ロード・トゥ・ゼロトラスト

Road to Zero Trust

ジャパンサーベイ 2021 年版

paloalto NETWORKS

目次

はじめに

企業のビジネス環境はいま、テクノロジーによって大きく変化し始めています。テレワークやクラウドの普及で、従業員は場所を問わずどこからでもビジネスリソースにアクセスして業務を行えるようになりました。

それだけではありません。業務効率化や企業競争力の強化を可能にするデジタルトランスフォーメーション (DX) や、IoT の利活用もますます進んできています。その結果、企業のインフラからは従来の「社内」「社外」という概念はなくなり、サイバー攻撃や内部犯行といったサイバーリスクも大きく多様化、深刻化しています。

このような企業インフラとサイバーリスクの変化にともない、国内・海外問わず、多くの企業・組織から注目が集まっているのがゼロトラスト (Zero Trust) です。ゼロトラストは、Forrester Research が生み出した「Never trust, always verify(信頼せず、常に検査する)」というサイバーセキュリティ戦略です。ゼロトラストの採用には、単なるセキュリティツールの導入ではなく、原理・原則に対する理解と、それを踏まえた自組織環境への実装、徹底が不可欠になります。

サイバーセキュリティのリーディングカンパニーであるパロアルトネットワークスでは、国内企業のゼロトラストに対する取り組みの現状、課題や障壁を明らかにする目的で、「ロード・トゥ・ゼロトラスト ジャパンサーベイ 2021 年版」を 2021 年 7 月に実施しました。今回の調査では、企業のサイバーセキュリティの取り組みを、ゼロトラストの観点を含めて全般的に定量的に評価しています。ゼロトラストの原理・原則の理解度や適用度合い、採用にあたっての格差をはじめ、ゼロトラストの採用やサイバーセキュリティの取り組みが全般的に進んでいる企業と進んでいない企業間での違いを明らかにしています。

「ロード・トゥ・ゼロトラスト ジャパンサーベイ 2021 年版」をより多くの国内企業・組織の皆様にご一読いただき、ゼロトラスト採用への取り組みの一助としてご活用いただくことを期待しています。

染谷征良
パロアルトネットワークス株式会社 チーフサイバーセキュリティストラテジスト

調査概要

調査名	**ロード・トゥ・ゼロトラスト ジャパンサーベイ 2021 年版**	
目的	国内企業のゼロトラスト採用に向けた取り組みの現状と、採用に当たっての課題を明らかにする	
調査対象 (単位 : 名)	国内民間企業において、サイバーセキュリティに関連した決裁権者、意思決定権者、ならびに関与者 401 名	
	売上高別	• 1 兆円以上 : 90 • 5,000 ～ 9,999 億円 : 67 • 1,000 ～ 4,999 億円 : 126 • 500 ～ 999 億円 : 118
	従業員規模別	• 10,000 名以上 : 103 • 5,000 ～ 9,999 名 : 95 • 1,000 ～ 4,999 名 : 103 • 500 ～ 999 名 : 100
	役職別	• 経営者・CxO: 32 • 執行役員・本部長 : 43 • 部長・課長 : 224 • 主任・チームリーダー : 81 • 現場担当者 : 21
手法	インターネット調査	
実施時期	2021 年 7 月 1 日～ 5 日	

エグゼクティブサマリー

大多数の国内企業がゼロトラストに注目

- ゼロトラストのサイバーセキュリティ戦略を採用済みとする企業は少数派
- 多くの企業はゼロトラストに関する情報収集や採用の是非の検討段階
- インフラとサイバーリスクの変化が企業のサイバーセキュリティの再考を促す

ゼロトラストの原則を理解している企業は少数派

- 「すべてのリソースから信頼を排除する」がゼロトラストの原則
- 様々な解釈が存在していることが市場の混乱状況を反映
- ゼロトラスト実現の大前提として原則の理解に基づく取り組みが重要

国内企業の「ゼロトラスト成熟度」は、平均的には決して高いレベルにはない

- セキュリティレベルが最も高いレベルに属する企業はわずか
- 各ドメインでのセキュリティツールの導入自体は進んでいる
- ツールを活用した実装の粒度には特に課題が残る

ゼロトラスト成熟度の高い企業とそうでない企業には決定的な違い

- ゼロトラストの原則に忠実な取り組みがインフラ全体で行われているか
- 各ドメインにおけるセキュリティファンクションの実装粒度
- 単なるセキュリティツールの導入だけでなく原則に基づいた取り組みが国内企業には急務

ゼロトラスト成熟度が高く取り組みが進んでいる企業にも課題

- セキュリティ運用を効率化、高度化させる取り組みが今後の注力分野
- 特にインフラ全体から集めたデータのアナリティクスや自動化・自律化などの取り組みが優先事項
- アクセス制御に注目が集まる傾向があるが運用をセットでの取り組みが重要

ゼロトラスト成熟度が高い企業ほどサイバーセキュリティを「投資」と位置付け

- 経営層やビジネス部門との共通理解が存在する可能性
- 成熟度が低い企業では、ゼロトラストの取り組み以前に解決すべき課題が存在する可能性
- ビジネス・インフラ・サイバーセキュリティをセットで検討することが有効

国内企業のゼロトラストへの取り組みの現状

テレワークやクラウドを活用した働き方の多様化、DX や IoT の活用で、企業のインフラは境界のないものに変化し、従来の「社内」「社外」という概念はなくなりました。結果、従来のメールやウェブを経由したリスクに加えて、開放ポート・プロトコル、対策が十分ではない海外・国内拠点、MSP(マネージドサービス事業者) を含む業務委託先、アプリケーションや開発ベンダーなど、サイバー攻撃や内部犯行のリスク要因も大きく多様化、深刻化しています。

このような企業を取り巻く環境の変化を受けて、国内・海外問わず多くの企業・組織が注目するのが「ゼロトラスト」です。ゼロトラストは、「サイバーリスクはすでに組織の中に内在している」という前提のもとに、「信頼せず、すべて検査する」サイバーセキュリティ戦略です。

2020 年 8 月に NIST(National Institute of Standards and Technology、米国標準技術研究所) から「SP800-207 Zero Trust Architecture」が公開され、米国バイデン政権が 2021 年 5 月に発表した「Executive Order on Improving the Nation's Cybersecurity (国家のサイバーセキュリティ向上に関する大統領令)」でも、ZTA(Zero Trust Architecture、ゼロトラストアーキテクチャ) の実装に向けた戦略策定を米国政府機関に求める条項が盛り込まれたことでも注目されています。

この章では、以下の調査結果を総括します。

1. 国内企業におけるサイバーセキュリティの位置付け
2. 国内企業におけるゼロトラストの着手状況
3. 国内企業におけるゼロトラストの理解度
4. 国内企業の「ゼロトラスト成熟度」
5. ゼロトラスト成熟度向上のポイント

国内企業におけるサイバーセキュリティの位置付け

セキュリティをコストとみなす企業がわずかに多数派

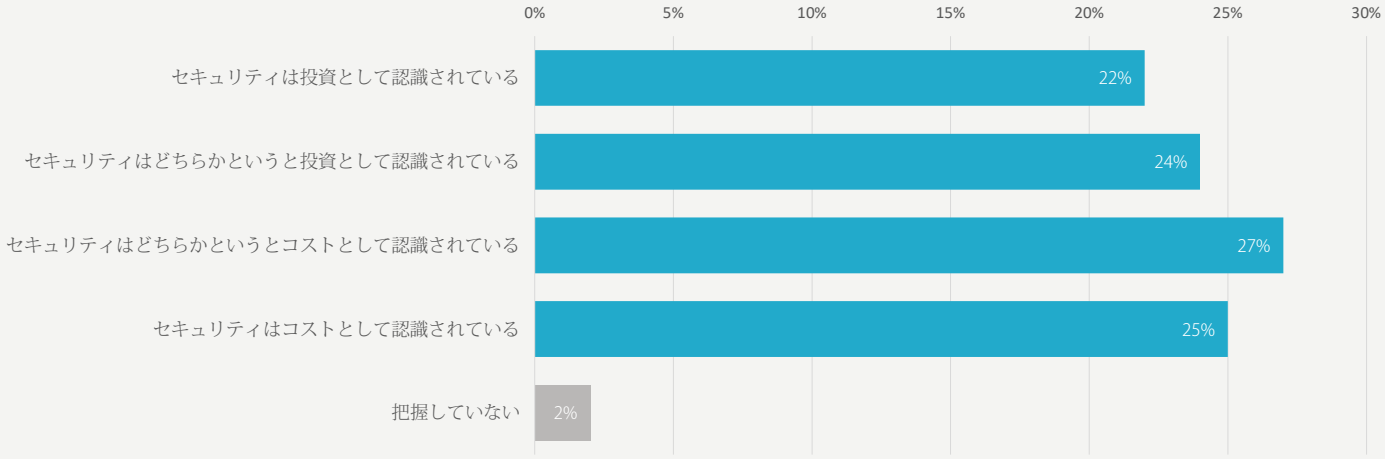
企業がサイバーセキュリティにかける費用を「投資」と位置付けるべきか「コスト」と位置付けるべきかは、たびたび議論されてきました。歴史的には、管理部門やサイバーセキュリティ、IT などの部門は、営業やマーケティングのように直接売上や利益を生み出す「プロフィットセンター」ではないことから「コストセンター」と位置付けられ、この「コスト」を最小限に抑えることが大半の組織で求められてきました。

ただし近年は、経済産業省・独立行政法人情報処理推進機構の公開する「サイバーセキュリティ経営ガイドライン」でもセキュリティ対策の実施を「コスト」として捉えるのではなく、将来の事業活動・成長に必須なものと位置付けて「投資」と捉えることが重要と説明しています。企業に対する社会全体、サプライチェーン、顧客からの信頼の醸成、事業継続性や企業の成長を支える投資と位置付けるべきという発想です。

今回の調査では、サイバーセキュリティを明確に「投資」と位置付けている企業は全体の 22％にとどまることが分かりました。やや消極的な回答を含めた場合には、投資は全体の 46％、コストは 52％と、コストと位置付ける企業の割合がわずかに上回る結果となっています。

セキュリティインシデントが発生した場合、影響範囲や原因を明らかにするフォレンジック調査、データやシステムの復旧や再発防止策、対外的な公表のための社告、問い合わせ対応用のコールセンター開増設・増員などの被害コストが発生します。これらのコストは、インシデントの深刻度、影響範囲、収束にかかる時間に応じて大きく変動します。インシデント発生で被った機会損失による短期的な売上や利益の逸失に加え、レピュテーションリスクによる中長期的な事業への影響も考えなければなりません。サイバーリスクによる被害を防ぎ、被害を最小化し、事業継続を維持するためにも、サイバーセキュリティの位置付けを組織の中で変えていくことがこれまで以上に重要になっています。

企業内でのサイバーセキュリティの位置付け (n=401)



