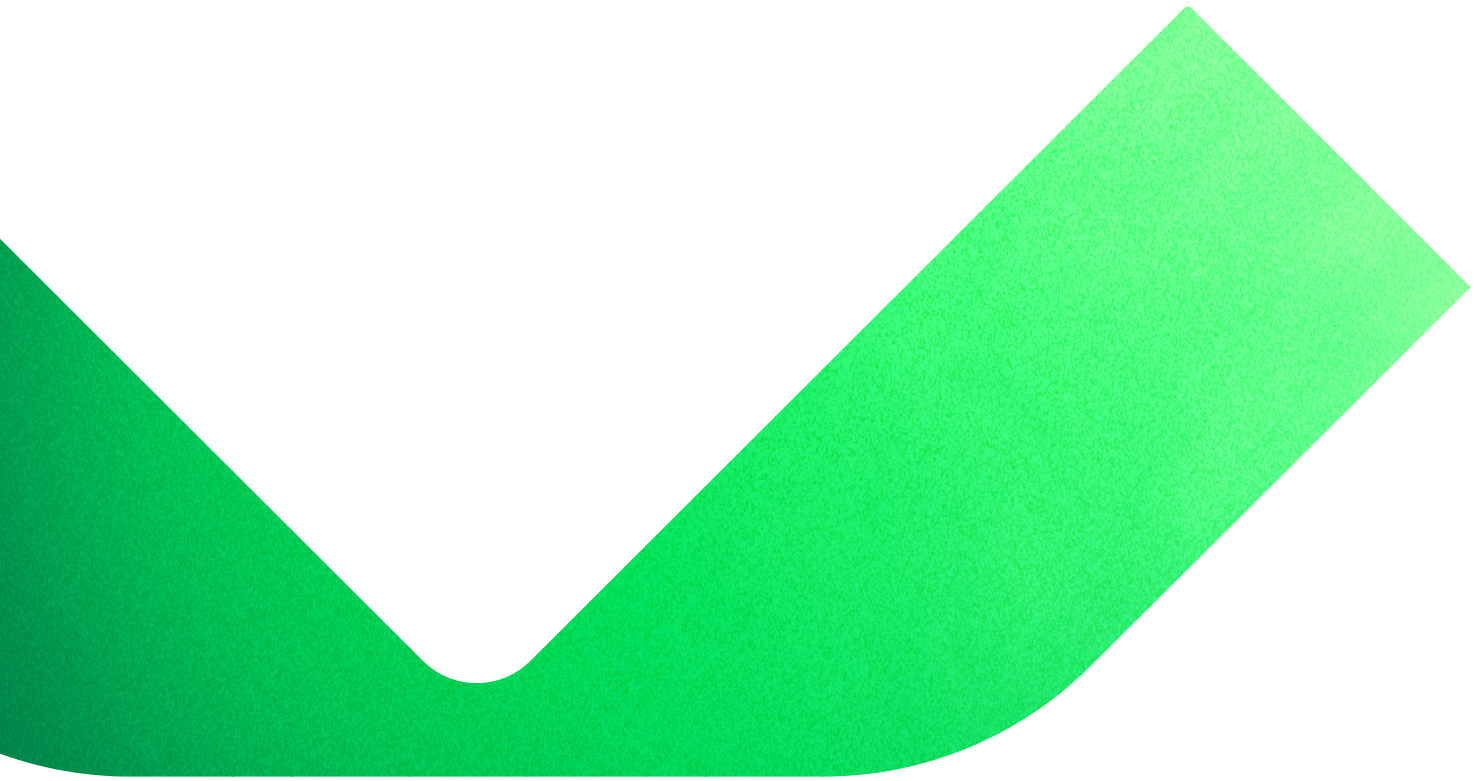
ゼロトラストのデータレジリエンス

セキュアなデータの
バックアップと復元のモデル



コンテンツ

エグゼクティブサマリ

今日の企業は、特にランサムウェアやデータ窃取攻撃から悪意のある攻撃者から自社のデータやネットワークを保護することについて、継続的かつ重大な課題に直面しています。これらの懸念に対処するために、「ゼロトラスト」として知られる戦略は、情報セキュリティ業界で注目を大いに集め、世界中のエンタープライズで広く採用されています。

しかし、最も広く利用されているゼロトラストモデルでさえ、特定の重要領域、特にデータのバックアップと復元に関する包括的なガイドラインが欠けています。このギャップを埋め、ゼロトラストの原則をこの分野に適用することの重要性を認識し、ゼロトラストのデータレジリエンスの概念を紹介します。これは、一連の要件、アーキテクチャ、および既存のゼロトラスト成熟度モデルの拡張で構成されます。

