

2023年版 ゼロトラスト トランスフォーメーションの現状

予防から実行まで：

高度にモバイル化、クラウド化する企業がゼロトラストの可能性を最大限に活用するために



ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラ
ウドの実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト ア
プローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange

目次

- 03. [本書の要旨](#)
- 05. [ゼロトラストの現状：早わかり](#)
- 06. [セクションI:ゼロトラスト採用の背景にあるクラウドの実態](#)
- 13. [セクションII:真のゼロトラストの理解](#)
地域の視点：南北アメリカからの声
- 22. [セクションIII:ハイブリッドワークを実現するゼロトラストへの転換](#)
地域の視点：アジア太平洋からの声
- 30. [セクションIV:新興技術を統合するためのゼロトラストアプローチの採用](#)
地域の視点：EMEAからの声
- 35. [セクションV:ゼロトラストの可能性を最大限に引き出すための取り組み](#)
- 38. [ZscalerとZscaler Zero Trust Exchangeについて](#)
- 40. [調査方法](#)

ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange

本書の要旨

Nathan Howe | VP、新興技術&5G、Zscaler

デジタル トランスフォーメーションの流れが加速する中、ゼロトラストは高度に分散したクラウドとモバイル中心の世界でユーザー、ワークロード、デバイスを保護する理想的なフレームワークとして頭角を現しています。



何十年にもわたる従来型のセキュリティとネットワークの原則が崩壊し、ゼロトラストが主流となりつつある今、世界中のITリーダーはこのフレームワークに着目し始めています。

クラウドへの移行を開始したITリーダーの90%以上は、ゼロトラスト セキュリティ戦略をすでに実施済みか、今後12か月以内の

実施に向けて取り組みを進めています。これは、Zscalerがアプリケーションとサービスのクラウド移行をすでに開始している組織の1,900人を超えるCIO、CISO、CDO、CTO、インフラ責任者を対象に行った最新のグローバル調査の結果によるものです。

この結果は良い兆候であり、その背景には今後1年以上にわたってゼロトラスト アーキテクチャーの実装に対する楽観的な見通しが続いていることが示されています。

ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange

22%

クラウド インフラの可能性を最大限に活用していると強く確信する組織はわずか22%にすぎず、この結果は、今後セキュリティを超えた枠組みで考える必要があることを示しています。

実際、クラウド移行のプロセスが進む中、ゼロトラストのセキュリティ ケースは当然ながらより明確になっていきます。3分の2以上(68%)のITリーダーは、従来型のネットワーク セキュリティ インフラでは安全なクラウドトランスフォーメーションは不可能であること、またアプリケーションへのリモート アクセスの保護に関しては、従来型のファイアウォールやVPNよりもゼロトラスト ネットワーク アクセスのほうが明らかに優れていることを認識しています。

しかし、クラウド インフラの可能性を最大限に活用していると強く確信する組織は

わずか22%にすぎず、この結果は、今後セキュリティを超えた枠組みで考える必要があることを示しています。ITの全体的な観点からアプローチした場合、ゼロトラストはデジタル化プロセス全体でさまざまなチャンスを引き出す可能性を秘めています。ゼロトラストは大規模なサイバー セキュリティ攻撃を防ぐことができますが、それだけではありません。より大きな変化をもたらすイノベーションの推進から従業員エンゲージメントの向上、さらにはコストの効率化まで、はるかに多くの効果をもたらします。

ハイブリッドなアプローチでIoT/OT、5G、さらにはメタバースなどの多くの新興技術を活用した先進的な職場環境や働き方の提供に取り組む組織は、ゼロトラストとデジタルトランスフォーメーションの両方を考慮する視野を広げる必要があります。ゼロトラスト プラットフォームには、ビジネスと組織のインフラ要件を再設計する力があります。それは従業員が求めるハイブリッド ワーク モデルを提供できるだけでなく、敏捷性と効率性から将来を見据えたインフラまで、これに伴うすべてのメリットを備えた完全にデジタル化された組織への変

革を可能にする真のビジネス ドライバーでもあります。

私たちは、現在の組織におけるゼロトラストトランスフォーメーションの現状を明らかにするためにこの調査を実施しました。実装率が高いという調査結果には期待が持てますが、その背後にある理論的根拠はより野心的です。ITリーダーにはビジネスの意思決定者にゼロトラストを教育し、それを価値の高いビジネスドライバーとして取り上げる絶好の機会がありますが、これは、企業が将来のテクノロジーに対応できるようにするためのミッシングリンクなのです。

ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange

ゼロトラストの現状

90% クラウドへの移行を開始した組織の90%以上は、ゼロトラスト セキュリティ戦略をすでに実施済みか、今後12か月以内の実施に向けて取り組みを進めています。

88% 全世界のITリーダーの88%は、自社がクラウド インフラの可能性を活用しているとある程度確信しているものの、強く確信しているリーダーはわずか22%にすぎません。

クラウド インフラの可能性を最大限に活用していると確信する組織の割合(地域別):



#1 ZTNAは今後12か月間のゼロトラスト技術への投資の最優先事項であり、これはハイブリッド ワークにおけるリモート アクセスの重要性を示しています。

68% 3分の2以上(68%)のITリーダーは、従来型のネットワーク セキュリティ インフラでは安全なクラウド トランスフォーメーションは不可能であること、またアプリケーションへのリモート アクセスの保護に関しては、従来型のファイアウォールやVPNよりもゼロトラスト ネットワークアクセス(ZTNA)のほうが明らかに優れていることを認識しています。

54% ITリーダーの54%がVPNや境界ファイアウォールはどちらもサイバー攻撃からの保護や、アプリケーションのトラフィックおよび攻撃の可視化には効果がないと考えています。

クラウドの可能性を最大限に活用するうえでの主な障壁:

45% クラウドのデータ保護に関する課題とデータ プライバシーの懸念

42% 複雑なネットワークと拡張が困難なセキュリティ ハードウェア

40% IoTとOTへのサードパーティー アクセスおよびリモート アクセス

33% 一貫性のない接続とユーザーのリモート アクセス エクスペリエンスの低下

セキュリティ、アクセス、複雑性以外にゼロトラスト アーキテクチャーを実装する主な理由に戦略的なビジネス目標は含まれていない:

65% 高度な脅威やWebアプリケーション攻撃の検出の改善と機密データの保護の強化

44% ベンダー、パートナー、運用技術のリモートアクセスの保護

27% ハイブリッド ワークの接続の安全性の改善

24% 従来型のネットワーク セキュリティのコストと複雑性の低減

ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange

セクションI

ゼロトラスト採用の背景にあるクラウドの実態

本調査では、「クラウド」は企業ネットワーク内のローカル データ センターではなく、インターネットを介してホストされたサービスとして提供されるアプリケーション、データ、ワークロードを意味します。Software as a Service (SaaS)、Infrastructure as a Service (IaaS)、Platform as a Service (PaaS)、クラウドに組み込まれているまたはホストされているプライベート アプリケーションなどがこれに該当します。

ゼロトラストを解説する前に、ゼロトラストが採用される背景、つまりゼロトラストを取り巻く広範なIT環境で何が起きているのか、特に組織がクラウド化への道のりでどのような状況にあるのかを検証します。

過去数年間の出来事がクラウドへの移行を加速させたことは間違いありませ

ん。すべてのプロセスが完了していないにしても、多くの組織が移行を順調に進めています。

本調査では、アプリケーションとサービスのクラウド移行をすでに開始している世界中の組織の1,900人を超えるCIO、CISO、CDO、CTO、インフラ責任者を対象とし、そのうち、ほぼ半数(46%)

が移行プロセスを100%完了したと回答しています。

しかし、ITリーダーの88%がクラウドへの移行を最大限に活用しているとある程度の自信を持っている一方で、自社がクラウド インフラの可能性を最大限に活用していると確信しているリーダーはわずか22%にとどまっています。

自社が現在クラウド インフラの可能性を最大限に活用していると強く確信している回答者の割合：

22% 合計

14% ヨーロッパ

42% 南北アメリカ

24% アジア太平洋

ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange

自社が現在クラウド インフラの可能性を最大限に活用
していると強く確信している回答者の割合：

 国にマウス カーソルを
合わせて詳細を表示

ヨーロッパ：

- 9% ドイツ
- 11% フランス
- 11% スペイン
- 19% 英国

南北アメリカ：

- 41% 米国
- 51% ブラジル

アジア太平洋：

- 16% シンガポール
- 55% インド



ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange

地域の違いを調べると、ヨーロッパのITリーダーはクラウド インフラの使用に最も懐疑的で、確信を持っているのはわずか14%でした。しかし、南北アメリカではこの数は42%に跳ね上がります。

この差の明確な要因は1つではありませんが、ヨーロッパは伝統的に慎重なアプローチをとり、さらにデータ プライバシーに重点を置いているため、革新的技術の採用スピードが文化間で異なることが考えられます。また、ヨーロッパでは接続インフラが整備され、製造業が中心となっていることから、5Gのようなイノベーションをすぐに受け入れる動きは少なく、既存のビジネス プロセスを変更するには長いリード タイムが必要になってきます。後のセクションで詳しく説明しますが、南北アメリカの組織は人工知能、機械学習、拡張現実などの新興技術に重点を置いており、より高度なユース ケースをサポートするクラウド インフラの計画がすでに存在していることが見て取れます。

しかし、さらに広く考えた際、なぜ組織にとってクラウドの可能性を最大限に引き出すことが困難だったのでしょうか。

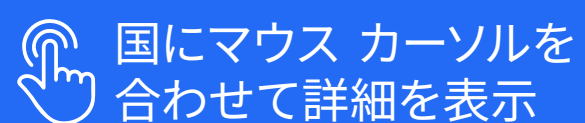
表面上はセキュリティが最大の障害のように思われますが、ITリーダーの見解としては2つのセキュリティ関連の理由が挙げられます。

クラウドの可能性を最大限に活用するうえでの主な障壁：

- 45%** データ プライバシーの懸念とクラウドのデータ保護に関する課題
- 42%** ネットワークは適応が非常に複雑で、ネットワーク セキュリティの拡張が困難
- 40%** IoTとOTシステムへのサードパーティー アクセスとリモート アクセスを可能にする際の課題
- 33%** 一貫性のない接続とリモート アクセス時の低品質なユーザー エクスペリエンス

ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange

クラウドの可能性を最大限に活用するう えでの主な障壁(国別):

国にマウス カーソルを
合わせて詳細を表示

ヨーロッパとアジア太平洋ではデータ プライバシーの懸念が圧倒的:

- 36% スペイン
- 34% インド
- 33% イタリア
- 32% オーストラリア
- 28% フランス

南北アメリカの組織はクラウドのデータ保護の 課題に取り組んでいる:

- 44% ブラジル
- 30% 米国

特にシンガポールと日本では、ネットワーク セキュ リティ ハードウェアの拡張が大きな課題:

- 41% シンガポール
- 30% 日本



ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange

クラウドベースの環境では攻撃対象領域が爆発的に増加し、インターネットに接続するすべてのサービス、ユーザー、デバイスが潜在的なエントリー ポイントとなり、脅威からの保護が必要な脆弱性の高い玄関口となります。

これは組織にとっては十分懸念すべき事態です。クラウドベースの環境では攻撃対象領域が爆発的に増加し、インターネットに接続するすべてのサービス、ユーザー、デバイスが潜在的なエントリー ポイントとなり、脅威からの保護が必要な脆弱性の高い玄関口となります。これについては、次のセクションで詳しく説明します。

