くはグローバルに事業を展開しています。APAC の金融サービス機関に対する攻撃件数が増加したのは、その方が見返りが大きいとハッカーが認識しているためかもしれません。しかし、だからといって、他の地域の金融機関が安全だというわけではありません。ラテラル攻撃により、ある地域で発生した攻撃が別の地域へと広がることもあるからです。

2 つ以上の資産をセグメント化していると述べた回答者が最も多かったのは LATAM で、次いで APAC でした。これは、ランサムウェア攻撃件数の増加を受けて、APAC の金融機関がセグメンテーションを進めていることを示しています。

2 つ以上の資産／領域をセグメント化していると回答した金融サービス機関（地域別）

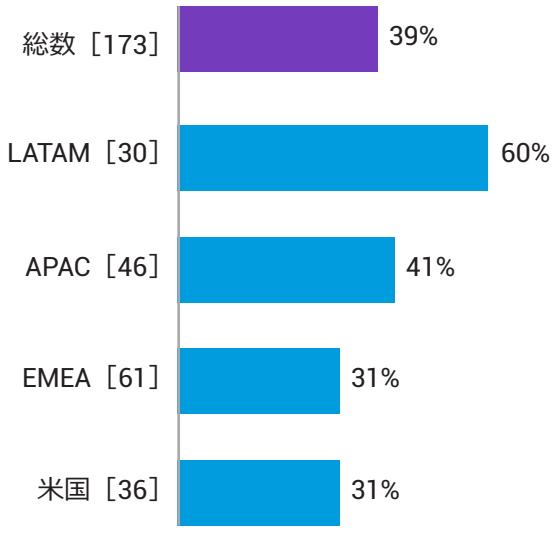


図 2：以下の IT セキュリティ対策について、どの資産を対象としていますか？セグメンテーションのセキュリティ対策のみに関する回答と、重要資産の保護にセグメンテーションを使用している割合を地域別に示しています（カッコ内は回答者数）。金融サービス機関の回答のみ表示。

2023 年と 2021 年を比較すると、ランサムウェア攻撃は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とデータの損失が増加していると回答しており、この両方がセキュリティチームへの負担を大きくしています。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（米国では 56%）。この保険料は、個人データだけでなく、企業データも保有する金融機関がどれだけのリスクを抱えることができるかを示しています。

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金融サービス機関の数は、2021 年の 3% から 2023 年には 18% 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。

