ゼロトラストのデータレジリエンス（ZTDR）

セキュアなデータバックアップおよび復元アーキテクチャ
ゼロトラストを実装するための実践的なアプローチ

概要

あらゆる業界のあらゆる規模の組織が、データとビジネスの安全性を確保する上でのゼロトラストの重要性を理解しています。しかし、現在のゼロトラストモデルは、データのバックアップと復元に実質的な形ではまだ適用されていません。ゼロトラストの原則をデータのバックアップと復元にまで拡張するという考え方は、サイバーセキュリティの包括的な性質に一致するものであり、機密情報を保護することには、境界セキュリティ以上のものが含まれます。

この課題に対処するため、Veeamはゼロトラストのエキスパートである Numberline セキュリティの Jason Garbis 氏と共同で、リスクを最小限に抑えてデータ保護を強化し、組織のセキュリティ体制を変革することを目的としたゼロトラストデータレジリエンスフレームワークを開発しました。このフレームワークは、Cybersecurity and Infrastructure Security Agency（CISA）のゼロトラスト成熟度モデル（ZTMM）に基づいて構築されており、ZTMMの主な原則をバックアップとリカバリのシナリオに拡張します。ゼロトラストデータレジリエンスフレームワークとは、信頼を前提としないことや、バックアップと復元のプロセスなどのデータライフサイクル全体にわたってセキュリティ対策を一貫して適用することを意味します。ITチームとセキュリティチームの両方がリスクを大幅に軽減し、データ保護を強化し、組織のセキュリティ態勢を劇的に向上させるのに役立つ実用的なモデルです。

ゼロトラストのデータレジリエンスについてさらに詳しく知りたい方は、ホワイトペーパーを ダウンロード

ゼロトラストに対するVeeamのアプローチ：ゼロトラストのデータレジリエンス（ZTDR）

ゼロトラストは組織のセキュリティ戦略の基盤となるものであり、最も重要なデータ資産のセグメンテーション、最小特権アクセス、Identity and Access Management（IAM）のベストプラクティスによる継続的な認証と認可などの主要な原則は、バックアップ環境の保護において特に重要です。ゼロトラストのデータレジリエンス機能を組み込むことで、組織は、オンプレミス、クラウド、ハイブリッド環境のいずれであっても、データ保護ソリューション固有の課題に対処し、包括的なセキュリティ戦略を確保できます。

ゼロトラストの重要な考え方は、どのような環境のセキュリティであっても侵害が発生すると常に想定することです。ZTDR手法では、このリスクに対抗するための重要な技術として、バックアップ管理ソフトウェアとバックアップストレージを別々のレジリエンスゾーンまたはセキュリティドメインに分離し、その脅威が内部か外部かを問わず、脅威からバックアップデータをバックアップ管理ソフトウェアに隔離します。Veeamは複数のテクノロジーをサポートし、安全性が高いイミュータブルストレージでレジリエンスゾーンを構築します（図1を参照）。