国内企業におけるゼロトラストの着手状況

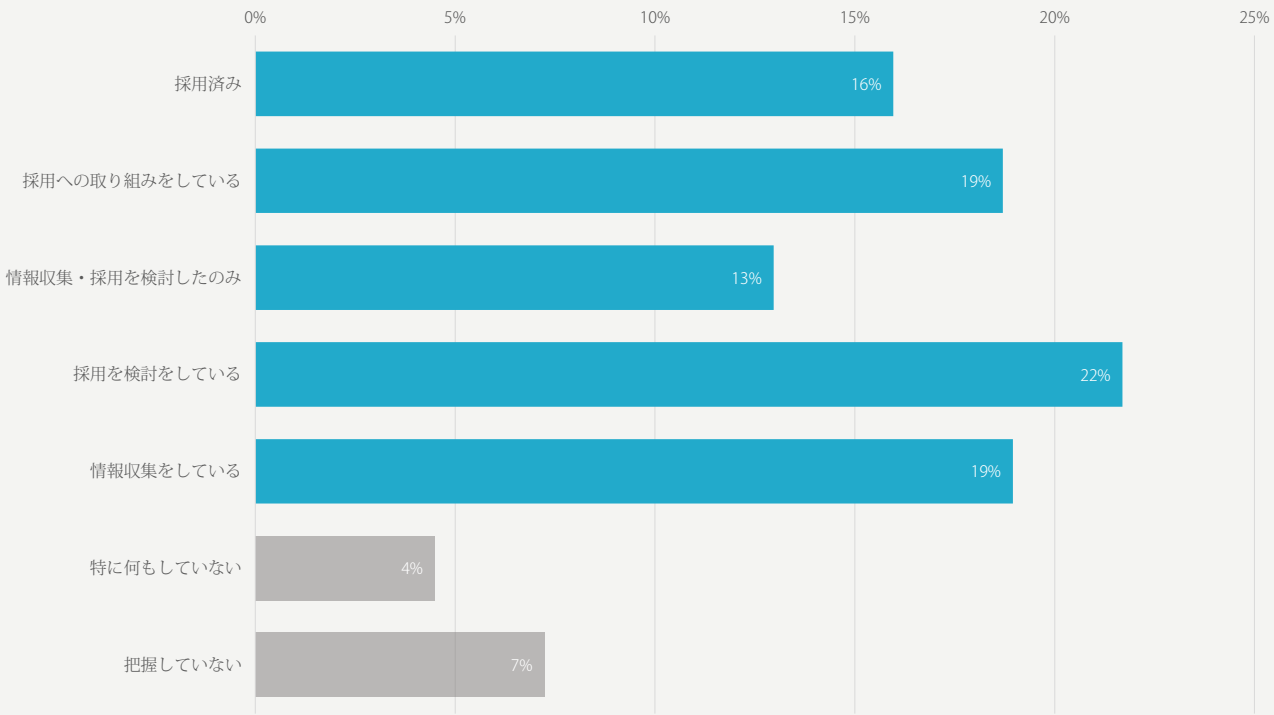
90%の組織が関心を寄せるゼロトラスト

今回の調査の結果、段階は違えど、国内企業の多くがゼロトラストに関する何らかの取り組みを行っていることが明らかになりました。しかしながら、すでに自社のサイバーセキュリティの取り組みにゼロトラストを「採用済み」と回答する企業は、全体の 16%にとどまります。

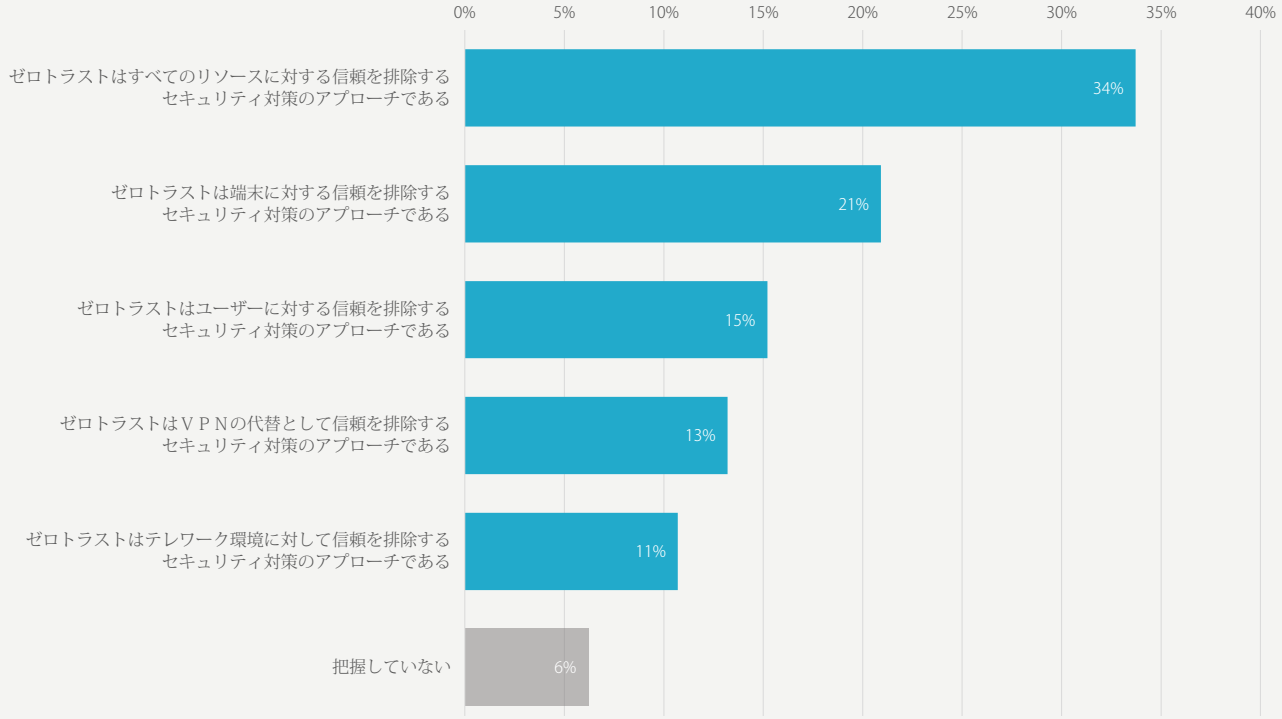
「採用の取り組みをしている」(19%)、「採用を検討している」(22%)、「情報収集をしている」(19%) を含めると、実に 75%の企業がゼロトラストに向けて取り組みを現在行っており、「情報収集・採用の検討をしたのみ」(13%) を含めるとその数値は 88%にも上ります。

従業員規模別や年間売上高別で見ると、その取り組みの進捗度合は比例はしているものの、決定的な違いは見られません。約 9 割の企業が何らかの取り組みをしていることを考えても、国内においてもゼロトラストがサイバーセキュリティ戦略として単に広く認知されるだけでなく、その重要性自体にも理解が進み始めているものと考えられ、企業インフラとサイバーリスクの変化がセキュリティの再考を促している転換期にあるとも言えます。

ゼロトラストに対する取り組みの現状 (n=401)



ゼロトラストに対する認識 (n=401)



国内企業におけるゼロトラストの理解度

「ゼロトラスト」の解釈は多様化

前述の NIST SP800-207 においてゼロトラストは次のように定義されています (以下原文をパロアルトネットワークスで翻訳したものです)。

「攻撃者は環境の中に既に存在しており、自社環境はそれ以外の環境と異なるものでも信頼性が高いものでもない、という前提に基づくものである。この新しいパラダイムにおいては、企業は暗黙の信頼をすべて排除し、資産やビジネスファンクションに対するリスクを継続して分析・評価し、リスクを緩和するための対策を講じる必要がある」

つまり、「あらゆるものに対する信頼を排除すること」がゼロトラストのポイントです。

国内企業における理解で最も多かったのは、この NIST の定義にそった「すべてのリソースに対する信頼を排除するセキュリティのアプローチ」でした。ただし、そのように回答した割合は全体の 34％にとどまり、「端末に対する信頼を排除するもの」(21％)、「ユーザーに対する信頼を排除するもの」(15％) という解釈が続いています。このほか「VPN の代替として信頼を排除するもの」(13％)、「テレワーク環境に対して信頼を排除するもの」(11％) といった認識も見られました。多くのメディアやセキュリティベンダーがゼロトラストについての情報を発信していることから、結果としてこのように解釈が多様化している可能性があります。

ゼロトラストは戦略でありパラダイムであり、この最初の理解が異なると、本来取り組むべき対策の方向性が大きくぶれる危険性があります。

セキュリティインシデントが世間を騒がせるたび、特定のセキュリティツールに注目が集まり導入が進む傾向はあります。たしかにゼロトラストの取り組みにおいてツールは重要ですが、それに先立つ全体設計が必要です。ゼロトラストでは、「原則を正しく理解すること」がスタート地点となります。

国内企業の「ゼロトラスト成熟度」

20 の評価ドメインで成熟度を評価

本レポートでは、企業のサイバーセキュリティ全般に対する取り組みを「ゼロトラスト成熟度」として定量的に評価しました。これにより、ゼロトラストやインフラ全体でのサイバーセキュリティの取り組みを行っている企業とそうでない企業との違いを明らかにすることを目的としました。

NIST SP800-207 では、ゼロトラストアーキテクチャの設計、構築にあたって則るべき 7 つの原則 (下表) があると定義しています。「すべてのものをリソースとみなし、ネットワークの場所に関係なく通信全体を可視化・制御し、デバイスやワークロードの完全性とセキュリティの状態を継続的に監視・評価し、インフラから情報を集めて継続的にセキュリティを改善する」というのがポイントです。これらの原則を押さえた上でセキュリティファンクションやポリシーをインフラ全体に実装していきます。ツールの導入にあたっては「そのツールで何を実現するか」といった目的やゴールが明確でなければなりません。

次に本レポートの「ゼロトラスト成熟度」評価は、ゼロトラストの原則に基づくポリシー実装、各セキュリティスタックにおけるファンクション実装の粒度にいたる 20 の評価ドメイン (下表) で組織の成熟度を独自に評価します。

20 の評価ドメインごとに採点したうえで、合計最大 100 ポイント、最小 0 ポイントでスコアリングし、最後に「成熟度レベル」(下表) に示す 5 段階に 20 ポイント刻みで企業を分類しました。

NIST SP800-207 の提唱する 7 つの原則

1. データソースとコンピューティングサービスすべてをリソースとみなす
2. ネットワークの場所に関係なく、すべての通信を保護する
3. 個々の組織リソースへのアクセスはセッション毎に許可する
4. リソースへのアクセスは、クライアントアイデンティティ、アプリケーション・サービス、要求をしている資産の状態を含む動的ポリシー、その他の挙動や環境属性に応じて決定される
5. 組織は、所有および関連するすべての資産の完全性とセキュリティの態勢を監視、評価する
6. すべてのリソースの認証と認可は動的に行い、アクセスが許可される前に厳格に実施する
7. 組織は、資産、ネットワークインフラ、通信の現在の状態についてできる限り多くの情報を収集した上で、その情報を用いてセキュリティ状態を改善する

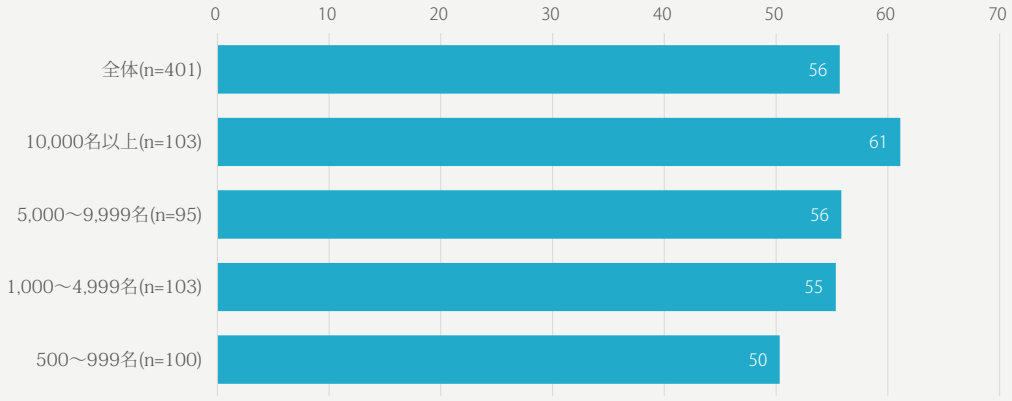
20 の評価ドメイン

1. 保護対象領域の特定
2. 最小特権の原則
3. 場所に関係ない一貫したポリシー
4. コンテキストベースのアクセス制御
5. CDM (Continuous Diagnostics and Mitigation)
6. 脅威インテリジェンスの活用
7. Extended Detection and Response (脅威の検出とレスポンス)
8. セキュリティ対応の自動化・自律化
9. アタックサーフェスマネージメント
10. エンドポイント : PC・タブレット
11. エンドポイント : サーバー
12. ネットワーク : 本社・データセンター
13. ネットワーク : テレワーク
14. ネットワーク : 拠点間通信
15. パブリッククラウド
16. アプリケーション : SaaS アプリケーション
17. アプリケーション : 社内アプリケーション
18. サプライチェーンマネージメント
19. データ保護
20. 業種特有環境

