CISCO
SECURE

シスコ発行：ゼロトラスト成熟度ガイド

すばやく成果を上げる秘訣

cisco SECURE

目次

I. エグゼクティブサマリー

ゼロトラストは、流行語から国際的な使命へと進化しました。米国、英国、オーストラリアなどの政府機関はすべて「信頼を前提とせず、常に検証する」という立場に沿った要求事項を表明しています。

ゼロトラストを採用するビジネスリーダーは、担当部門のセキュリティレジリエンスの実現に向けて着実に前進しています。実際、ハイブリッドワークを実現し、セキュリティチームのパフォーマンスを最適化することで、シスコのお客様はデータ侵害のリスクとコストの半減に成功しているほか、他の企業も 191% の ROI を達成できているのです。

ゼロトラストは SOC チームの効率を高め、対応を強化できます。たとえばシスコのお客様は、SOC 効率を 90% 向上させてきました。つまり、ゼロトラストが価値あるイニシアチブであることは明らかです。

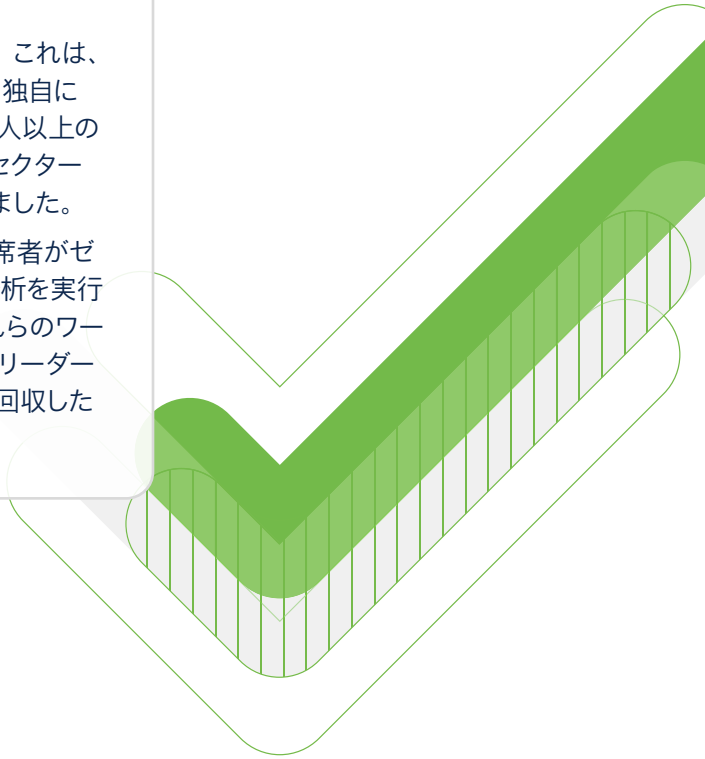
とはいえ、重要なビジネス上のメリットと整合性が保てる方法でゼロトラストの原則を導入する方法については、依然として混乱が存在しています。それでもシスコを含む多くの企業は、実質的なメリットを証とするゼロトラストセキュリティの採用に向けて、目に見える進歩を遂げています。

では、これらの部門の違いは何でしょうか？成功の秘訣はどこにあるのでしょうか？

本ガイドで使用するデータについて

『シスコセキュリティ成果調査、第 2 巻』の調査結果を使用しました。これは、特定のセキュリティプラクティスがこれほど成功している理由について独自に検証されたレポートです。この調査では、27 ヵ国で活躍する 5,000 人以上の IT、セキュリティ、プライバシーの専門家を対象に、さまざまな業界セクターにまたがって、何がセキュリティ機能と成果を改善できるかを調査しました。

また、シスコは定期的な ゼロトラストワークショップを開催して、出席者がゼロトラストの採用過程を理解し、実践的な活動に参加し、ギャップ分析を実行し、アクションプランを作成できるようにしています。これまでに、これらのワークショップに登録したのは、実務者に加えて IT およびセキュリティのリーダーも約 3,000 人います。このガイドでは、これらのワークショップから回収したアンケートの回答を取り上げています。



シスコは、『シスコセキュリティ成果調査、第 2 巻』を提供したチームによって収集および分析されたフィールドデータに加えて、過去 1 年間に開催した数多くの Zero Trust ワークショップの参加者からの回答を活用しました。

図 1 : ゼロトラストの採用に関する回答者の進捗状況

収集したデータから得られた知見の一部は ゼロトラストを追求する チームに以下のインサイトを提供しています。

- **ゼロトラストは、組織の規模や IT インフラストラクチャの複雑さを問わず導入可能である :** IT 環境が複雑でも単純でも、あらゆる規模の組織がゼロトラストセキュリティに向けて目に見える進歩を遂げられることがわかりました。
- ゼロトラストの導入が成熟段階にあると報告した組織は、**導入**が制限されている組織よりも、**ビジネスレジリエンス**（63.6%）を達成する可能性が 2 倍以上高い。
- ゼロトラストの導入が成熟段階に達した組織は、次の **5 つのセキュリティプラクティスに優れている**と報告する割合が **2 倍**に到達。
  - 正確な脅威検出
  - プロアクティブなテクノロジーの更新
  - 迅速なディザスタリカバリ
  - タイムリーなインシデント対応
  - テクノロジーの十分な統合
- ゼロトラストの導入が成熟段階にあるとした組織は、**経営陣からの信頼の向上**（47%）、**同僚の賛同**（45%）、**最新のビジネスへの対応**（46%）、**セキュリティの文化を作る**、といった望ましい結果について、他社より秀でていると回答した割合が **2 倍**に到達。
- **最新の IT インフラストラクチャ**を備えた組織では、ゼロトラストの導入が成熟段階にある可能性が **2 倍以上**に向上。
- **統合はゼロトラストの成熟を促進する :** 統合を選択した組織内でさえ、**優先ベンダーから統合テクノロジー**を調達するプラットフォームアプローチを採用している組織は **51%** であり、これに対して、すぐに使用できる統合を利用している組織は **28.8%** でした。
- ゼロトラスト導入が成熟段階にある組織は、ゼロトラスト セキュリティ モデルが実行できるアクションを改善するために、**自動化**（64.4%）を活用。

ゼロトラストの成熟度に関するこのガイドは、ゼロトラストに関する現状を把握し、すばやく成果を上げ、勢いをつけ、ゼロトラストのセキュリティに向けて前進し続けるための一助となるように執筆されています。

II. 概要

ゼロトラストの発展はこれからも続きます。しかし、導入の道はなぜこれほど険しいのでしょうか？そして、困難の塊のように思えるこのタスクに対して、チームはどこから勢いを得ているのでしょうか？

ゼロトラストの導入で一部のチームは抜き出ていますが、彼らの秘訣はどこにあるのでしょうか？導入の道半ばにいる組織が得られる教訓は何でしょうか？

具体的な考慮点：

1. 成功したチームは、セキュリティの成果をどのように達成しているか。また成功率はどれぐらいか。
2. ゼロトラストのベンダーとプロバイダーを選択する際に、彼らは何を優先しているか。
3. ゼロトラストを展開するための統合および自動化戦略は何か。
4. 準拠しているゼロトラスト基準は何か。
5. セキュリティプロセスはどの程度自動化されているか。

III. ゼロトラストとは？

ゼロトラストは、組織の環境から**信頼を排除するという**コンセプトに重点を置いた、セキュリティに対する**戦略的なアプローチ**です。

信頼とは、『できる』『できない』と断定できるものでも、永続するものでもありません。内部エンティティが信頼できることを前提に、それらを直接管理することでセキュリティリスクを軽減できる、または一度確認するだけで十分である、などと想定することは、もはやできないのです。

ゼロトラスト セキュリティ モデルでは、アクセス試行が発生するたびに、その試行がどこから行われたかに関わらず、**信頼する根拠**を必ず確認するよう求められます。

ゼロトラスト戦略では、すべての企業リソースへのすべての接続要求に対して、「信頼を前提とせず、常に検証し、適用する特権アクセスは最小限にとどめる」ポリシーを展開します。アプリケーション、デバイス、およびネットワーク全体でアクセスを許可する前に、常に信頼を確認することで、実際に情報を必要とする人だけがアクセスできるようにします。

この決定を下して適用するのが、ポリシー決定ポイント（PDP）とポリシー適用ポイント（PEP）です。実際、PDP/PEP は差別化されたアーキテクチャの特徴であると言えます。これらのコンポーネントは、ゼロトラストの原則を適用し、接続時に監視可能な内容に基づいて信頼境界を拡張または取り消します。

ゼロトラストとは ...