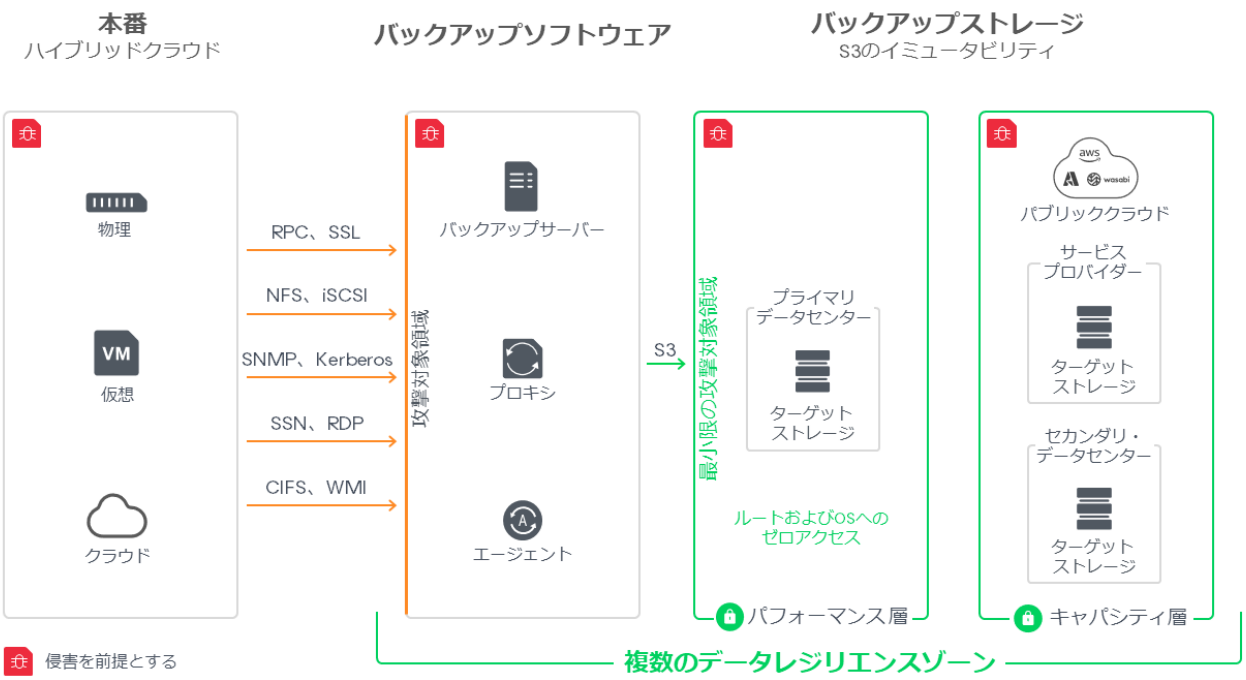

図1

データ保護ソリューションでは、組織全体にわたって、そして多くの場合は最も重要なデータに対して、本番データに対する最高レベルの読み取り/書き込みアクセス権が付与されています。そのため、組織のバックアップ環境を安全なものにして、ゼロトラストのベストプラクティスによって保護することが不可欠です。

