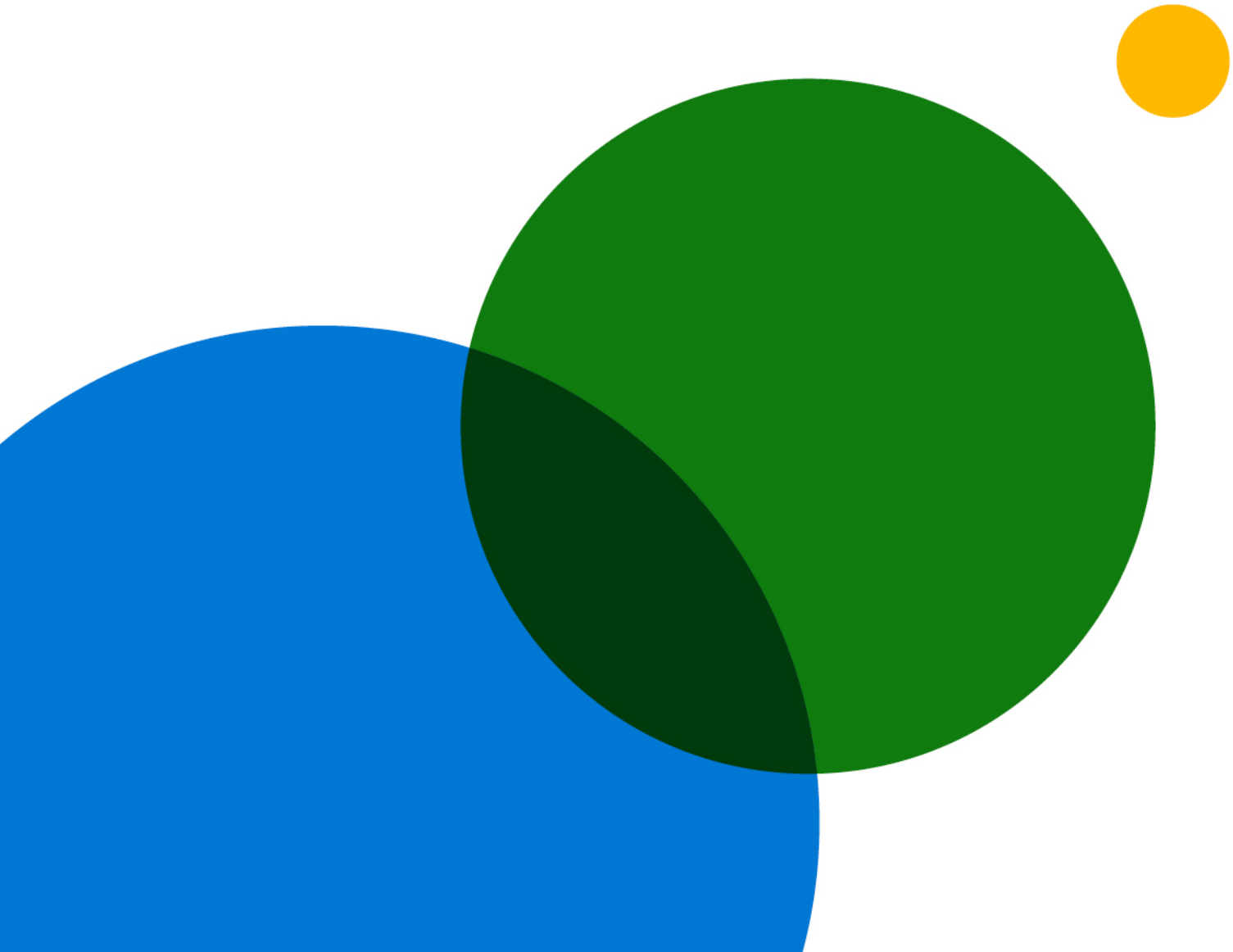
Microsoft Security

hypothesis

ゼロ トラスト導入 レポート



目次

はじめに

Vasu Jakkal 氏 / セキュリティ、コンプライアンス、ID 担当コーポレート バイス プレジデント

この一年間におけるサイバーセキュリティの進化とゼロ トラストの台頭は、世界中の業界や組織を誘導する戦略として注目を集めてきました。

パンデミックが到来したとき、職場は一夜にしてほぼ完全にリモートに移行しました。多くの組織はこの移行により、個人デバイスの使用、クラウド サービスによるコラボレーション、企業ネットワークの境界外でのデータ共有を通じてあらゆる場所での業務の遂行を可能にするための社員の支援に迅速に対応することを余儀なくされました。組織はこの変革に適応していく中で、標的の特化、戦術、リソースの調達を進化させ続けている、ますます高度化するサイバー犯罪者にも直面していました。

今日では、ハイブリッド ワークが新たな現実となっています。このような背景と、急速に変化しつつある状況により、弊社が調査した組織は、ゼロ トラストに頼ってセキュリティとコンプライアンスの俊敏性の向上、脅威の検出および修復の加速化、セキュリティ分析の簡素化と可用性の向上を目指していると回答しています。

包括的なゼロ トラスト アーキテクチャは、明示的な検証、最小限の特権アクセスの使用、侵害の想定という原則に基づいて、可視性、オートメーション、オーケストレーションを強化し、ID、エンドポイント、アプリ、インフラ、ネットワーク、データの領域にわたる保護を確立しています。マイクロソフトでは、このアプローチをお客様やパートナーに推奨しているだけでなく、自社でのグローバルなセキュリティおよびソフトウェア開発へのアプローチにも採用しています。

このレポートでは、さまざまな市場や業界におけるゼロ トラストの導入への道のりを明らかにしていきます。この調査によって得た学びがゼロ トラスト戦略の導入を加速し、同業者全体の進歩に貢献して、急速に進化し続けるこの領域の将来の状況に関するインサイトを提供できることを願っています。

方法

マイクロソフトでは、インサイト、設計、および戦略機関である Hypothesis Group にゼロ トラスト導入レポートの作成と調査を委託しました。調査には米国における 2 つのフェーズが含まれていました。最初のフェーズでは、ゼロ トラストの導入におけるトレンドとモメンタムを調査し、2 番目のフェーズではさらに市場を追加して、グローバルなトレンドを明らかにしました。

最初の調査は 2020 年 8 月に実施し、米国におけるさまざまな業界のエンタープライズ企業でゼロ トラスト戦略の意思決定に関与している 300 人のセキュリティ意思決定者 (SDM) を対象として、15 分間のオンライン調査を行いました。オンライン調査に加えて、2020 年 9 月には米国のさまざまな業界の SDM を対象とした 5 つの詳細なインタビューをオンラインで実施しました。

2021 年 4 月には、米国、ドイツ、日本、オーストラリア/ニュージーランドにおいて、同様のセキュリティ意思決定者を対象としたグローバル調査を実施しました。900 人以上の参加者がゼロ トラスト戦略の導入、ベストプラクティス、メリット、課題、将来の投資計画についての質問を含む 15 分間のオンライン調査に回答しました。

ゼロ トラストの導入について知っておくべきこと

01 / 組織はハイブリッド ワークプレースへの移行と Covid-19 によって加速されたゼロ トラスト戦略の活用準備ができている

セキュリティ意思決定者 (SDM) は、ゼロ トラスト戦略を策定することがセキュリティの最優先事項であり、96% はそれが組織の成功にとって重要であると回答しています。ゼロ トラスト戦略を導入するための主な動機は、全体的なセキュリティ態勢とエンド ユーザー エクスペリエンスの向上にあります。Covid-19 によって加速されたハイブリッド ワークプレースへの移行も、ゼロ トラスト戦略の導入を拡大しています。エンタープライズ組織の 81% はハイブリッド ワークプレースへの移行を開始しており、31% は移行を完全に完了しています。ただし 94% の組織は、移行、主に社員による不正利用、IT ワークロードの増加、サイバー攻撃について懸念を抱いています。そのため戦略の重要な考慮事項には、社員のトレーニングの強化と多要素認証 (MFA) によってユーザー エクスペリエンスと移行を円滑に進めることが挙げられます。