特に、企業は、イミュータブルなデータストレージと設定を提供すると同時に、本番環境やバックアップデータのソースデータに対して、状況に応じた強力に認証されたアクセスを適用する、データのバックアップと復元のシステムを使用する必要があります。このシステムは、今日の企業で一般的なハイブリッドアーキテクチャをシームレスにサポートし、異なる環境への復元に柔軟に対処できる必要があります。

これらの要件を満たすゼロトラストアーキテクチャを導入することで、エンタープライズはデータ、ネットワーク、アプリケーションを悪意のある攻撃者からより適切に保護できます。ゼロトラストは、従来のアプローチと比較して明らかに優れたセキュリティを提供しているため、組織はそれを採用せずにはいられません。このホワイトペーパーで提案されている新しいデータレジリエンス要件は、ゼロトラストを強化および拡張するものであり、エンタープライズのセキュリティ戦略の一環として必須のものと見なす必要があります。

はじめに

ゼロトラストはセキュリティ戦略であり、必然的にその範囲は広くなります。しかし、広く利用されているゼロトラストのモデルとフレームワークには、すべてが含まれているわけではありません[1]。これが原因で、エンタープライズのセキュリティアーキテクチャに対応するギャップや欠落が生じる可能性があります。具体的に言うと、データのバックアップと復元のシステムは、一般的に使用されているゼロトラストフレームワークには含まれていません。これは遺憾なギャップですが、それはランサムウェア攻撃でもデータ窃取攻撃でも、悪意のある攻撃者の主なターゲットはエンタープライズデータであることが非常に多いためです。

データのバックアップと復元のシステムは、エンタープライズITの重要な要素であり、そのように扱う必要があります。彼らは、それをバックアップするために、重要なすべてのものへの読み取りアクセス権を持っています。また、データリストア機能を実行するために、本番環境にデータを書き込む能力も必要です。また、エンタープライズで最も重要なデータの完全なコピーも含まれています。これらの属性を総合すると、データのバックアップと復元のシステムの重要性が浮き彫りになるとともに、悪意のある攻撃者の標的としてのその価値が浮き彫りになります。

もちろん、データのバックアップと復元のシステムは、何十年にもわたってITの責任の一部となってきましたが、セキュリティチームの範囲や責任範囲に含まれていたことはほとんどありませんでした。しかし、エンタープライズが現在直面しているセキュリティ脅威のレベルと巧妙さを考えると、データのバックアップと復元について、ネットワークとITインフラストラクチャの視点だけではもはや十分ではありません。当社は実際に、これらのシステムの設定が不十分で監視されていなかったために、重大なリスクを引き起こしているさまざまなエンタープライズに遭遇してきました。

最新の効果的なセキュリティは、ゼロトラストの原則に基づいています。そのため今こそ、データのバックアップと復元のシステムをゼロトラストの視点から見つめ直すときです。このホワイトペーパーでは、「ゼロトラストのデータレジリエンス」という新しい概念を提案することで、これを実現します。このアプローチを採用することで、企業は、より強力な防御、より効率的な運用、より迅速な復元を実現するための明確で具体的な道筋を手に入れることができます。

[1] CISA ZTMMの文書には、「ZTMMは、フェデラルエンタープライズにとって非常に重要なサイバーセキュリティの多くの側面をカバーしていますが、サイバーセキュリティの他の側面、たとえば復元については対応していません」と記載されています。

アプローチ

情報セキュリティの古典的な基本要素である、CIAの3本柱である機密性、整合性、アベイラビリティは、すべてデータのバックアップと復元に適用できます。企業は、データの流出を回避し（機密性）、ランサムウェアによるデータの暗号化をブロック（整合性）、システムを攻撃から保護し、攻撃後に迅速にリストアできるようにする必要があります（アベイラビリティ）。

ゼロトラストのコア原則は、この領域に確かに関連しており、ユーザーと企業のITシステムへのアクセス、およびデータのバックアップと復元のシステムに適用する必要があります。これらの原則には、暗黙の信頼と未分割のネットワークの排除、ポリシー適用ポイント（PEP：Policy Enforcement Point）を介した動的かつコンテキスト依存のポリシーによるすべてのアクセスの制御、すべてのサブジェクトの適切に強力な認証の要求、侵害の想定、システムとデータの整合性の確保と検証が含まれます。このホワイトペーパーでは、これらの原則が、ゼロトラストのデータレジリエンスのアーキテクチャについて提案されている新しい一連の要件にどのように反映されるかを見ていきます。

ゼロトラストの成熟度を把握するための事実上の標準のフレームワークは、図1に示されているCISAのゼロトラスト成熟度モデル[2]で、5本の中核となる柱を定義しています。それはアイデンティティ、デバイス、ネットワーク、アプリケーションとワークロード、およびデータです。また、次の3つの横断的な機能も定義しています。それは可視性と分析、自動化とオーケストレーション、および管理です。