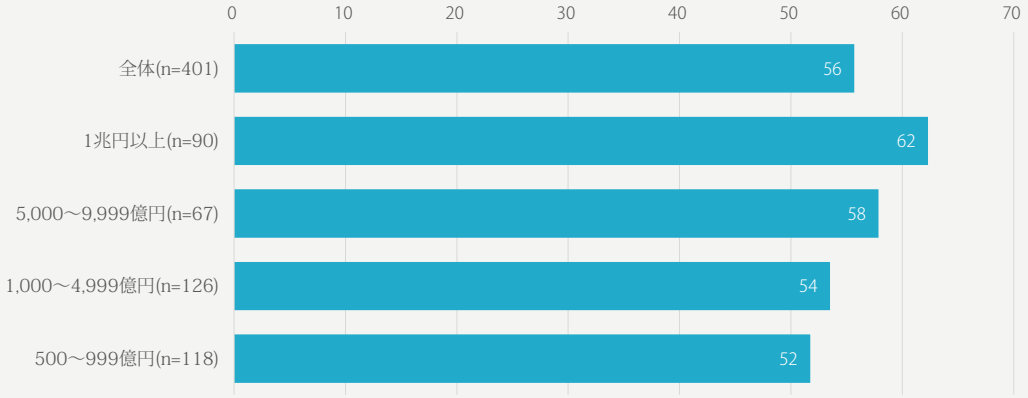
成熟度レベル

成熟度	スコア	評価
レベル 5	81 ～ 100	原則からポリシー、ファンクションの実装に至るまで、 ゼロトラストに向けた取り組みがインフラ全体で進んでいる先進的企業
レベル 4	61 ～ 80	原則からポリシー、ファンクションの実装に至るまで、その粒度に課題はあるもの、 ゼロトラストに向けた取り組みがある程度進みはじめている企業
レベル 3	41 ～ 60	ファンクションの実装はある程度行われているものの、原則からポリシーに至るまで、 ゼロトラストには依然として程遠い企業
レベル 2	21 ～ 40	サイバーセキュリティの取り組みが全般的に不足しており、 総合的にゼロトラストには程遠く、全体的に様々な課題がある企業
レベル 1	0 ～ 20	サイバーセキュリティに対する取り組みは決定的に不十分で、 総合的にゼロトラストには程遠く、全体的に課題の大きい企業

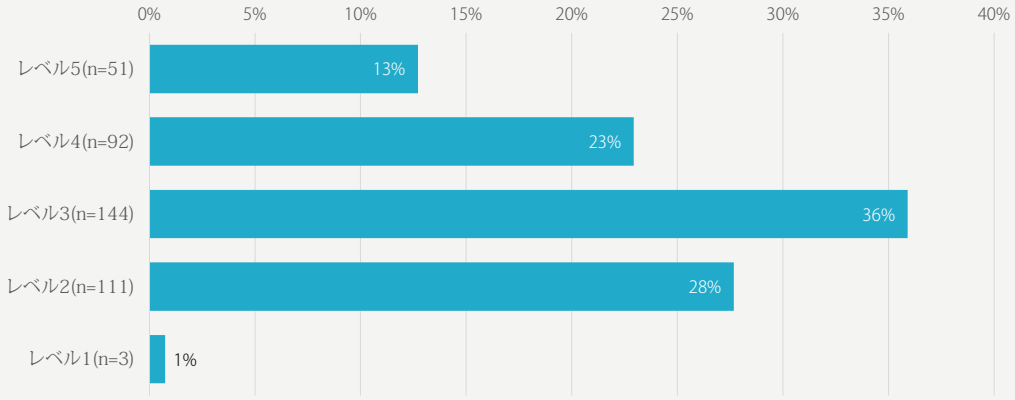
ゼロトラスト成熟度 (従業員規模別 単位 : 点)



ゼロトラスト成熟度 (年間売上別 単位 : 点)



ゼロトラスト成熟度レベル分布



規模・売上高で大きな違いがないゼロトラスト成熟度

国内企業のサイバーセキュリティに対する取り組みを「20 の評価ドメイン」で評価した結果、「ゼロトラスト成熟度」スコアは平均で 56 ポイントでした。

従業員規模別、年間売上高別で平均スコアを見ると、その差は約 10 ポイントでした。確かに売上高や企業規模とは正の相関は見られますが、スコアに大幅な違いがないことから、ゼロトラスト成熟度の決定的な違いには結びついておらず、サイバーセキュリティの取り組みを組織的に進める要因は別にあると推察されます。

最高レベルの企業はわずか 13%

5 段階の成熟度レベル別で分布を見ると、インフラ全体でのサイバーセキュリティの取り組みやゼロトラストの原則やポリシーの適用が進んでいると評価されたレベル 5 に分類できる企業は、全体の 13%でした。

分布をみると、セキュリティツールの導入は一定レベル行われていると考えられるものの、原則に基づくポリシーの実装を中心にゼロトラストにはほど遠いと評価できるレベル 3 の企業が全体の 36%を占めています。

ゼロトラスト成熟度向上のポイント

「コストではなく投資」の意識で大きな差

サイバーセキュリティの取り組みは、従業員規模、年間売上高など様々な企業属性で評価できますが、ゼロトラスト成熟度に決定的といえるほどの差は生んでいませんでした。今回の調査で、ゼロトラストをはじめとしたサイバーセキュリティの取り組みに関する企業間格差は、サイバーセキュリティを「コスト」と位置付けるか「投資」と位置付けるかに関係していることが分かりました。

ゼロトラストを採用済みの企業の 75%、ゼロトラスト成熟度レベル 5 の企業の 63%の企業は、サイバーセキュリティを「投資」と明確に位置付けています。一方、ゼロトラスト未採用の企業、成熟度レベル 1 ～ 4 の企業の場合、サイバーセキュリティを投資と位置付けている割合は、それぞれ 12%、16%にとどまりました。つまり、ゼロトラスト成熟度が高い企業、ゼロトラストに積極的に取り組んでいる企業ほど、サイバーセキュリティを「投資」として位置付けている傾向が顕著に高いことがわかります。

サイバーセキュリティを「投資」と位置付けている企業の大半が、ゼロトラスト採用の取り組みを進めています。「コスト」とみなす企業のような「最小化」へのインセンティブが働かないことから、インフラ全体での包括的で成熟した取り組みへとつながっていることが推測されます。

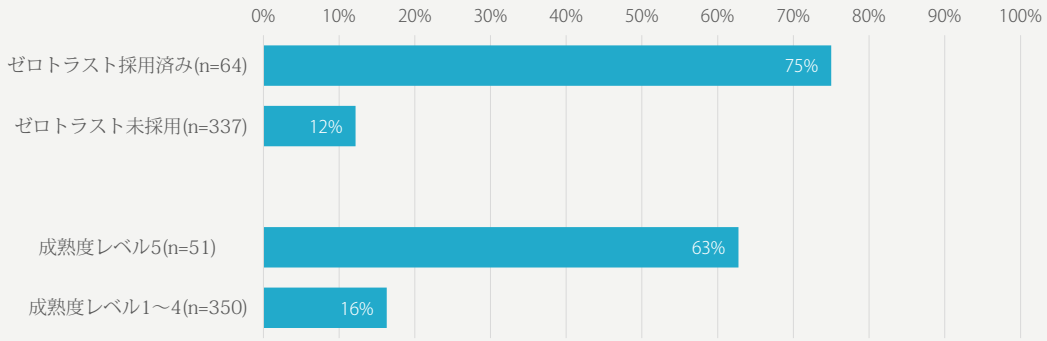
当然ながら、ゼロトラスト採用済みの企業と未採用の企業、ゼロトラスト成熟度レベル 5 の企業と 1 ～ 4 の企業で比較した場合、平均成熟度スコアの差は明確です。逆を言うと、サイバーセキュリティを投資と位置付けているからこそ、インフラ全体で包括的にサイバーセキュリティの取り組みが実施できていると解釈することができます。

ゼロトラストに対する認識の観点で見ても、大きな違いがあります。ゼロトラスト採用済みの企業の 77%、ゼロトラスト成熟度レベル 5 の企業の 78%が、ゼロトラストを「すべてのリソースに対する信頼を排除するもの」と認識している一方で、ゼロトラスト未採用の企業、ゼロトラスト成熟度レベルが 1 ～ 4 の企業の場合、その割合はそれぞれ 26%、27%にとどまります。

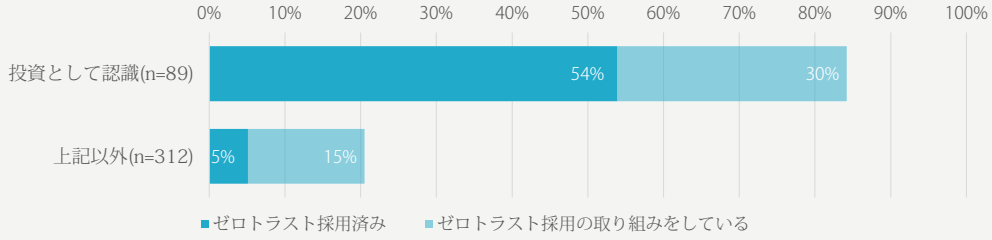
前述の通り、ゼロトラストに関する解釈は多様化しており、これがゼロトラストを取り巻く「混乱」の裏返しとも評価できます。ゼロトラストに関する取り組みがどの段階にあるかも認識の違いに影響を及ぼすと考えられますが、ゼロトラストの原理・原則の正しい理解が、ゼロトラスト実現への道のりを進めるうえで不可欠であると言えます。

今回もう 1 つ明らかになったのは、ゼロトラストを採用済みと回答する企業でも、成熟度を評価すると必ずしも高い訳ではない点です。各ドメインでどのようなツールを活用しているかではなく、ツールを使って何をどの粒度で実装しているかの違いと解釈できます。つまり、ツールありきではない、原則に基づくゼロトラストの実装が重要であることを示唆しています。

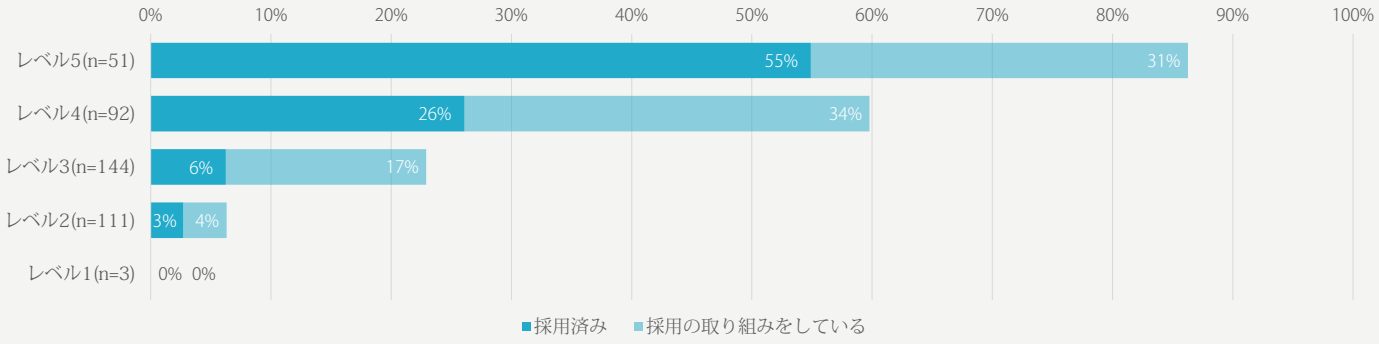
サイバーセキュリティを投資と認識している割合（ゼロトラスト採用状況・成熟度レベル別）