02 / ゼロ トラスト戦略は、組織が導入を開始する領域に柔軟性をもたらすため、ニーズに合わせてアプローチを調整できる

同じセキュリティ リスク領域でゼロ トラスト戦略を導入し始めた組織は 15% 未満です。これは、一連のさまざまな個別のテクノロジとしてではなく、セキュリティ アーキテクチャの柱と機能全体にわるエンドツーエンド プロセスとしての導入アプローチが採用されていることが大きな理由です。同様に、セキュリティ リスク領域内でゼロ トラストの個々の構成要素が導入される順序は多様であり、セキュリティ専門家が最初に導入を開始する構成要素は大きく異なっています。

03 / ゼロ トラスト戦略は広く導入されており、組織の脅威管理能力を向上しているが、行うべき作業が残っている

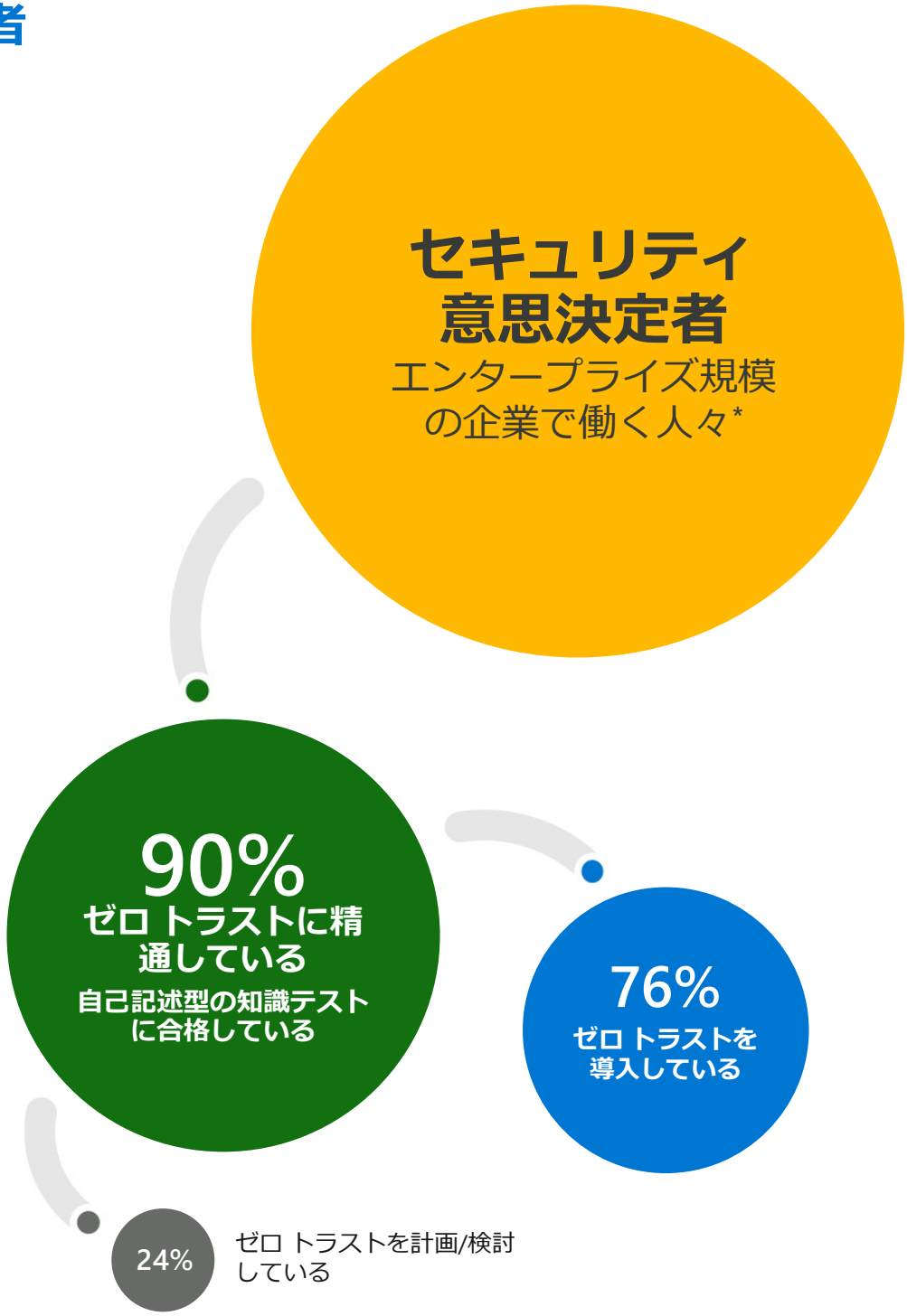
組織の 76% は少なくともゼロ トラスト戦略を導入し始めており、35% は完全に導入したと主張しています。しかし、完全に導入したと主張している組織は、すべてのセキュリティ リスク領域と構成要素にわたってゼロ トラスト戦略を導入していないことを認めています。ゼロ トラスト戦略は、機敏性の向上、脅威の検出速度、モノのインターネット (IoT) および運用技術 (OT) のセキュリティ管理能力の向上を実現できるため、魅力的です。米国での導入は拡大しています (2020 年 8 月 には 70%、2021 年 4 月には 79%)。また米国は、後で導入を開始した他国と比較してゼロ トラストの導入がはるかに進んでおり、米国の組織は予算の制約がより少ないことも明らかになっています。ただし、組織の 57% は他の組織より導入が進んでいると主張していますが、すべてのセキュリティリスク領域と構成要素にわたってゼロ トラストを完全に導入していないため、約半数は依然としてやるべき作業を抱えています。

04 / 将来を見据えると、ゼロ トラスト戦略は最優先事項であり続けるが、社員とベンダーに関して慎重な意思決定が必要である

ゼロ トラスト戦略は 2 年後もセキュリティの最優先事項であることが予想され、組織は投資の増加を予期しています。社員にまつわる課題 (セキュリティ チームの人員配置やリーダーシップの賛同を含む) は、ゼロ トラストの投資を倍増させる鍵となります。ベンダーの戦略に関して言えば、ベンダーの選択は社内の専門知識の有無に依存していることが多いため、セキュリティ意思決定者は包括的または統合的なプロバイダーとの連携を好む傾向が若干あります。ベストインスイート アプローチ (全機能が 1 つのスイートにまとめられたアプローチ) のメリットには、専門知識、リソース、シンプルさの向上が挙げられますが、導入に時間がかかり、既存のセキュリティ アーキテクチャへの統合が難しくなり、潜在的な脆弱性が高まる可能性があります。

調査対象者

グローバル



*米国では 1000 人以上の社員、ドイツ、日本、オーストラリア/ニュージーランドでは 500 人以上の社員

総合的な調査研究の概要

組織はゼロ トラスト戦略を活用する準備が整っている

ゼロ トラスト戦略は、あらゆる市場と業界にわたって今日のセキュリティ最優先事項となっており、多くの組織が近年ゼロ トラスト戦略を導入しています。ゼロ トラストはあらゆる組織にとって最優先事項 (53%) となっていますが、特に米国 (56%) とドイツ (53%) の組織にとって高い優先事項となっています。

ほぼすべてのセキュリティ専門家 (96%) は、ゼロ トラスト戦略が組織の成功にとって重要であると考えています。(図 1 参照) セキュリティ専門家は、全体的なセキュリティ態勢を強化し、エンドユーザー エクスペリエンスを向上させるだけでなく、社員のセキュリティ手順を簡素化するためにゼロ トラスト戦略を模索しています。(図 2 参照)