- 1 つの製品またはテクノロジーではなく、セキュリティフレームワークです。
- 「購入」または「販売」するものではなく、フレームワーク内にソリューションを位置付ける機会です。
- 一度限りのプロジェクトではなく、より優れたセキュリティを実現するための継続的な取り組みです。

ビジネスの動きが速すぎてセキュリティが入り込む余地がないというのは、単純な真実です。また、セキュリティの革新が行われていることを考慮しても、リスクの影響はかつてないほど大きくなっています。1 件のサイバー セキュリティ インシデントが組織の将来を大きく左右しかねないケースも往々にしてあります。

シスコが考えるゼロトラストセキュリティ戦略とは、ユーザーではなく攻撃者を苛立たせる方法でアクセスを保護することです。

A. 今すぐ導入すべき理由

ゼロトラストは新しい概念ではありません。しかし、今日の採用の増加は、急速に変化する現実を反映しています。かつては企業データへのアクセスを保護するためにあった境界はもはや存在しません。現在、企業は、サプライヤー、パートナー、顧客の統合されたエコシステムとして運営されているからです。これらが結びついていることにより、攻撃対象領域が拡大し、リスクと複雑さが増し、攻撃からの回復がより困難になります。

サイバー攻撃が収益に与える影響を踏まえ、ビジネスリーダーの間では、エンドツーエンドのセキュリティを導入する新しい方法を検討する準備が整っています。そこでは（システムの変更が生産性や運用に影響を与えないことを前提として）ゼロトラストアクセスの原則が道案内の役割を果たします。

利害関係が非常に大きく、壊滅的な影響を受ける可能性もあるため、変革をもたらす変化は今や歓迎されるようになりました。このため、ゼロトラストのセキュリティ原則は広く受け入れられています。

ゼロトラストは、IT インフラストラクチャの複雑さを問わず導入できます。シンプルな IT 環境から複雑な IT 環境まで、組織は成果を向上させながらゼロトラストに向けて前進することができるのです。

ゼロトラストと IT インフラストラクチャ

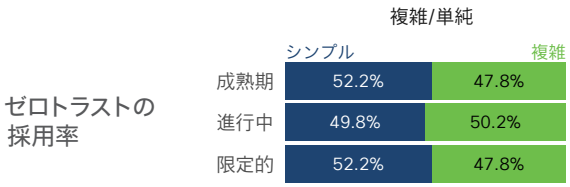


図 2：インフラがシンプルな組織と複雑な組織の間で比べた、ゼロトラストの採用率

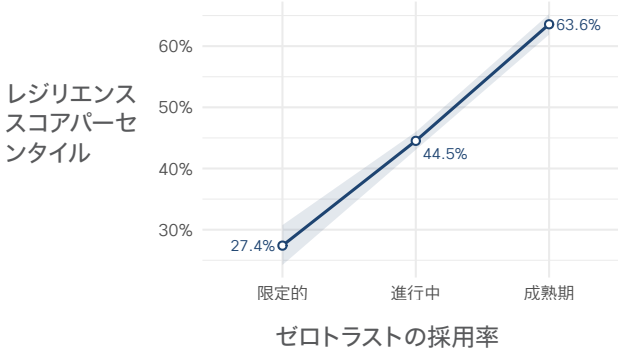
ゼロトラストは、ビジネスレジリエンスを高めることができます。ゼロトラストは単なるマーケティング上の流行語のように思えるかもしれませんが、実際には、ゼロトラストアーキテクチャに移行することで、組織全体を保護し、ビジネスパフォーマンスを向上させ、脅威への対応を促進できます。

ゼロトラストの導入が成熟段階にある組織は、導入が制限されている組織と比べて、ビジネスレジリエンスを達成する可能性が 2 倍以上高いことが判明しています。

回復力に特に関連する 12 のセキュリティ結果のうち 4 つを使用して「回復力スコア」を作成しました。

- 最新のビジネスへの対応（セキュリティは、ビジネスを妨げるものではなく支援するものである）
- 重大なインシデントの回避（およびそれに伴うビジネスへの影響の回避）
- 事業継続の維持（災害時も運営する）
- 優秀な人材の確保（競争はまず人材から）

レジリエンスのスコアが高いほど、これらの点で成功率が高くなります。



課題は、生産性と俊敏性への悪影響や、ビジネスレジリエンスの低下を恐れて、組織がどこからゼロトラストを始めればよいかを理解していないことです。

しかし重要なのは、まず一歩を踏み出し、正しい手順に注力して進めていくことです。ゼロトラストの成熟した導入と、『シスコセキュリティ成果調査、第 2 巻』でセキュリティプログラムの成功の「トップ 5」ドライバーとして言及されている 5 つのセキュリティプラクティスとの間に明確な相関関係があることが判明しています。

