



ゼロトラスト ビジネスプラン

ゼロトラスト フレームワークを実装する組織のため
の実務ガイド



目次

- 03 [はじめに](#)
- 04 [デジタル トランスフォーメーションのセキュリティにはゼロ
トラストが必要](#)
- 05 [ゼロ トラストに対して現実的なアプローチを取る](#)
- 06 [ゼロ トラスト導入の 3 つのフェーズ](#)
 - 07 [ゼロ トラストへの行程の計画を立てる](#)
 - 10 [組織にゼロ トラストを実装する](#)
 - 11 [進行状況を測定する](#)
- 15 [ゼロ トラストはサバイバル スキル](#)
- 16 [次のステップ](#)

デジタル トランスフォーメーション が新常态を形成

組織がデジタル トランスフォーメーションを採用するのは、次のようなビジネス環境の継続的な変化を管理するためです。

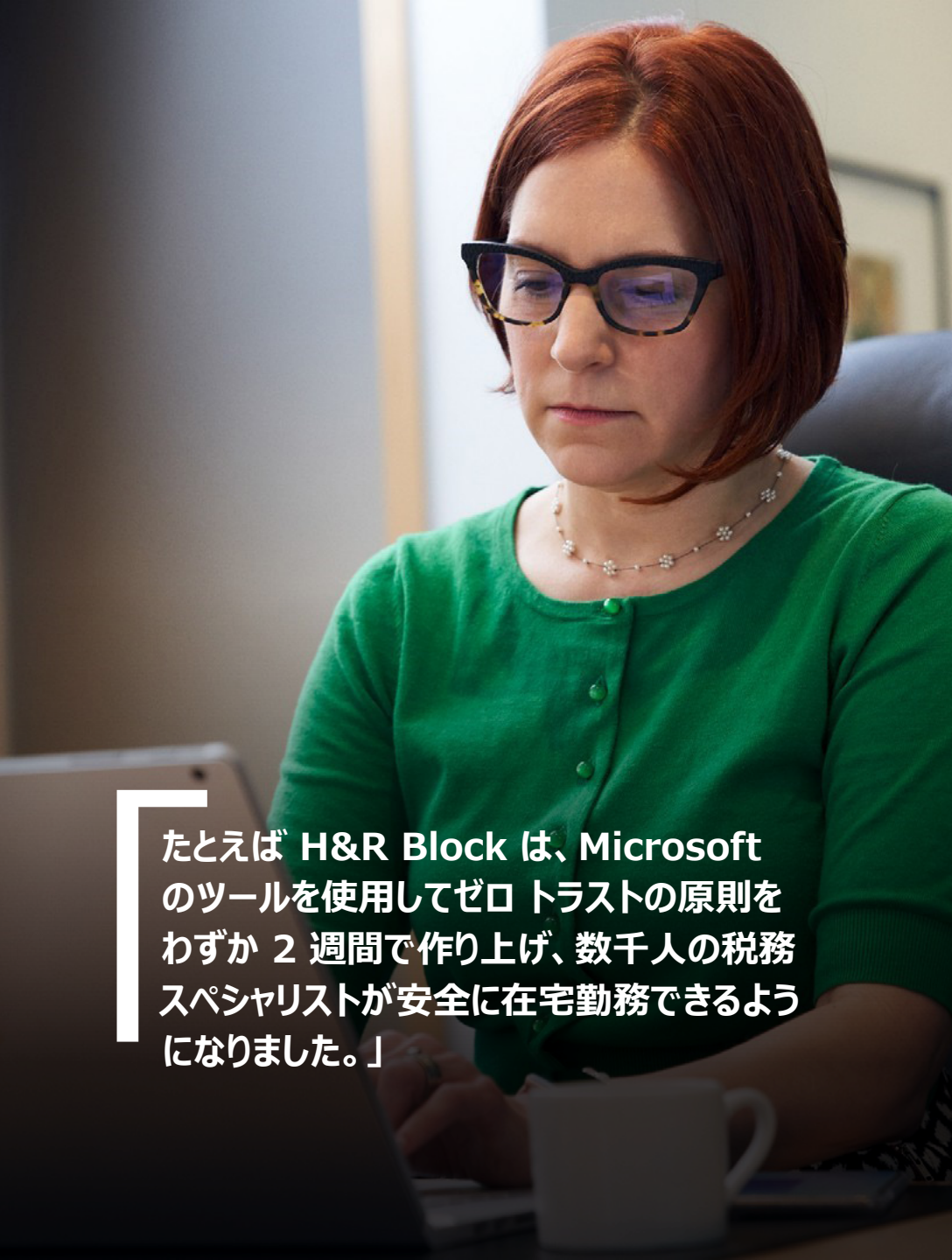
- ビジネス モデルとパートナーシップの変遷
- テクノロジーのトレンド
- 規制、地政、文化の力