レジャー産業における 1 人の米国のセキュリティ意思決定者は次のように説明しています。「目標はセキュリティ態勢を全体的に改善することですが、最も大事なことは、エンドユーザー エクスペリエンスの摩擦を減らし、彼らの作業をさらに容易にすることです。」

さらに、31% のセキュリティ専門家はパンデミック後のハイブリッド ワークプレースへの差し迫った移行において、ゼロトラスト戦略を重要なツールと見なしています。この推進力はオーストラリア/ニュージーランドにおいて特に顕著です (44%)。

図 1. ゼロ トラストが重要

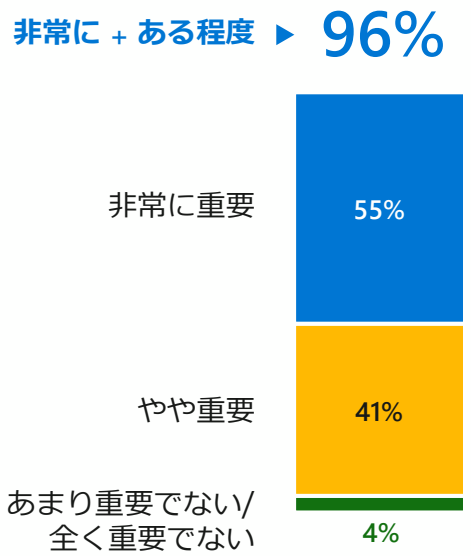


図 2. ゼロ トラスト導入の動機

上位の動機	
セキュリティ態勢の全体的な改善	47%
エンドユーザー エクスペリエンスと生産性の向上	44%
セキュリティ チームの連携方法の改革	38%
セキュリティ スタックの簡素化	35%
セキュリティ コストの削減	35%

ハイブリッド ワークプレースへの移行がゼロ トラスト戦略の導入を拡大している

エンタープライズ組織の 81% がハイブリッド ワークプレースへの移行を開始し、31% が既に完全に導入しています。しかし、完全な導入率は市場によってばらつきがあります。オーストラリアとニュージーランドは 37% で全体をリードしていますが、ドイツははるかに遅れており、ハイブリッド モデルに既に移行しているのはわずか 20% の組織です。(図 3 参照)

グローバル市場はそれぞれ異なる速度でハイブリッド ワークプレースに移行していますが、移行を完了していない組織の大多数 (91%) は、今後 5 年間で移行することを予期しています。ここで重要なこととして、94% は社員の不正利用、IT ワークロードの増加、サイバー攻撃のリスクの増加などを大きな懸念事項に挙げています。(図 4 参照)

図 3. ハイブリッド ワークプレースの導入状況

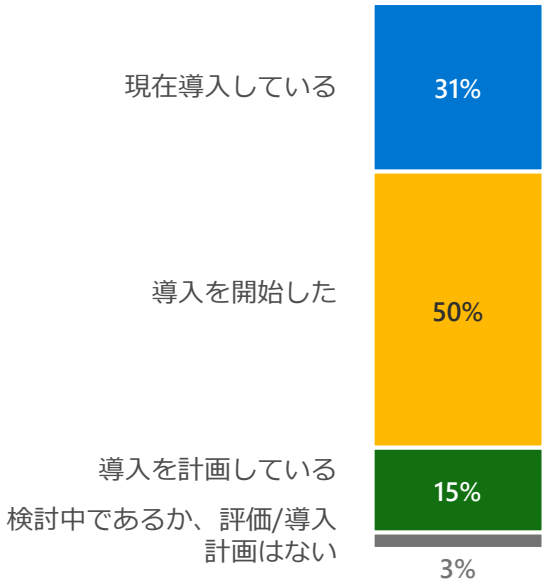
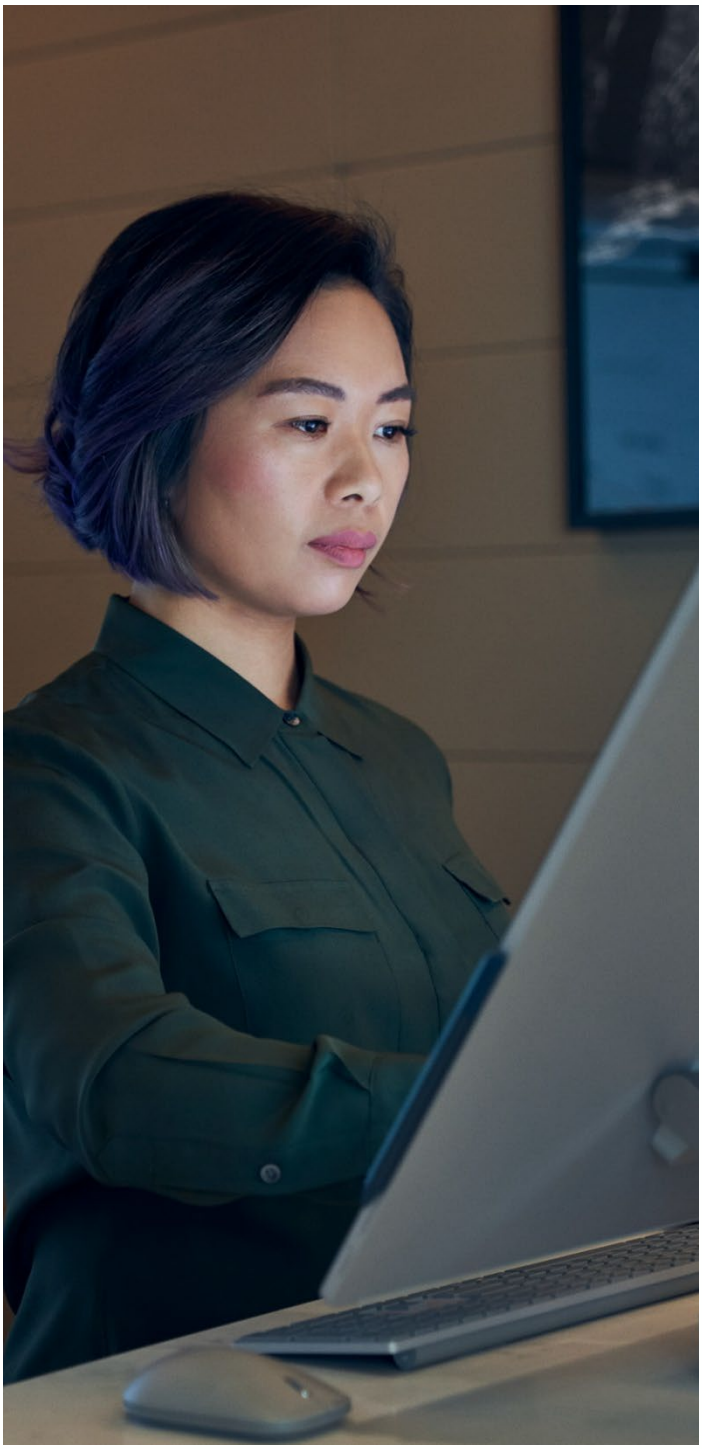


図 4. ハイブリッド ワークプレースに関する懸念事項

社員による安全でないアプリのダウンロード	37%
IT ワークロードの増加	37%
ランサムウェア攻撃	36%
フィッシング攻撃	35%
個人用デバイスの不適切な使用	34%
許可されていないデータへのアクセス	31%
すべてのデバイスの管理が不可能	30%
個人のメール アカウントの使用	30%
データ規制への準拠の不履行	24%