ゼロトラストのデータレジリエンスの原則

CISAのゼロトラスト成熟度モデル（図2を参照）を基に、組織が特にデータの柱に適用する必要がある追加の考慮事項があります。

CISOのゼロトラスト成熟度モデル

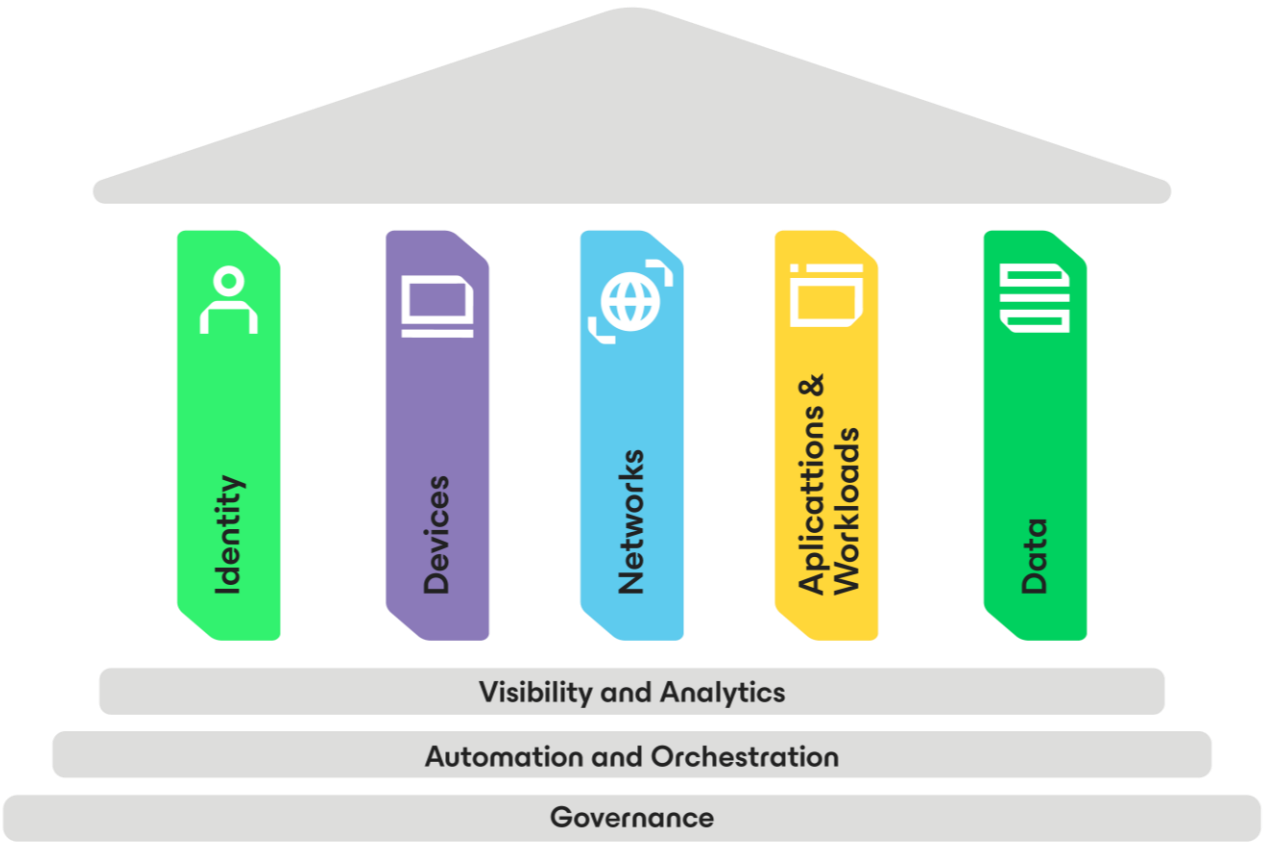

図2

ゼロトラストのデータレジリエンス（ZTDR）の調査レポートでは、組織の全体的なサイバーレジリエンス戦略を支援し、進化するサイバー脅威に直面した場合も重要なデータ資産を確実に保護するための、ゼロトラストのデータレジリエンス（ZTDR）の5つの基本原則に焦点を当てています。

最小特権アクセス

この原則は、意図した機能を実行するために不可欠な人、プロセス、デバイス、またはワークロードへのアクセスを許可することを強調しています。

バックアップインフラストラクチャへのアクセス制御：

- バックアップインフラストラクチャへのアクセスを制御するゼロトラストポリシーを導入すると、検証済みのユーザーのみがバックアップソリューションへの接続を確立できるようになります。これは、不正アクセスや潜在的なデータ侵害を防ぐための重要なステップです。

きめ細かいセルフサービスロールと制限されたバックアップ管理者ロール：

- Veeam内できめ細かいセルフサービスロールと制限されたバックアップ管理者ロールを提供することは、最小特権の原則へのコミットメントを示すことになります。これにより、ユーザーはタスクに必要な特定の機能にのみアクセスできるようになり、不注意や意図的な誤用の可能性が低くなります。

Identity and Access Management（IAM）のベストプラクティス

- マルチファクター認証（MFA）の使用など、IAMのベストプラクティスを徹底することで、バックアップ環境のセキュリティをさらに強化します。これは、特にバックアップソリューションに付随する高いレベルの特権を考えると、不正アクセスを防止するために重要な手段です。

重要な運用意思決定のための「Four-Eyes」原則：

- 重要な運用意思決定に「Four-Eyes」原則を取り入れることで、主要な活動には少なくとも2人の権限のある個人の承認か検証が必要になります。これにより、監督が強化され、悪意のある活動や誤った活動のリスクが軽減されます。

イミュータビリティ（不変性）

安全なネットワーク境界があっても、ゼロトラストの重要な概念は、侵害を想定することです。バックアップの不変性はパワフルな防御メカニズムになります。これは、内部または外部の脅威アクターによる重要なバックアップデータの変更や削除がなされないようにするためのものです。

攻撃対象領域と被害の範囲を最小限に抑えるためのセグメンテーション：

- バックアップソフトウェアとバックアップストレージを別々のレジリエンスゾーンにセグメント化することが、ZTDRの重要な概念です。これにより、重要なコンポーネントを分離することで、内部または外部の脅威の潜在的な影響を最小限に抑えます。バックアップソフトウェアがバックアップストレージに対するOS/管理レベルの権限を持たないようにすることで、保護をさらに強化することができます。

複数のレジリエンスゾーンと3-2-1-1バックアップルール：

- 複数のデータレジリエンスゾーンやセキュリティドメインは、多層構造のセキュリティを提供します。さらに、3-2-1-1バックアップルールはバックアップ戦略のベストプラクティスであり、データレジリエンスの原則とも合致しています。データのコピーを少なくとも3つ保持し、それらを2つの異なるタイプのメディアに保存し、そのうち少なくとも1つをオフサイトに保管し、少なくとも1つを物理的に隔離された状態にするかイミュータブルにしておくことで、多層構造のセキュリティが実現され、データ消失のリスクが軽減されます。