新型コロナウイルス感染症（COVID-19）が理由のリモート ワークはトランスフォーメーションを加速し、多くの場合はセキュリティをコスト センターから成長のための戦略的ドライバーへと変えています。



COVID から全員が学んだのは、すべてがバラ色になるとは限らないことと、これからはきわめて短時間で適応できる能力が求められているということです。ゼロ トラスト モデルに近づくにつれて、オペレーションをガレージでしているか、クラウドか、データセンターかは重要ではなくなります。”

–アイデンティティ & アクセス ソリューション担当マネージャー（金融サービス会社）



デジタル トランスフォーメーションの セキュリティにはゼロ トラストが必要

デジタル トランスフォーメーションによって従来のセキュリティ モデルの再検討が迫られています

以前のセキュリティの方法では、急激に進化するデジタル資産に必要なビジネス アジリティ、ユーザー エクスペリエンス、保護が得られません。多くの組織がゼロ トラストを実装しているのは、このような課題を軽減するとともに新常态を実現するため、つまりいつでもどこからでも、誰とでも仕事ができるようにするためです。

たとえば H&R Block は、Microsoft のツールを使用してゼロ トラストの原則をわずか 2 週間で作り上げ、数千人の税務スペシャリストが安全に在宅勤務できるようになりました。」

これらの学びとベスト プラクティスはお客様との会話から、および Microsoft 自身のゼロ トラスト実装の経験から得られたものです。

現実的なゼロ トラスト導入: 大きく 考え、小さく始めて、速く動く



次のことについての複数年ビジネス プランを策定します:

クイック ウィンを優先させる

そして、各イニシアティブを少しずつ前進させます。

既存のテクノロジーを受け入れる

つまり、展開済みまたはライセンス取得済みのものを活用します。

一貫性のあるイニシアティブを構造化する

アウトカム、ベネフィット、オーナーシップを明確にします。

ゼロ トラストを導入する

ゼロ トラストへの行程を進むのに役立てていただけるように、アクションにつながるベスト プラクティス フレームワークを作成しました。各フェーズにはお客様自身の実装の推進に役立つガイダンス、ベスト プラクティス、リソース、ツールが含まれています。



01 計画

組織のリスクと戦略的目標への整合性が最も高いアウトカムに焦点を当ててビジネス ケースを作成します。

02 実装

ゼロ トラスト展開の複数年戦略を作成し、ビジネスのニーズに基づいて早期アクションに優先順位を付けます。

03 測定

ゼロ トラスト展開の成功を追跡します。ゼロ トラストを実行に移すことによって数値として測定できる改善が見られるという確信を得るためです。



ゼロ トラストの計画:「良い」を明確に定義

推奨される優先事項:

→ **ビジョンを定義する**: ゼロ トラストは多面的な行程であり、何年にも及ぶことがあります。目標、アウトカム、アーキテクチャを明確に**定義する**ことによって、成功の可能性は事後対応的アプローチと比べて高くなります。

注: ベネフィットと実装は多くの場合、役割と責任によって大きく異なって見えます。

→ **リーダーシップの賛同を取り付ける**: ゼロ トラスト実装を成功させるには、ビジネス アウトカムに焦点を当てて、野心的な目標、予算配分、内部整合についてリーダーシップの支持を獲得します。