しかし、クラウド移行の背景にある全体的な動機に目を向けると、ITリーダーのクラウドに対する見方には根本的な壁があり、それこそがクラウドの有効活用に影響を与えていることがわかります。組織がデジタルトランスフォーメーション プロジェクトを推進する主要因を調査した結果、コストの削減、技術革新の促進、サイバー リスクの管理の3つが上位に挙がりました。

グローバルITリーダーがデジタル トランスフォーメーション プロジェクトを推進する主な理由：



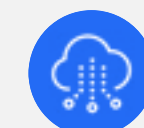
ITインフラのコスト削減



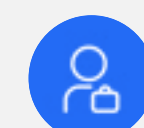
5Gやエッジ コンピューティングなどのイノベーションの促進



サイバー セキュリティ リスクの軽減



マルチ クラウド環境の管理



優秀な人材の確保と維持の強化

ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange

デジタル トランスフォーメーション プロ ジェクトを推進する主な理由(国別):

 国にマウス カーソルを
合わせて詳細を表示

ブラジルはグローバルな見解と一致しており、ほとんどの組織がITインフラのコスト削減を最大の動機として挙げています。

しかし、ヨーロッパ諸国の一部ではまったく別の状況で、フランスはハイブリッド ワークの実現に最も関心を示し、スウェーデンの最優先事項はユーザー エクスペリエンスとなっています。

5Gやエッジ コンピューティングなどのイノベーションの促進は、日本、メキシコ、シンガポールなどの将来性を重視する国で優先事項となっています。また、シンガポールでは収益の増加も同様に重要視されています。

また、ビジネス プロセスの最適化はブラジルとスペインでトップ3の要因に入りました。



すべて非常に現実的で、ITによって推進されています。実際、コスト削減の重要性が高いことは、現状を踏まえると当然の結果といえるかもしれませんが、これは同時にクラウドの主なメリットが十分に理解されていない可能性があることを示しています。そし

てこの事実が、本来クラウドをサポートするために存在しているテクノロジーへのアプローチとその使用に影響を及ぼしている可能性があるのです。今こそゼロトラストを考

過去数年間の出来事がクラウドへの移行を加速させたことは間違いありません

ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange

セクションII

真のゼロトラストの理解

ゼロトラストとは最小特権アクセスに加えて、ユーザーやアプリケーションは本質的に信頼されるべきではないという原則に基づく、現代の組織を保護するための包括的なセキュリティ アプローチです。すべてが敵対的であるという仮定から始まり、ユーザーのアイデンティティとコンテキストのみに基づいて信頼を確立し、ポリシーはあらゆる段階でゲート キーパーとして機能します。米国では、アメリカ国立標準技術研究所(NIST)がゼロトラスト アーキテクチャーの基本原則を「物理的な場所またはネットワークの場所(ローカル エリア ネットワークやインターネットなど)、あるいは資産の所有権(企業または個人所有)のみに基づいて、資産やユーザー アカウントに暗黙の信頼を付与することは一切しない」とことと定義しています。これは、昔からある「決して信用せず、常に確認せよ」という言葉になぞらえたものです。

セキュリティ、アクセス、複雑性がクラウドに対するITリーダーの懸念事項の上位に挙がっていることから、これらのハードルを克服する手段としてゼロトラストに関心を持つ組織が増えているのは当然といえるでしょう。今回の調査回答から、こういった新しい運用環境において、従来

のアプローチに対するゼロトラストのセキュリティ上の優位性について、組織が基本的な理解を深めていることがわかりました。

従来型のネットワークとセキュリティのインフラに関する質問に対しては、ITリーダーの54%がVPNや境界ファイアウォール

はどちらもサイバー攻撃からの保護や、アプリケーションのトラフィックおよび攻撃の可視化には効果がないと回答しています。また68%は、アプリケーションへのリモート アクセスの保護に関しては、従来型のファイアウォールやVPNよりもゼロトラスト ネットワーク アクセス

(ZTNA)のほうが明らかに優れていることを認識する一方で、従来型のネットワーク セキュリティ インフラでは安全なクラウドトランスフォーメーションを実現できないと考えています。

ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange 国にマウス カーソルを
合わせて詳細を表示

従来型のネットワーク セキュリティ インフラでは安全なクラウド トランスフォーメーションは不可能であること、またアプリケーションへのリモート アクセスの保護に関しては、ゼロトラスト ネットワーク アクセスが従来型のファイアウォールやVPNよりも明らかに優れていることを認識している回答者の割合：

- 85% インド
- 81% 米国
- 75% ブラジル
- 75% シンガポール
- 73% スウェーデン

VPNや境界ファイアウォールはどちらもサイバー攻撃からの保護や、アプリケーションのトラフィックおよび攻撃の可視化には効果がないと考える回答者の割合：

- 72% インド
- 65% シンガポール
- 64% 日本
- 57% ドイツ
- 56% 米国

セキュリティに加えて、IT部門にはユーザー エクスペリエンスの問題を効果的に分析、トラブルシューティング、解決するための統合ツールが必要と考える回答者の割合：

- 70% インド
- 63% メキシコ
- 62% 米国
- 56% シンガポール
- 51% スペイン
- 50% 日本



ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange

90%

クラウドへの移行を開始した回答者の90%以上は、ゼロトラスト セキュリティ戦略をすでに実施済みか、今後12か月以内の実施に向けて取り組みを進めています。



このような状況への意識付け以上に、最も期待感が高まる要素としてはITリーダーがそれに応じて行動を起こしているという点があります。クラウドへの移行を開始した回答者の90%以上は、ゼロトラスト セキュリティ戦略をすでに実施済みか、今後12か月以内の実施に向けて取り組みを進めています。

ゼロトラスト セキュリティ戦略の実装においては、イタリアとインドが一歩先を行き、イタリアの組織の97%、インドの組織の96%がゼロトラスト セキュリティ戦略を導入しているか、導入中であると報告しています。

ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange 国にマウス カーソルを
合わせて詳細を表示

ゼロトラスト セキュリティを導入済
みの組織、現在展開中の組織、展開
するための戦略的な計画の段階に
ある組織の割合：

- 97% イタリア
- 96% インド
- 95% 英国
- 95% 米国
- 94% 日本
- 93% ブラジル
- 93% シンガポール
- 92% ドイツ
- 91% メキシコ
- 90% オランダ
- 89% スペイン
- 89% フランス
- 88% オーストラリア
- 85% スウェーデン



ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange

ゼロトラストは依然としてサイロ化したIT中心(セキュリティ)のソリューションとみなされていますが、ゼロトラストは組織にこれ以上のものを提供する可能性があります。

残念ながら、ゼロトラスト セキュリティ システムを導入したり、展開する計画を立てたとしても、ビジネス イネーブラーとしての可能性を最大限に発揮しているとは言い切れません。

事実、調査結果を見ると、ゼロトラストが依然としてサイロ化したIT中心(セキュリティ)のソリューションとみなされており、差し迫ったセキュリティの課題に対処しつつ戦術的なメリットも達成していますが、ゼロトラストは組織にこれ以上のものを提供する可能性があります。

ゼロトラスト アーキテクチャーを実装する主な理由:

65% 高度な脅威やWebアプリケーション攻撃の検出の改善と機密データの保護の強化

44% ベンダー、パートナー、運用技術のリモート アクセスの保護

27% ハイブリッド ワークの接続の安全性の改善

24% 従来型のネットワーク セキュリティのコストと複雑性の低減

ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange

世界中でゼロトラスト インフラが実装される主な理由:

 国にマウス カーソルを
合わせて詳細を表示

高度な脅威の検出を改善するため:

- 52% インド
- 42% シンガポール
- 41% 米国
- 39% イタリア
- 35% スペイン
- 30% フランス
- 26% 英国

Webアプリケーション攻撃の検出を改善するため:

- 44% ブラジル
- 35% メキシコ

機密データの保護を強化するため:

- 44% ブラジル

ベンダー、パートナー、請負業者に安全なリモート アクセスを提供するため:

- 33% オーストラリア
- 32% 日本
- 24% オランダ



ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange

ゼロトラストへのこういったアプローチは、変革の最初の段階でのみセキュリティのために使用するもので、スピードと拡張性において組織のデジタル化や革新能力に依存しているときはその可能性が大幅に制限されます。

ゼロトラストを単なる技術や製品としてではなく、適切に理解することで、インフラの簡素化、ビジネスのあり方の再考、完全にデジタル化されたビジネスへの転換が可能になります。例えば、ゼロトラストを実現した企業は、自社のすべてのアプリケーションと組織内のすべてに対して完全かつ正確なイ

ンベントリを作成できます。このインベントリに基づいて、プロセスの最適化、コスト削減、旧式のハードウェアの排除、効率化などに関する戦略的な意思決定が可能になります。

しかし、こういった戦略的なメリットを享受するには、ゼロトラストに関するメッセージが取締役会で受け入れられ、より広範な事業戦略の一部とみなされる必要があります。ゼロトラストが持つ意味やビジネスに与える影響はいまだ不確実な要素も多く、スキルギャップが存在している可能性があります。ゼロトラストの目標は最高レベルのセキュリティを維持

しながら、管理負荷の高いハードウェアを排除してインフラ全体を簡素化し、組織が求めるビジネス成果をより簡単に実現することです。これを、CIOを含む経営陣に理解してもらうことが当面の緊急課題といえます。

組織が今後12か月間の投資を優先しているゼロトラスト技術の状況を見ると、事業上のメリットに関するこの理解が広まっているという事実が見て取れますが、国や地域でそのペースは著しく異なり、改善の余地も十分残されています。

組織が投資している主なゼロトラスト技術：

30%

ゼロトラスト ネットワーク アクセス(ZTNA)

29%

クラウド ファイアウォール

27%

情報漏洩防止(DLP)

ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange

地域の視点：南北アメリカからの声

Amit Chaudhry、プロダクト マーケティング担当シニア ディレクター



現在、組織はクラウド、モビリティ、AI、IoT、OT技術を採用して、ビジネスの敏捷性や競争力を向上させようとしています。ユーザーはどこにでもいて、それはデータについても同じです。しかし当然のことながら、高速で生産性の高いコラボレーションのために、ユーザーはいつでもどこからでもアプリに直接アクセスしたいと考えています。

急速なペースで進むデジタル トランスフォーメーションは、悪意を持ったアク

ターに何十年も前から使われているネットワークとセキュリティ アーキテクチャーを悪用する機会を生み出していました。特にランサムウェアやサプライチェーン攻撃は以前とは比較にならないほど増加しています。そして、攻撃がより巧妙化するにつれて、VPNやファイアウォールを使用した境界ベースのセキュリティはネットワークを安全に保護できず、優れたユーザー エクスペリエンスを提供できなくなっています。

安全なハイブリッド ワークを実現するために、組織はファイアウォールやVPNから脱却し、場所や時間を問わずアプリケーションへの高速なダイレクト アクセスを保護するゼロトラスト アーキテクチャーに急速に移行し始めています。アイデンティティとコンテキストに基づいて接続が確立される最小特権アクセスの原則で構築されたゼロトラストは、データを保護するうえで最もシンプルかつ重要な考え方といえます。

A photograph of two men in a professional setting. The man on the left, who is Black, is wearing a blue denim shirt and looking towards the right. The man on the right, who is Asian, is wearing glasses and a dark sweater, pointing his right index finger towards the right side of the frame. The background is dark and out of focus. A large blue graphic with a white dot pattern is overlaid on the right side of the image, containing the main text.