Covid-19 により、ゼロ トラスト戦略への移行を加速させる新たな考慮事項がもたらされている



潜在的な問題を最小限に抑えるために、利害関係者は社員向けトレーニングの増加 (54%) (特に日本 (61%) とドイツ (58%)) と多要素認証 (MFA) (50%) (特に米国 (52%) とドイツ (56%)) により、円滑なユーザー エクスペリエンスと移行を実現することの重要性を強調しています。

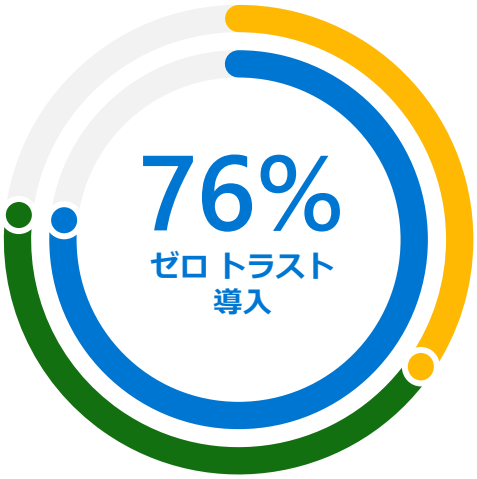
セキュアなリモートおよびハイブリッド ワークはゼロ トラスト戦略によって支援できるため、Covid-19 は 72% の組織のゼロ トラスト戦略の導入を加速しています。ただし、市場間ではばらつきが見られます。パンデミックによって米国 (76%)、日本 (71%)、オーストラリア/ニュージーランド (69%) では 10 社あたり約 7 社の導入が促進されていますが、導入率はドイツ (62%) では極端に低くなっています。これはおそらくハイブリッド ワークプレースへの移行が遅れているためと考えられます。

ゼロ トラストは世界中で広く導入されており、米国で拡大している

ゼロ トラストは単なる流行語ではありません。これは現実です。組織の 76% はこの戦略の導入を少なくとも開始しており、35% は完全に導入していると見なしています。ただし、完全に導入していると見なしている多くの組織はすべてのセキュリティ リスク領域での導入を完了していないことを自ら認めているため、このデータはかなり楽観的な実態を表しています。今日では、米国は他の市場と比較してゼロ トラスト戦略の導入を先行しており、急速に成長し続けています。米国におけるゼロ トラスト戦略の導入率は、2020 年 8 月時点の 70% から 79% に増加しています。これはわずか 8 か月間でかなりの急増です。(図 5 参照)

現在、ゼロ トラスト戦略はセキュリティ領域で優勢になっていますが、その普及は比較的新しいものです。企業の 82% が過去 3 年間にゼロ トラスト戦略を導入しており、そのうち 21% は過去 12 か月間に行われたものです。それでも、米国の組織の 26% は 3 年以上前に導入を開始しているのに対し、日本では 19% の組織、オーストラリア/ニュージーランドでは 6% の組織、ドイツでは 3% の組織に過ぎませんでした。米国での早期の導入は、予算の制約が少ないという事実と相まって、米国の組織が他の市場の組織と比較してゼロ トラストの導入で先を行っている理由を示している可能性があります。同様に、ドイツにおけるゼロ トラスト導入の相対的な遅れは、その低い導入率に現れています。ドイツの組織の 97% は過去 3 年間にやっと導入を開始しています。

図 5. ゼロ トラストの導入



	米 (2020 年)	米	独	日	豪/乳
ゼロ トラストの導入	70%	79%	75%	76%	71%
• 完全に導入	27%	44%	19%	32%	28%
• 導入中	43%	35%	56%	44%	43%

35% が完全に導入

42% が導入中

ゼロ トラストの導入アプローチはさまざまであり、どこからでも開始できる

ゼロ トラスト戦略の主なスタート地点として傑出している単一のセキュリティ リスク領域 (ID、エンドポイント、アプリ、ネットワーク、インフラ、データ、オートメーションとオーケストレーション) というものは存在しません。同じセキュリティ リスク領域から開始している組織は 15% にも満たないものです。組織は独自のニーズと利用可能な内部リソースに基づいて、さまざまな場所から導入を開始しています。最終的には、すべてのセキュリティ リスク領域でゼロ トラスト戦略を導入し、脅威からの保護をさらに強化することを求めています。このためゼロ トラストは、長期間にわたって完了するエンドツーエンド戦略として認識されています。(図 6 参照)

組織ではゼロ トラスト戦略のセキュリティ リスク領域の域を超えて優先順位を付けるにあたり、各セキュリティ リスク領域の個々の構成要素を特定する必要があります。エンドポイント、アプリ、ネットワーク、データ、オートメーション/オーケストレーションについては、明確なスタート地点というものはありません。最優先事項としてランク付けされている構成要素は、セキュリティ専門家の間で大きく異なります。ただし、ID に関しては通常は強力な認証が最初に導入され、インフラ内では脅威検出ツールが明確な優先事項となっています。(図 7 参照)

図 6. 現在のゼロ トラストの導入状況 – セキュリティ リスク領域

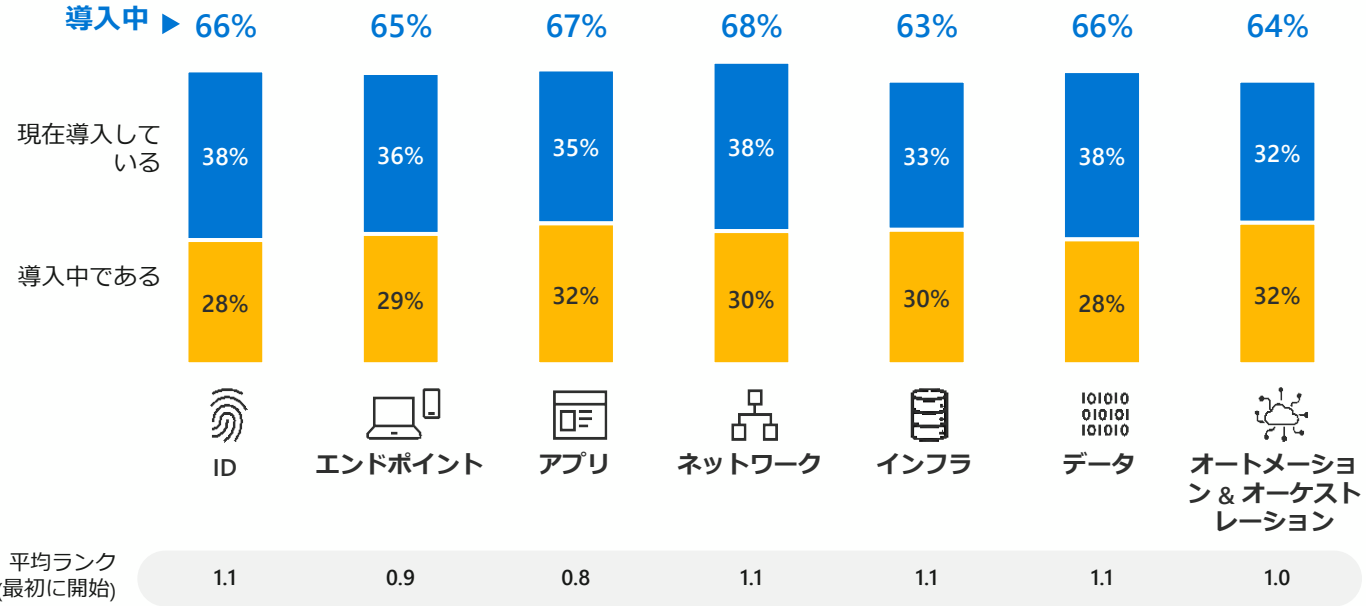


図 7. ゼロ トラスト構成要素の導入 (上位 3) – No. 1 ランク (最初に導入)