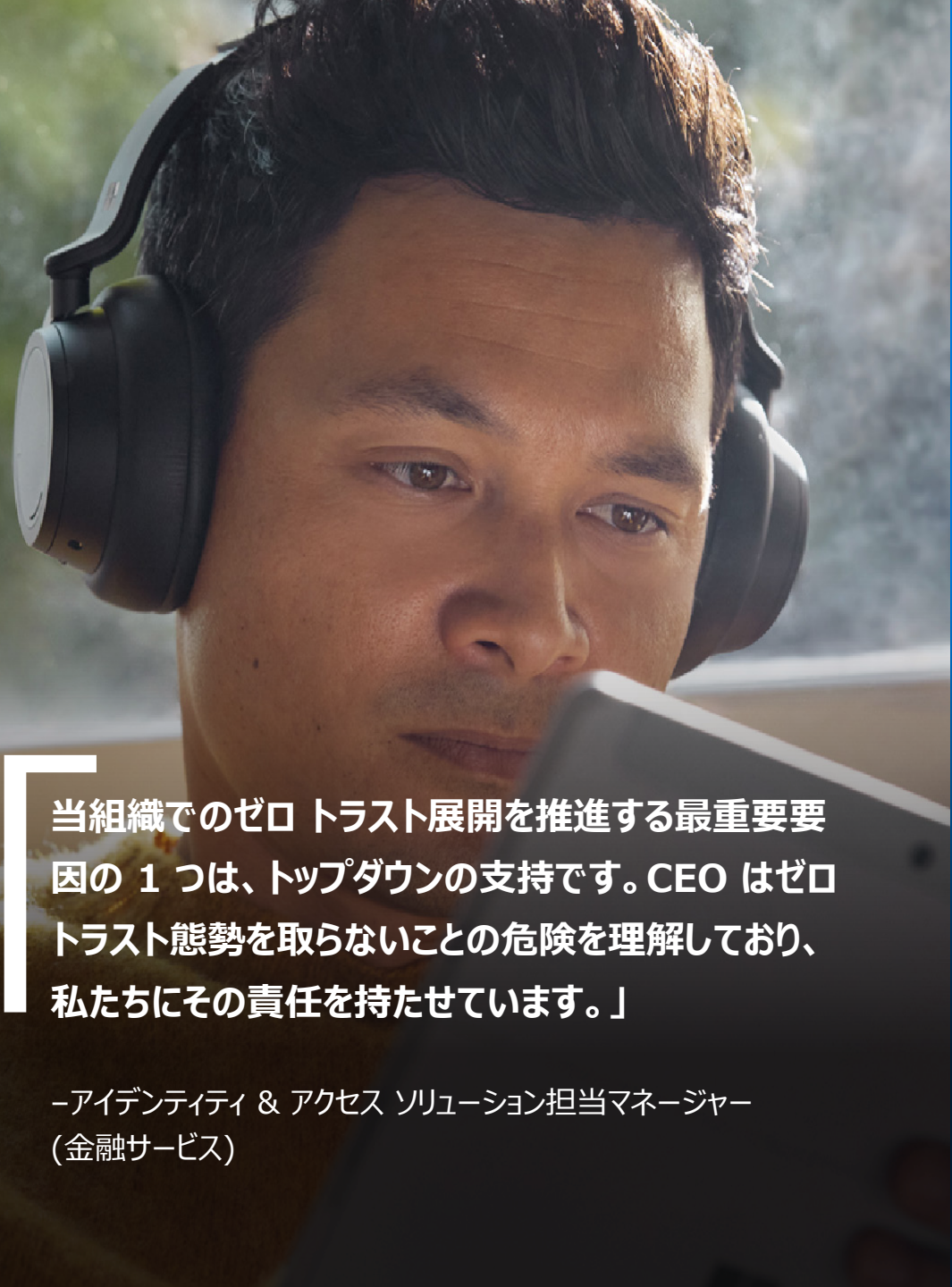
→ **エンド ユーザーをエンパワーメントする**: ゼロ トラストが実現すると、技術チームとエンド ユーザーとの直接エンゲージメントが可能になり、セキュリティをエクスペリエンスと生産性の向上の推進力とすることが出来ます。

ビジョンを定義してリーダーシップの賛同を取り付ける

リーダーシップの支持獲得への最初のステップは、ビジネスの優先事項を聞き取ってから、ビジネス アウトカムに焦点を当てたビジョンを策定することです。

このビジョンは常に、ビジネスの優先事項と文化に合うように作成する必要がありますが、多くの組織に共通するテーマとして次のようなものが見られます。

- **ビジネス アジリティ**: 新しい機会をすばやく追求して獲得すると同時にリスクを管理し、リモートワークを可能にし、クラウドに移行します。
- **複雑さを管理する**: この複雑さとは、ビジネス パートナーシップの継続的な変遷、競争、動的な技術的環境に由来するものです。
- **測定可能性**: ビジネスとリスクのアウトカムに対する説明責任を確実にするためです。