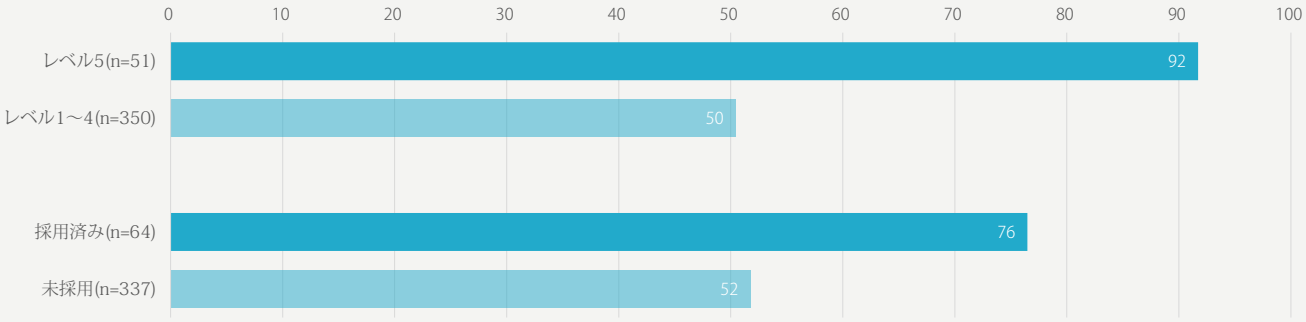
ゼロトラスト採用の取り組み（「投資」「コスト」の意識別）



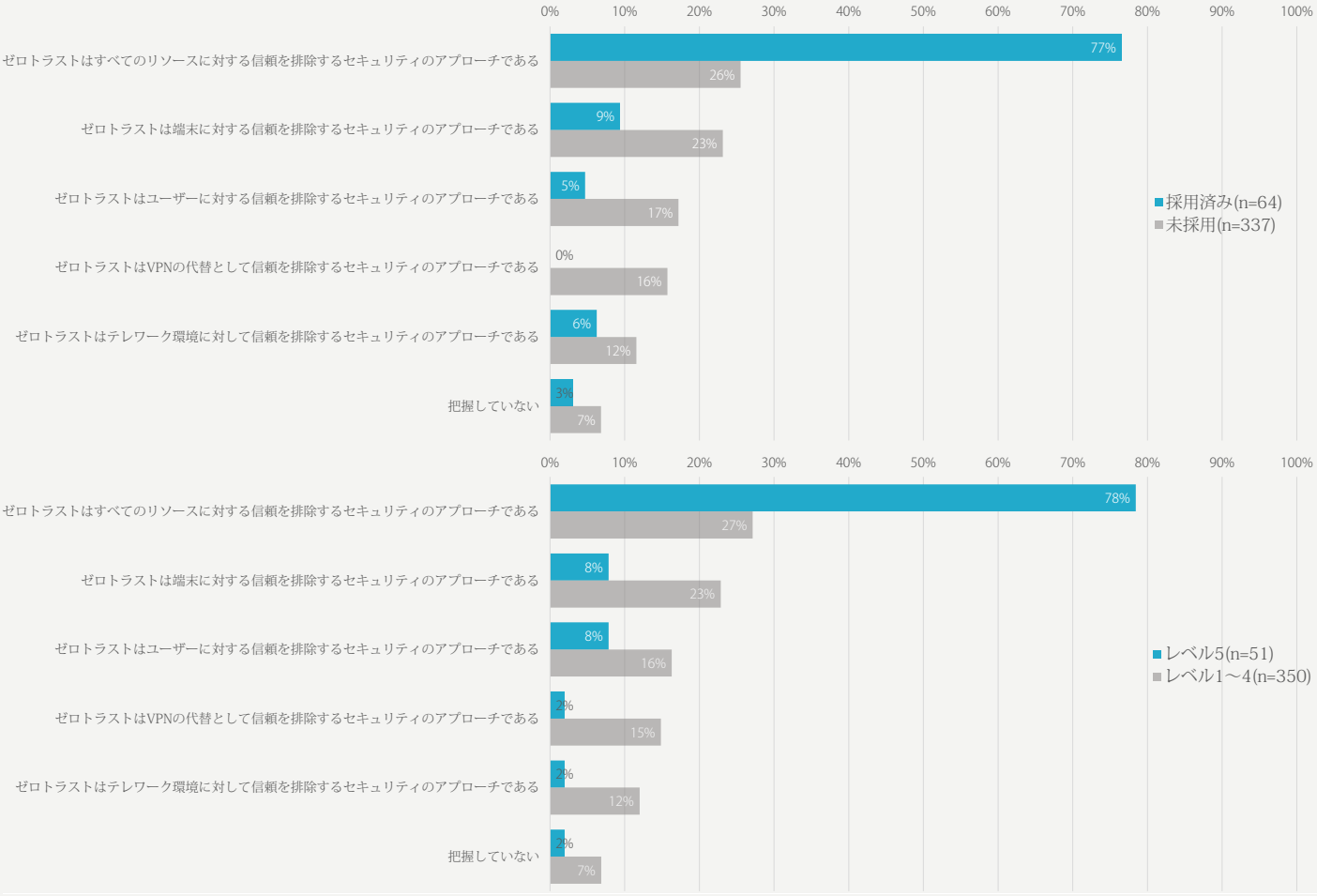
ゼロトラスト採用の取り組み（ゼロトラスト成熟レベル別）



ゼロトラスト成熟度平均スコア (ゼロトラスト採用状況・成熟度レベル別 単位 : 点)



ゼロトラストに関する認識 (ゼロトラスト採用状況・成熟度別)



Road to Zero Trust: Evaluation of 20 Domains

評価ドメイン別で見る取り組みの現状

前章では、国内企業におけるサイバーセキュリティの位置付け、ゼロトラストへの取り組みの現状、原則の理解度、成熟度と成熟度向上のポイントの全体像を総論として見てきました。

この章では各論として 20 の評価ドメインの調査結果を解説します。

1. 保護対象領域の特定
2. 最小特権の原則
3. 場所に関係ない一貫したポリシー
4. コンテキストベースのアクセス制御
5. CDM (Continuous Diagnostics and Mitigation)
6. 脅威インテリジェンスの活用
7. Extended Detection and Response (脅威の検出とレスポンス)
8. セキュリティ対応の自動化・自律化
9. アタックサーフェスマネージメント
10. エンドポイント : PC・タブレット
11. エンドポイント : サーバー
12. ネットワーク : 本社・データセンター
13. ネットワーク : テレワーク
14. ネットワーク : 拠点間通信
15. パブリッククラウド
16. アプリケーション : SaaS アプリケーション
17. アプリケーション : 社内アプリケーション
18. サプライチェーンマネージメント
19. データ保護
20. 業種特有環境

評価ドメイン 1-3: 原則の遵守

多くの企業がゼロトラストの中心部分に課題

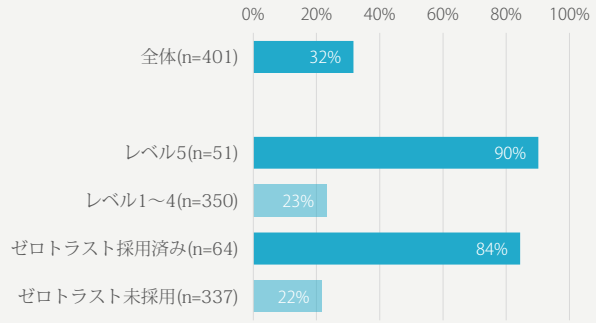
ゼロトラストの取り組みで最初にやるべきことは、侵害された場合に事業継続性に影響を与えうる重要な資産、つまり「保護対象領域 (Protect surface)」を明確にすることです。保護対象領域は、DAAS(Data(データ)、Assets(アセット)、Applications(アプリケーション)、Services(サービス)) と定義することができ、個人情報や知的財産、制御システムや IoT デバイス、業務アプリケーション、Active Directory など、事業継続に影響を与えうる極めて重要な資産が含まれます。

「保護対象領域」を明確にした上で、それに対する「最小特権の原則」を徹底します。最小特権の原則は、「守るべき重要な資産に対して、誰あるいは何がアクセスできるか、どのようなアクセス権限を持つべきかを必要最小限にすること」で、不要なアクセス権は取り除かれます。

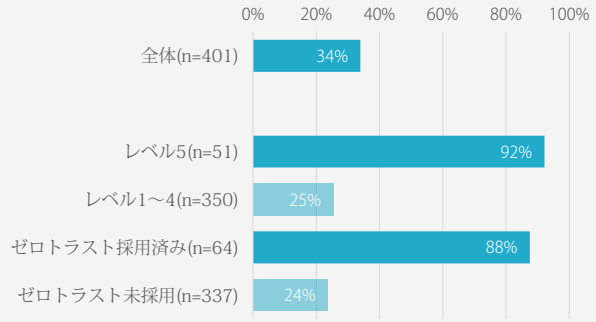
次に、「場所に関係ない一貫した動的なポリシーを適用」し、資産へのアクセス可否を定義します。オフィスやテレワーク、クラウドや社内アプリケーションなど、ユーザーやアプリケーションの場所ごとに異なるツールで異なるポリシーを適用するケースが散見されます。しかし、これは場所によって信頼レベルが異なるということを意味しており、ゼロトラストの原則が徹底できているとは言えません。

今回の調査で、「保護対象領域の明確化」、「最小特権の原則の徹底」、「場所を問わない一貫したポリシーの適用」というゼロトラストにおいて特に重要な原則・ポリシーの実装がされているのは、調査対象企業全体でそれぞれ 32%、34%、31%となりました。成熟度レベル別、ゼロトラスト採用状況別で評価した場合には、特に決定的な差が見られました。

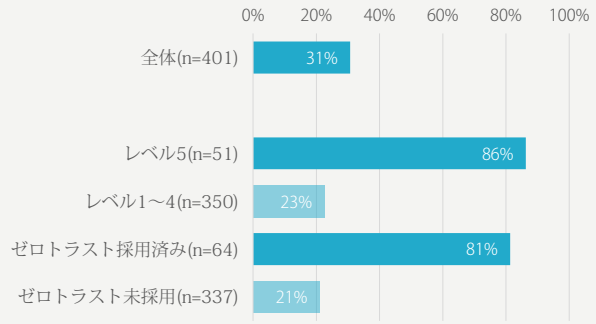
1. 保護対象領域の特定



2. 最小特権の原則



3. 場所に関係ない一貫したポリシー



評価ドメイン 4:
コンテキストベースのアクセス制御

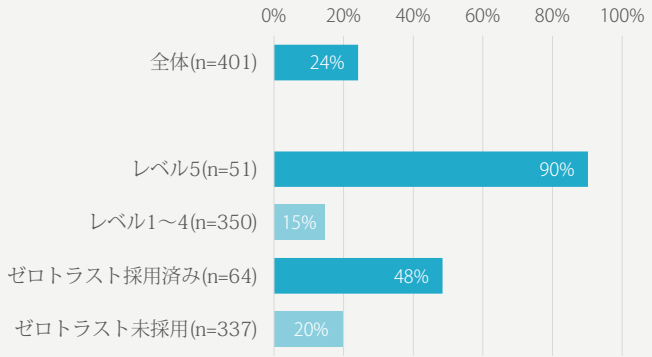
通信内のコンテンツ検査や多要素認証利用に課題

ゼロトラストでは「コンテキスト」に基づいてアクセスを制御します。「コンテキスト」とは、「だれが・いつ・どこで・なぜ・なにを・どのように」といういわゆる Kipling Method の 5W1H のことです。例えば、ユーザー、デバイス、アプリケーション、コンテンツなどが、このコンテキストを構成する要素になります。これらの要素の相互関係をコンテキストとして把握し、その結果から総合的・動的にアクセスを制御します。

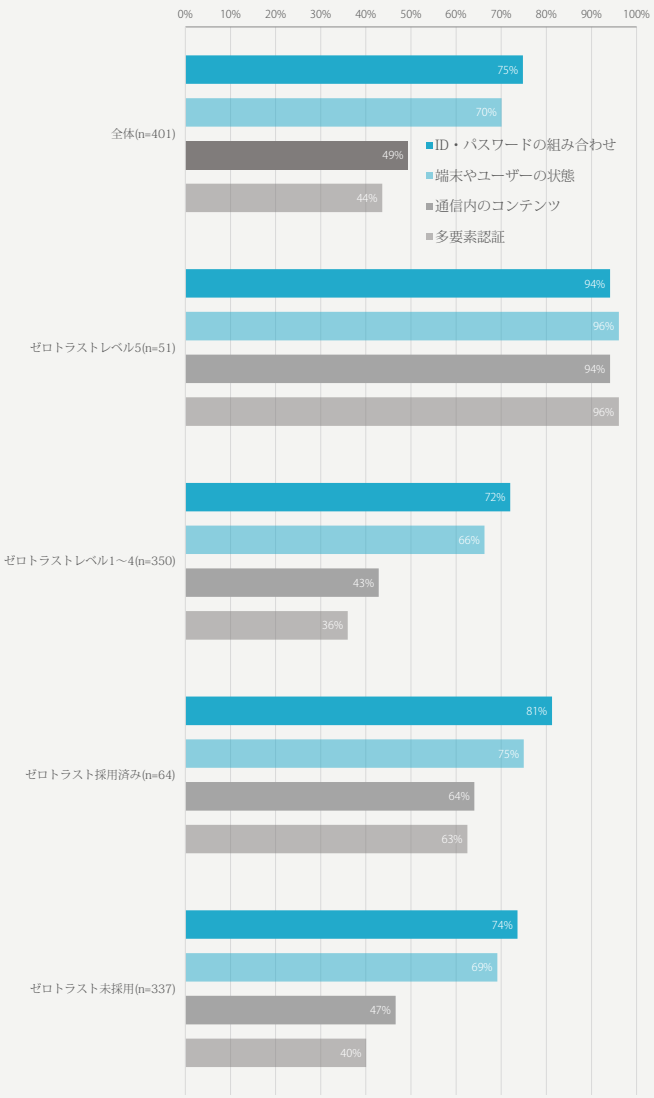
ゼロトラスト成熟度が高い企業では、コンテキストに基づいて、きめ細かいアクセス制御を実現しています。例えば、ID・パスワードが正しいかどうかの確認に加えて、ワンタイムパスワードやデバイス認証などの多要素認証を組み込む、利用するデバイスの状態やユーザーによる利用パターンが通常と異なっていないかを確認する、通信の中身に不正なコンテンツがないかを確認するなど、つど包括的な制御を実現できていました。