ID	
強力な認証 (多要素認証、パスワードレス認証など)	32%
自動化されたリスクの検出と修復	27%
リソースへのゲート アクセスに対するアダプティブ アクセス ポリシー	22%

アプリ	
継続的なシャドウ IT の検出とリスク評価	23%
アプリへの詳細なアクセス制御 (制限された可視性や読み取り専用など)	22%
アプリに対するポリシーベースのアクセス制御	20%

インフラ	
脅威検出ツールへのセキュリティ運用チームのアクセス	25%
ハイブリッドおよびマルチクラウド全体でのクラウド ワークロードの保護	19%
ワークロード全体における詳細な可視性とアクセス制御 (仮想マシン、サーバーなど)	17%

オートメーション & オーケストレーション	
調査と対応のための一元的なプラットフォームによってエンドツーエンドの可視性が確立されている	29%
ドメイン全体 (ID、エンドポイント、アプリ、ネットワーク、インフラ) で脅威データを収集し、分析している	28%
調査と対応が自動化されている	22%

エンドポイント	
管理対象外のデバイスと管理対象デバイスのデータ損失防止ポリシー/制御	27%
リアルタイムのデバイス リスク評価 / エンドポイント脅威の検出	26%
デバイスが ID プロバイダーに登録されている	24%

ネットワーク	
セキュアなアクセス制御によるネットワークの保護	25%
コンテキストベースのシグナルによる脅威からの保護とフィルタリング	24%
すべてのトラフィックが暗号化されている	20%

データ	
アクセスの意思決定はセキュリティ ポリシー エンジンによって管理されている	21%
データは分類され、ラベル付けされている	21%
最も機密性の高いファイルは暗号化によって永続的に保護されている	20%

私たちはそれを単なる一連のテクノロジとしてではなく、すべてのユーザー リソースはネットワーク内またはネットワーク外かにかかわらず、検証されるまで信頼できないものとして取り扱うための戦略およびアプローチとして捉えていました。”

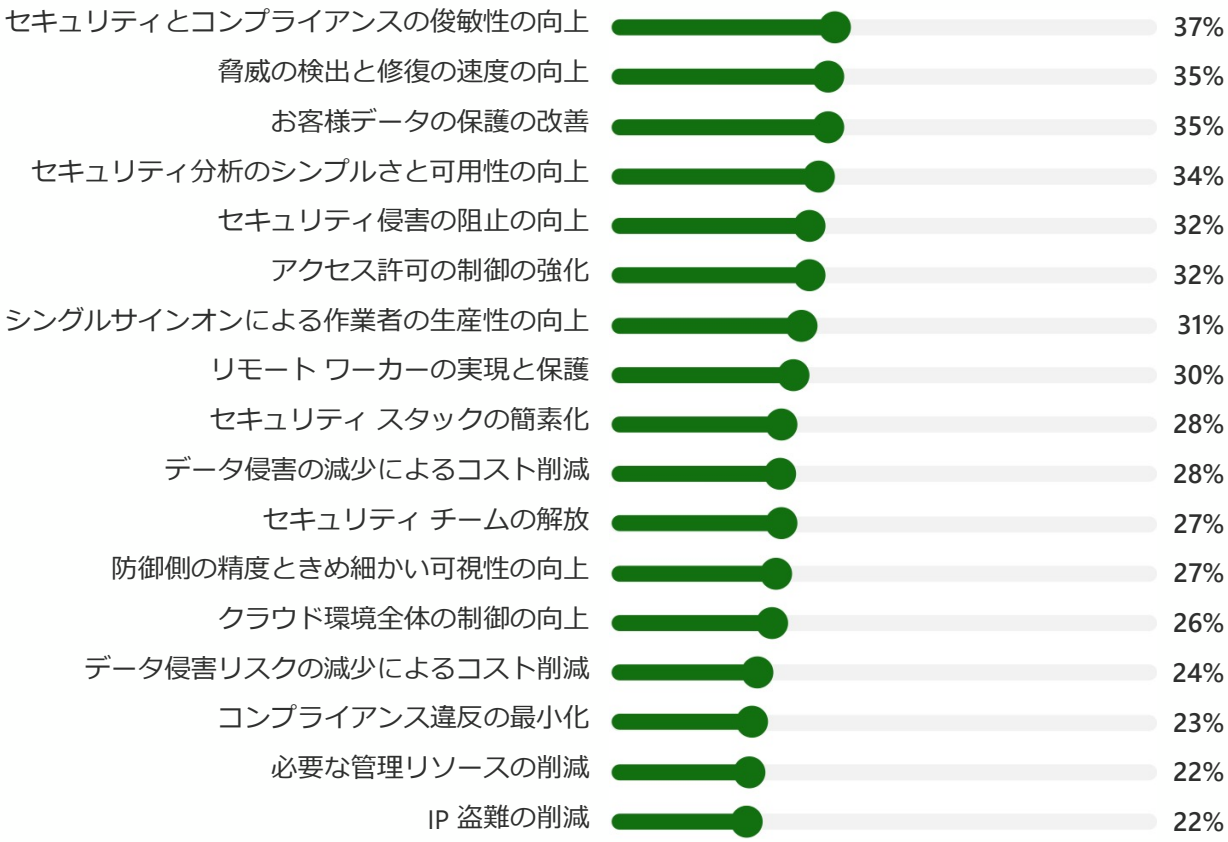
米国セキュリティ意思決定者
レジャー産業

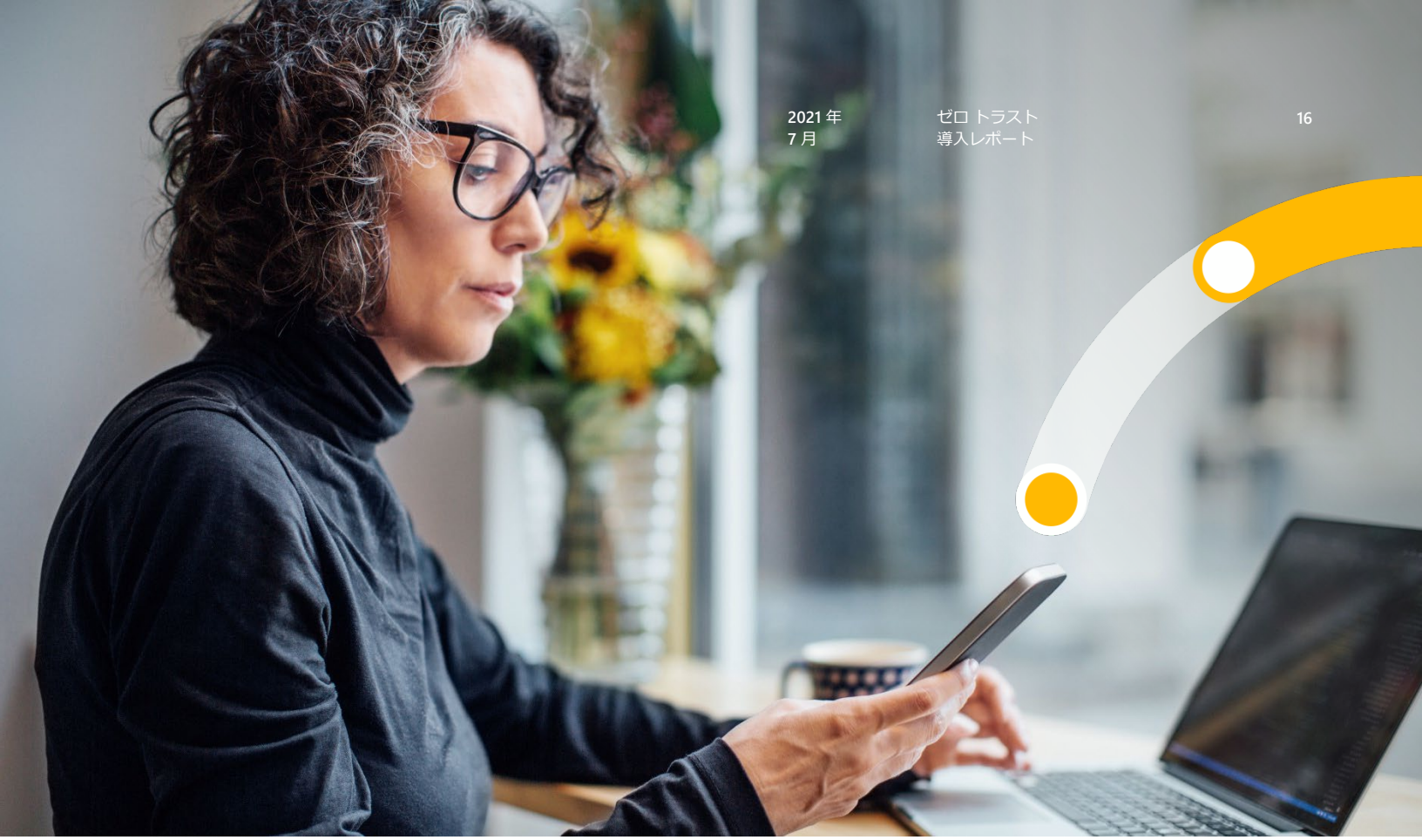
ゼロ トラスト戦略の導入を開始した組織には、俊敏性、スピード、保護の向上などのメリットがもたらされる。リソースのメリットは一般的ではない