ゼロトラストが持つ意味やビジネスに与える影響はいまだ不確実な要素も多く、スキルギャップが存在している可能性があります



ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange

セクションIII

ハイブリッド ワークを実現するゼロト ラストへの転換

ハイブリッド ワークのインフラとは、制限や複雑な管理を一切発生させずに、従業員が物理的な場所とリモート間で仕事環境をシームレスに切り替えられるインフラを指します。

最初のロックダウンが発生し、多くの組織が自宅勤務の準備に追われていたときは、この「一時的な措置」が新しい働き方への扉を開き、これまでの働き方が二度と元のようにには戻らないなどとは誰も予測していませんでした。

現在は自宅やオフィス、それ以外の場所

から勤務できるようになり、それを実現するための技術も準備できています。

回答者は自社の従業員がさまざまな選択肢を活用し、今後12か月間の働き方は完全なオフィス勤務(38%)、完全なリモート勤務(35%)、ハイブリッド(27%)に分かれると予測しており、この数字は世界中で比

較的一貫しています。

ITリーダーの3分の2近く(62%)は、自社がハイブリッド環境を活用している、またはリモートで作業するための柔軟性を十分に提供していると回答している一方で、3分の1以上(38%)がいずれ完全にオフィスに戻ると予測していることは驚くと同時

に、懸念すべき結果といえます。これは、対面でのやり取り(医療やサービス業など)が必須となる特定の業界にとっては十分理解できます。しかし、それ以外の業界の場合、ここ数年間で定着した柔軟な仕事環境を従業員に提供できなければ、人材の確保や維持に苦労する可能性があります。

ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange

19%

調査対象となった全世界のIT意思決定者の中で、ハイブリッドワークに特化したゼロトラストベースのインフラがすでに整備されていると回答したのはわずか19%でした。

今後12か月間に予想される完全なリモート勤務、完全なオフィス勤務、ハイブリッド勤務の従業員の割合：

38% 完全なオフィス勤務

35% 完全なリモート勤務

27% ハイブリッド

本来の意図は別として、ITとセキュリティのインフラが、このように進化する働き方の多様化に対処できるかどうかはまったく別の問題です。調査対象となった全世界のIT意思決定者の中で、ハイブリッドワークに特化したゼロトラストベースのインフラがすでに整備されていると回答したのはわずか19%にとどまり、高度に分散した仕事環境を大規模

に処理する準備が整っていないことが浮き彫りになりました。すでにインフラを更新した企業に続き、50%の企業がゼロトラストベースのハイブリッド戦略を実装中または計画中であることがわかりました。

また、ベンダー、パートナー、請負業者、工場や機器のオペレーターなど、性質上ハイブリッド環境で働く従業員に安全なリモートアクセス

を提供するためにゼロトラストを実装または計画している企業においては、ゼロトラストネットワークアクセスが今後12か月間の優先投資分野であることが明確に示されています。これは、ハイブリッドワークへの移行が進む中で、差し迫った課題に対応するための需要の高さを示唆しています。

ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange国にマウス カーソルを
合わせて詳細を表示

ゼロトラスト ベースのハイブリッド戦略
の実装が最優先事項となっている国：

- 37% インド
- 36% シンガポール
- 33% 日本
- 29% ドイツ
- 29% オランダ

依然として計画中の段階にある国：

- 34% メキシコ
- 27% 米国
- 27% フランス
- 25% スウェーデン

全体として、英国はゼロトラスト ベースのハイブリッド戦
略の採用に最も消極的であるとみられ、21%の組織が現
時点でハイブリッド インフラを実装する計画はなく、さら
に20%がこれまでのリモート アクセス技術を使い続け
ると回答しています。



ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange

当然ながら、ハイブリッド化が一層進む組織にとってセキュリティは最大の懸念事項です。

ハイブリッド ワークに移行する組織が最も懸念するセキュリティの課題：

54%

運用技術(OT)システムとインター
ネット アクセスの両方

53%

オンプレミスのプライベート アプリ、
またはクラウド内のプライベート ア
プリとワークロード(IaaS、PaaS)

32%

モノのインターネットとリモート アク
セス インターネットへのアクセス

しかし、今回の調査結果はハイブリッド
ワーク環境におけるセキュリティとは脅
威を防ぐだけでなく、従業員からサード
パーティーのサプライヤーやビジネス
パートナーまで、幅広いユーザーにインフ
ラへのアクセスを安全に提供することが
重要な課題であることが示されている点
に留意する必要があります。

さらに、セキュリティに対してはすでに当
然の期待がされている中で、ゼロトラスト
ベースのハイブリッド ワーク インフラを
実装または計画している企業ならではの
採用理由も加わり、従業員のエクスペリ
エンスや生産性に影響をもたらすゼロト
ラスト ソリューションがより広範にビジネ
スへの影響を与えることがわかってきて
います。

ゼロトラストベースのハイブリッド ワーク インフラを実装する、または実装を計画する理由：

52%

従業員がオンプレミスとクラウド ベースのアプリケーショ
ンやデータにアクセスする際に、一貫性のないエクスペリ
エンスが発生している

46%

ネットワーク アクセスが原因で従業員の生産性が低下し
ている

39%

従業員個人のデバイスからアプリケーションやデータにア
クセスできない

ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange 国にマウス カーソルを
合わせて詳細を表示

一貫性のないアクセス エクスペリエンスが
多く発生すると報告した国：

- 70% 日本
- 68% インド
- 64% 米国
- 62% シンガポール

ヨーロッパでは、一貫性のないエクスペリエンス
を課題と考えているのは調査対象となった組織
の約半数にとどまる：

- 52% スウェーデン
- 49% オランダ
- 47% フランス
- 45% ドイツ

ネットワーク アクセスに起因する生産性の低
下が新しいインフラに変更した主な理由とし
て挙げた国：

- 55% メキシコ
- 48% スペイン
- 47% 英国



ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウ
ドの実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange

従来型のVPNベースのハイブリッド ワーク インフラを使用していると回答した企業は、より根本的なリモート ワークの問題に今も取り組んでいると報告しています。

ハイブリッド ワーク環境で生産性を維持するにはユーザー エクスペリエンスが極めて重要 — これは昨年度の学びの1つです。また、当社の調査結果によれば、現在までエクスペリエンス問題に対処するための自社インフラの現代化に関しては、対応スピードは地域ごとに異なっています。