- 正確な脅威検出
- プロアクティブなテクノロジーの更新
- 迅速なディザスタリカバリ
- タイムリーなインシデント対応
- テクノロジーの十分な統合

ゼロトラストの導入が成熟段階に達した組織は、これらの 5 つのセキュリティプラクティスで優れていると報告する割合が 2 倍になりました。

着実に実践している回答者の割合

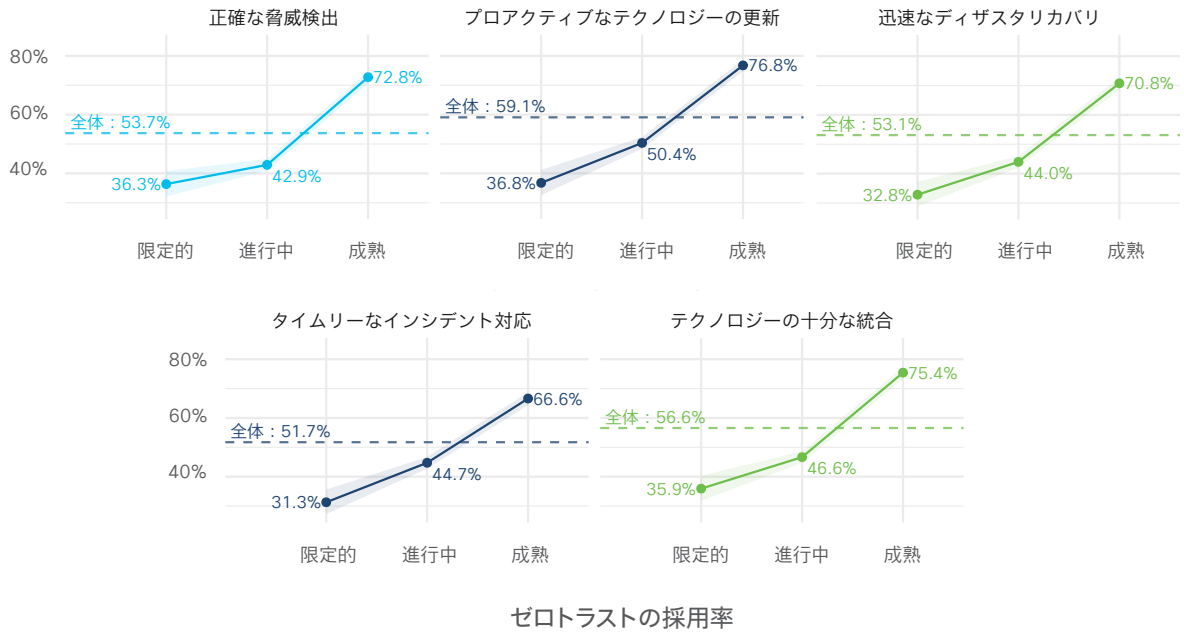


図 3：ゼロトラストの採用レベルとセキュリティプラクティス

プロからのヒント：ゼロトラストが 200 億ドルの市場シェア（しかも拡大中）を占めている現在[1]、世界のどこでも対応でき、ゼロトラストという分野全体を統合することが可能であり、かつ自社の採用過程で進歩を遂げたパートナーを慎重に選ぶことが重要です。

[1] Grandview Research 社によると、世界のゼロトラストセキュリティ市場規模は 2020 年には 198 億米ドルに達しており、2021 年から 2028 年にかけての複合年間成長率（CAGR）は 15.2% になると予想されています。
https://www.grandviewresearch. com/industry-analysis/zero-trust-security-market-report

IV. 成功の秘訣

A. 文化から始める

ゼロトラストの導入を成功させる主な要因は、トップからの賛同、同僚からのサポート、およびセキュリティ文化を確立する能力です。賛同と予算が不足している場合や、セキュリティプログラムが社内の文化に反している場合、セキュリティチームは苦労します。

> 文化による反動作用ほど迅速にイニシアチブを止めるものはありません。

シスコのケーススタディからわかるように、これらの要因はすべて、トップダウンのリーダーシップにより組織全体に存在していました。『シスコセキュリティ成果調査』もこれを裏付けており、成熟段階にある導入では**より高い経営陣の信頼**（47%）と**同僚の賛同**（45%）が報告されています。また、**最新のビジネスに対応すること**（46%）と**セキュリティ文化を作ること**（48%）にも、一致する傾向が見られます。実際、ゼロトラストの導入が成熟していると主張する**組織は、これらの分野で優れていると報告する割合が 2 倍になりました。**

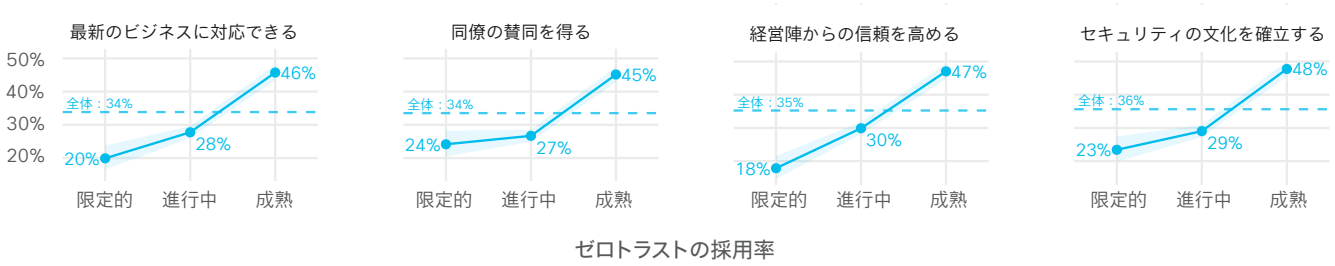


図 3：望ましい結果と、ゼロトラストの採用レベルの相関

人脈によって組織の変化を促進する：ホワイトボードで計画を書き出す前や、コンソールを開いてポリシーを構成する前に、セキュリティチームと経営陣との関係を強化することから始めてください。これには、IT、ネットワーキング、アーキテクチャ、プロジェクト管理、および監査の各部門における担当者を巻き込むことを意味します。これらの関係により、ゼロトラストプログラムをより迅速に成熟させることができるため、変革の重要な要素である成功度を向上できます。

変化を組織の上部から始める：良いサポートがあれば、より明確な道が開けます。CEO がゼロトラストをイニシアチブにするよう求めている場合や、顧客がサプライチェーン管理の一環としてゼロトラストを要求している場合は、ゼロトラストイニシアチブをいかにビジネスに結び付けるかが問題となります。そのような場合は逆手に利用し、勢いを使ってプログラムを前進させましょう。

信頼の文化を構築する：テクノロジーについて話したり、ゼロトラストのビジネスケースを作成したりする前に、セキュリティリーダーは、まず同僚や経営幹部の賛同を得て、信頼と信用を構築する必要があります。組織の文化に合った方法で話し合いを促進していく必要もあります。

人間関係の強化に目を向ける：ゼロトラストを設計して導入する際は、人間関係を強化する方法を特定します。ワークフローを計画し、ポリシーエンジンを導入し、組織にとってゼロトラストが何を意味するかについて話し合い、脅威を防ぎながらビジネスを躍進させることに焦点を当てる。これらすべてのステップが関係を強化します。

ケーススタディとデータから明らかなように、各ステップはいずれもゼロトラストの導入を成功させるための重要な要素です。

B. 推進力の高いビジネスケースを作成する

シスコでは、社内のゼロトラストワークショップや社外の広範な市場において、ゼロトラスイニシアチブの明確な傾向を見てきました。

初期のゼロトラストプロジェクト = パイロットプログラム：つまりセキュリティリーダーにとって、何が機能し、何が機能しなかったかを確認する試行錯誤の場だったのです。これらの初期のパイロットプログラムは、組織が何をできるかを知るきっかけになりました 2018 年から 2020 年にかけては、経営陣からの通達や顧客からの要求、または最新化のニーズのために、多くのゼロトラストイニシアチブが発動しました。

ビジネスの成果に向けてシフトする：最近では、ゼロトラストに限定したビジネスケースを回避する傾向が強まっています。ゼロトラストの原則を適用しながらビジネスニーズを満たすビジネスケースへと、明確に移行しているのです。ビジネスニーズの例としては、リモートファーストの従業員、デジタルファーストの顧客ベース、デジタル トランスフォーメーション、クラウドへの移行、IT の最新化などがあります。ゼロトラストプログラムを成功させるには、組織を改善すると同時にセキュリティを強化する機会が必要です。

ユーザー体験を優先させる：ビジネスケースにおけるゼロトラストで今中心的な要素にあるのがユーザー体験です。これがゼロトラストの「信頼」コンポーネントです。成熟したプログラムは、日常業務で従業員にセキュリティを意識させないようにすることで、ユーザー体験を向上させます。セキュリティ制御は、信頼できない接続や敵対行為の可能性がある場合など、実際のリスクがある場合にのみ介入する必要があります。

セキュリティの効率を改善させる:ビジネスケースに関するもう 1 つの考慮事項は管理性です**『セキュリティ成果調査』によると、ゼロトラストの導入が成熟段階にある組織は、計画外の作業を最小限に抑え (43%)、コスト効率よく実行している (47%) と報告しています。**シスコ ゼロトラスト ワークショップの参加者の間では、ツールの統合を必ず目標として挙げるなど、可視性の向上に次ぐ最優先事項になっています。成功している組織は、組織を保護する能力を高めながら、セキュリティを維持するためのワークロードを削減しています。