ゼロ トラスト戦略を導入した組織には、俊敏性の向上 (37%)、スピードの向上 (35%)、お客様データの保護の強化 (35%) などのメリットがもたらされます。(図 8 を参照)しかし、セキュリティ チームの解放を含む社員へのメリット (27%) や、インフラ管理に必要なリソースの削減 (22%) などの直接的なメリットはあまり実現されていません。

重要なこととして、組織は特に IoT と OT のセキュリティに関してゼロ トラスト戦略がほとんどの脅威や環境への変化の管理に役立つと考えています (47%)。

図 8. ゼロ トラストのメリット





組織はゼロ トラスト戦略を最大限に活用することに自信を持っている

79% が、セキュリティの脅威全体に対応する能力に自信を持っています。ただし、脅威が事実の捏造にかかわる場合には、この自信は弱まっています。SDM (セキュリティ意思決定者) は、合成 ID (20%) およびディープ フェイク (10%) が関与する脅威への対応について、最も不安を感じています。

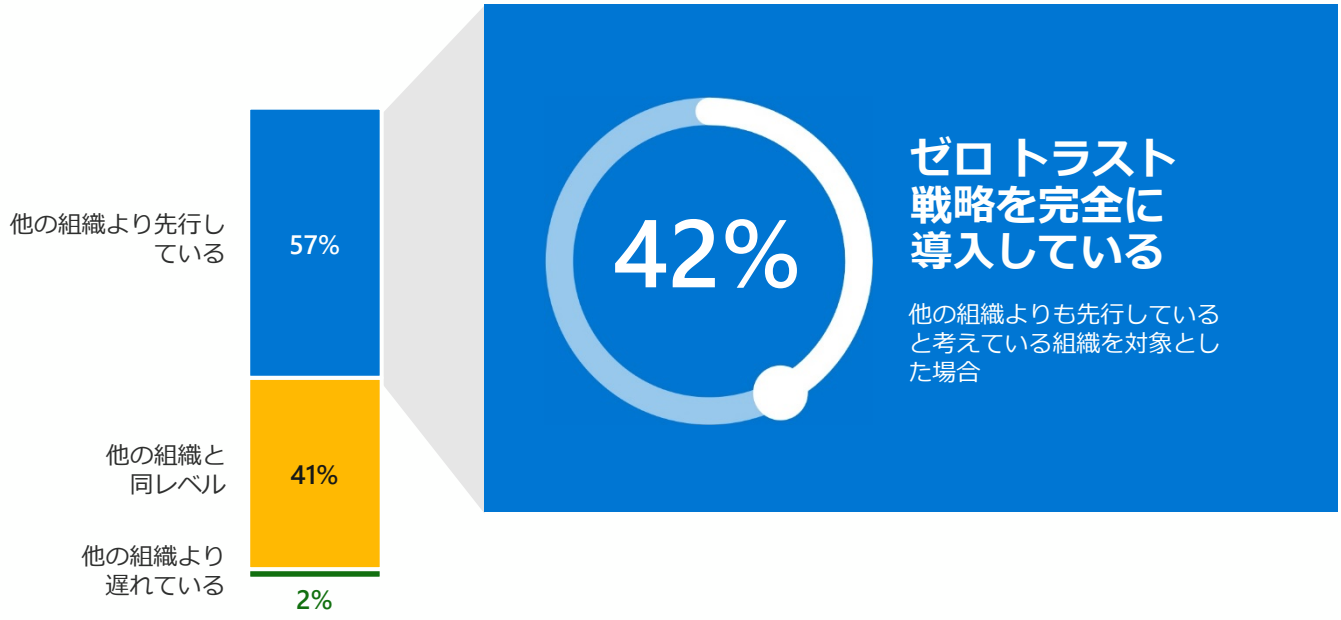
得られたメリットを踏まえて、ゼロ トラストは一般に肯定的な関連性を獲得しています。SDM は、4 つの市場全体にわたって組織のアプローチを実用的で向上心に溢れたものとして捉えており、自信がある (37%)、効率的 (31%)、モチベーションが高い (25%)、刺激的 (25%)、エキサイティング (25%) という言葉でそれを表現しています。特に日本では、セキュリティ専門家はゼロ トラストを需要が高く (27%)、革新的 (25%) であると捉えており、導入は容易ではないが、導入後のメリットは広範囲に及ぶことを示唆しています。

多くの組織はゼロ トラストの導入を先駆けていると考えているが、依然として多くの作業が残されている

ゼロ トラスト戦略を完全に導入した組織はわずか 35% に過ぎませんが、52% は計画よりも進んでいると回答しており、57% は他の組織よりも先行していると考えています。特に、日本 (66%) とオーストラリア/ニュージーランド (63%) の組織は他者よりも先行していると考えています。自信はあらゆる市場に溢れていますが、認識と現実の間には大きな隔たりがあるように見受けられます。他の組織よりも先行していると感じている組織のうち、ゼロ トラスト戦略を完全に導入したと主張しているのはわずか 42% です。(図 9 参照)

多くの組織はゼロ トラスト戦略に自信を持っており、将来のセキュリティ脅威に対処できると感じていますが、リスク領域全体にわたって戦略を完全に導入するには依然として多くの作業が残されています。たとえば、ゼロ トラスト戦略を完全に導入したと見なしている組織のうちの半数近くはセキュリティリスク領域全体での導入をまだ完了しておらず、特にインフラと ID の領域での導入率が低い傾向があります。

図 9. ゼロ トラストの導入比較



	米	独	日	豪/乳
先行している	59%	46%	66%	63%
同レベル	40%	52%	34%	32%
遅れている	2%	2%	0%	6%

今後 2 年間を見据えると、ゼロ トラスト戦略はセキュリティの最優先事項となり続ける

組織はゼロ トラスト戦略を全面的に支持しており、意思決定者は今後 2 年間にわたってそれがセキュリティの最優先事項となり続けるものと述べています。セキュリティ イニシアティブとしてのゼロ トラスト戦略の相対的な重要性は、セキュリティ意思決定者が戦略は総合的な成功にとって重要であり続けると予想している (96%) ことから、2023 年までに高まる (53% から 58%) と予測されます。(図 10 参照)