当組織でのゼロ トラスト展開を推進する最重要要因の 1 つは、トップダウンの支持です。CEO はゼロ トラスト態勢を取らないことの危険を理解しており、私たちにその責任を持たせています。」

–アイデンティティ & アクセス ソリューション担当マネージャー
(金融サービス)

ゼロ トラストに向けて強固なビジネス ケースを作る

強固なビジネス ケースは、上層部の支持を獲得してビジネス機能横断での整合性を推進するのに役立ちます。ゼロ トラスト セキュリティ モデルには多くのベネフィットがありますが、成功度が最も高くなるのは一般的に、次の 4 つのビジネス ケースを使うときです。

- 「いつでもどこからでも仕事」をサポートします。
- 安全で迅速なクラウド移行を可能にします。
- セキュリティ スタックのシンプル化を通してコスト削減を実現します。



結果としてビジネスにもたらされる、次のようなベネフィットに焦点を当てます：

- **先回り式のリスク回避と管理**。
- **パートナーのリスク管理**を、弱いセキュリティ プログラムのパートナーについて行う。
- **セキュリティとコンプライアンスのアジリティ**で、役割と組織の状態の急速な変化に対応する。

計画 › 実装 › 測定

ゼロトラストの実装:「良い」を明確に定義

プログラムを構造化して明確で、一貫性のある一連のイニシアティブにまとめます。Microsoft は、技術面の戦略とアーキテクチャが自然に、次のようなセキュリティ イニシアティブにグループ分けされることを発見しました。

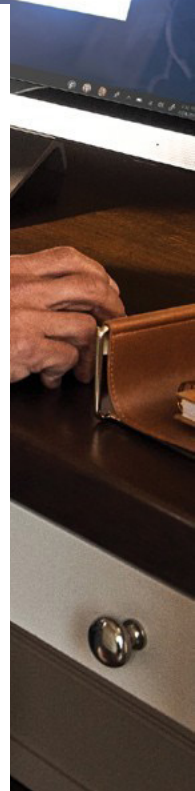
- 生産性セキュリティ
- モダンなセキュリティ オペレーション
- 運用技術 (OT) とモノのインターネット (IoT)
(該当する組織の場合)
- データセンター、サービス、API

これらは Microsoft の経験と、お客様の実装の成功に基づくものです。



イニシアティブに優先順位を付けて計画します:

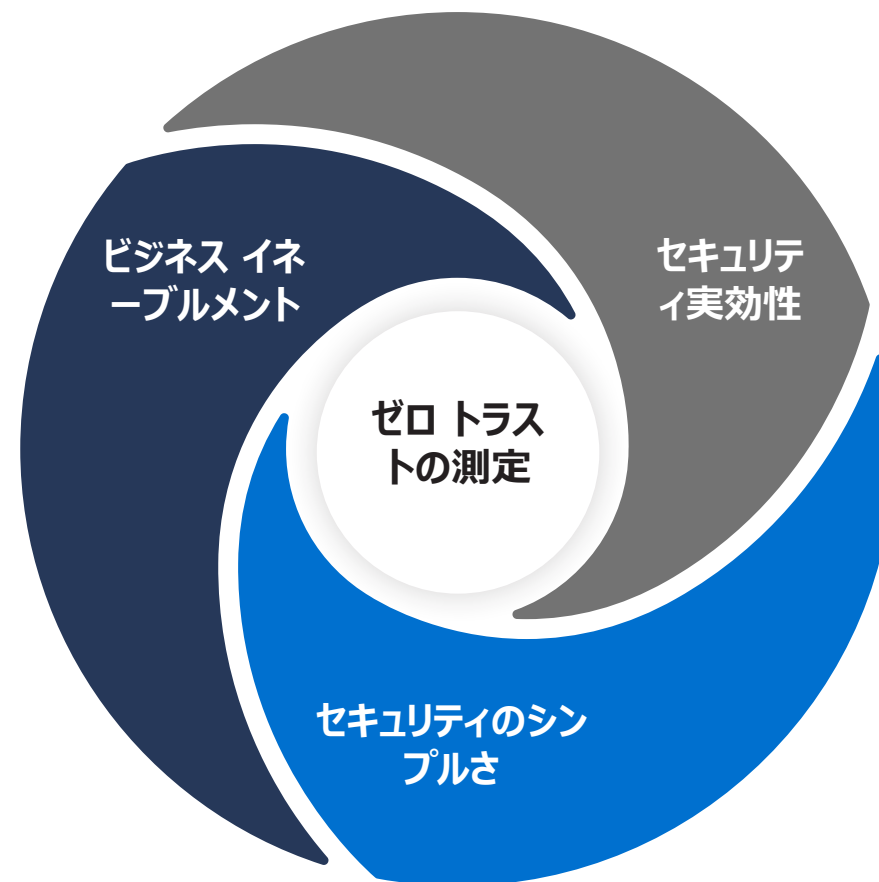
- **各イニシアティブをビジネス目標に整合させる**とともに、想定されるポジティブなビジネスへの影響、摩擦、課題を評価します。
- **短期計画を作成します。**クイック ウィンから始めて、エグゼクティブ スポンサーを見つけます。
- **長期ロードマップを作成します。**