簡単に言えば、ゼロトラストのビジネスケースの原動力は、ユーザーではなく攻撃者を苛立たせることです。

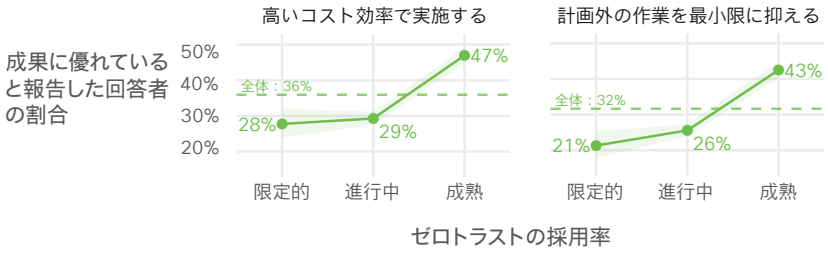


図 6：ゼロトラストセキュリティの費用対効果

攻撃対象領域を縮小する：これは、ゼロトラストの「ゼロ」コンポーネントであり、過度の暗黙の信頼を減らしてセキュリティリスクを軽減します。ほとんどの組織は、フィッシングやランサムウェアなどの脅威を念頭に置いていますが、より広い意味では攻撃対象領域を減らすためにゼロトラストを使用しています。

監査を活用する:特に米国連邦部門では、コンプライアンス義務によるゼロトラストの需要が高まっています。組織がゼロトラストを採用し、サプライチェーンのリスク管理の一部としてそれを導入する方向に進むにつれて、コンプライアンスの要素は増えることが予想されます。

結論：ビジネスケースは、まずビジネスニーズを満たす必要があり、そのニーズを満たすことによって、ゼロトラストの原則を適用してセキュリティを強化する必要があります。

C. IT スタックを保護する

ゼロトラストとは、動的な境界を作成することです。この境界は有効期間が短く、範囲が厳しく制限されており、ポリシーが適用され、信頼シグナルとテレメトリによって通知されます。つまり、サブジェクト（通常はデバイス上の人物）とリソース（通常はその人物がアクセスしているアプリケーション）との間の信頼境界です。

IT スタックは、セッションごとおよび接続ごとに、これらの信頼境界の確立を実現できる必要があります。

成熟段階にあるゼロトラストは、時代遅れではなく最新である可能性が高く (68% 対 31.3%)、オンプレミスよりもクラウドファーストである (46% 対 23.6%) 傾向にある:これらの最新のクラウドファーストスタックは、セッションごと / 接続ごとの信頼境界を確立するというポリシーの要求を、より確実に満たすことができます。

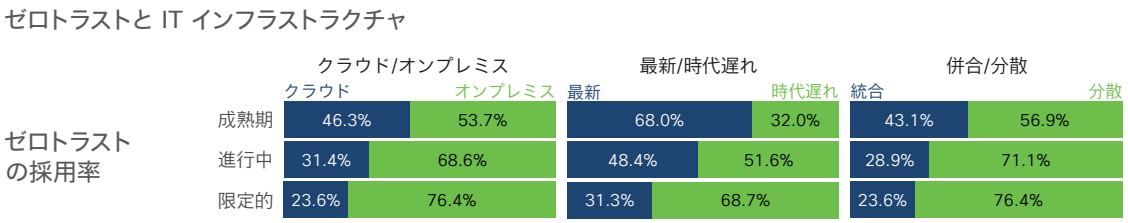


図 7 : IT インフラストラクチャ属性におけるゼロトラストの採用

各要素から全体を作り上げる : ゼロトラストの制御ポイントには、人、デバイス、ネットワーク、アプリケーションワークロード、およびデータが含まれます。これらの制御ポイントが分散していると、重複した作業と調整を必要とするサイロになる可能性があります。したがって、**成熟段階にあるゼロトラストが分散インフラよりも統合インフラに多く見られるのは驚くことではありません (43.1% 対 23.6%)。**経済メカニズムの原理が反映されていると言えます。

パッチを適用する : 環境を最新の状態に保つことは、成功するための要因です。ゼロトラストにより、認証と承認のためのアーキテクチャパターン、標準、プロトコル、および共有トラストシグナルのプロトコルは進化を続けています。

ゼロトラスト導入がより成熟段階にある組織は、積極的なアップグレードよりもベンダー主導のアップグレード戦略に依存 (45.8% 対 30.9%): 計画的な更新（従来の複数年更新戦略）によりテクノロジーを何年間も停滞させるのではなく、自動的に更新される SaaS アプリケーションを活用します。SaaS アプリケーションはクラウドにあるため、より高度な柔軟性とポリシー制御を実現できるからです。

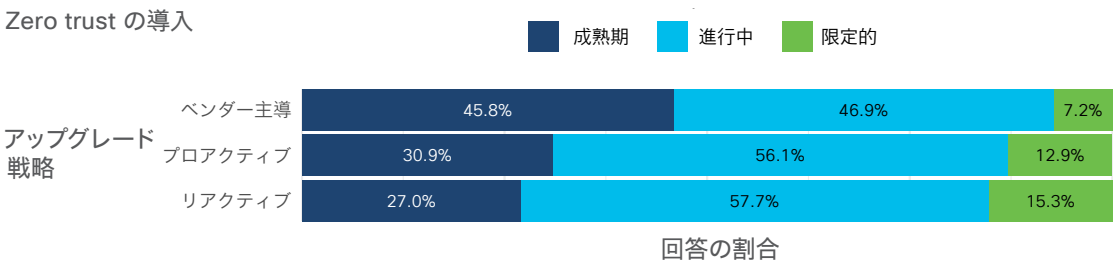


図 8 : アップグレード戦略におけるゼロトラストの採用レベル

認証を一元化する：認証管理が最新のテクノロジースタックに統合されている場合、より簡単に成熟状態に到達できます。しかし、そのスタックの構築を目指している場合は、過程全体の早い段階でゼロトラストの原則とアーキテクチャパターンを活用できるため、千載一遇の好機にあると言えます。

レガシー技術も置き去りにせず活用する：ゼロトラストにおける進行中の課題の 1 つは、これらの原則をレガシー環境とエッジケースに適用することです。最先端の IT 技術がセキュリティ制御ばかりに向けられており、それ意外の多くの環境が取り残されているケースも珍しくないからです。

結論：クラウドへの移行と同様に、ゼロトラストへの移行でも、レガシーと新しいセキュリティモデルを組み合わせたハイブリッド アプローチを採用すべきです。

D. ユーザー、アプリ、デバイスから始める

セキュリティプログラムとしてのゼロトラストは、特定のユースケースを対象としています。成功している組織では、次のようなユースケースが多く採用されています。

- 従業員の保護
- アプリケーションの最新化
- モノのインターネット（IoT）、IT、および運用技術（OT）システムの保護

ここでの特徴は、上記の要素すべてを、ポリシーエンジンを介して保護することです。

さらに、考慮が必要な補完的なセキュリティプログラムが他にもいくつかあります。これらは、ゼロトラストの原則に沿ったものです。その手始めとなるのが、次のような基本的な運用分野です。

- アイデンティティとアクセスの管理 – 承認されたユーザーは誰か、どのようにして把握できるか、どのリソース（アプリなど）にアクセスする必要があるか。
- 資産管理 – IoT、IT、および OT 環境を構成するデバイスは何か。それらが安全に構成されているかどうかを確認するにはどうすればよいか。

これらの質問に対する答えを得ることは、決して容易ではありません。

たとえば、**シスコゼロトラストワークショップ**での参加者からは、アイデンティティ管理プログラムで重大な問題を抱えているという声がよく聞かれます。**組織のアイデンティティ戦略が未定義、不明確、または部分的だと答えたのは、実に参加者の 74% に登ります。**アイデンティティが新しい境界であると提案しているのに、アイデンティティ制御が欠如していることは問題です。