予想される重要度は日本の組織において特に高く、全体の平均である 56% と比較して、70% がゼロ トラスト戦略は今後 2 年間で非常に重要になると述べています。ゼロ トラスト戦略の予算も、73% の組織が予算を増やすことを予期しているため、増加が見込まれます。ただし、この数字はドイツでは若干低く (67%)、31% は予算は変わらないと予測しています。(図 11 参照)

図 10. 今後 2 年間に予測されるゼロ トラストの重要度

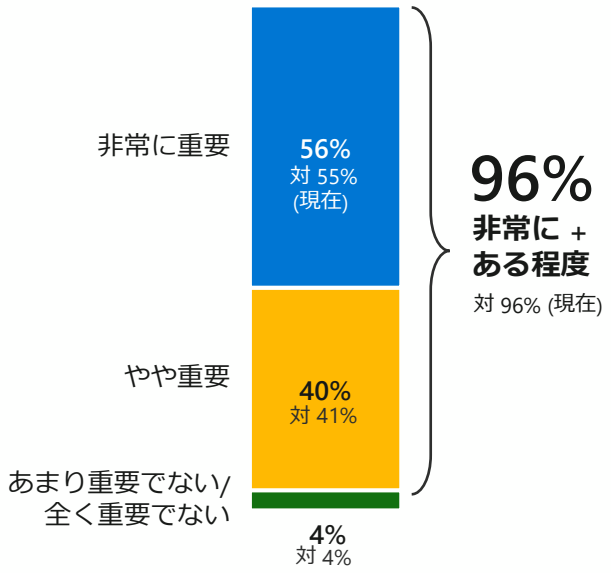
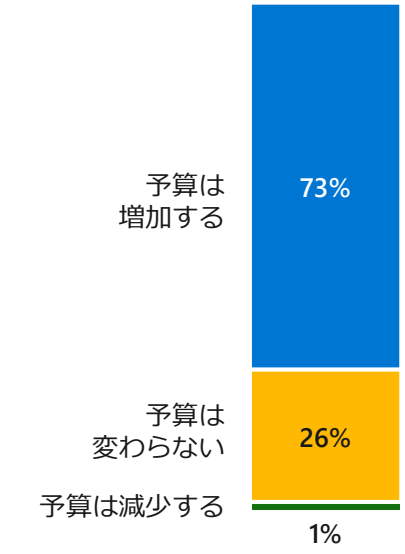
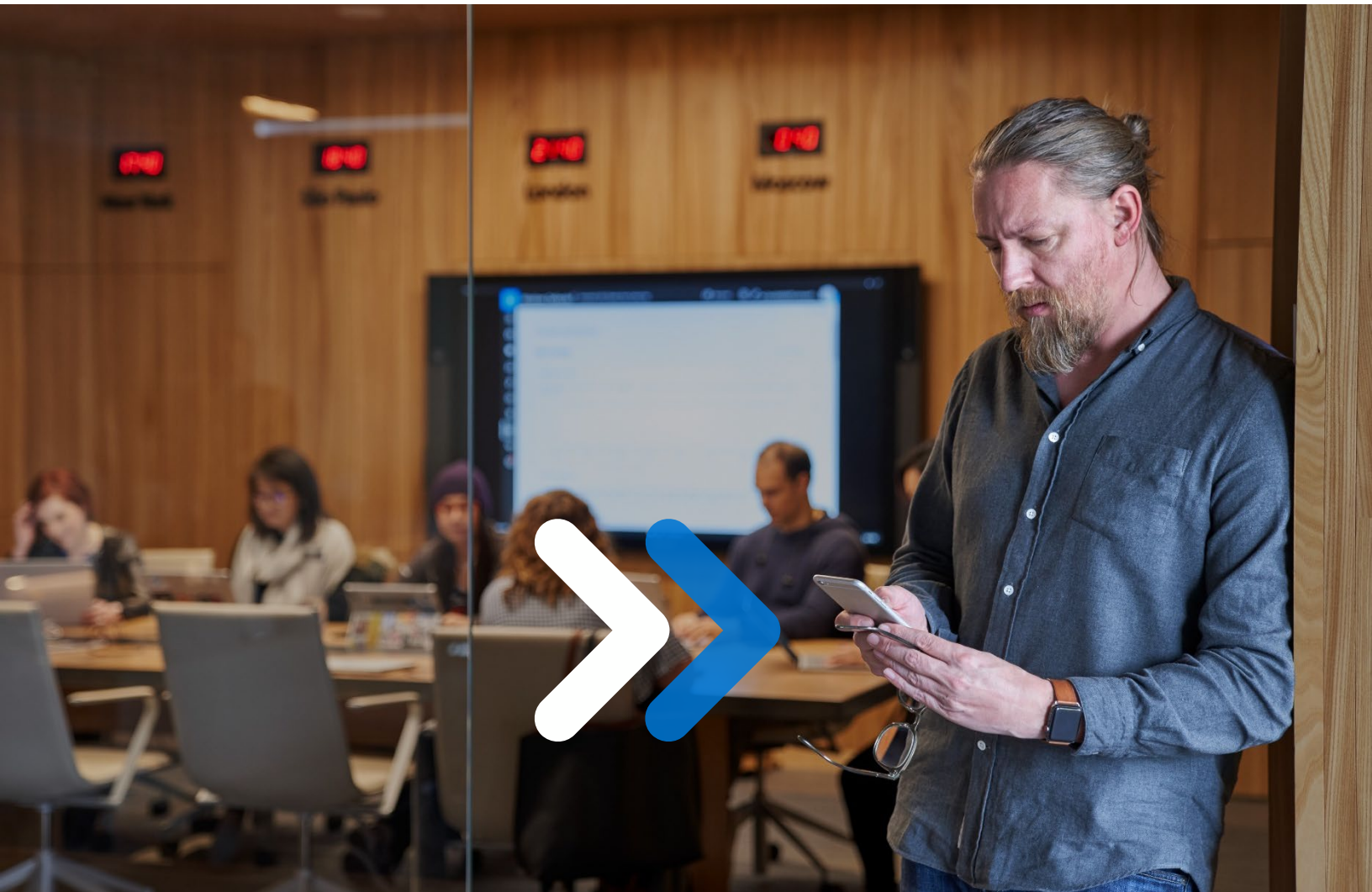


図 11. 今後 2 年間に予期されるゼロ トラストの予算



ゼロ トラスト戦略の成功を実証することで、さらなる投資が促進される可能性がある

ゼロ トラストを一途に受け入れた組織は、今後 2 年間に投資額を倍増させることを予期しており、導入をまだ始めていない組織はさらに遅れをとっています。これらの組織は、セキュリティ計画の中でゼロ トラストを優先させることと、予算の増加の予測において、完全に導入している組織よりも遅れを取っている (それぞれ 42% 対 66% と 66% 対 72%) だけでなく、今後の IoT および OT のセキュリティ管理に関する自信もかなり低くなっています (40% 対 53%)。



社員の課題を克服することがゼロ トラストの投資を倍増させる鍵となる

ゼロ トラスト戦略の導入が急速に進展しているにもかかわらず、組織は導入をさらに進めるにあたって無数の課題を克服しなければなりません。(図 12 を参照) リソースとリーダーシップの課題は、これらのカテゴリ内で最も一般的なものです。ゼロ トラスト戦略の導入に必要な時間と、経営幹部によるサポートの欠如が障壁の上位を占めており、後者は特にオーストラリア/ニュージーランドで顕著になっています (65%)。

