ESG エグゼクティブサマリー

Zero Trust Impact Report：日本に関する主要な調査結果

日付: 2022 年 6 月 著者:John Grady（シニアアナリスト）、Adam DeMattia（カスタムリサーチディレクター）

攻撃対象領域が拡大しゼロトラストへの関心が増加

デジタルトランスフォーメーションにより生み出された、ユーザー、アプリケーション、データ、モノのハイパーコネクティビティによって、攻撃対象領域は大きく拡大され、リスクが増大しました。このトレンドを悪用しようとする攻撃者はあらゆる手法で標的を侵害しており、攻撃の多くが重大な業務の混乱を引き起こしています。これら問題に対処するため、多くの組織はゼロトラストアーキテクチャの実装を開始し始めており、サイバーセキュリティプログラムをモダナイズし、攻撃の影響を制限しようとしています。ゼロトラストに対する組織の立ち位置や、セグメンテーションが組織の戦略において具体的にどのように組み込まれているかといった詳細を把握するため、Illumio は米 Tech Target Inc.の調査部門 Enterprise Strategy Group（ESG）に委託し、北米、ヨーロッパ、アジア太平洋地域、日本に拠点を置く組織の IT およびセキュリティの専門家 1,000 人を対象にグローバル調査を実施しました。日本の回答者から得られた主な調査結果は、次の通りです。

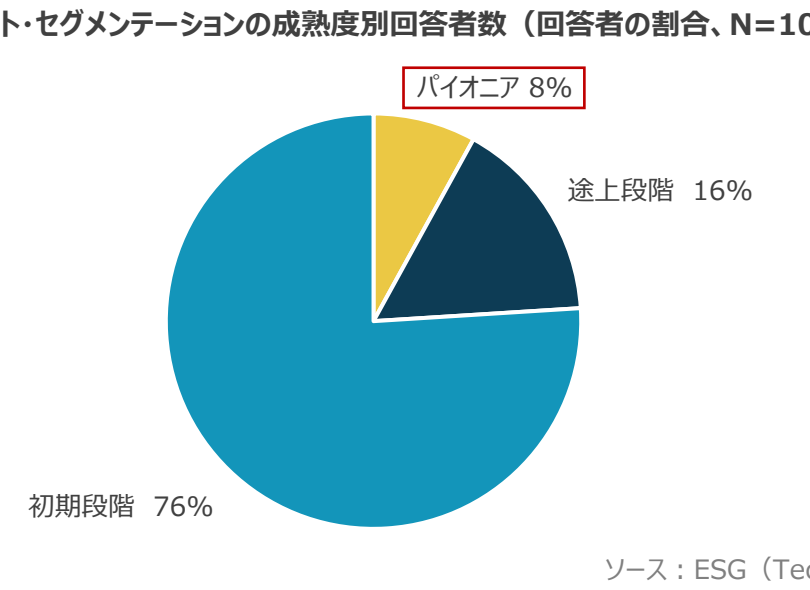
- 日本の回答者の内、自身の組織は侵害に対処する準備ができていると回答したのはわずか 10%で、そのような侵害が甚大な被害につながりかねないと認識している回答者は 48%でした。これに対して、米国の回答者では、侵害に対処する準備ができていると回答したのは 26%でした。
- ランサムウェア攻撃によりデータやシステムを人質に取られたことのある日本の回答者の半数以上の 58%が、直接またはサイバー保険会社を介し身代金の支払いを強いられていました。日本における身代金支払い額の平均は¥23,800,000 以上でした。
- 日本の組織はゼロトラストを優先しており、回答者の 83%がゼロトラストがサイバーセキュリティの優先事項上位 3 つのうちの 1 つであると回答しました。また、セキュリティ予算全体の平均 31%をゼロトラストへの取り組みに割り当てています。
- ゼロトラストに関する知識が浸透している日本の組織では、攻撃の被害を受ける可能性があるにも関わらず、回答者の 53%が、侵害されるということを前提にしたオペレーションを行っていません。日本はシンガポールの回答者（38%）と比較しても大幅な遅れをとっており、組織の行動および発言と、実際のオペレーションに明らかな齟齬があることが示されています。