成熟度をこれから高めていくべき企業では、評価項目数に限りがあり、特に通信内のコンテンツの確認や多要素認証の利用による認証の強化は今後の課題となっていることが分かりました。

4. コンテキストベースのアクセス制御



コンテキストベースのアクセス制御 : 評価項目



評価ドメイン 5-9: セキュリティ運用

インフラ全体の継続した改善の必要性

ゼロトラスト対応ではアクセス制御に注目が集まる一方で、インフラ全体から集約した様々な情報を活用してセキュリティ態勢改善につなげる「セキュリティ運用」も、NIST SP800-207 の 7 つの原則で言及されている大切な取り組みの 1 つです。ツールの導入とその運用はセットで考えねばなりません。

残念ながら、セキュリティ運用のドメインは、成熟度に関係なく全般的に取り組みが遅れている傾向にあることが、本調査から明らかになりました。

特に、インフラ全体から情報を集約して XDR(Extended Detection and Response) の AI・機械学習で分析するアプローチは、技術自体が比較的新しいこともあり、全体の 10%と導入が進んでいません。SIEM(Security Information and Event Management) で集約したログデータを手作業で解析しているケースが最も多く (24%)、次いで EDR (Endpoint Detection and Response) によるエンドポイントのデータの分析が多い (23%) 結果となりました。

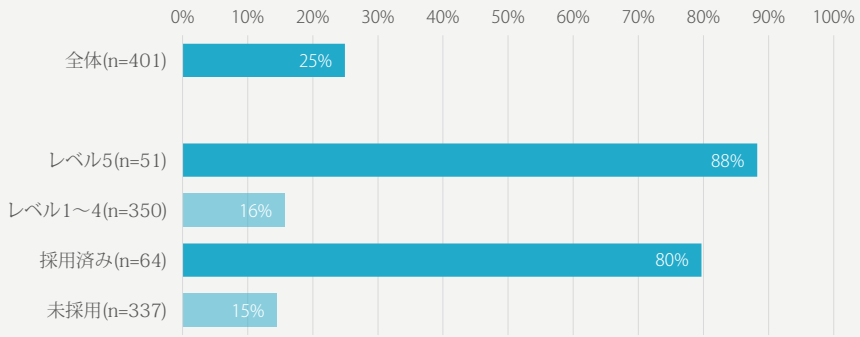
MDR(Managed Detection and Response) を活用している企業も比較的多い (22%) 傾向にありますが、エンドポイントなどの一点だけでなく、ネットワークや認証基盤を含むインフラ全体の複数のソースから情報を収集し、AI・機械学習を活用して分析し、疑わしい振る舞いや高度な脅威を特定する取り組みはこれまで以上に重要です。

SOAR(Security Orchestration, Automation and Response) のような技術を活用して、セキュリティ運用を自動化・自律化させる取り組みは、自社 SOC(Security Operation Center) や CSIRT(Computer Security Incident Response Team) を有する企業ほど活用が進んでおり、これが数値にも表れています。従来のセキュリティ運用には定型の反復業務が多いため、これらを人手を介さずテクノロジーで処理することが今後のセキュリティ運用のあるべき姿と言えます。

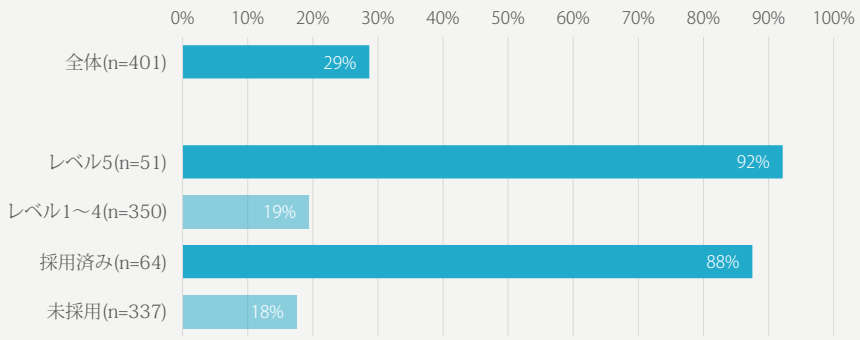
攻撃者の視点でインターネット上に晒されている資産を明らかにするアタックサーフェスマネージメント、社内外から得られる脅威インテリジェンスを対策に反映させていく、CDM(Continuous Diagnostics and Mitigation) の仕組みによってインフラ全体の状態の改善を継続する取り組みも全体的には進んでいません。

国内企業はセキュリティ運用を外部に委託する傾向が強いですが、自社か委託かに関わらずセキュリティ運用改善への取り組みは積極的に検討すべきでしょう。

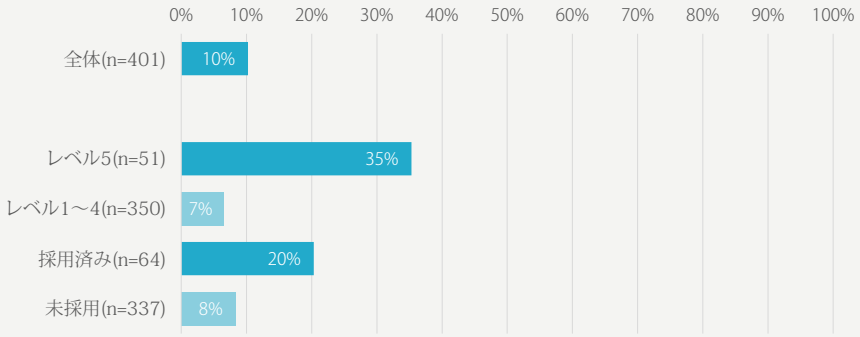
5. CDM (Continuous Diagnostics and Mitigation)



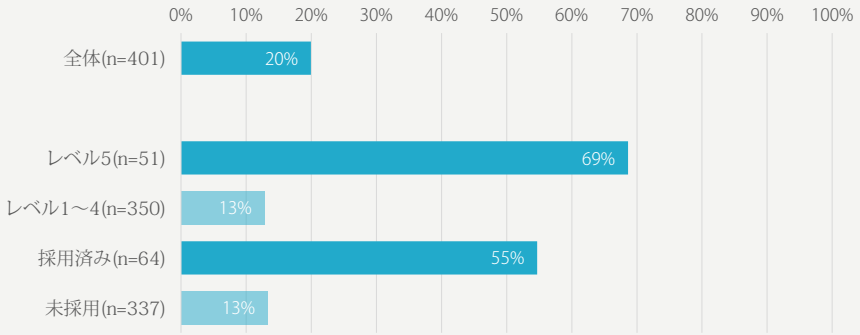
6. 脅威インテリジェンスの活用



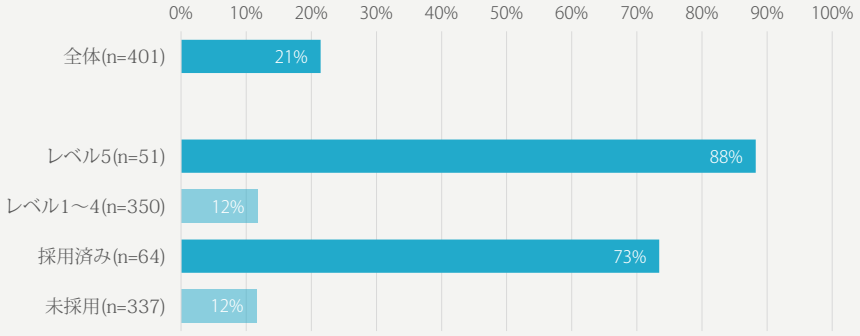
7. Extended Detection and Response (脅威の検出とレスポンス)



8. セキュリティ対応の自動化・自律化



9. アタックサーフェスマネージメント



評価ドメイン 10-11: エンドポイント

高度な脅威への対策に課題

従来の EPP(Endpoint Protection Platform) では業務端末やサーバーを十分保護できないことから、ここ数年は特に、これまでとは違うアプローチでセキュリティを強化しようとする動きが強まっています。

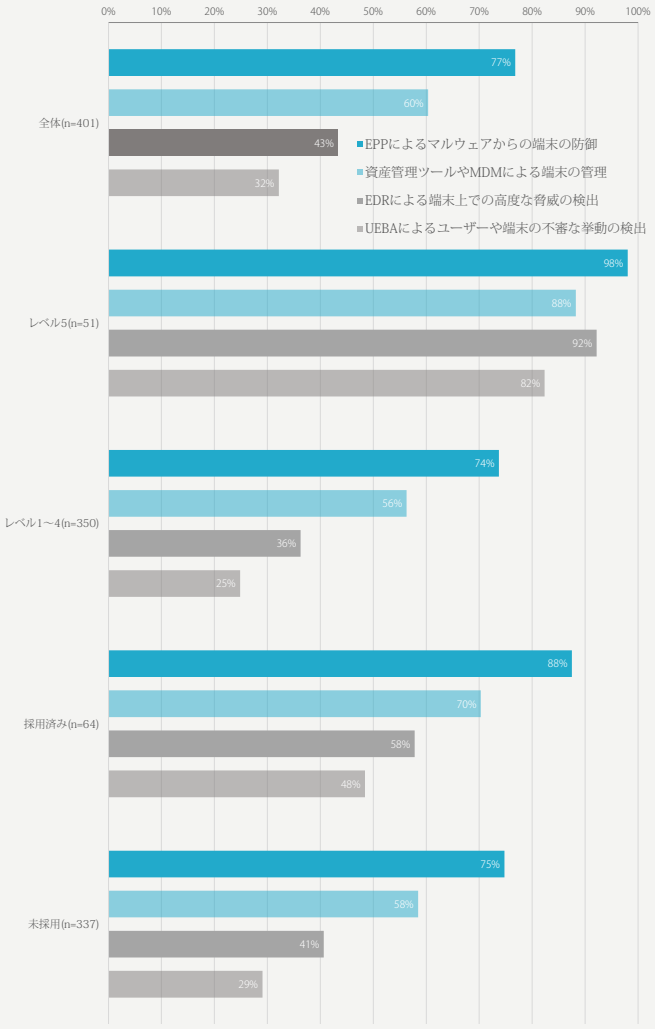
例えば、資産管理ツールや MDM(Mobile Device Management) を活用して PC やタブレット、サーバーの管理を徹底したり、EDR を使ったセキュリティ強化が行われるようになってきました。

こうした状況に加え、コロナ禍でテレワーク移行が急速に進んだこともあり、特に業務用のデバイスについては「常にオフィスで使う」という「場所」の前提が崩れています。さらにそれらのデバイスは企業管理下のネットワークから離れ、セキュリティの状態が不明なネットワークで業務に利用されます。