ゼロトラストが引き続き課題となっているもう 1 つの分野は、資産管理プログラムです。**デバイスの可視性がまったくないか、低い、または限定的だと答えたのは、参加者の 55% に登っています。**信頼境界は、デバイス上のユーザーとアプリケーションの間に設定されます。その可視性や優れた構成管理データベースがない場合、どのようにしてゼロトラストを提供できるでしょうか。

考えられる答えの 1 つは、アイデンティティおよびデバイス管理を、一度限りの作業ではなく、オンデマンド アクティビティとして捉えることです。つまり、ユーザーが認証するときに実行されるアクティビティや、デバイスがリソースにアクセスするときに実行されるアクティビティです。

対照的に、ゼロトラストを組み込んだセキュリティプログラムの中には、大きな成功を収めているものもあります。**成熟したゼロトラスト組織は、リスク管理プログラムからより良い成果を報告しています(49%)。**リスク管理プログラムを通じて特定された的確なリスクポスチャとリスク決定を、ゼロトラストでポリシーによって適用することの効果を裏付けている結果だと言えます。

また、ゼロトラストの導入が成熟段階にある組織は、インシデント対応（43%）およびビジネス継続性（41%）プログラムにおける成果も向上する傾向にあることが判明しています。

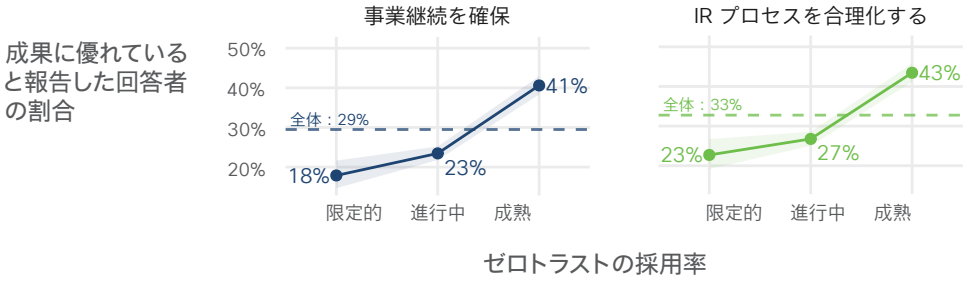


図 9：ゼロトラストの採用レベルと、事業継続性・インシデント対応

新たなテーマは、ゼロトラストプログラムを他の進行中のセキュリティプログラムと組み合わせて、より良い成果を達成することです。資産管理、アイデンティティ管理、または検出・応答のアクティビティといった従来の手動プロセスは、セキュリティチームの手を離れつつあります。状況を踏まえてポリシー違反が検出され、信頼を取り消すべきだと判断された場合の対応は、自動的でなければなりません。

結論：ゼロトラストの導入の成功は、コラボレーションと技術的統合を通じた他のプログラムの強みに基づいています。

E. ゼロトラスト機能

ゼロトラストでは、最新の技術スタックにいくつかの機能を提供できるよう、ビジネスケース / プログラムの構築段階から配慮する必要があります。

高みを目指す：分析（可視化）、統合、自動化された、調和の取れたワークフロー。これは、目指すべき成熟度モデルとリファレンスアーキテクチャに存在するゼロトラストの機能です。つまり構築の目標とするべきマイルストーンだと言えます。

成熟した組織は統合に重点を置いている:図 10 のデータは、業界における次の議論を反映しています。既存のインフラに統合し、すぐに使用できるソリューションを購入する方がよいのか（28.8%）、それともネイティブ統合または大規模プラットフォームの利用という観点から、ソリューションを単一ベンダーから調達してゼロトラストを確立する方がよいのか（51%）。**いずれのアプローチでも成功例が報告されており、これは製品が進化していることを示していると言えそうです。**

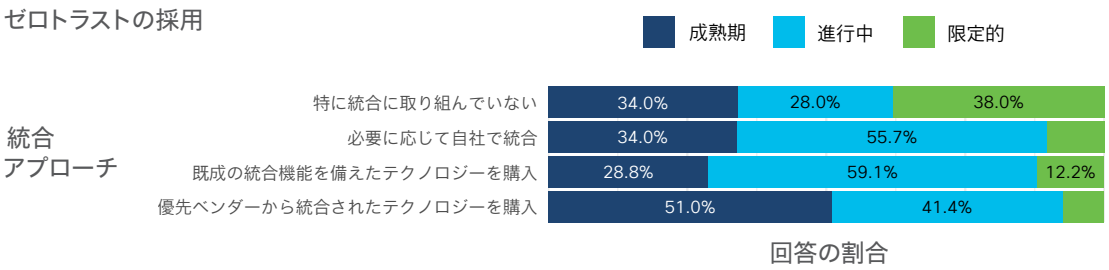


図 10：統合戦略における ゼロトラストの採用

信頼シグナルを共有することで、ポリシーに十分な情報を反映させる: ゼロトラストを成熟させる 1 つの方法は、脅威の検出、脆弱性の特定、資産の保護、インシデントへの対応、オペレーションの迅速な回復のために、他の信頼シグナルとより高度に統合することです。言い換えれば、ポリシーの施行の観点から、信頼に基づいた決定を下すために何を消費し、何を使用しているのか?信頼境界を拡張するために使用および適用しているシグナルは何か?ということになります。成熟した組織からの回答でも裏付けられているように、これらの質問に答えるには十分に統合されたテクノロジーが必要です。

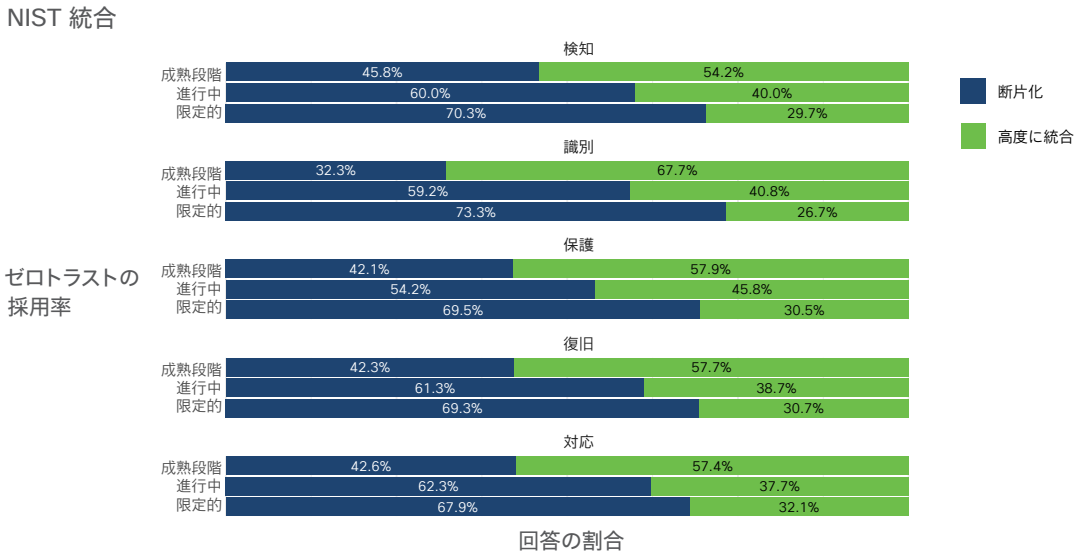
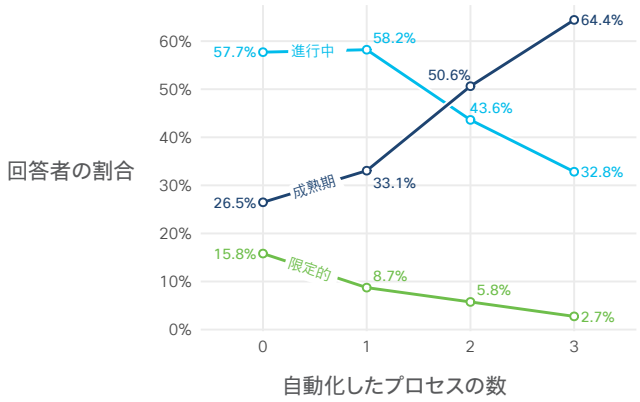


