ゼロトラストへの移行

これからの組織は、いつ、どこで、どんなデバイスを使っても、セキュアな環境で仕事ができることが前提となります。これは、COVID-19のパンデミックからも明らかです。パンデミックにより、何百万人ものビジネスパーソンは、会社管理あるいは個人保有のデバイスを使った在宅ワークで業務を行うことを強いられました。デジタルトランスフォーメーションが企業の優先課題であることに加え、サイバーセキュリティ攻撃の速度と執拗さが日に日に増していることから、「ゼロトラスト」という概念が急速に脚光を浴びてきています。組織のデータやアイデンティティ、ネットワーク、ワークロード、エンドポイントのセキュリティを継続的に強化するために、ゼロトラスト・アーキテクチャへの移行が不可欠であると私たちは考えます。

ゼロトラストとは?

ゼロトラストとは、ネットワークの境界内にあるものはすべて信頼できるという前提で成立していた、従来の境界ベースのセキュリティアーキテクチャからの、サイバーセキュリティにおけるパラダイムシフトです。従来のアーキテクチャでは、外部との通信はDMZ（Demilitarised Zone）や特殊なネットワークセグメントにより分離され、境界のゲートウェイでの検査を通過することにより正規の通信として信頼されます。この仕組みでは、攻撃者がひとたび境界を突破すると、あらゆるデータやシステムが危険にさらされることとなります。

ゼロトラストは単一の仕組みではなく、リスクベースで、データやワークロードに重きを置き、アイデンティティに基づくセキュリティアプローチを実現するためのアーキテクチャガイドラインです。ゼロトラスト・アーキテクチャでは、信頼できるものは何もないという前提に立ち、すべてのアクセスは検証され、継続的に監視・評価されます。また、アクセス要件の変更や、以前に許可されたアクセスの削除などの条件を評価します。

ネットワークセキュリティベンダーからクラウドプラットフォームプロバイダまで、ゼロトラストのソリューションベンダーはそれぞれに独自の対応技術を持っていますが、下記のような共通点もあります。

- ポリシーに基づくデータ保護
- リスクベースの条件付きアクセス制御
- 適応型認証（リスクベース認証）のような予防的統制と、IDガバナンスのような発見的統制の双方を含むID管理
- 脅威の封じ込めのためのマイクロセグメンテーション
- 従来のVPNを代替する、より優れたリモートアクセス手段（ゼロトラストアクセス）
- 機械学習技術を使って継続的に脅威を特定するためのツールを備えたエンドポイントやインフラストラクチャ
- デバイス信頼（デバイス認証）による認証の強化
- 脅威の特定、リスクスコアの更新、監査可能性のための継続監視

ゼロトラストの起源と発展

前述の通り、ゼロトラストは、「never trust, always verify」の原則に根ざしています。これは主に、マイクロセグメンテーションを活用し、ユーザー、データ、場所に基づいて境界を再定義することで、ネットワーク内の別セグメントに侵入拡大する水平移動（ラテラルムーブメント）の脅威に対処するために設計されました。

マイクロセグメンテーションで制御されたアクセスポイント、アイデンティティの検証、継続的な認証、セキュリティポスチャー（デバイスのセキュリティ構成）の継続的な評価を行うことで、組織は攻撃対象を減らし、水平移動（ラテラルムーブメント）の可能性を減らすことができます。

この10年間で、ゼロトラストはクラウドコンピューティングの概念とともに進化し、ビジネスエコシステム全体に波及しました。今やゼロトラストは、業務やデータを物理的な場所にかかわらず強力に保護するために、組織のテクノロジーの運用環境全体に広く適用されるサイバーセキュリティの原則とリファレンスアーキテクチャ要素の集合体となっています。

現在、政府機関（NIST SP-800-207など）、商用ベンダー（Microsoft、Palo Alto Networks、Netskope、Oktaなど）、研究機関（Forresterなど）から、さまざまなゼロトラスト・アーキテクチャモデルが提供されています。ほとんどのモデルが相乗効果を発揮し、企業は既存の投資やリスクプロファイルに最も適したモデルを選択することができます。

ゼロトラストでは、アクセスに関するポリシーとコンテキスト（誰が、何を、いつ、なぜ、どのように）が継続的に評価され、アクセス制御に使われる最新のリスクスコアが提供されます。このような、状況に応じた柔軟な制御アプローチは、サイバーセキュリティプログラムを完全に刷新することを必要としないため、ゼロトラスト導入のカギとなると考えられます。同時に、ゼロトラストは、GDPRやCCPAなど、刻々と変化する複雑なプライバシー規制への対応にも効果的だといえます。