レジリエンスゾーン

ネットワーキングのためのゼロトラストのコアコンセプトは、セキュリティ境界をより小さなゾーンに分割するマイクロセグメンテーションであり、これにより攻撃対象領域、侵害されたゾーンの被害の範囲、攻撃者のネットワーク内移動を減らします。ZTDRにおいて、このコンセプトはデータのレジリエンスゾーンを使用することで適用できます。レジリエンスゾーンは、バックアップストレージを分離し、ストレージコントロールプレーンをバックアップソフトウェアとそのコントロールプレーンから分離します。これにより、バックアップソフトウェアが侵害された場合でもバックアップデータの存続可能性を確保する重要な境界線が提供されます。このような侵害は、内部の脅威アクターなど、さまざまな理由で発生する可能性があります。バックアップシステムは、バックアップソフトウェアのクリーンインストールからバックアップデータを簡単かつ迅速に復元できるよう確保するものである必要があります。

本番
インフラストラクチャ

Veeam
インフラストラクチャ

自律的な
バックアップデータ

イミュータブル　暗号化　3-2-1-1-0

データの整合性と強化されたセキュリティ：

- 互換性のあるバックアップリポジトリを構成し、イミュータブルバックアップの保持期間を設定することは、データの整合性と強化されたセキュリティを確保するためのプロアクティブな手段です。イミュータブルバックアップは、ランサムウェア攻撃やその他の形式のデータ操作に対する保護手段として機能します。

システムレジリエンス

ITセキュリティに対する包括的なアプローチには、プラットフォーム、ツール、テクノロジー、プロセスを含むエコシステム全体のレジリエンスが含まれます。Veeamの多様なレジリエンスオプションは、全システムの消失を含む、各種の中断に耐えられるツールを組織に提供するというコミットメントを示すものです。

イミュータブルバックアップのタイムシフト検出：

- タイムシフト検出の実装は、NTP（Network Time Protocol）が侵害された場合でも、書き換え不能なバックアップが削除されないようにする事前予防的な手段です。この機能によりバックアップリポジトリのセキュリティと信頼性が強化され、重要なバックアップデータの整合性が確保されます。

柔軟な復元オプション：

- Veeamは、組織が運用する多様なITインフラストラクチャに合わせるため、異種環境であっても柔軟な復元オプションを実現し、物理環境や仮想環境だけでなく、ハイブリッド環境もサポートします。この柔軟性により、組織は高速な復元が可能になります。たとえば、オンプレミスのVMwareからAWSやAzureへ、元の環境が利用できない場合はAWSからAzureへ復元できます。

きめ細かいデータリストアオプション：

- さまざまな環境に、さまざまなきめの細かさで柔軟にデータをリストアできるため、データレジリエンス全体が向上します。この適応性により、組織は、さまざまなシナリオの特定のニーズに基づいて復元プロセスを調整できます。

プロアクティブな検証

機能的な側面とプロセスを継続的に検証することが、データを保護し、異常を迅速に検出して対処するための鍵になります。

継続的な監視と検証：

- 24時間365日稼働する監視システムを強調するのは、サイバーセキュリティの脅威はいつでも出現する可能性があるということへの理解を反映しているからです。環境の状態をリアルタイムで把握することで、管理者は異常を早期に検出でき、潜在的なサイバー攻撃やデータ消失が発生する前に調査と対応に当たることができます。

- Veeam ONEのような監視用ツールを活用することは、バックアップと復元環境の正常性とセキュリティを維持するためのプロアクティブなアプローチになります。CPU使用率、データストア書き込み速度、ネットワーク送信速度、増分バックアップのサイズなどのさまざまなパラメータを監視することができるVeeam ONEの機能により、組織は、潜在的な問題に対する価値ある洞察を得ることができます。

エンド・ツー・エンドの可視性：

- エンドツーエンドの可視性というコンセプトは、データ保護インフラストラクチャ全体で必要不可欠です。バックアップと復元システムの健全性と状態を包括的に把握できるため、情報に基づいた意思決定と、必要な場合は迅速な対応が可能になります。