より一層分散化が進む現代の企業環境で最適なユーザー エクスペリエンスを実現するには、ユーザー トラフィックを可能な限り最短のルートを経由してアプリケーションに誘導して、レイ

テンシーと輻輳を回避する必要があります。現代のハイブリッド ワーカーは、自宅、オフィス、外出先などからでも最適な帯域幅で必要なアプリケーションに動的にアクセスするため、その流動性の考慮が企業に求められます。エクスペリエンス以外でも、従業員が業務上不可欠なアプリケーションへのアクセスのパフォーマンスに満足しない場合、セキュリティ制御を回避する方法を模索することもあり、マイナスの影響が発生する可能性がさらに高まります。

それに対し、従来型のVPNベースのハイブリッド ワーク インフラを使用していると回答した企業は、より根本的なリモート ワークの問題に引き続き取り組んでいると報告しています。この問題には、オンプレミスとリモートの従業員で異なるセキュリティ インフラの管理が複雑である(47%)、従業員がアプリケーションのパフォーマンス低下を経験している(39%)、IT部門がリモートユーザー向けのユーザー エクスペリエンスのモニタリングとトラブルシューティングを簡単にできない(37%)が挙げられます。

ハイブリッド ワークへの移行は多くのセキュリティ上の懸念を残しますが、今回得られた回答をみると、ハイブリッド形式での業務というものがアクセス、エクスペリエンス、パフォーマンスにわたる大きな課題を組織にもたらすことがわかります。

ゼロトラストが正しく理解されれば、こういったすべての課題に答えを出すことができます。そして、IT部門が変わり続ける期待値やビジネス要件への対応に集中できるように簡素化することも可能です。

ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange

地域の視点：アジア太平洋からの声

Heng Mok、APJ CISO



アジア太平洋(APAC)地域は、「1つのシステムがすべてに対応できるわけではない」ことを示す良い例です。文化やライフスタイルが混じり合ったこの地域では、市場ごとに仕事へのアプローチが異なります。パンデミック以前から、日本やシンガポールではより階層的な構造に従っている一方で、オーストラリアやインドの労働スタイルはよりリラックスしたものという大きな違いが見られていました。

アジア太平洋地域には、世界で最も厳格にロックダウンされた都市が含まれており、こういった違いはロックダウンから解放されるにつれてむしろより顕著になっています。調査回答者のうち、日本とシンガポールのIT意思決定者の過半数は、従業員が完全にオフィス勤務になると予測しており、完全にリモートになると予想しているオーストラリアとインドとは著しく対照的です。

ただし、長期的には今より多くの組織がハイブリッド ワーク モデルを倍増させていくと予測しています。私が話を聞いた多くの組織では、人材を確保するという目には見えないメリットのためにハイブリッドワークのスタイルを選択しています。限られた人材をめぐって競争が激化する中、多くの企業が同様のポリシーを取り入れつつ、この移行をよりシームレスにサポートするためのテクノロジー スタックを検討していることは至極当然のことといえるかもしれません。



ハイブリッド ワーク環境で生産性を
維持するにはユーザー エクスペリエ
ンスが極めて重要 — これは昨年度
の学びの1つです

ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange

セクションIV

新興技術を統合するためのゼロトラスト アプローチの採用

新興技術とは、まだほとんど実用化は実現していないものの、ビジネスに大きな影響を及ぼして競争上の優位性を促進することが期待される新しい技術または急速に発展している技術を指します。

当然ながら、組織が求めている技術はリモートワークを可能にするデジタルソリューションだけではありません。現代のデジタル社会では、運用技術の果たす役割はますます大きくなっています。この分野のビジネスモデルは、歴史的に従来型のシステムとプロセスに大きく依存してきましたが、ビジネスプロセスのさらなる簡素化と自動化を目的として、独自の可能性を備えた新しい新興技術に向けて根本的な

変革が行われると予測されます。

しかし、組織としては今後のさらなる技術的進歩も考慮に入れて、将来を見据えてインフラを決定する必要があります。ITの意思決定者は、イノベーションに基づくビジネスのさまざまな方向性を把握し、新興技術がいかに効果的にビジネス機能をサポートできるかについて、オープンな姿勢で臨む必要があります。ゼロトラストはその際にパズルの最後のピースになる可能性

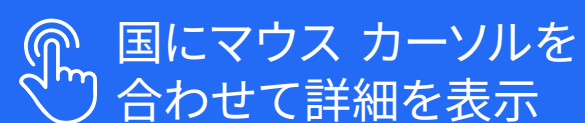
があり、現在、企業を強力にサポートしつつ将来的に登場する技術への準備という面でも役立ちます。

クラウド移行やデジタルトランスフォーメーションの一般的な動機と同様に、より幅広い戦略的成果に焦点を当てることが、組織が新興技術プロジェクトを計画する際に欠けていることが今回の結果で明らかになりました。

新興技術プロジェクトの実施で最も大きな課題となるのは何かという質問に対しては、30%が十分なセキュリティと回答し、さらなるデジタル化のための予算要件(23%)がそれに続きました。しかし、戦略的なビジネスの意思決定への依存を課題として挙げたのはわずか19%にとどまりました。

ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange

新興技術プロジェクトの実施における最も大きな課題(地域別)

国にマウス カーソルを
合わせて詳細を表示

セキュリティ上の懸念が最大の課題となっている国:

- 54% ブラジル
- 41% 日本
- 37% インド
- 37% イタリア
- 35% スペイン
- 31% 米国

主に予算関連の要件が課題となっている国:

- 27% シンガポール
- 27% フランス
- 23% 英国

組織と新興技術の間に立ちはだかる壁がビジョンの欠如と考えている国:

- 24% オランダ

ほとんどの企業が戦略的なビジネス上の意思決定への依存を最大の障害として挙げた唯一の国:

- 28% スウェーデン





ゼロトラスト
の現状

ゼロトラスト
採用の背景
にあるクラウド
の実態

真のゼロトラ
ストの理解

新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用

ゼロトラストの
可能性を最大
限に引き出すた
めの取り組み

およびZscaler Zero
Trust Exchange

予算上の懸念は予測可能ですが、戦略的なビジネスの整合性を考慮しないままネットワークのセキュリティ確保に注力するというのは一筋縄ではいきません。多くの組織はセキュリティがもたらすビジネス上のメリットを十分に理解せずに、セキュリティに焦点を当てていますが、これはゼロトラストが依然としてビジネス イネーブラーとして理解されていないことを証明しています。

拡張現実、デジタル ツイン、仮想建設などの新興技術のユース ケースを計画する組織にとっては、低レイテンシーで高性能なアプリケーション アクセスも懸念事項になります。特に南北アメリカでは今後3年間の新興技術への関心も高く、その傾向は顕著です。

今後3年間における低レイテンシーで高性能なアプリケーション アクセスの重要性



2025年までに最優先となる技術	世界全体	ヨーロッパ	南北アメリカ	アジア太平洋
運用技術や産業用制御システムへのクラウド ベースのアクセス	34%	29%	40%	38%
接続を強化するための5G技術の実装	32%	29%	39%	32%
事業のカーボン フットプリントの削減	29%	28%	28%	30%
人工知能/機械学習プロジェクトの実装	27%	22%	39%	28%

ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange 国にマウス カーソルを
合わせて詳細を表示

運用技術や産業用制御システムへのクラウドベースのアクセスに着目している組織：

- 46% メキシコ
- 45% インド
- 44% シンガポール
- 36% オーストラリア
- 33% フランス

5G技術の実装を優先する組織：

- 47% ブラジル
- 45% インド
- 41% イタリア
- 36% スペイン
- 28% 英国

カーボン フットプリントの削減が最優先事項と考える組織：

- 41% イタリア
- 28% ドイツ
- 32% スウェーデン

エッジ コンピューティングの拡大を最も重要視しているのはオランダの組織のみで(29%)、アメリカの組織はAIおよびMLプロジェクトの実装に力を入れています(43%)。



ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange

私たちは、こういった優先順位をつけた新興技術がより大きなビジネス成果につながる可能性があることを認識していますが、今回の調査結果は依然として組織内に広い視野が欠けていることを示唆しています。組織を保護する方法だけでなく、新興技術やその戦略的展開から得られる競争上の優位性について、社内全体で認識をすり合わせる必要があります。



地域の視点: EMEAからの声

Nathan Howe、新興技術担当主任

ヨーロッパの組織が新技術や新興技術への適応における先駆者となる可能性は低いとみられます。ヨーロッパは機械の発明において産業革命の発祥地となりましたが、デジタル技術の採用に関してはこの地域は以前から大幅な後れをとっています。APJはチップ製造に関する技術の中心となっており、イノベーションを起こす知識を持った才能が世界各地からSilicon Valleyに集まり、変革的技術の開発が進んでいます。

このような背景を考えると、アジアが5Gの力を認識してデジタル化の基盤としてワイヤレスを超えた次世代の接続手段に移行していることは驚くべきことではありません。南北アメリカはその中間あたりに位置しますが、ヨーロッパはデジタル化の取り組みの一環として5Gにシフトする方法がいまだに不鮮明です。しかし、チップ不足やサプライチェーン問題などの地政学的傾向の変化により、各国がこの地域にオンショア拠点を設立する必要があるため、ヨーロッパは今後デジタル クラウドと新興技術において劇的に成長していく可能性があります。

ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange

セクションV

ゼロトラストの可能性を最大限に引き出すための取り組み

今回の調査結果をもとに、組織はどのようにゼロトラストに取り組むべきなのでしょう。

従来型のネットワークとセキュリティのアーキテクチャーがもたらす課題は広範囲かつ長期間にわたるため、現代社会で接続を確立する方法を改めて考える必要があります。そこで活用できるのが、いかなるユーザーやアプリケーションも信頼しない構造となっているゼロトラスト アーキテクチャーです。最小特権アクセスに基づくゼロトラストでは、アイデンティティとコンテキストが認証され、ポリシー チェックが実施された場合にのみ信頼が与えられます。

このアプローチではすべてのネットワーク通信を敵対的なものとみなし、アイデンティティベースのポリシーによって検証されるまで、ユーザーとワークロード間、ワークロード間の通信をブロックします。これにより、不適切なアクセスや水平移動を確実に防止できます。この検証はあらゆるネットワーク環境に適用されるため、ネットワークでのエンティティの場所は関係なくなり、厳密なネットワークセグメンテーションには依存しません。

ゼロトラストは、ネットワークを保護する新しい手段として始まりました。最終的に、ゼロトラストはオンプレミス ネットワークを超えて拡張されましたが、それでも主に

プライベート アプリケーションのトラフィックの保護に重点を置いていました。あまりにも長い間、トラフィックはネットワークと合わせて完全に排除するのではなく、ネットワークとの関係に基づいて考慮されていましたが、現在、組織はSaaSアプリケーション、パブリック クラウドとの間のトラフィック、さらにはパブリック インターネットにアクセスするユーザーを保護するために、ゼロトラストの最大の可能性に着目しています。そして、トラフィックの送信元はユーザーだけでなくワークロードである場合もあります。転送手段に依存しないアクセスを可能にし、ルーター、有線または無線、4Gまたは5G、そして将来的に拡張される任意のネットワーク経由でトラフィックが送受信されます。