金融サービス機関に対するランサムウェア／サイバー攻撃の影響

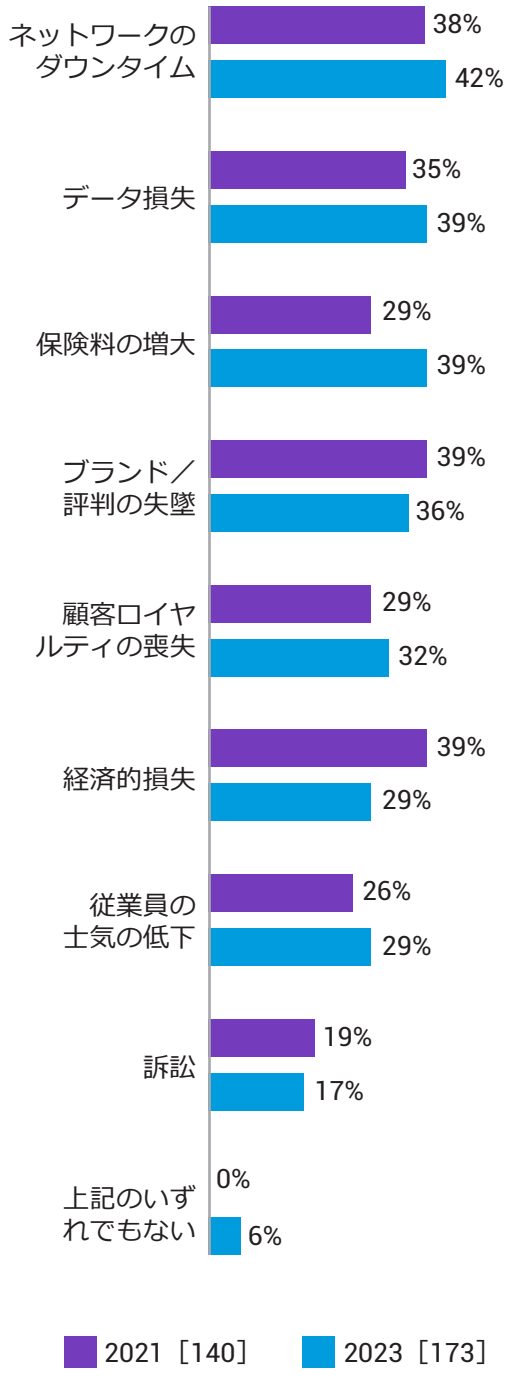


図 3： 過去にランサムウェアやその他のサイバー攻撃を検知した際に、組織に及んだ影響は次のうちどれですか？金融サービス業界の各年のデータを並べて表示しています。カッコ内は回答者数です。回答選択肢の一部のみ表示しています。

セグメンテーションはゼロトラストの基盤

金融サービス業界の回答者は、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。66% が「非常に重要」と回答し、92% が「打撃となる攻撃を阻止するためには不可欠」と回答しています。

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たところ、「ゼロトラストを推進するため」との回答が最も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（99%）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 47% にとどまりました。

金融サービス機関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。88% 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、39% が最優先事項だと回答しています。最優先事項だと述べた回答者の割合が最も高かったのは LATAM（50%）で、最も低かったのは EMEA（31%）でした。最優先事項だと回答した割合が LATAM の方が高かったことは、ランサムウェア攻撃を受けた回数（図 1）にも表れており、マイクロセグメンテーションを重視することのメリットを示しています。

さらに、金融サービス業界の意思決定者の 99% 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。これは、マイクロセグメンテーションがほぼすべての金融サービス機関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。

粘り強い取り組みが変革的な成果をもたらす

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金融サービス機関はわずか 39%（2021 年は 26%）にとどまっています。45% 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。

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、パフォーマンスのボトルネックの増加（41%）、セグメンテーションのスキルや専門知識の不足（39%）、コンプライアンス要件（35%）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遅延の主な原因である一方で、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。

ただし、遭遇する障壁は地域によって異なります（図 4 参照）。これは、特定の障壁が、多かれ少なかれ、その地域の条件（米国におけるスキル不足、APAC におけるコンプライアンス要件など）に起因しており、グローバルな問題ではないことを示しています。

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 17% 増加し、サーバーをセグメント化している組織の割合は 17% 増加しました。これらの増加率は全業界の平均増加率（それぞれ 12% と 8%）を上回っています。これは、金融サービス機関の IT 部門は他の業界と比べて、遭遇した障壁に対応する能力がいくぶん高いことを示しています。セグメント化している金融サービス機関の割合が高い理由は、金融サービス業界では一般的にコンプライアンス要件が厳格であり、より強力なセキュリティが求められるためだと考えられます。また、金融サービス機関が支払う保険料が高いこと、そして特定の問題に速やかに対応することを保険会社が金融サービス機関に義務付けていることも理由の 1 つかもしれません。