さらに、組織の 45% が障壁として特定している予算上の制約も、リソースとリーダーシップの課題に影響を与える可能性があります。

たとえば、SDM (セキュリティ意思決定者) の 21% は、導入の障壁としてゼロ トラストへの投資の ROI を実証することが困難であると言及しています。これは、経営幹部の合意の欠如につながる可能性があります。米国以外の市場では予算上の制約があることが多いため (日本の組織の 60%、ドイツの組織の 57%、オーストラリア/ニュージーランドの組織の 57%)、これが波及効果をもたらし、日本、ドイツ、オーストラリア/ニュージーランドでのゼロ トラスト戦略の導入が米国と比較して低く、遅れる可能性があります。

図 12. ゼロ トラストの障壁

リソースの課題 60%	リーダーシップ 53%	技術的 46%	ベンダー 46%	予算の制約 45%
20% 導入に時間がかかりすぎる	20% 経営幹部からの幅広い支援が不足している	21% セキュリティ ソリューションの統合が難しい	21% ベンダーの導入サポートが必要である	21% ゼロ トラスト戦略の導入コスト
19% 内部の変更管理が欠如している	19% 利害関係者からの支援が不足している	19% レガシー システムとの互換性がない	21% 適切なベンダーの特定が難しい	21% ROI の実証が難しい
18% さらに多くの教育用資料が必要である	19% 説得力のあるビジネス ケースの作成に援助が必要である	19% 組織全体でのスケーリングが難しい	17% 革新的なパートナーを見つけられない	14% 十分な予算がない
17% 自分たちの規模の組織には必要ない	18% 組織の賛同が得られない			
16% 適切な導入に必要な人材を確保していない				

“賛同を得ることは最初は困難でしたが、このプロジェクトに投資することに利害関係者として合意した後は、全員が前向きに取り組みました。“

米国セキュリティ意思決定者

FinTech

セキュリティ意思決定者は包括的または統合プロバイダーを好む傾向がある

ゼロ トラスト ベンダー戦略に関して言及すると、組織はベストインスイートまたはベストインブリードのアプローチを取ることに直面しています。前者の戦略では、包括的または統合プロバイダーからゼロ トラスト アーキテクチャ全体を構築するための一連の製品を購入します。社内のリソースが限られている組織にとって、これはより多くの専門知識、リソース、シンプルさを提供するソリューションであると SDM は考えています。ただし、このアプローチでは脆弱性の高まりと柔軟性の欠如が懸念されます。(図 13 参照)

後者のベストインブリード戦略では、特化したベンダーからゼロ トラスト テクノロジ構成要素を個別に取得します。ベストインスイート戦略とは異なり、この戦略は、特定の分野を専門とする各プロバイダーに依存するため、柔軟性が高く、組織の戦略にさらに沿ったものになります。しかし、セキュリティ専門家はベストインブリード戦略をよりコストがかかり、より多くのリソースを必要とし、可視性が阻害されるものと捉えています。これは最終的にベンダーや予算の課題につながる欠点となります。(図 14 参照)

組織の意見は大きく別れています。SDM の半数強 (55%) は、包括的な (ベストインスイート) プロバイダーとの連携を好んでいます。(ただし、オーストラリア/ニュージーランドの組織は反対の方向に傾いており、52% がベストインブリードを好んでいます)。

図 13. ベストインスイートのメリットと障壁 – 上位 2 位

ベストインスイートのメリット	
ベンダーはソリューション全体にわたって業界固有の専門知識を持っている	24%
ゼロ トラスト戦略の計画に役立つより多くのリソースを使用できる	23%
セキュリティ スタックの簡素化	22%

ベストインスイートのデメリット	
単一のベンダーに依存するため脆弱性が増加する	34%
レガシー アーキテクチャとのより複雑な統合が必要となる	33%
特殊機能に対する柔軟性に劣る	29%

図 14. ベストインブリードのメリットと障壁 – 上位 2 位

ベストインブリードのメリット	
ゼロ トラスト戦略の特定の構成要素に最適なソリューションを追求できる柔軟性がある	33%
自分の組織のアーキテクチャまたは戦略により密接にソリューションを合わせられる	30%
さまざまなベンダーとの提携によりイノベーションの機会が増加する	26%

ベストインブリードのデメリット	
コストが高くなる	29%
さまざまなソリューション間でデータを共有できない	26%
社内チームが導入および管理するソリューションが大量になる	26%

最終的な考察

セキュリティ リスクがさらに増えるだけでなく、悪質化するにつれて、市場や業界にまたがる組織は、「決して信用せず、常に検証する」ことを説くゼロ トラスト戦略を採用しています。ゼロ トラスト戦略は、総合的なセキュリティ態勢、エンドユーザー エクスペリエンス、生産性を向上させて、社員のセキュリティ手順を簡素化し、コストを削減することを目指している組織にとって、セキュリティの最優先事項となっています。ただし、ゼロ トラスト戦略のメリットは十分に確立されている一方で、限られたリソースと、リーダーシップの間での懐疑心が全体的な導入を妨げています。

ゼロ トラスト戦略の導入は、COVID-19 パンデミックの影響もあり、過去 3 年間で加速しています。重要なこととして、リモートおよびハイブリッド ワークプレースへの移行は、ゼロ トラスト アプローチの導入をさらに拡大させています。このアプローチでは、社員が時には個人のデバイスを使用してオフサイトからアクセスするシステムやデータを保護することができます。COVID による導入の加速は、パンデミック中に戦略を取り入れた組織が、他の組織より多くのセキュリティ リスク領域において導入を展開していることから、ゼロ トラストの総合的な準備状況の適切な予測要因となっています。

しかし、最も先進的なゼロ トラスト戦略の導入者にとっても、やるべきことは残されています。組織のゼロ トラスト成熟度に関する誤った認識により、気づかないうちに脆弱性がもたらされることがあります。

市場全体の組織の大部分では、ゼロ トラスト戦略の重要度は時間とともに増加すると考えており、それに伴って予算が増えることを予想しています。予期されるこの優先順位の移行は、予算に関する懸念が導入の大きな障壁となっている米国以外の市場にとって特に重要です。完全な導入を目指すことは、ファイナンスに関してもロジスティクスに関しても困難に感じるかもしれませんが、ゼロ トラスト アプローチのメリットは否定しがたいものであり、マイクロソフトでは組織がこのような急成長を遂げるにあたってガイダンスや支援を提供する準備を整えています。

ゼロ トラストの詳細を確認し、組織のゼロ トラストの成熟度を評価するには、以下をご覧ください。

aka.ms/zerotrust

詳細な調査目標と対象者の募集

調査の目的は次のとおりです。

1. ゼロ トラスト アプローチの現状を理解する
2. ゼロ トラスト アプローチの導入に関する考え方、ベスト プラクティス、メリット、課題を明らかにする
3. ゼロ トラスト アプローチの未来を探る
4. ゼロ トラスト アプローチにおけるイノベーションとトレンドを状況に当てはめて可視化する

審査基準を満たすために、セキュリティ意思決定者は以下に該当する必要がありました。

サイバー セキュリティ、セキュリティ運用、脅威からの保護、ID 管理、リスク管理、アプリケーション セキュリティ、デジタル フォレンジック、インシデント対応などの組織内のセキュリティの責任を担っている

エンタープライズレベルの企業 (米国では社員 1000 人以上、ドイツ、日本、オーストラリア、ニュージーランドでは社員 500 人以上) でフルタイムで雇用されている

年齢層 25 - 75 歳

ゼロ トラストに精通している

ゼロ トラスト戦略の開発/導入に関する意思決定に関与している

2021 年 4 月の調査サイクル中にインタビューした 911 人のセキュリティ意思決定者のうち:

米国では 477 人の SDM をインタビュー

ドイツでは 201 人の SDM をインタビュー

オーストラリア/ニュージーランドでは 126 人の SDM をインタビュー

日本では 107 人の SDM をインタビュー

注: 調査はさまざまな拡大/封じ込めの段階にあったグローバルな COVID-19 パンデミックの最中に実施されました。