進行状況を測定する - 「良い」を明確に定義

組織の主要なマイルストーンとパフォーマンス目標を定義し、これらを測定し、成功と学びを報告します。

- **ビジネス イネーブルメント:** ユーザー エクスペリエンスにおける摩擦を測定し、イニシアティブの内部セキュリティ承認にどれくらいかかるかを数値化します。
- **セキュリティの実効性:** 組織がゼロ トラスト戦略を導入した後にセキュリティ インシデントの数または影響がどれだけ減少したかを明らかにします。
- **セキュリティのシンプルさ:** 統合が必要なセキュリティ ベンダーの数を減らすとともに、手作業のタスク (パスワード リセットの依頼など) から生じるコストを削減します。

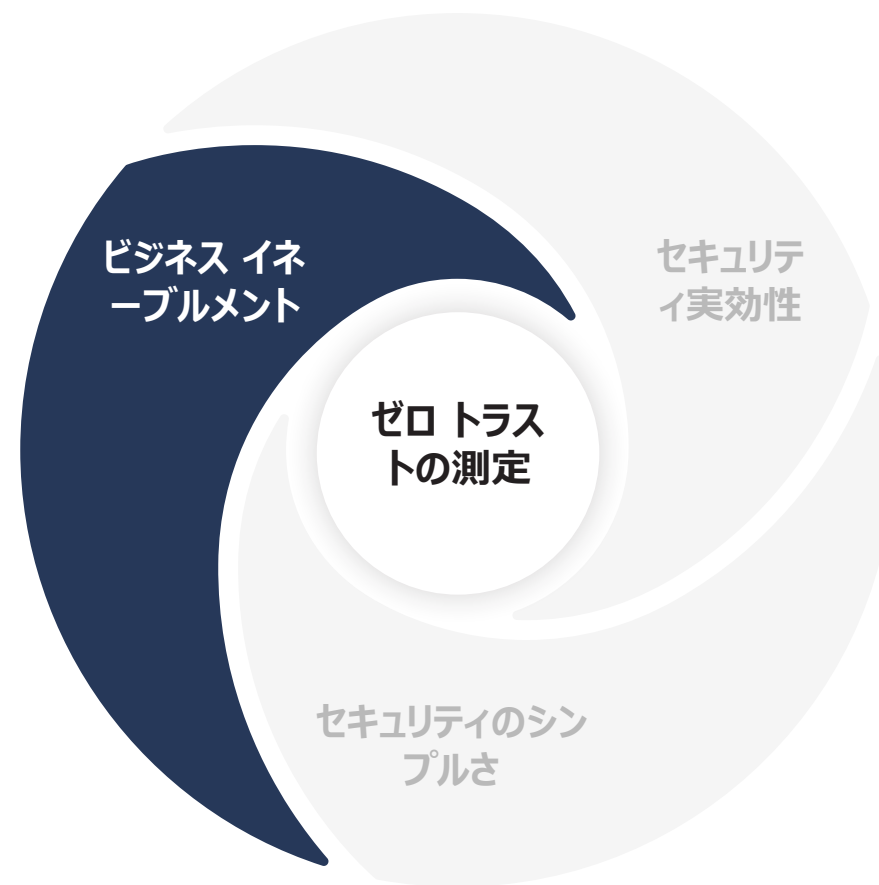


ビジネス イネーブルメントの向上を測定する

ゼロ トラストは、ユーザーと開発者にとって摩擦のないエクスペリエンスであることが必要です:

- セキュリティが理由のユーザー ワークフロー中断の数 (たとえば 1 日に多要素認証が求められる回数)。
- 展開のマイルストーン (たとえば、シングル サインオンを通してアプリにアクセスしている従業員の割合)。
- 可視性のマイルストーン (たとえば、質の低いログイン エクスペリエンスが原因でアプリの使用率が低下すること)。
- 管理対象デバイスの起動に要する時間の平均 (秒)。
- アプリケーションのセキュリティ評価の平均日数。

エンド ユーザーの意見を聞くことを忘れないでください。アクセスのしやすさ、パスワード リセット プロセスなどについてユーザーにアンケートを取ります。

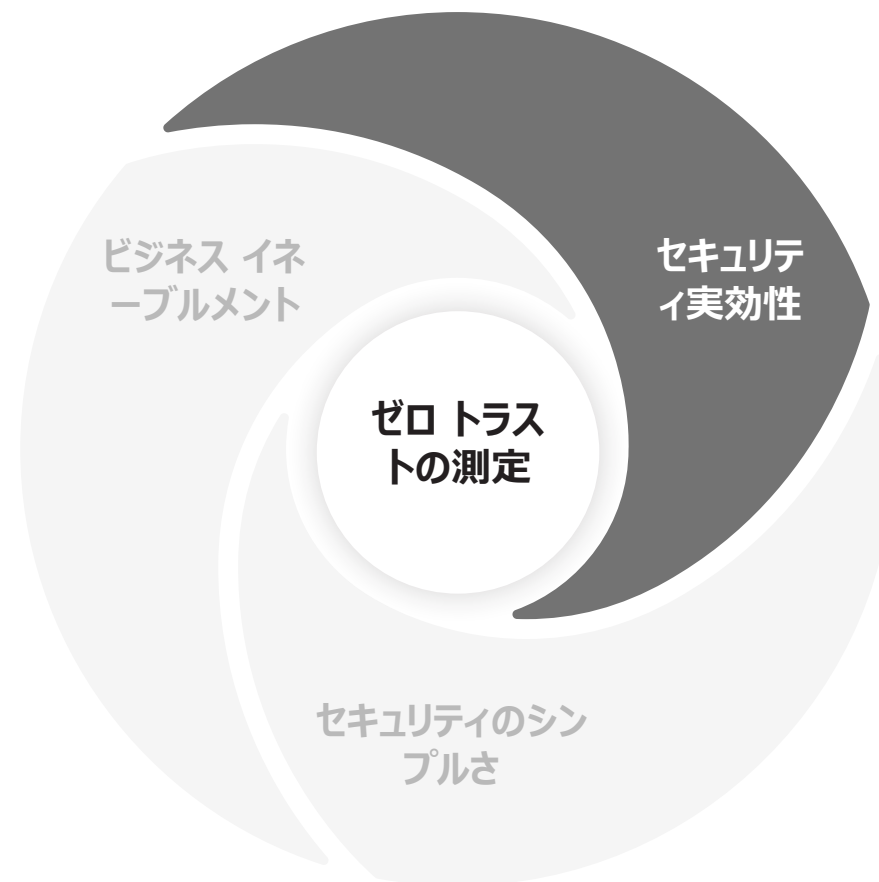


セキュリティ実効性を測定する

組織のセキュリティ態勢と、セキュリティ インシデントから生じる影響を測定します:

- セキュリティ インシデントの数 (重大度別)。
- 展開のマイルストーン (たとえば、積極的に MFA を使用している従業員の割合)。
- 可視性のマイルストーン (たとえば、管理対象のデバイス/アプリの割合)。
- セキュリティ態勢: 改善状況を [Microsoft セキュア スコア](#)で追跡します。