図 10 : 統合戦略における ゼロトラストの採用

自動化とオーケストレーションにより、ゼロトラストを大規模に導入可能にする: 統合によってポリシーの意思決定が改善されると、自動化とオーケストレーションによってゼロトラストが実行できるアクションも改善されます。**ゼロトラストの導入が成熟段階にある場合は、脅威の監視、イベント分析、インシデント対応全体で最高レベルの自動化を実施していることが報告されています (64.4%)。** 統合のレベルは、ポリシーが決定され、脅威を遡って検査する (または脅威を予防する) ためのポリシーデータが利用可能になるにつれて高くなります。



自動化が進むほど良い成果が得られます。自動化とオーケストレーションは、信頼が改善されるまでの間、信頼境界の変更、特権レベルの変更、ロールの調整、アイデンティティが動作するコンテキスト自体の調整など、さまざまな場面で活用できます。

図 12 : 自動化を活用する、成熟したゼロトラスト組織

成熟段階に至ったゼロトラスト組織からは、より多くの自動化プロセスが報告されています。これは、オーケストレーションと自動化を全面的に適用するという、ゼロトラストの全体的なテーマを反映していると言えます。

重要なポイント：ゼロトラストでは、最初に基礎としてポリシーを設定します。次に、ポリシーを適用するポイント全体を可視化します。そして、ポリシーエンジンと増え続ける信頼シグナルとの統合を計画します。最後に、自動化とオーケストレーションを強化して、より多くの環境でアクションを実行できるようにします。これらを段階的に行っていきます。

F. 過程を進めるための準備

セキュリティプログラムを 1 つの過程と見なしたときに懸念されるのは、経営幹部のサポートと同僚の賛同を長期にわたって維持することです。

ゼロトラストプログラムとは、マラソンや短距離走ではありません。ビジネスにセキュリティを組み込む方法なのです。

ビジネスの価値観と優先順位に合わせる：ゼロトラストのイニシアチブを成功させるには、ビジネス価値のあるもの、経営陣と同僚にとって関心のあるもの、およびセキュリティ機能にとって重要なものにゼロトラストの原則を結び付けられるよう、必要なステップを踏む必要があります。これにより、結果がタイムリーに得られます。

リファレンスアーキテクチャとプロジェクト管理フレームワークを活用する：ゼロトラストとは変革への取り組みであり、エンタープライズ アーキテクチャとプロジェクト管理を活用する必要があります。そうすることで、人、サービス、デバイスなど各種のアイデンティティを持つさまざまな環境に対しても、一貫した手段を確立してゼロトラストの原則を導入できます。ゼロトラストを確立するための初期段階におけるの最初のステップは、ガバナンスを確立することだと言えるでしょう。

アーキテクチャをガバナンスに結び付ける：組織に強力なエンタープライズ アーキテクチャ チームがある場合、チームが開始すべき 1 つの領域は、ゼロトラストのリファレンスアーキテクチャを確立することです。組織に強力な GRC（ガバナンス、リスク、コンプライアンス）チームがある場合は、ゼロトラストの原則をガイドラインや規程に適用し、最終的にはポリシーに体系化するための作業を開始してください。ゼロトラスト ポリシー デシジョン ポイント（PDP）とポリシー デシジョン エンジン（PDE）を使用して、GRC ポリシーを決定して適用します。

主要業績評価指標（KPI）を確立して伝達する：まず監査担当者をガバナンスの目的に結び付けることができなければ、監査担当者にゼロトラストの統制を効果的に伝えることは困難になると予想されます。内部監査の GRC 部門がこの困難を克服するには、ゼロトラストを測定・報告する方法を決定し、第三者および外部監査担当者に何を期待するかについて教育することが必要です。このことは、コンプライアンスへの対応や顧客の要求を伴うビジネスケースで特に重要になります。ゼロトラストが第三者によってどのように評価・測定されるかを早期に決定し、それを同僚や経営幹部と共有します。

すばやく成果を上げて勢いを得る：組織を問わず、セキュリティスタック全体に長所と短所があり、その程度はさまざまです。非常に強力なクラウド アクセス セキュリティ ブローカ（CASB）ソリューションがある場合は、アプリケーションの動的リストを取得できる可能性があります。非常に強力なシングルサインオン（SSO）または多要素認証（MFA）が導入済みであれば、デバイスデータの動的なセットを取得できる可能性があります。重要なことは、自社の強みを活かし、その強力な基盤を使用して、可視性とコンテキスト認識を獲得することです。

可視性を重視する：可視性を確保し、これらのインベントリプロセスを確立することは、初期段階ですばやく上げられる成果です。これには、多要素認証とシングルサインオンを展開することで、これらの制御におけるポリシー適用の可視性を高めることも含まれます。最終的な目的は、ポリシーエンジンを配置し、可視化を開始すると同時に、どのレベルのポリシー施行を維持するかを決定することになります。そこから、他のセキュリティプログラムとのコラボレーションポイントを定義します。

「前進中」から「成熟」に進むためのゼロトラスト導入ロードマップ

「前進中」の導入状態から「成熟」状態へと移行するには、次の 3 つのポイントがあります。		
・1 番目は**導入の幅**、つまり制御の対象範囲を増やすことです。たとえば、より多くのユーザーを MFA に登録したり、より多くのデバイスを管理したり、より多くのアプリケーションを保護したりすることが挙げられます。	・2 番目は、**ポリシーの深さを増す**ことです。ポリシーエンジン内のテレメトリ、コンテキスト、条件を活用して、より適切な信頼の決定を下します。そこから、統合を他のセキュリティテクノロジーに拡張します。	・そして 3 番目は、**自動化とオーケストレーションの強化です**。信頼できないものがあると気づいた際のプロセスのうち、さらに自動化できる部分はどれでしょうか。

結論：ゼロトラストは、一連のステップを駆使した段階的なアプローチとして導入するのが最適です。個々のステップは個別のセキュリティプロジェクトとして管理する必要があります。

各ステップにより得られること：

- セキュリティ関係とセキュリティ文化を強化する機会の拡大
- アイデンティティ管理から資産管理まで、あるいはインシデント対応からディザスタリカバリまで、長年の懸案だったセキュリティ強化をすぐに開始する方法
- 費用対効果が高く、適切に統合・自動化された、ビジネス価値を提供するセキュリティテクノロジー

V. ゼロトラスト導入の要点

A. CISA ゼロトラストフレームワークを使用する

アーキテクチャ戦略としては、業界標準に基づいてゼロトラストを追求するのが最善です。ゼロトラストアーキテクチャに関しては、CISA（サイバーセキュリティおよびインフラストラクチャ セキュリティ庁）が標準を策定しています。CISA は、米国国土安全保障省（DHS）内のデジタル クリティカル インフラストラクチャを保護するための官民パートナーシップとして 2018 年に設立されました。「パートナーと協力して現在の脅威を防ぎ、将来に向けて、より安全でレジリエンスのあるインフラストラクチャの構築に共同で取り組む」ことを使命としています。[2]

「ゼロトラストは、我が国の防衛を最新化し、強化するための重要な要素です。」
– CISA ディレクター、Jen Easterly 氏

ゼロトラストの CISA 成熟度モデルは、ゼロトラストの追求を目指す組織にとってロードマップとなります。このフレームワークは、ゼロトラストの 5 つの主要な柱の概要を示しています。