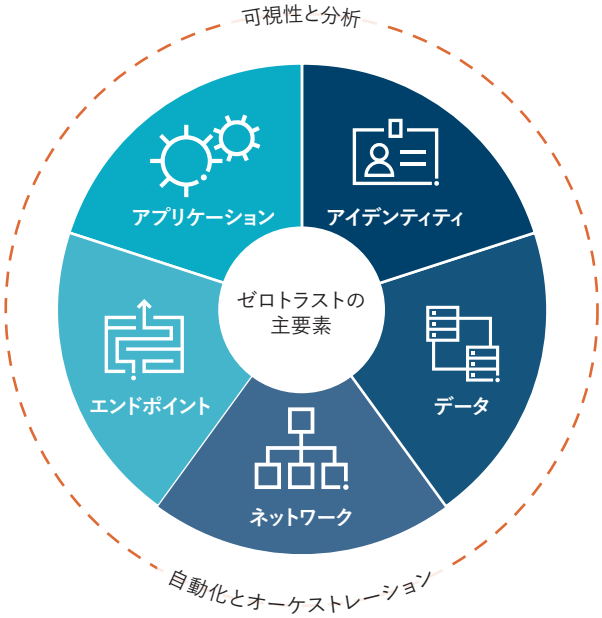
ゼロトラストの主要素

ゼロトラストには多くのトレンドがありますが、そのほとんどは、ゼロトラストのアーキテクチャの一構成要素または機能を実現するソリューションに焦点を当てています。これは主に、ID・アクセス管理を提供するベンダーが、多要素認証（MFA）や条件付きアクセスなどのゼロトラスト・アーキテクチャの原則を取り入れ、市場展開をしているためです。

ID・アクセス管理は重要な要素であり、主な入り口でもありますが、プロティビティではゼロトラストを7つの設計要素で構成された全体的な戦略とプログラムとして捉えています。このような捉え方により、組織はゼロトラストの採用において現在の強みを生かすことができます。

ゼロトラストの主要素は以下の通りです。

- **ID・アクセス管理：**管理するデータ空間全体にわたり、すべてのユーザーのアイデンティティは、多要素認証、適応型アクセス、条件付きアクセス、役割ベースのアクセス制御などの強力な認証方法を用いて検証され、保護されるべきです。
- **データガバナンス：**構造化および非構造化データの両方について発見可能性を確保するため、データ分類とラベルによりデー



タを定義すべきです。データ保護は画一的に行うのではなく、データの価値に比例して異なるレベルで施されるべきです。

- **ネットワーク：**ネットワークは、ほとんどの組織にとって、引き続き主要な統制ポイントとなるでしょう。水平移動（ラテラルムーブメント）を制限し、データフローを可視化できるよう、マイクロセグメンテーションとマイクロ境界を導入すべきです。

- **エンドポイント：**エンドポイントは、ネットワーク上で識別され、隔離され、保護されなければなりません。認証プロセスにおいて、ユーザーと同じくエンドポイントも認証し、承認された安全なシステムからのアクセスであることを確認する必要があります。

- **アプリケーション：**ユーザーがデータにアクセス・利用するのは、アプリケーションやアプリケーション・プログラミング・インターフェース（API）を通じてです。シャドーITを発見し、すべてのアプリケーション（自社開発、サードパーティ製など）についてリアルタイム分析・監視とアクセス制御を施すための対策が不可欠です。

これらは、次に挙げる2つを重要な中核要素としています。

- **セキュリティの自動化とオーケストレーション：**人間は、ITの発達した現代におけるセキュリティ制御を手作業で処理できるスピードを持ち合わせていません。セキュリティの自動化は、既知のイベントが発生した際に、自動的に反応できる仕組みのことです。オーケストレーションにより、チームは日常業務やインシデント処理のプロセスを高度化し、より迅速な対応とリクエストの遂行を実現します。

- **可視性とアナリティクス：**ゼロトラストは、組織が様々なインフラストラクチャとアプリケーションコンポーネントから十分なログ、可視性、信号を得ることができるかどうかの判断に依拠します。アナリティクスでは、ログの記録という基本的な機能に加え、ビジネスの動向を反映したメトリクスや重要業績評価指標への適用を可能にしています。

デジタルトランスフォーメーションとゼロトラスト

COVID-19により「Bring Your Own Device」（BYOD）やリモートワークが普及したのは間違いありませんが、一方でIoT（Internet of Things）デバイスやクラウドアプリケーションなどのクラウドサービスのセキュリティ攻撃に対する脆弱性も明らかになりました。例えば、タブレットからクラウドアプリケーションに接続しようとした際に、企業のデータセンターから何百マイルも離れた場所にいた場合、複数のシステムにまたがって企業データのセキュリティが必要になることが想定されます。ゼロトラスト・アーキテクチャにより、アイデンティティ、コンテクストデータ、デバイスデータを活用した、そうした障壁の打破が期待されています。もちろんゼロトラスト・アーキテクチャにおける一連のアクティビティは継続的に検証・監視されます。こうして、認証されたユーザーとデバイスにのみデータとアクセスを提供することがゼロトラスト・アーキテクチャの目的です。

企業は何をすべきか

- **ゼロトラスト戦略へのコミットメント：**ゼロトラスト・アーキテクチャを成功させるためには、複数のビジネスラインにまたがる最高レベルのリーダーの参画が必要になります。