金融サービス機関がネットワークをセグメント化する際に遭遇する障壁のトップ 3（地域別）

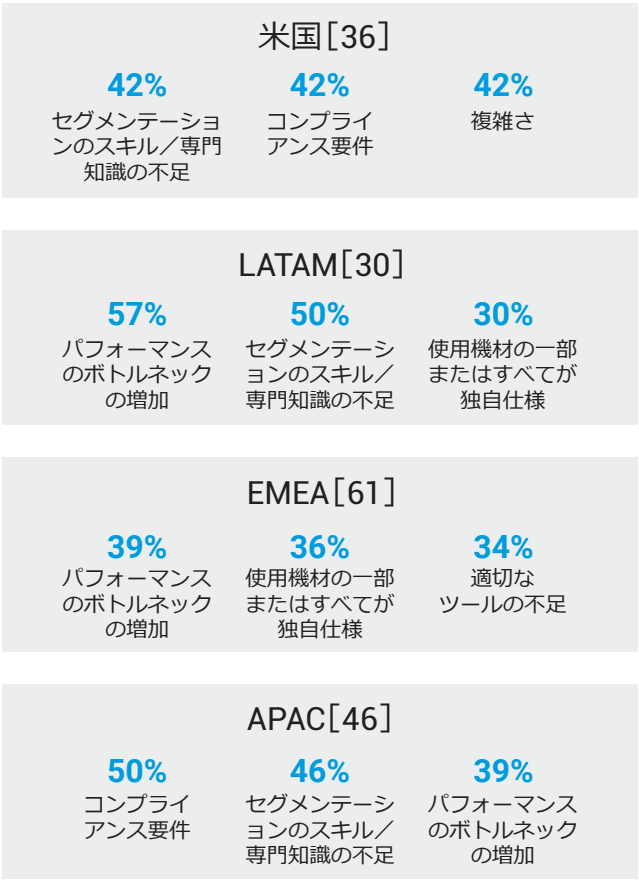


図 4：ネットワークをセグメント化する際に、どのような問題が発生しましたか？ネットワークをセグメント化していると回答した組織にのみ質問し、各地域のトップ 3 の回答を表示しています。金融サービス機関の回答のみ表示。カッコ内は各地域の回答者数。

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

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、金融機関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。未成熟または不明瞭なセグメンテーション戦略を導入すると脆弱性が増すだけですが、適切にセグメント化することで、サイバー攻撃への耐障害性を強化して、ランサムウェアやセキュリティ侵害が重要なシステムやデータに広がるのを阻止し、大規模な業務中断を回避できます。

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 13 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、16 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。

この 11 ～ 13 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：**16 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

金融機関は、ワークロードをクラウドに移行することで、スケーラビリティの強化、既存の投資の活用、コストの最適化、アジリティと柔軟性の改善を実現しようとしています。また、多くの組織がオンプレミスのデータセンターをプライベート／パブリッククラウドと統合しています。アプリケーションレベルのセキュリティに対するより柔軟で合理化された、コスト効率の高いアプローチとして現在注目されているのが、Akamai Guardicore Segmentation のような、ソフトウェア定義のセグメンテーションソリューションです。このようなソリューションにより、実装を大幅に加速して、メンテナンスをシンプル化し、脅威を効果的に緩和できます。ファイアウォールや VLAN などのインフラベースのアプローチよりも迅速かつ簡単に導入できるため、金融機関は自社の加速するビジネスニーズに対応しながら、広範囲にわたってセキュリティを確保し、最先端のテクノロジーを通じて革新的な顧客体験を提供できます。さらに、さまざまなシステムと環境にわたってシームレスに動作するため、ベアメタルサーバー、マルチクラウド導入、レガシーシステムのすべてを一元管理できます。物理的所在地を問わず、ひとつのソリューションを通じて、環境全体にわたる接続を可視化して制御できるのです。

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。

マイクロセグメンテーションによるコンプライアンスの実現

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）、GDPR、DORA など、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は複雑な作業となる場合があります。しかし、本レポートが示すように、効果的に実装した組織は、ネットワークセキュリティの強化、ネットワークパフォーマンスの改善、コンプライアンスの確保、ネットワーク管理のシンプル化などのメリットを獲得しています。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、作業時間も短くなります。

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。

各地域の調査結果

LATAM よりも EMEA と米国の方がセグメンテーションとマイクロセグメンテーションを重視している：EMEA（70%）および米国（60%）の IT セキュリティ意思決定者は、LATAM（57%）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述べた回答者は LATAM の方が多い：LATAM が 50% だったのに対して、米国は 42%、APAC は 41%、EMEA は 31% でした。

セグメンテーションをまったく行っていないと述べた回答者は EMEA が最も多い：ビジネスクリティカルな資産をまったくセグメント化していないと述べた回答者は EMEA（7%）が最多でした。他の地域はある程度セグメント化しています。

セグメンテーションを最も推進しているのは LATAM の組織：LATAM（60%）の金融サービス組織は、APAC（41%）、EMEA（31%）、米国（31%）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。

どの地域でも、組織は難題に直面している：ネットワークをセグメント化する際に障壁に遭遇していると回答した組織は、APAC が 98% で、米国もほぼ同水準の 97% でした。一方、EMEA は 89%、LATAM は 87% と、いくぶん低くなっています。

ゼロトラスト・セキュリティ・フレームワークの展開に関しては、LATAM の金融サービス機関の方がはるかに成熟度が高い：LATAM（57%）の回答者は、EMEA（48%）、米国（47%）、APAC（41%）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した割合が高くなっています。

調査対象

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。

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、さまざまな業界の組織を対象に実施しました。

このレポートでは、金融サービス業界に従事する 173 名（2023 年）および 140 名（2021 年）の回答を分析しました。

Akamai Guardicore Segmentation の詳細はこちら

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。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 の金融機関向けソリューションの詳細については、akamai.com/finserv 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。