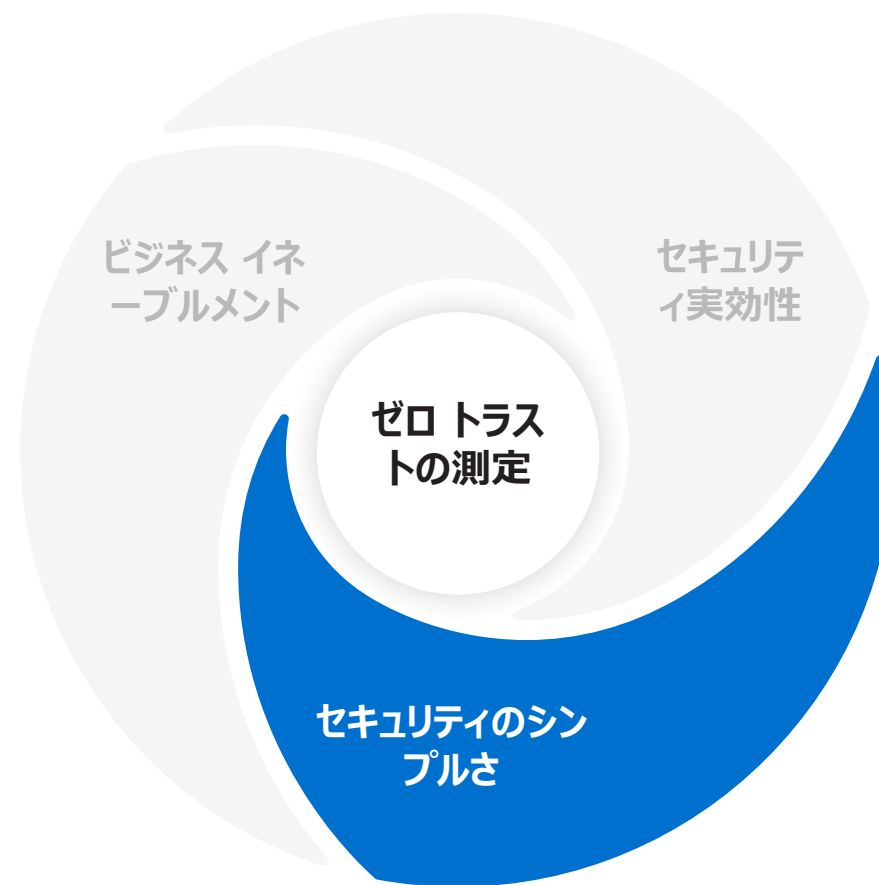
コンテキストを常に明確に: 可視性がゼロ トラストで向上するにつれて、以前ならば見逃されていたインシデントの発見が増えることもあります。



セキュリティのシンプルさを測定する

ゼロトラストはセキュリティ達成の要件をシンプルにするのに役立ちます

- 類似または同一の機能を実行する、重複するセキュリティ ツールの数。
- カスタム統合を必要とするセキュリティ ツールの数。
- IT ヘルプ デスクが低価値の活動（パスワード リセットなど）に費やす時間の割合。
- 繰り返し型ワークフローにおける手作業のステップの数（たとえば、一般的なアラート/インシデントの調査、手作業でのユーザー プロビジョニング、コンプライアンス報告のタスク）。
- セキュリティ チームが調査した誤検知アラートの割合。
- ツールの保守と実際のインシデント対応に費やした時間の比率。



ゼロ トラストはデジタル トランスフォーメーションの鍵となるサバイバル スキル

始めるにあたって、テクノロジーをすべて入れ替える必要はありません。

始めるには、ゼロ トラストへの投資を現在のビジネス ニーズに整合させるとともに、クイック ウィンの獲得に焦点を当てます。ウィンのたびに、価値が増加して大きくなり、リスクが縮小するとともに、デジタル資産のセキュリティ態勢が向上します。

始めるのに遅すぎるということはなく、スコープが小さすぎるということもありません。



Microsoft 365 のテクノロジーを使用してゼロ
トラスト戦略を実装して以来、従業員は会社の
任務を世界のどこからでも遂行できるようになり、
その一方で中核的なセキュリティのニーズに対す
る厳格な制御を維持しています。」

–Igor Tsyganskiy 氏 (Bridgewater Associates
最高技術責任者)

次のステップ°

ゼロ トラスト ベスト プラクティス ガイドをご覧ください、ありがとうございました。
まだの場合はぜひ、[Microsoft ゼロ トラスト成熟度モデルのビジョン ペーパー](#)
(クリックするとダウンロードできます) をご覧ください。ゼロ トラストの中核となる
原則と、成熟度モデルについて詳しく説明しています。このモデルでは、最上位レ
ベルの要件を 6 つの基本的要素に分けています。

また、有益な学習、技術ガイダンス、その他のリソースを外部の [Microsoft ゼロ
トラスト サイト](#)にまとめています。