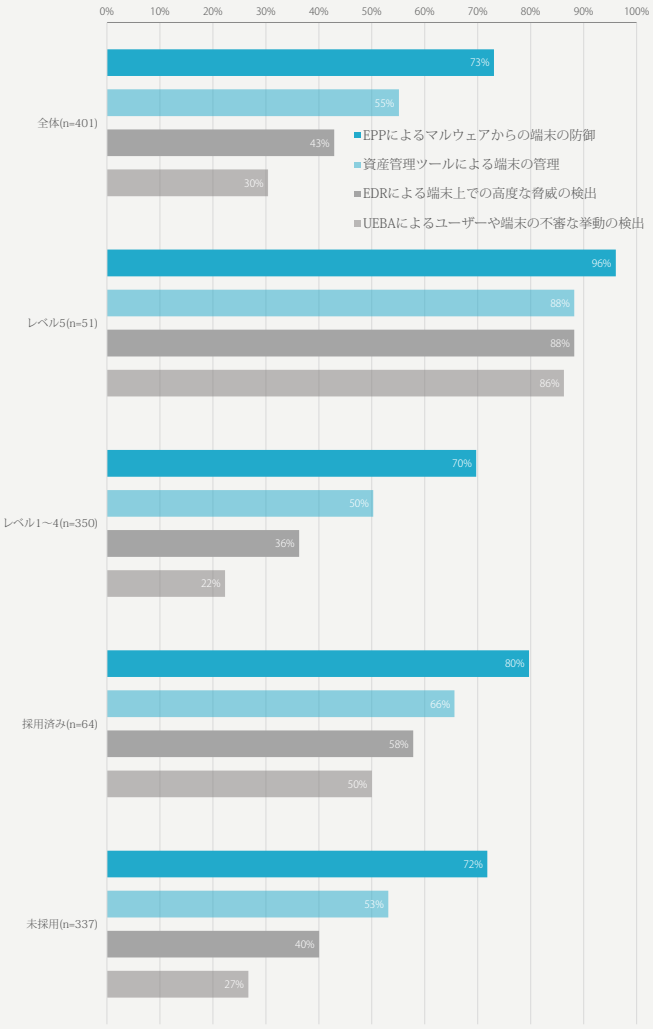
サイバー犯罪者や内部犯行者は重要データが保存されているサーバー上で様々な活動を行います。業務用デバイスやサーバーを含むエンドポイントのセキュリティ強化はこれまで以上に重要となっています。

今回の調査から、ゼロトラスト成熟度が高い組織では UEBA(User and Entity Behavior Analytics) によりユーザーの振る舞いに不審なところがないかを分析したり、複数のセキュリティファンクションやツールを併用して対策を一層強化する動きが顕著に見られることがわかりました。一方で、対策が十分行われていない企業では、特に EDR や UEBA の活用で遅れが目立っており、より高度な脅威への対策は今後に向けた大きな課題とも言えます。

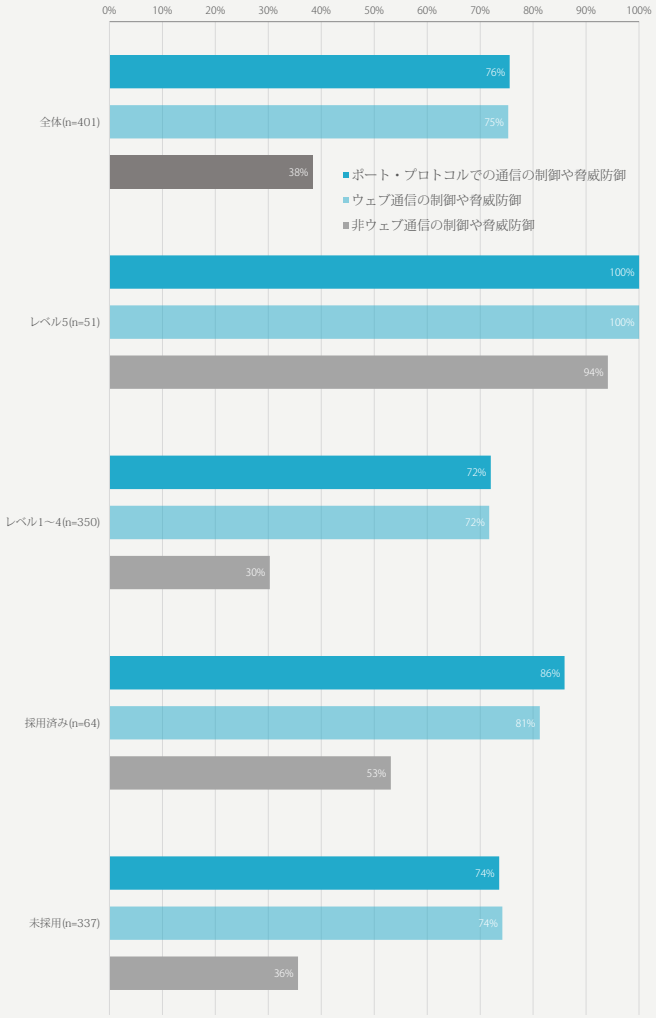
10. エンドポイント : PC・タブレット



11. エンドポイント : サーバー



12. ネットワーク : 本社・データセンター



評価ドメイン 12-14: ネットワーク

従来型対策に加えた可視化の改善が必要

ネットワークセキュリティは、ゼロトラストベースのセキュリティファンクション実装で中心となる要素です。テレワークによってユーザーやデバイスの場所が変わり、クラウドへの移行でビジネスリソースの場所も多様化していますが、これらすべての通信を場所に関係なく検査しなければなりません。

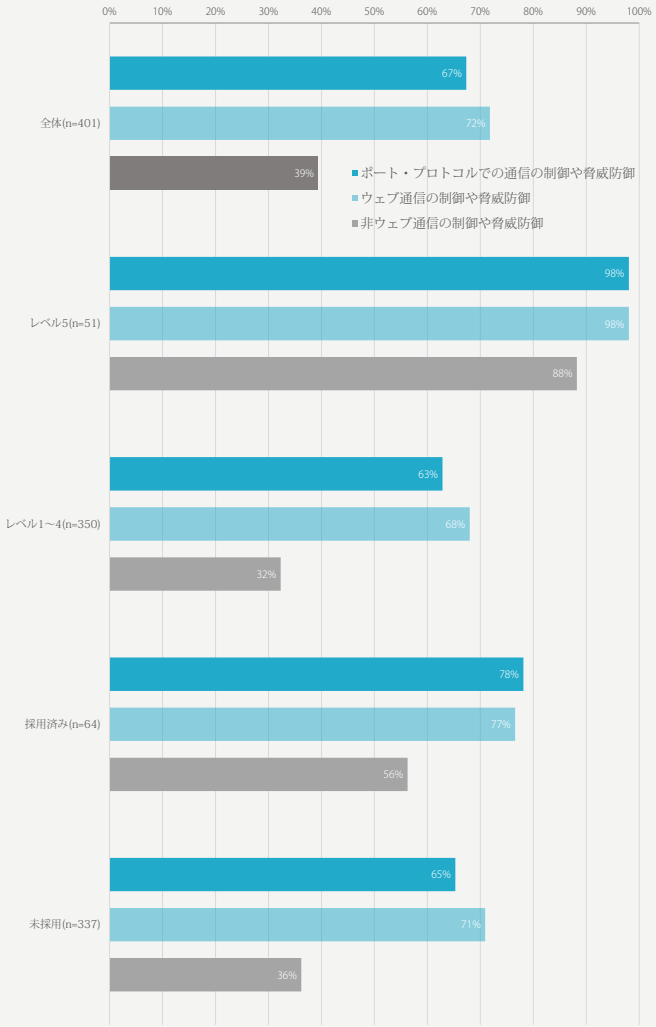
ゼロトラスト成熟度が高い企業では、ポート・プロトコルベースの制御の他に、HTTP/HTTPS によるウェブ通信と社内アプリケーションなどの非ウェブ通信も検査対象としていました。こうした企業については「すべての通信を検査する」というゼロトラスト原則が徹底できていたと言えます。

ただし全体的には、ポートやプロトコルベースの制御やウェブ通信の制御はある程度行われているものの、「本社・データセンター」、「テレワーク」、「拠点間通信」と、「非ウェブ通信」に関しては可視化に改善の余地があることがわかります。

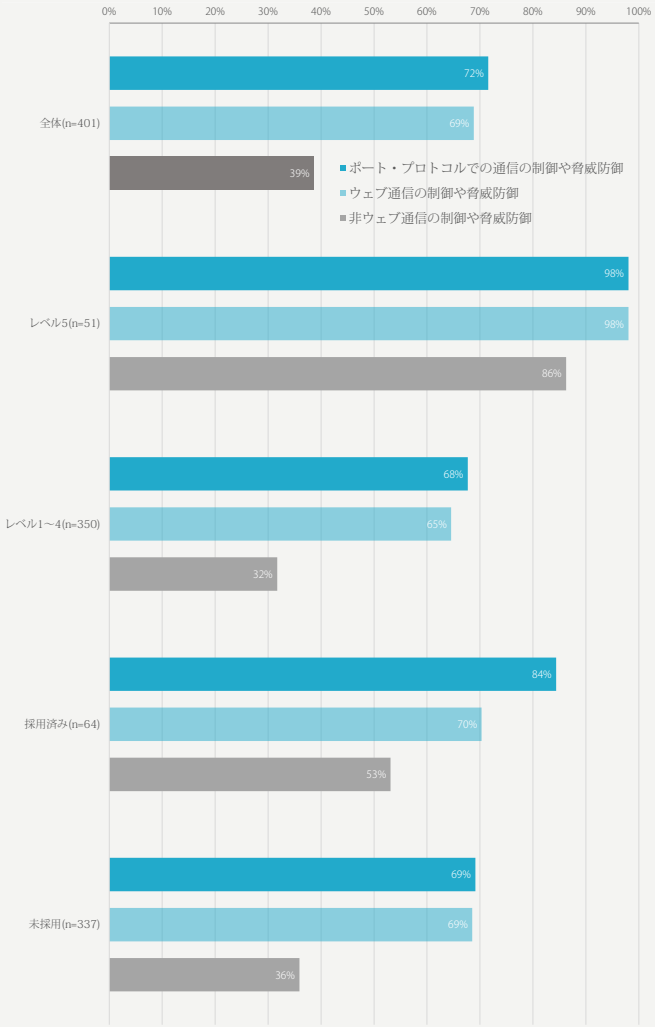
なお「拠点間通信」の制御は「ラテラルムーブメントの観点から、拠点間で行われる通信に対する制御を行っているか」を意図していますが、セキュリティチェックは実施していないというケースを頻繁に目にすることから、ここでは拠点から発生するすべての通信に関して回答者は答えているものと推測されます。

