ホワイトペーパー

ゼロトラストを実現する

統一IDセキュリティを有効化する

ゼロトラストとは

ゼロトラストとは、堅牢なセキュリティの選択肢となる実証済み実装モデルで、脆弱性のある権限、不要なアクセス権、および過剰なアクセス権を排除し、特定の委任や適切なプロビジョニングを細部にわたり実現します。

- ゼロトラストを有効化すると、管理者パスワードを共有することがなくなり、管理者のアクションすべてに対し、個別かつ動的に認証を行うことができます。
- 最小権限を確実に実装する場合、ある管理者の仕事に必要な権限のみを過不足なく発行する作業が含まれます。

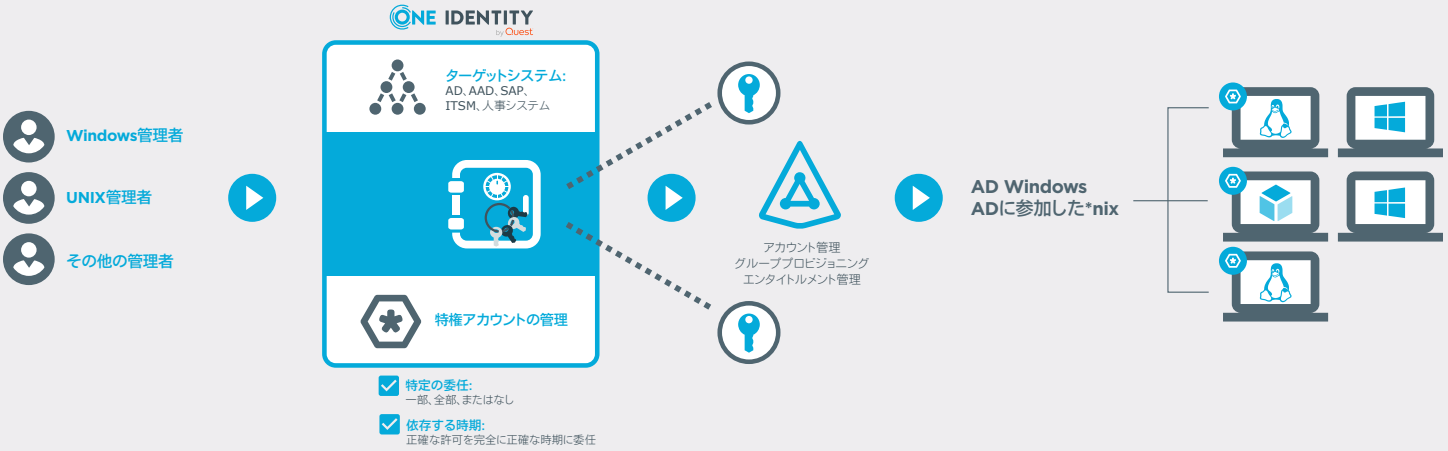
概要

ゼロトラストは、IDセキュリティに対する確実かつ信頼性の高いアプローチであるため、これをセキュリティモデルとして選ぶITリーダーが急速に増えています。「決して信用せず、常に認証を行う」というゼロトラストの原則は、セキュリティと特権アクセス管理に対しより意図を反映させやすいという点で、最小権限モデルとは異なります。この技術概要では、以下に示す点を含む、堅牢なセキュリティ態勢を達成するためのコンポーネントについて説明します。

- 「IDを境界とする」態勢を確立することで、このセキュリティモデルの中心原則の多くに対処できます。このアプローチでは、特に信頼性の高いプロビジョニング、エンタイトルメント管理、PAM、強力な認証システム、安全なアクセス、およびガバナンスのための統一されたソリューションが必要とされます。
- ゼロ・トラスト・モデルでは、すべての通信のセキュリティは確保されますが、通信自体は信頼されていません。
- 「単一の信頼できる情報源」つまり、一元管理で同期されたIDデータを提供することで、企業はIDおよびリソースを完全に制御することができます。エンタイトルメントの概念を最初に確立しない限り、これを正しく達成することはできません。
- パズルのピース1個だけでは、完全なセキュリティモデルを実現することはできませんが、ソリューションを組み合わせることで可能になります。

多くの企業においては、特権アクセス管理（PAM）、Active Directory（AD）/Azure AD管理、イベント収集、およびIDガバナンスと管理（IGA）など、モジュラー式の統合ソリューションが基盤となっている場合、ゼロトラストは十分に手が届く範囲にあります。この統合アプローチにより、ゼロトラストの中心原則を実現し、最適なエンドユーザ体験を提供することができます。