送信元や送信先に関わらず、すべてのトラフィックにゼロトラストの原則を適用すべきときが来ているのです。そして、どのエンティティがどのネットワークに接続するかという考えから脱却し、ゼロトラストを採用してビジネス ポリシーですべてのエンティティを直接接続するアプローチにシフトしていく必要があります。クラウド時代が到来した今、インターネットが新しい企業ネットワークとなりつつあります。すべてのトラフィックにビジネス ポリシーを使用して、正しいエンティティ同士を直接接続させることが重要です。

ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange

今日のマクロ経済環境だけでなく、新興技術の要件に対応できる安全性、俊敏性、柔軟性、効率性を備えた企業になるには、何から始めればいいのでしょうか。重要な推奨事項として以下の3つが挙げられます。

1

ゼロトラストを安全なデジタル トランスフォーメーションの必須の要素、そして事業成果へと導く推進力と捉えて、ゼロトラストに対する理解を見直す必要がある

可視性と制御が向上したゼロトラストベースのアーキテクチャーにより、現代のITの複雑性が解消され、組織はパフォーマンスやユーザー エクスペリエンスの強化からコストの削減に至るまで、テクノロジーから必要となる成果を得ることに集中できます。

では、ゼロトラストが真のビジネス イネーブラーであるという認識に考え方が変わったら、組織はどのようにゼロトラスト アーキテクチャーを活用して事業成果を達成すればいいのでしょうか。

2

ゼロトラストが持つ意味やビジネスに及ぼす影響について、恐怖心、不確実性、疑念を払拭するためのさらなる教育が必要である

CIOやCISOはゼロトラストを広い視野で捉えて取締役会で説明し、ビジネス戦略との整合性に焦点を当てるといった重要な役割を担っています。

3

新興技術は競争力の高いビジネスの優位性と考えられるもので、現時点でゼロトラストに対応しているインフラは将来への基盤となる

新興技術の採用を決定する際は、トレンドや流行に左右されるのではなく、全体的なビジネスのビジョンと組織の現在および将来のニーズによって推進される必要があります。ゼロトラストは新たなトレンドに求められる安全でパフォーマンスの高い接続をサポートするために存在します。

ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解ハイブリッド
ワークを実現
するゼロトラ
ストへの転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange

Zscalerは、Zero Trust Exchangeの中核となるアーキテクチャーのコンポーネントとしてゼロトラストを実装し、SSEフレームワークのあらゆる要素に組み込んでいます。これには、内部または外部のすべてのアプリケーションにアクセスするユーザー、IoT/OT接続、マルチクラウド環境やインターネット自体のリソースにアクセスするワークロードに対するゼロトラスト アプローチが含まれます。ゼロトラストの原則により、事業戦略としてどこからでも安全なハイブリッド ワークが可能になり、従業員、ビジネスパートナー、顧客がそれぞれの生産性に最適な場所から作業できるようになります。これは、事業継続、遠隔地からの人材獲得、ますます普及するハイブリッドワーク環境の実現に必要な要件です。

Zscaler Zero Trust Exchange は、場所、デバイス、ネットワークを問わず、従業員、パートナー、顧客に外部および内部アプリケーションへの高速、直接、安全なアクセスを提供するクラウドネイティブなサービスです。

ゼロトラスト アーキテクチャーには7つの重要な要素があり、これらの要素は次の3つのカテゴリーに分類されます。



検証

ゼロトラスト アーキテクチャーは最初に接続を終了して確立します。

1. 接続元の確認
2. アクセス コンテキストの検証
3. 接続先の確認



制御

ゼロトラスト アーキテクチャーは次に以下を実行します。

4. リスクの評価
5. 侵害の防止
6. 情報漏洩の阻止



施行

最終的に接続を確立する前に、ゼロトラスト アーキテクチャーは以下を実行します。

7. ポリシーの施行

これらの要素を念頭に置くことが、クラウド ファーストの組織がデジタル トランスフォーメーションを加速させ、どんな未来にも対応できる組織に進化するための基盤となるのです。

ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態ハイブリッド
ワークを実現
するゼロトラスト
への転換新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange

ZscalerとZscaler Zero Trust Exchangeについて

Zscalerは、使いやすく成熟度の高い、世界最大規模のゼロトラスト プラットフォームを備えたゼロトラストのリーダーとして世界的に認められています。

当社のクラウド ネイティブ プラットフォームであるZscaler Zero Trust Exchangeは、ゼロトラストへの取り組みに最適なソリューションです。従来のネットワークやセキュリティ製品とは異なり、専用のクラウド プラットフォームであるZero Trust Exchangeは、接続を毎回終了することで、コンテンツを詳細に検査し、アイデンティティとコンテキストに基づいてアクセス権を検証します。

全世界150拠点のデータ センターで稼働するZero Trust Exchangeは、Microsoft 365やAWSなどのクラウド プロバイダーやアプリケーションと併置されており、ユーザーに近い場所でサービスを提供します。これにより、ユーザーと接続先の経路を最短にし、包括的なセキュリティと優れたユーザー エクスペリエンスを提供します。

Zscalerプラットフォームの詳細については、[こちら](#)をご覧ください。

Zero Trust Exchangeは世界 150拠点のデータ センターで稼働し ています



ゼロトラスト
の現状ゼロトラスト
採用の背景
にあるクラウド
の実態真のゼロトラ
ストの理解新興技術を統
合するためのゼ
ロトラスト アプ
ローチの採用ゼロトラストの
可能性を最大
限に引き出すた
めの取り組みおよびZscaler Zero
Trust Exchange

調査方法

ATOMIK Researchは、EMEA(英国、ドイツ、フランス、オランダ、スウェーデン、イタリア、スペイン)、AMS(米国、メキシコ、ブラジル)、APAC(日本、インド、オーストラリア、シンガポール)の1,908人の上位の意思決定者(CIO/CISSO/CDO /ネットワーク アーキテクチャー責任者)を調査しました。調査は2022年5月31日から6月28日の間に実施され、組織規模の内訳は、従業員4,999人以下の組織が43%、従業員5,000人以上9,999人以下の組織が32%、従業員10,000人以上の組織が25%となっています。