- アイデンティティ
- デバイス
- ネットワーク（または環境）
- アプリケーション（またはワークロード）
- データ

[2] https://www.cisa.gov/about-cisa

図 13 の各柱は、可視性と分析、自動化とオーケストレーション、およびガバナンス（またはコンプライアンス）という 3 つの要件を土台にしています。また、いずれの柱にも、制御の強さや展開方法に基づいた成熟度レベル（従来、応用、最適）があります（図 14）。

CISA のゼロトラストの成熟度モデルは、ゼロトラストセキュリティが「1 回限りの」プロジェクトではなく、継続的な探求であるという現実を反映しています。このモデルを使用することで、チームは自分たちがどこにいるか、どこにギャップがあるか、どのように進展すべきかを評価できます。

CISA モデルによると、「最適」レベルにおけるゼロトラストの導入には、以下の使用が含まれます。これは、シスコの調査データとも一致しています。

- 自動化
- 統合されたワークフロー
- 継続的な信頼性の検証
- データインベントリ
- 暗号化
- マイクロ境界

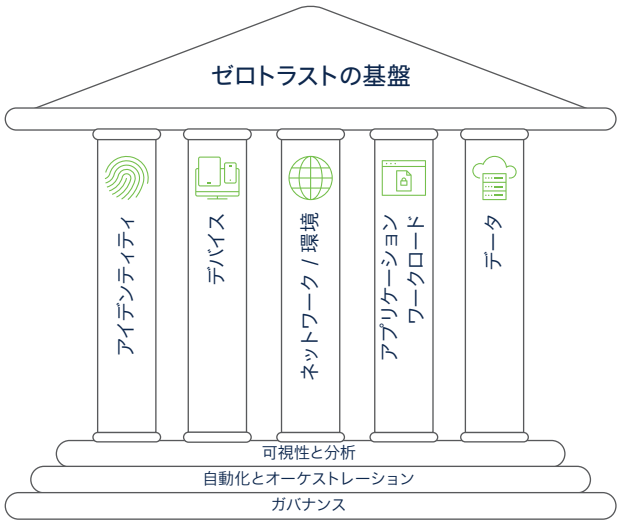


図 13 : 米国サイバーセキュリティおよびインフラストラクチャ セキュリティ庁（CISA）のゼロトラストの柱

CISA ゼロトラスト成熟度モデル

	アイデンティティ	デバイス	ネットワーク / 環境	アプリケーション ワークロード	データ
従来レベル	・多要素認証（MFA） ・限定的なリスクアセスメント	・コンプライアンスへの限定的な可視性 ・簡素なインベントリ	・大規模なマクロセグメンテーション ・内 / 外トラフィックの最小限の暗号化	・ローカル認証に基づくアクセス ・ワークフローとの最小限の統合 ・限定的なクラウドアクセシビリティ	・十分なインベントリがない ・静的制御 ・暗号化されていない
応用レベル	・MFA ・クラウド / オンプレミスシステムとの部分的なアイデンティティ フェデレーション	・コンプライアンス適用を使用 ・データアクセスは最初のアクセス時のデバイスの状態に依存	・入口 / 出口のマイクロ境界によって定義 ・基本的な分析	・一元認証によるアクセス ・アプリケーションワークフローへの基本的な統合	・最小権限の制御 ・クラウド / リモート環境上のデータを保存時に暗号化
最適レベル	・継続的な検証 ・リアルタイムの機械学習分析	・デバイスの常時セキュリティ監視と検証 ・データアクセスはリアルタイムのリスク分析に依存	・入口 / 出口のマイクロ境界を完全に分散 ・機械学習ベースの脅威保護 ・すべてのトラフィックを暗号化	・アクセスを継続的に許可 ・アプリケーションワークフローへの強力な統合	・動的ストレージのサポート ・すべてのデータを暗号化

可視性と分析 | 自動化とオーケストレーション | ガバナンス

図 14 : 米国サイバーセキュリティおよびインフラストラクチャ セキュリティ庁（CISA）のゼロトラストの成熟度モデル

米国政府はゼロトラストのマインドシェアを推進

2021 年 5 月、バイデン大統領はサイバーセキュリティに関する最初の大統領令（EO）に署名し、連邦政府にゼロトラスト アーキテクチャへの移行を義務付けました。2022 年 1 月、管理予算局（OMB）は、特定の要件の期限に関して、ゼロトラストの義務化に「法的実効性」を与えるメモを発行しました。OMB メモの範囲は民間の連邦機関に限定されていますが、多くの業界アナリストは、商業ベースのゼロトラスト市場の分析において CISA フレームワークに依存しています。

B. シスコのゼロトラストの経験から得られた教訓

2020 年、シスコは従来のネットワーク ベースの境界および VPN モデルからゼロトラストフレームワークへの移行に着手しました。当初の目標は、ユーザーまたはアプリケーションの場所を問わず、アプリケーションに安全かつ均質にアクセスできる環境を整えることでした。

シスコのチームは、セキュリティを改善し、10 万人を超えるユーザーの体験を改善することに着手しましたが、5 ヵ月もしないうちに根本的な変化が起こりました。

では、シスコのゼロトラストとはどのようなものでしょうか。シスコが考えるゼロトラストとは、誰かがアプリケーションにアクセスしようとするたびに、次の 4 つのことが発生する必要があります。

1. 多要素認証を使用して本人を確認する
2. デバイスが最新で正常であることを確認する
3. シスコが管理するデバイスが使用されていることを検証する
4. アプリケーションには VPN なしでアクセスできる

毎回というのは文字どおり「毎回」であり、日単位やアプリケーション単位ではなく、絶えず起きる必要があります。

「セキュリティを向上させながらユーザー体験も向上させるというのは、非常に珍しいことですが、今回の導入ではそれが実現できています。」
- シスコ IT ディレクター、Josephina Fernandez

C. すばやく成果を上げる方法を見つける

すばやく成果を上げる方法を見つけるヒント 1：シンプルなメッセージで賛同を得ましょう。他のイニシアチブで見られたよくある間違いの 1 つは、非常に複雑であるために理解や支援が難しくなってしまうことでした。しかしシスコの目標は、メッセージをシンプルかつ具体的で、期限のあるものにすることでした。そうすることで、他の人が覚えやすく簡単に繰り返せるようになります。

すばやく成果を上げる方法を見つけるヒント 2：スコープを明確に定義し、ステータスを十分に伝達しましょう。シスコでは、ユーザー体験の向上、リスクの軽減、ガバナンスの改善という目標を明確に伝えました。これらの目的を超えてプロジェクトを拡大しようとする試みはすべて打ち切られましたが、その一方で、すべての関係者にロールアウトステータスを常に最新の状態に保つようにしました。

すばやく成果を上げる方法を見つけるヒント 3：ゼロトラストの需要を喚起しましょう。ユーザー体験が向上したことを、最も広範で実感できるよう、使用頻度が高い 10 ～ 15 のアプリケーションから始めました。最も重要なアプリに簡単にアクセスできることをユーザーが理解すると、アプリケーションの所有者から部門長まで、組織内で需要が高まりました。

すばやく成果を上げる方法を見つけるヒント 4：今いるところから始めて、すでに持っているものを活用しましょう。シスコの SVP であり、最高セキュリティおよび信頼責任者である Brad Arkin は「白紙の状態からのスタートなどあり得ない」と述べています。社内のチームは、ゼロトラストの目標を達成するために使用できる既存のセキュリティ制御と、廃止する必要があるテクノロジーを決定しました。