- Veeamの最新リリース12.1では、新しいVeeam脅威センターが登場しました。これで、プラットフォームとインフラストラクチャ全体からの情報を集約して単一の画面にまとめ、脅威を浮き彫りにしたり、リスクを特定したりするほか、データ保護環境全体の状態をシンプルでパワフルなセキュリティスコアカードで確認できるようになりました。

運用のシンプルさ

災害やサイバーセキュリティ事象の発生時に運用のシンプルさが重要となるのは、シンプルであることが効果的な復元において重要な役割を果たすと認識されているためです。ダウンタイムが長ければ長いほど、組織の業務と収益への影響は大きくなります。

ランサムウェア攻撃による平均ダウンタイム：

- Veeamの2023ランサムウェアトレンドレポートによれば、ランサムウェア攻撃による平均ダウンタイムは3週間となっています。このことから、迅速に復元することの緊急性と重要性が浮き彫りになりました。一刻を争うプレッシャーのかかる状況では特に重要になります。

ツール、人材、プロセスのバランス調整：

- ツール、人材、プロセス間の適切なバランスを取ることは、特に組織が災害やサイバー攻撃に対処している場合、重要な課題です。運用のシンプルさには、ワークフローの合理化、プロセスの最適化、効率的な復元のための適切なツールの配置が含まれます。

リストア機能の簡素化への投資：

- Veeamのような業界のリーダーは、復元の複雑さに対処することで復元機能の提供に積極的に投資しています。あるプラットフォームから別のプラットフォームにデータをリストアし、Veeam Recovery Orchestratorなどのツールを活用する機能は、複雑なリストアシナリオの簡素化に専念していることを示すものであり、これにより、フェイルオーバープランを最新の状態に保ち、自動化し、徹底的にテストした状態を維持し、大きなプレッシャーのかかるシナリオに備えることができます。

バージョン12.1の最新のセキュリティ機能の詳細はこちら

結論

デジタル環境が進化・拡大するにつれて、サイバー攻撃や脅威アクターの能力も進化・拡大しています。その結果、組織のデータ、デバイス、人材をより適切に保護および防御するために、ITとセキュリティのコラボレーションと有効性を統合および強化することが急務となっています。この成熟に向けた取り組みは一朝一夕に成し遂げられるものではありませんが、早期に始めることが不可欠です。最初のステップはゼロトラストです。CISAのゼロトラスト成熟度モデル（ZTMM）は、組織のセキュリティと保護に不可欠な基本原則を提供しますが、すべてを網羅しているわけではありません。CISAのゼロトラスト成熟度モデル（ZTMM）の拡張としてゼロトラストデータレジリエンス（ZTDR）を導入することは、進化するサイバー脅威の状況に対処するための戦略的かつ先進的なアプローチです。

最小特権アクセス、不変性、システムの回復力、プロアクティブな検証、運用のシンプルさなど、ZTDRの原則を組み込むことで、組織のデータをセキュリティで保護するための包括的な戦略が示されています。ZTDRを採用することで、組織はセキュリティ態勢を強化するための明確で具体的な手段を取ることができます。これは、運用の効率化と、ITチームとセキュリティチーム間の連携を意味するものであり、これが最終的には、より迅速で安全な復元につながります。

Veeam Softwareについて

データ保護とランサムウェアからの復元におけるNo.1グローバルマーケットリーダーであるVeeamは、すべての組織がデータの停止や消失から回復するだけでなく、前進することができるようサポートすることを使命としています。Veeamは、ハイブリッドクラウドのデータセキュリティ、データの復元、データの自由を通じて、根源的な回復力を実現します。Veeam Data Platformは単一のソリューションで、クラウド、仮想、物理、SaaS、Kubernetesの各環境に対応し、アプリケーションとデータが常に保護され、利用可能であるという安心感をITリーダーやセキュリティリーダーに提供します。米国オハイオ州コロンバスに本社を置き、30か国以上に事業拠点を構えるVeeamは、世界中で45万社を超えるお客様を保護しています。お客様の中にはGlobal 2000の73%の企業も含まれており、事業継続性の維持にVeeamをご利用いただいています。根源的な回復力はVeeamから始まります。詳細については、www.veeam.com/jpにアクセスするか、LinkedIn（@veeam-software）やX（@veeam）でVeeamをフォローしてください。