デジタルトランスフォーメーションとゼロトラスト

プロティビティでは、現在の組織の多くで、多数のDXプロジェクトが互いに整合性のない形で進められていると認識しています。

これにより、製品販売の遅延や役に立たないユーザエクスペリエンス、重大な**セキュリティリスク**を引き起こしてしまいます。

ゼロトラストを活用することで、DXの展開、検証や製品にまつわるセキュリティレベルを高めることにつながります。

- **現状のプロジェクトロードマップの把握：**現在実行中の、および将来予定されているセキュリティプロジェクトを特定して理解し、ゼロトラストの原則を達成するため、適時に整合性をとれるようにします。

- **データの識別とマッピング：**機密データを識別し、どこに保存され、処理され、送信されているかを理解することが重要です。さらに、企業の機密データの流れをマッピングして、ゼロトラストの主要素（業務量、データなど）の分類を効果的に記述する必要があります。

- **セキュリティポリシーおよび基準の策定と更新：**ゼロトラストの原則に基づいて企業のリソースに加えられた変更に対応するために、セキュリティポリシーと基準を更新する必要があります。

- **将来のネットワークの設計：**組織は、セグメント内およびセグメント間のトラフィックを制御するために使用されるネットワークセグメントを論理的に作成することで、マイクロセグメンテーションを構築する必要があります。この方法は、水平移動（ラテラルムーブメント）の拡大を制限するために使用され、これによりデータ中心アプローチによる細粒度のポリシー構成が可能となります。

- **IDガバナンスおよび管理（IGA）の実施：**誰が何にアクセスできるかについて、予防的および発見的な統制の双方を重視した、堅牢な IGA プログラムを開発する必要があります。

- **アクセス管理手法の強化：**組織は、多要素認証を採用し、適切なユーザーが適切なリソースに適切なタイミングでアクセスできるかどうかに基づいて、適応的かつタイムリーな決定が行われるようにすべきです。

- **モニタリングおよび可視化ツールの導入：**ゼロトラストの主要素のセキュリティを可視化するために、既存のテクノロジー活用範囲の拡大や、最新のテクノロジーの導入により、ゼロトラスト・エコシステムを継続的にモニタリングすることが重要です。

- **セキュリティの自動化とオーケストレーションの導入：**企業のリソースから情報を収集し、可視化を可能にするとともに、フィードバックループやスコアリングモデルを作成するための自動化とオーケストレーションの利用を拡大します。

- **継続的な取り組み：**ゼロトラストの方法論を確立は手探りとなるため、ネットワーク全体や関連する構成要素に広がるまでには数年かかる可能性があります。

プロティビティの支援

ゼロトラストへのパラダイムシフトが起こり、企業がデジタルトランスフォーメーションを模索する中、プロティビティはあらゆるフェーズにおいて、業界をリードする専門知識の提供を通じて、より安全かつ堅牢なセキュリティ態勢の実現を支援します。ゼロトラスト手法の導入を実現する、当社サービスは以下の通りです。

- **ゼロトラスト戦略の事前準備：**当社のデザイン・シンキング・ワークショップでは、スタッフ、役員、取締役会など各レベルの関係者を交えたセッションを通じ、組織がゼロトラスト・アーキテクチャ戦略を策定し、コミュニケーションを行うことを支援します。

- **ゼロトラスト・アーキテクチャ移行のための組織態勢アセスメント：**既存のガバナンス関連文書や既存のテクノロジー投資の状況などを検討し、ゼロトラスト・アーキテクチャに移行するための組織の適合性やギャップを評価します。また、ゼロトラスト・アーキテクチャの構成要素を長期的に展開するためのロードマップ作成を支援します。

- **ID・アクセス管理の評価：**ギャップを評価し、ゼロトラスト・アーキテクチャに沿った、ID・アクセス管理プログラムを持つためのロードマップを構築します。

- **データアセスメント：**組織の最も重要なデータがどこにあるのか、またどのように使用されているのかを発見します。自動化されたツールを使用して、構造化データと非構造化データにまたがるデータ抽出業務を支援します。

- **インフラ、オペレーションを対象とした移行準備のためのワークショップ：**ビジネスチームとセキュリティチームの協力を得て、ゼロトラスト・アーキテクチャを実装・運用するための基盤を確立します。

- **技術ソリューション導入支援：**ID・アクセス管理管理、ネットワークセキュリティ、マネージド・セキュリティ・サービスの主要ベンダーとの協業のもと、導入を迅速化、簡素化します。

プロティビティLLC　*protiviti.jp*

〒100-0004 東京都千代田区大手町 2-6-4 TOKYO TORCH 常盤橋タワー 24F Tel. 03-4577-3980
〒530-0001 大阪市北区梅田 2-2-2 ヒルトンプラザウエストオフィスタワー 18F Tel. 06-6450-9367

P.J.2206