ゼロトラスト・セグメンテーションの成熟度

ESG は調査の一環として、ゼロトラスト・セグメンテーションに向けた進捗状況を評価して回答者を分類しました。ゼロトラスト・セグメンテーションは、データセンターからクラウドまで、ハイブリッドな IT 環境も含め、侵害が拡散することを防止するための最新の手法です。これには、「すべてのアプリケーションタイプ、ロケーション、エンドポイントによる包括的な可視化」、「発生した攻撃に対する迅速かつ効果的な阻止」、「さまざまな IT 環境の適切なセグメント化（OT からの IT のセグメント化、本番環境からの開発環境のセグメント化など）」、「最終的にこれらの機能を環境全体に拡張して優先度の高いリソースを囲い、すべてのアプリケーションで適切なセグメンテーションを行うことで環境内のあらゆる場所でラテラルムーブメントを防止すること」が含まれます。

「SIEM および SOAR ソリューションとの統合」、「環境の分離」、「感染を封じ込める力」、「環境全体ののの一貫した可視性と制御」というセグメンテーションのテクノロジーと実践に関連する 5 つの重要な質問に対する回答への評価、に基づき、3 つのカテゴリーに調査対象の回答者を分類しました。「初期段階」カテゴリーに分類された回答者は 5 つの質問のうち 0～2 つの質問で非常に優れた能力を有しており、「途上段階」カテゴリーに分類された回答者は 3～4 つの質問で非常に優れた能力を有しています。「パイオニア」カテゴリーに分類された回答者は、5 つのすべての質問で非常に優れた能力を有しています。日本では、この「パイオニア」に分類された回答者は 8%のみでした。この数字は他の多くの国よりも高い結果でしたが、日本では多くの組織がゼロトラストの重要性を認識しているにも関わらず、「侵害を前提とする」という考え方に基づくセグメンテーションの導入には、まだまだ長い道のりがあることについては変わりありません。

図 1. 日本におけるゼロトラスト・セグメンテーションの成熟度



ソース：ESG（TechTarget, Inc.の一部門）

なぜ、このようなグループ分けが重要なのでしょうか？「パイオニア」に分類された回答者には、その他の回答者にはないセキュリティおよびビジネス上の大きな優位性が認められます。国を問わず、ゼロトラスト・セグメンテーションの「パイオニア」からは以下の調査結果が得られました。

- **優れた可視性：**環境全体のトラフィックを包括的に可視化できる可能性が 4.3 倍高く、すべてのアプリケーションアーキテクチャを包括的に可視化できる可能性が 5 倍高い。
- **年間ダウンタイムコストの削減：**攻撃による重大な業務の停止を回避する確率が 2 倍高く、また、平均修復時間（MTTR）が 68%短い。業務停止の回避および攻撃発生時の迅速な修復の結果、「パイオニア」ではダウンタイムコストを年間 2,010 万ドル削減している。
- **迅速なデジタルトランスフォーメーション：**今後 1 年間で、セキュリティに対する信頼性の懸念により導入されていなかった 14 の本番環境アプリケーションをクラウドに移行予定。これにより、週あたり平均 39 人時を短縮している。
- **甚大なサイバー被害の防止に対する信頼性**：2 倍以上がサイバー攻撃に対処する準備ができていると認識しており、年間 5 件の甚大なサイバー被害を防止している。

ゼロトラスト・セグメンテーションの「パイオニア」の成功事例およびその結果に至るまでの過程に関する詳細は、レポートの全文で確認できます。

Enterprise Strategy Group は、テクノロジー分析、調査、戦略の統合企業であり、マーケットインテリジェンス、実用的なインサイト、市場開拓コンテンツサービスをグローバルITコミュニティに提供しています。

www.esg-global.com contact@esg-global.com 508.482.0188