One Identityでゼロトラストを有効化する



ゼロ・トラスト・セキュリティ・モデルへの道のり

最新化の取り組みにより、コンピューティングテクノロジーの適用、利用、およびアクセスの基本的な方法が変化するにつれて、IDセキュリティの重要性がますます高まっています。アプリケーション近代化、クラウド優先の義務、ソフトウェア定義ネットワーキング（SDN）のようなネットワーキングのイノベーション、および競合ビジネスのプレッシャーなど、イニシアチブは、ユーザおよびその他の人事以外によるアクセスを管理および保護することが課題になっています。企業がクラウドベースのテクノロジーを安全に実装する一方で、ミッションクリティカルなオンプレミスのリソースを維持するにはどうすればよいでしょうか。

誰もがクリーンで整然としたプロセスを希望するものですが、現実には、ほとんどの企業が、当面の間、オンプレミスとクラウドベースのシステムが混合したハイブリッドの状態で運用することになります。セキュリティを維持し、コンプライアンス要件に対応して、スムーズなユーザ体験を提供することは、不可能なタスクのようにも思えます。

ところが、そうとも限りません。そのタスクは、デジタル変革を進める中で、このセキュリティモデルを導入することで達成できます。モデルが導入されると、煩雑さを軽減し、情報およびIDセキュリティにカスタマイズされたベストプラクティスを策定するための基本指標を定義することができます。

NISTのゼロ・トラスト・アーキテクチャ

1. すべての**データソースとコンピューティングサービス**をリソースと見なす。

2. すべての**通信**は、ネットワークの場所にかかわらずセキュリティが**確保される**。

3. 個々のエンタープライズリソースへのアクセスは、**セッションごとを基本**として承認される。

6. すべてのリソースの認証および承認は、**アクセスを許可する前に動的かつ**厳密に**実行される**。

4. リソースへのアクセス権は、**動的なポリシー**により決定される。これはクライアントID、アプリケーションやサービス、および要求する資産の観測できる状況を含み、その他の挙動および環境の属性が含まれる場合もある。

5. 企業は、所有する資産および関連する資産すべての完全性とセキュリティ態勢を**監視および測定**する。

7. 企業は、**資産、ネットワークインフラストラクチャ、および通信の現状**に関する情報をできる限り収集し、セキュリティ態勢の改善に使用する。

参照：NIST SP 800-207「ゼロ・トラスト・アーキテクチャ」

IDが新しい境界になる

仮想ネットワーキング環境の一部となるネットワーキング機能が増えるにつれ、これまでのオンプレミスのファイアウォールや静的ルーティングは、仮想結合リソースで置き換えられつつあります。IDセキュリテイが新しい境界になります。IDを保護するためには、強力な認証システム、安全なアクセス、およびガバナンスが必要です。ゼロ・トラスト・セキュリティ・モデルでは、すべての通信のセキュリティは確保されますが、通信自体は信頼されていません。

この新しいモデルでは、オンプレミスまたはクラウドベースのリソース用の統一されたポリシーとアクセス制御を動的に調整および提供する、堅牢なIDセキュリティ基盤が重要なコンポーネントとなります。「単一の信頼できる情報源」（一元管理で同期されたIDデータ）を提供し、IDのライフサイクル全体を通じて権限、属性、およびエンタイトルメントを保証することで、企業は制御を完全に行うことができます。エンタイトルメントの概念を最初に確立しない限り、ゼロトラストを正しく達成することはできません。

7つの中心原則

ゼロ・トラスト・モデルの中心原則は、NIST SP800-207により定義されています。テクノロジーのユーザが、効率的かつ予測可能な形でサービスを採用し、セキュリティモデルを実装できるようなソリューションをデザインする場合、ベンダーはこれらの原則を参考にすることができます。

NISTの原則には、以下のような内容が含まれます。

1. **すべてのデータソースとコンピューティングサービスをリソースと見なす。**
2. **すべての通信は、ネットワークの場所にかかわらずセキュリティが確保される。**
3. **個々のエンタープライズリソースへのアクセスは、セッションごとを基本として承認される。**

   このIDセキュリティの主要コンセプトは、特に特権昇格の管理に注目しています。特定のタスク実行のためにユーザまたはアカウントが特権の昇格を必要とする場合、そのアクセス許可をいつまでも必要とするわけではありません。One Identity Manager、Active Roles、およびOne Identity Safeguard（Just-in-Timeプロビジョニング使用）がこれを可能にします。

4. **リソースへのアクセス権は、動的なポリシーにより決定される。これはクライアントID、アプリケーションやサービス、および要求する資産の観測できる状況を含み、その他の挙動および環境の属性が含まれる場合もある。**

   ここでのキーワードは「動的」です。動的なポリシーにより、ユーザがリアルタイムで必要とする特定の要件に合わせて、アクセス権を変更することが可能になります。Identity ManagerとActive Rolesはいずれもこの機能を備える他、詳細な監査証跡も提供するため、アクセスが承認（または拒否）された場所、要求したユーザ、ユーザが承認された場所、および削除された時期を証明できます。