シスコが行った大規模なゼロトラストのロールアウトの全容については、こちらをご覧ください。

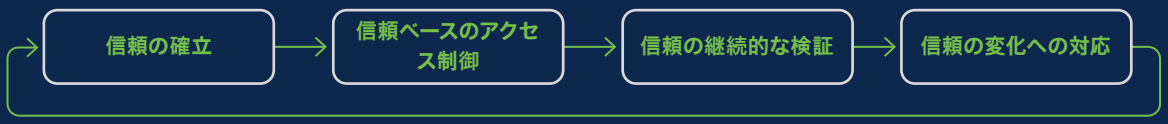
数字で見るシスコのゼロトラスト

パイロット指標	月次指標	年間の節約額
・5 ヵ月のタイムライン – 98 ヵ国の従業員と請負業者を含む ・VPN なしで保護された 10 ～ 15 個のプライベート アプリ（現在は 100 以上） ・ヘルプデスクに問い合わせるユーザーは 1% 未満（対 7%） ・17 万台のデバイスを保護	・576 万件のヘルスチェック ・86,000 以上のデバイスが自己修復 ・VPN 認証が 410,000 回減少	・従業員の生産性向上による 340 万ドルの節約 ・IT ヘルプデスクサポートの年間コストを 50 万ドル削減

D. レジリエンスの構築 : Cisco Secure がゼロトラストを実現する方法

シスコのソリューションなら、複数環境の IT エコシステム全体にゼロトラストを組み込み、ユーザーではなく攻撃者を苛立たせる方法でアクセスを保護することができます。これは、ビジネスの完全性を守るものであり、セキュリティレジリエンスには欠かせません。

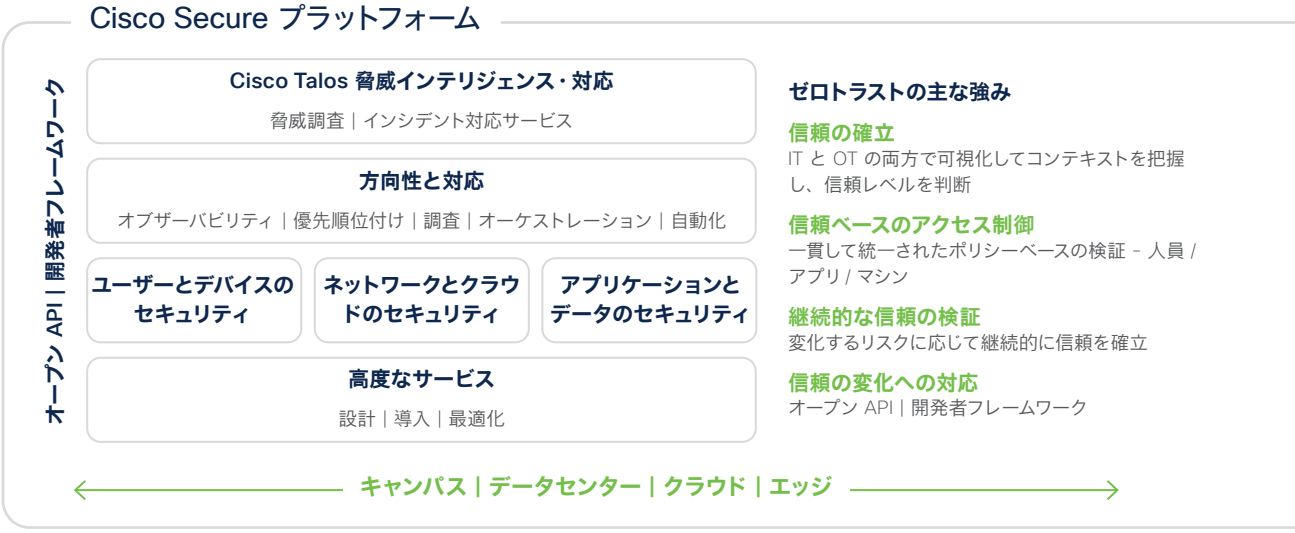
シスコが提供する中核的なゼロトラスト機能は、次のことを実現します。



シスコの統合アプローチにより、組織はネットワーク、デバイス、アプリケーション、およびクラウド全体に統合されたポリシー ライフサイクル管理を適切に導入できます。

最終的には、価値を最大限に発揮して目標を達成することができます。しかも、強力なセキュリティと高い生産性の両方が備わります。その結果、より優れたセキュリティ、より高いパフォーマンス、より迅速な脅威への対応を実現できます。

シスコは、グローバル オペレーション全体にゼロトラストを導入している企業として、世界中の 30 万を超えるお客様に信頼できる専門技術を提供しており、予測不可能な脅威や変化に耐え、より力強く成長できるよう、ビジネスの全面的な保護を支援しています。



シスコのソリューションは、CISA のゼロトラストの成熟度モデルの 5 つの主要な柱にまたがり、キャンパス、クラウド、およびオンプレミスネットワーク全体に可視性と制御を提供します。

cisco SECURE

VI. 次のステップ

ゼロトラストで協力しているお客様やパートナー様の多くは、いくつかの重要な課題の解決を目指しています。標的型の脅威から資産を保護することが目的の場合もあれば、ハイブリッドワークを保護することによってビジネスパフォーマンスを向上させることが目的の場合もあります。また、サプライチェーンリスクの軽減とクラウド環境の保護を目的としているケースもあります。

エスカレートする脅威には、セキュリティに対する新しいアプローチが必要です。ゼロトラストでシスコと提携することで、脅威への対応を強化し、より深い可視性でレジリエンスを構築できます。さらに、脅威の影響を減らしてより迅速に回復し、顧客へのサービスを短時間で再開することもできます。

ゼロトラストで最初の一歩を踏み出す準備はできていますか？適切なユーザーと安全なデバイスだけがアプリケーションにアクセスできるようにします。Cisco Secure Access by Duo の無料トライアルにお申込みください。

ゼロトラストをすぐに開始する方法の詳細については、いずれかのシスコ ゼロトラスト ワークショップに登録してください。

cisco.com/go/zero-trust-workshops

DUO

シスコグループの一員となった Duo Security は、業界をリードする多要素認証（MFA）およびセキュアアクセスのプロバイダーです。Duo は、Cisco Secure の Zero Trust 製品の重要な柱の 1 つであり、デバイスや IT アプリケーション、環境を問わずあらゆるユーザーを保護する最も包括的なアプローチです。Duo は、Bird、Facebook、Lyft、ミシガン大学、Yelp、Zillow など、世界 35,000 社以上のお客様に信頼されているパートナーです。Duo はミシガン州アナーバーで設立され、テキサス州オースチン、カリフォルニア州サンフランシスコ、ロンドンにもオフィスを構えています。

duo.com から、無料で製品をお試しいただけます。

cisco SECURE

シスコは長年にわたりネットワーク分野のリーダーとしての地位を守り続け、総合的かつオープンなサイバーセキュリティ ソリューションのポートフォリオを構築してきました。Cisco Secure は、最高水準のセキュリティを目指して開発されています。セキュリティを簡単に導入、管理、利用でき、強力な連携を特長としており、合理的でお客様本位のアプローチを提供します。シスコは、人とお客様が私たちの行動の中心にあるという事実を原動力としています。Cisco Secure は SecureX プラットフォームにより、現在も将来も脅威防御における安心感を皆様に提供します。現在、すべてのフォーチュン 100 企業が、世界で最も包括的なシスコの統合型サイバーセキュリティ プラットフォームにより現在と将来の脅威から守られています。

シスコのソリューションがエクスペリエンスをどのようにシンプル化し、成功を加速させ、未来を保護するかについては、www.cisco.com/c/ja_jp/products/security/index.html をご覧ください。

850253879　08/22