自社・自組織によって「場所を問わず」の「場所」が何かと「すべての通信」が何かを明確にすることが、未成熟の組織では急務といえるでしょう。

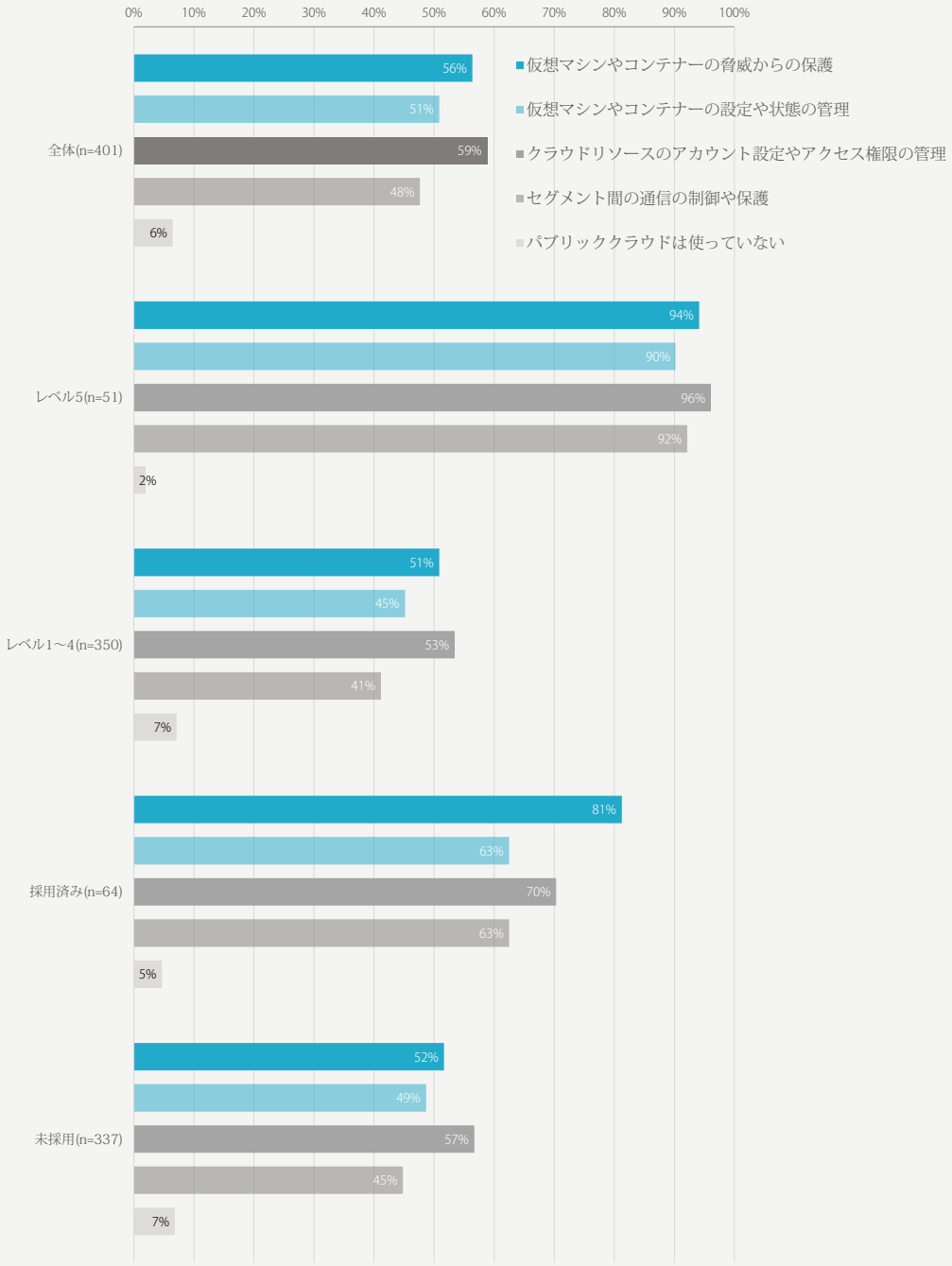
13. ネットワーク : テレワーク



14. ネットワーク : 拠点間通信



15. パブリッククラウド



評価ドメイン 15: パブリッククラウド

マルチクラウド環境に求められる一貫性

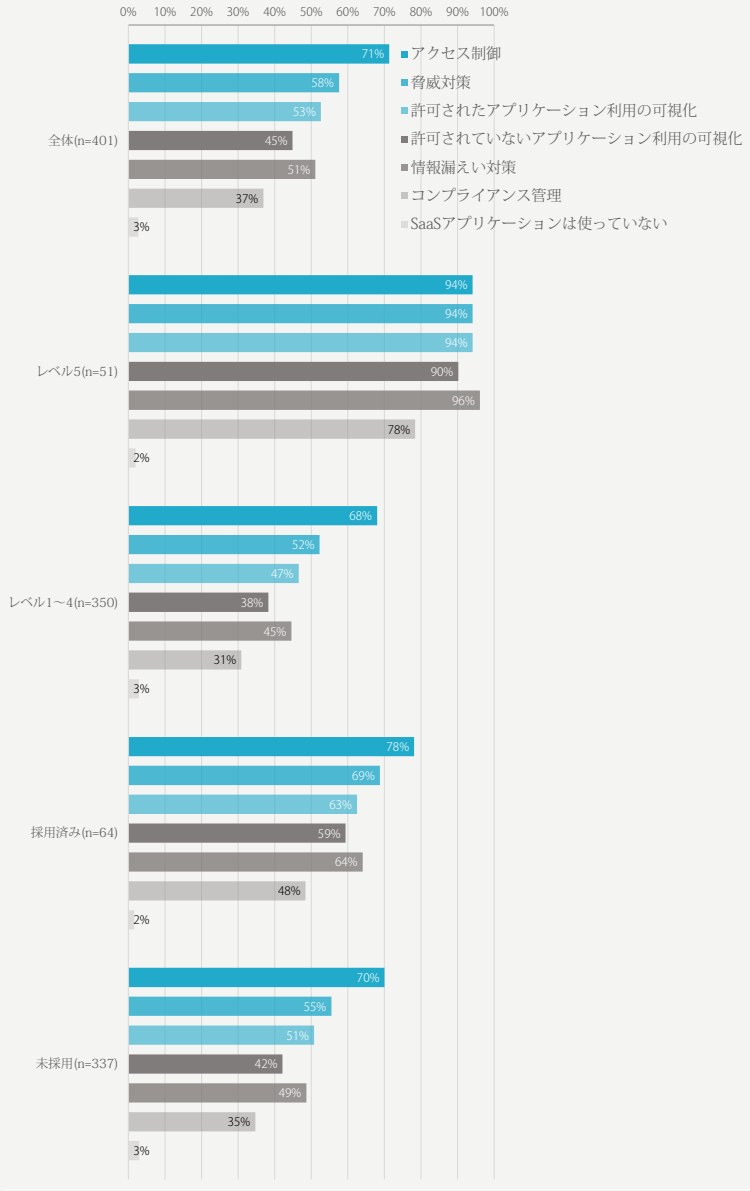
ビジネス俊敏性やコスト削減を目的として、国内企業もワークロードのクラウド移行を進めています。2021 年 4 月にパロアルトネットワークスが実施した調査でも、クラウドワークロードもシングルクラウドからマルチクラウドへ、そして仮想マシンだけでなくコンテナーやサーバーレスなど様々なコンピューティングオプションの活用が始まっていることが明らかになっています。マルチクラウド上の様々なワークロードを一元的にどう可視化し、保護できるかが課題となります。

クラウド上のワークロードに対するセキュリティは、CWPP(Cloud Workload Protection Platform) を活用した仮想マシンやコンテナなどの脅威からの保護、CSPM(Cloud Security Posture Management) を活用した設定や状態の管理、CIEM(Cloud Identity Entitlement Management) を活用したアカウント設定や権限の管理、そしてマイクロセグメンテーションによるセグメント間の通信の制御と多岐にわたります。

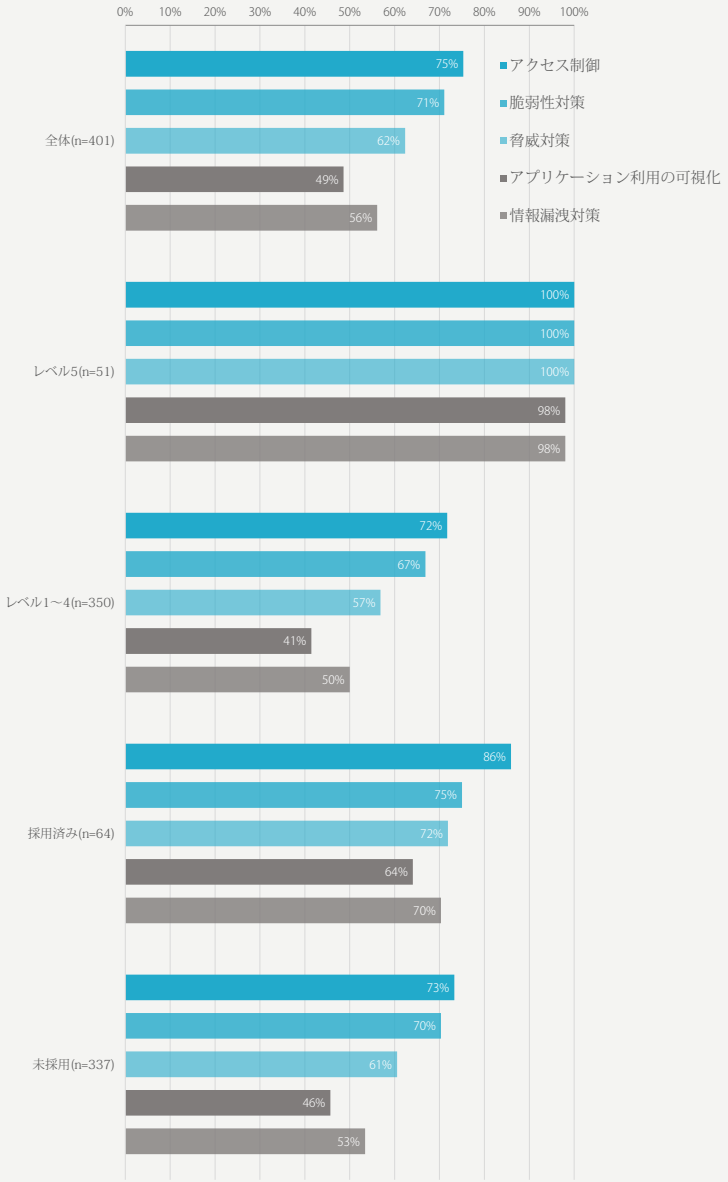
今回の調査からは、ネットワークやエンドポイントなどの他のドメインと比較しても、全体的には各セキュリティファンクションの実装が十分進んでいないことが分かります。

一方で、ゼロトラスト成熟度が高い企業は、様々なファンクションを活用してクラウドワークロードを可視化し、保護・対処しており、クラウドの特性に応じたネイティブなセキュリティのアプローチに対する必要性を十分理解したうえで、クラウドを活用していると言えます。

16. アプリケーション : SaaS アプリケーション



17. アプリケーション : 社内アプリケーション



評価ドメイン 16-17: アプリケーション

可視化とコンプライアンスが次のステップ

ユーザーは様々なアプリケーションを通じて個人データから機密情報にいたるデータにアクセスします。このため最小特権の原則に基づいたアプリケーションアクセスや、アプリケーションレベルのコンテンツ検査、ユーザーごとのアプリケーション利用の可視化、情報漏えいリスクの確認などの対策が必要です。

今回の調査では、ゼロトラスト成熟度が高い企業では多様なセキュリティファンクションを活用した取り組みが行われている一方、成熟度がまだ低い企業では、アプリケーション利用の可視化やコンプライアンスについて特に課題が残っていることが分かりました。

なお、ゼロトラスト採用済みの企業の一部でも同様の課題がありました。これらの企業では、アクセス制御などの別ドメインの課題の解決に優先的に取り組んでいたことが推測されます。

業務アプリケーションの SaaS 移行は急速に進んでおり、それだけアプリケーションを取り巻くリスクも高まっています。アプリケーションレベルの対応はまだこれからという企業は、アプリケーションの識別とそれに基づく制御、利用状況の可視化、脅威や情報漏えいリスクの排除のための取り組みなどを次の課題として取り組んでいくことが望ましいでしょう。

評価ドメイン 18:
サプライチェーンマネージメント

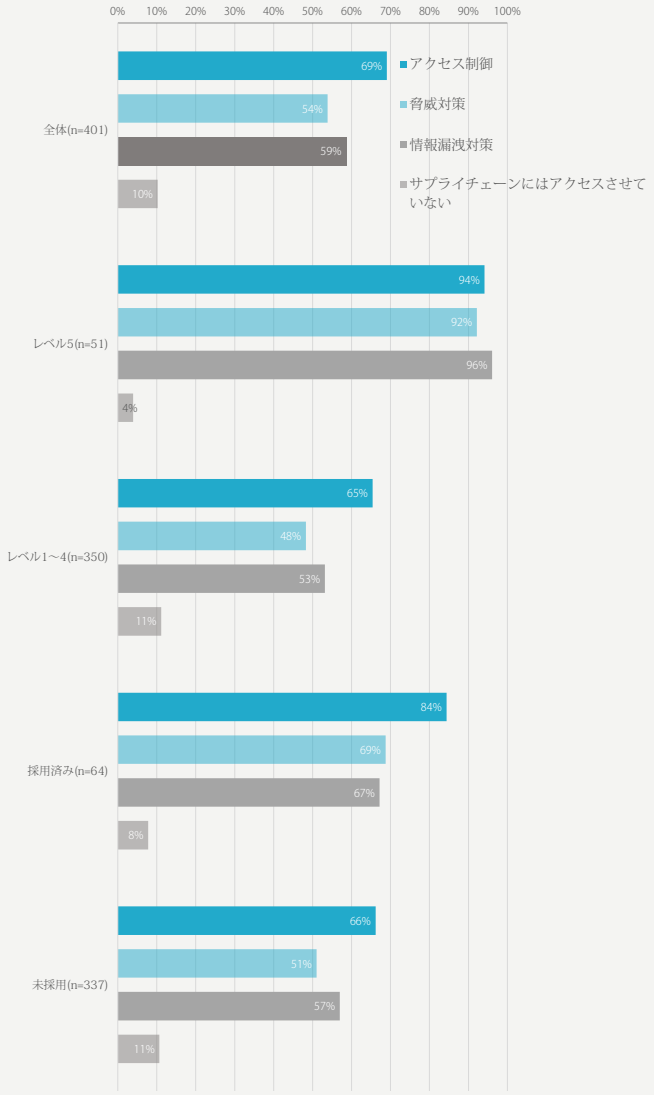
アクセス制御を中心に進む取り組み

企業インフラのアプリケーションやデータにアクセスするのは従業員だけではありません。企業インフラの変化に加え、業務委託先による機密情報の流出問題がたびたび話題になるなかで、サプライチェーンからのアクセスはゼロトラストに取り組む企業にとっては課題の 1 つです。