5. **企業は、所有する資産および関連する資産すべての完全性とセキュリティ態勢を監視および測定する。**

   企業の「資産」には、多くのものが含まれています。アクセス権を持つユーザ、アクセス権が承認された方法、および特権モデルに基づき計算されたセキュリティの脆弱性などを可視化すると、企業に重要な意思決定の情報が提供されます。One Identity Managerは、管理する資産および問題両方の側面からIDに注目するため、正確な情報に基づきアクセス権決定とレポート提供を行うことができます。

6. **すべてのリソースの認証および承認は、アクセスを許可する前に動的かつ厳密に実行される。**

   あらゆるシステムにおいて、アクセス権制御を厳密に実行することが絶対に必要です。One Identityソリューションは、アクセス権制御を動的に行う機能も備えており、規制上またはビジネス上の必要に応じてID変更を検知し、ただちにエンドシステムを操作して、必要なアクセス権の変更を反映させることができます。

7. **企業は、資産、ネットワークインフラストラクチャ、および通信の現状に関する情報をできる限り収集し、セキュリティ態勢の改善に使用する。**

   あらゆるシステムのセキュリティ確保のためには、可視性が鍵となります。観察対象がアクセス権の現状か、変更のために生じたイベントかにかかわらず、One Identityソリューションではこの中心原則を維持します。One Identity Managerがアクセス権の現状と変更に可視性とガバナンスを提供する一方、Active Rolesは Active Directoryオブジェクトの変更を監査し、Safeguardは特権アクセスを制御します。またOne Identity syslog-ngはすべてのイベントデータを収集し、企業が状況を完全に把握できるようにします。

「魔法のボタン」を押せばゼロ・トラスト・モデルを実装できる、というようなソリューションはありません。新しいシステム、アプリケーション、ネットワーク、また物理的なセキュリティを実装する場合は、ゼロトラストを思想として取り込む必要があります。これらの概念を取り入れ、組み合わせることで、企業があらゆる可能性を利用してインフラストラクチャのセキュリティを確保するフレームワークを提供することができます。IDセキュリティは、現代の労働においては重要な役割を果たします。

パズルのピース1つではゼロトラストは実現できません。複数のピースを強力な形で組み合わせる必要があります。特権アクセス管理（PAM）、Active Directory（AD）/Azure AD管理、イベント収集、IDガバナンスと管理（IGA）のサービスを含む、One Identityの統一IDセキュリティプラットフォームを活用することで理想のセキュリティモデルを実装し、同時にエンドユーザーが納得できるセキュリティ環境を提供できます。

ゼロトラストを実現する方法

企業でゼロトラストを達成可能にするには、統一IDセキュリティプラットフォームによる統合アプローチが必要です。IDのセキュリティ確保と管理のための手法を熟考の上作り出すことは非常に複雑なタスクですが、セキュリティにおける重要なピースは、その実装方法です。

企業はOne Identityのソリューションにより、NISTのゼロトラストアーキテクチャに準拠したID中心の手法をさまざまな環境に実装することができます。NISTにより、堅実な技術ガイドラインが与えられ、重要な情報のセキュリティを確保するために大きな一歩を踏み出すことができます。オンプレミスとクラウドのどちらのセキュリティと明示されているわけではありませんが、毎日あらゆる組織にアクセス権の決定を提供するシステムに、このガイドラインを適用することが重要です。

One Identityは、NISTの特定の原則に正しく対応するソリューションを提供します。当社のソリューションは、以下の内容を含んでいます。

One Identity Managerアクセス権制御のためにデザインされており、確実に最小権限モデルを実装し、接続されたシステムで不要となったアクセス権を動的に削除します。

Active Rolesアカウントのライフサイクル管理や動的なロールおよびアクセス権の制御を提供し、Active Directoryや接続されたすべてのシステムへのアクセスにおいて最小権限モデルを厳密に実行することで、ゼロトラストの概念をActive Directoryに適用します。

Safeguard完全な特権アクセス管理ソリューションを提供し、企業を活動させる強力なIDとアカウントが厳密な制御下にあり、またそれが詳細な監査証跡およびレポートにより証明されるようにします。

syslog-ngによるログ収集。企業全体で柔軟かつスケーラブルなログ管理を実行し、SEIMを最も効率的に、また最大限のコスト効率で利用できるようにします。

One Identityについて

One Identity by Questは、オンプレミスやクラウドサービス、あるいはハイブリッド環境であっても、組織によるIDを重視したセキュリティ戦略の実装を実現します。アカウント管理、IDのガバナンスおよび管理、特権アクセス管理などを含む当社独自の広範に統合したID管理サービスのポートフォリオにより、組織はプログラムの中心にIDを据えることでセキュリティが実現できる潜在能力を最大限に発揮し、すべてのユーザタイプ、システム、およびデータにわたって適切にアクセスできるようになります。詳細については、OneIdentity.comを参照してください。

WhitepaperAD-MakingZeroTrustReal-RS-JA-WL-65397