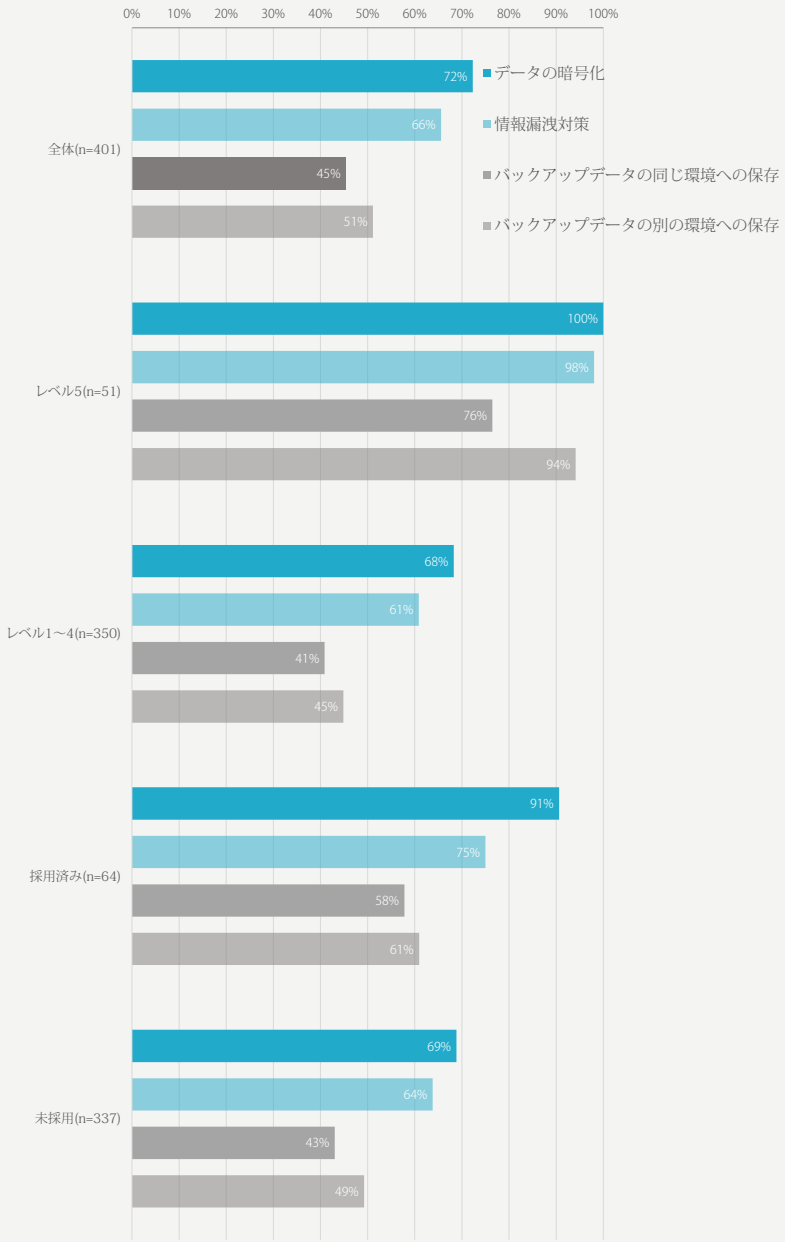
今回の調査では、サプライチェーンのアクセスに対するセキュリティチェックは、他のドメインと比べて相対的に進んでいる傾向があることがわかりました。特に、ゼロトラスト成熟度の高い企業では、アクセス制御に加えて不正コンテンツの有無、機密情報流出の有無のチェックが行われていました。

様々な分野で人材不足が問題になる中、今後も多くの場面で業務委託が進むことが予測されます。業務委託先の担当者にアクセス権を付与し、自社インフラ環境を利用してもらう機会もその分増えます。信頼のおける業務委託先であっても例外扱いはせず、ゼロトラストの観点で暗黙の信頼を排除し、ユーザー、アプリケーション、デバイス、コンテンツをすべて検査していかなければなりません。

18. サプライチェーンマネージメント



19. データ保護



評価ドメイン 19: データ保護

データ保護は進むもバックアップに課題

企業の重要データは、個人情報や知的財産など業種・業態に応じて多岐にわたります。特に現在はランサムウェアにより業務システムを使用不可能にされたうえ、インターネット上に重要データが不正に公開される脅威が深刻化しており、事業継続への影響をどのように最小化していくかが重要です。

本調査では、データの暗号化や情報漏えいの対策が、成熟度やゼロトラストへの取り組み状況に関係なく、全体に一定レベルは進んでいることがわかりました。しかしながら、ランサムウェア対策やデータ障害時の復旧で必要とされるバックアップについては、必ずしも取り組みが進んでいるとは言えません。

成熟度が高い企業では、バックアップデータを企業ネットワーク以外の直接はアクセスできない場所にオフラインで保存している傾向が見られました。こうした企業では「コピーを 3 つ、2 つの異なる媒体で取り、1 つは別の場所に保存する」という 3-2-1 ルールに基づくバックアップが徹底していることがうかがえます。

ランサムウェアの脅威は年々深刻化しています。データ可用性が事業継続により直接的な影響を与えることからも、適切なバックアップ戦略の実装が強く求められます。

評価ドメイン 20: 業種特有環境

繋がることで増す可視化の必要性

これまで産業機械などの制御系 (OT) ネットワークは、情報系 (IT) ネットワークから独立して閉域で運用されることが多く、外部からのアクセスが難しいことから、セキュリティ面の懸念は少ないと考えられてきました。

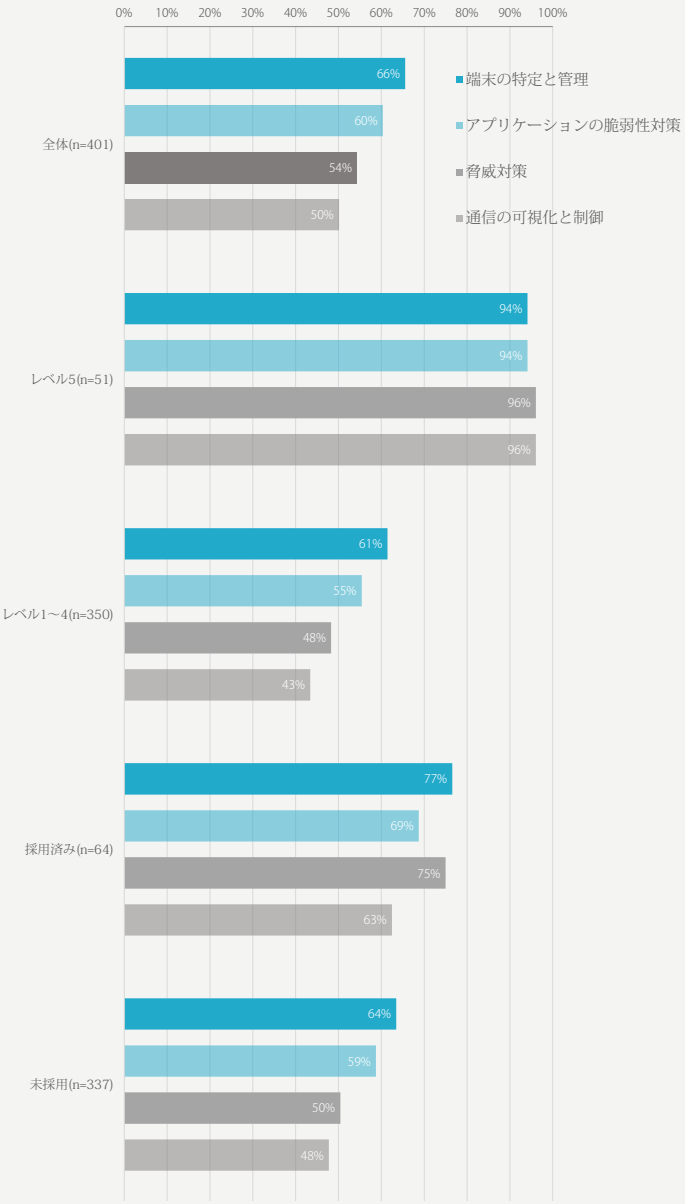
ところが近年、IoT デバイスの活用や IT ネットワークとの相互接続が進み、例えば製造業の工場や小売業の店舗ネットワークなどの業種特有環境のセキュリティは、情報系ネットワークと同様に重要視されるようになっています。情報系ネットワークから侵入した脅威による被害は、接続された業種特有のネットワークにも及ぶためです。

本項目で、特に成熟度が高い企業の大多数では、端末の管理から脆弱性への対策、マルウェアなどの脅威に対する防御、そして通信の可視化といった取り組みを実装していることが確認できました。

一方、成熟度の低い企業では、こうした取り組みが十分でないところが見られました。特に、脅威対策や通信の可視化と制御は、業種特有環境では課題となっているようです。

情報系ネットワークと業種特有環境の境界はなくなりつつあります。業種特有環境に侵害が及ぶと、工場の操業停止や店舗での決済不能など事業継続に直接影響します。「場所に関係なくゼロトラストを適用する」観点からも、業種特有環境を取り組みのスコープに入れることが求められます。

20. 業種特有環境



おわりに

企業インフラの変化はサイバーリスクの変化をもたらし、多数の組織がセキュリティの取り組みの見直しを迫られています。今、多くの企業や組織でゼロトラストへの関心が高まっているのも、こうした背景があってのことです。

その一方で「ゼロトラスト」は製品でも技術でもなく、もっとも高次な「戦略」、「パラダイム」であるがゆえに、多種多様な解釈が存在し、これが市場での混乱につながっています。

今回の調査では、ゼロトラスト戦略を採用している企業でも、原則の理解が不十分なままセキュリティベンダーの提供するツールの導入ありきで実装しようとするケースが少なからず見られました。ゼロトラスト実現のためには、原則を理解し、達成すべきゴールを設定し、ゴールに到達するためのツールを導入し、実装し、継続的に運用の改善をはかる必要があります。

サイバーセキュリティへの取り組みがインフラ全体で強化されるかどうか、ゼロトラストへの取り組みが本格的に行われるかどうかは、企業がサイバーセキュリティをどのように位置付けるかに大きく関係しています。今回の調査からは「サイバーセキュリティを投資ととらえること」が成熟度を分けることが明確になりました。

今後デジタル化を進める企業の多くは、ゼロトラスト戦略の採用を検討することになります。そしてその取り組みは、現場担当者だけでは成し遂げられません。経営層の主体的な協力が必要です。経営層は、ゼロトラストの必要性をただ認識するだけでなく、現場担当者に明確な権限とリソースを与えることが必要です。ゼロトラスト戦略のもとにセキュリティを強化するには、それを投資と位置付ける企業トップからのマインドセットの変革が急務です。

参考文献

1. National Institute of Standards and Technology. Special Publication 800-207 Zero Trust Architecture. https://doi.org/10.6028/NIST.SP.800-207 (参照 2021-09-10)
2. The White House. Executive Order on Improving thetion's Cybersecurity. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (参照 2021-09-10)
3. 経済産業省 , 独立行政法人情報処理推進機構 .「サイバーセキュリティ経営ガイドライン Ver 2.0」 https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf (参照 2021-09-10)
4. Palo Alto Networks. Understanding Zero Trust Terminology. https://www.paloaltonetworks.com/resources/zero-trust (参照 2021-09-10)
5. パロアルトネットワークス株式会社 .「クラウドネイティブセキュリティ ジャパンサーベイ 2021 年版」. https://start.paloaltonetworks.jp/2021-state-of-cloud-native-security-japan-survey.html (参照 2021-09-10)