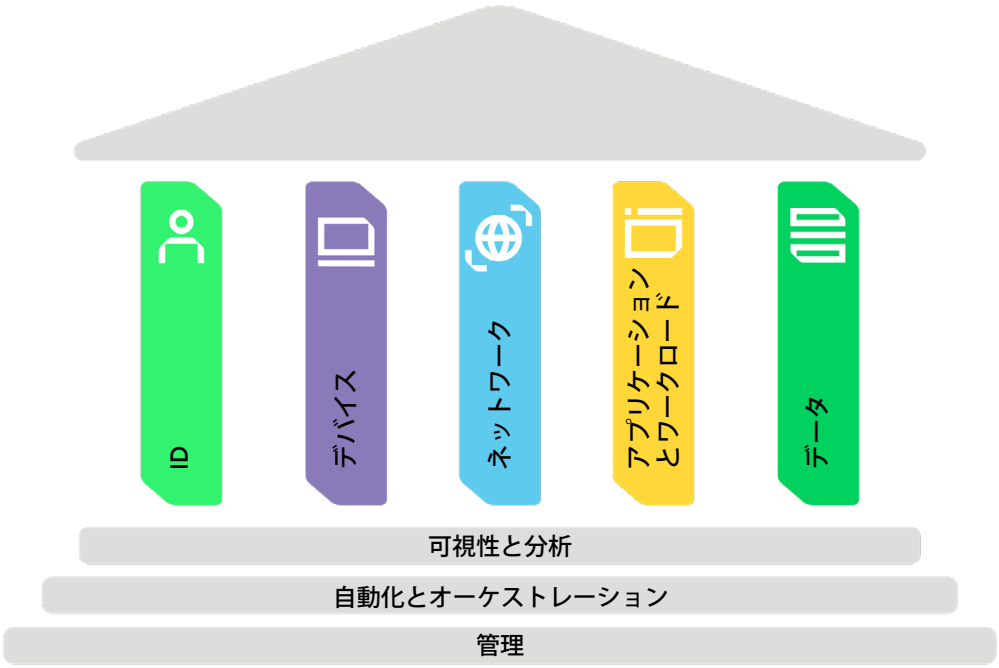


図1：CISAゼロトラスト成熟度モデル

[2] https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model

CISAモデルは、データの柱の中で、成熟度レベルごとに期待される機能と属性を持つ5つの詳細な機能を識別します。

ただし、これらの機能内では、データバックアップの整合性と復元のテーマは最小限にとどめられており、CISAは読者にゼロトラストに関連しない2020年のNISTドキュメントを読むように促しています。要約すると、CISAのゼロトラストモデルは、データのバックアップと復元のシステムの要件と成熟度レベルについては触れていません。この領域は、エンタープライズの機密性、整合性、アベイラビリティにとって非常に重要であるため、このギャップに対処する必要があると考えています。

そのために、当社では原則、リファレンスアーキテクチャ、そしてゼロトラスト成熟度モデルのための新しい機能セットを含む、「ゼロトラストのデータレジリエンス」という概念を導入しています。これらを総合すると、ゼロトラストの拡張と強化を表し、企業のセキュリティスタンスを強化することになります。

機能は以下の通りです。

- データインベントリ管理
- データの分類
- データのアベイラビリティ
- データアクセス
- データ暗号化

ゼロトラストのデータレジリエンス：原則

ゼロトラストのデータレジリエンス（ZTDR）の基本原則は次のとおりです。

最小特権アクセス

イミュータビリティ（不変性）

システムレジリエンス

プロアクティブな検証

運用のシンプルさ

これらのそれぞれについて順番に説明しましょう。

最小特権アクセス

この原則はゼロトラストの中心であり、あらゆるゼロトラストアーキテクチャに必須の部分です。ただし、それは複数のレベルで適用されるので、ZTDRの特定の側面に適用できるかどうかを検討する価値はあります。ネットワークの観点から見ると、バックアップ管理システム自体をネットワーク上で分離し、認証されていない、または権限のないユーザーやデバイスがアクセスできないようにする必要があります。同様に、バックアップ・ストレージ・システムを分離する必要があります。これにより、悪意のあるアクターがネットワーク偵察や脆弱性の悪用によってシステムを発見するのを防ぎます。

バックアップシステムへの正当で承認されたアクセスは、適切に強力な認証とデバイスの態勢チェックを備えたゼロトラストポリシー適用ポイント（PEP）を介してのみ行われなければなりません。また、ゼロトラストPEPは、本番データを読み取っているのが悪意のあるシステムやプロセスではなく、バックアップ管理システムであることを確認するために、適切な認証とある程度のデバイスまたはシステムの検証によって、ソースデータ（つまり、バックアップされるデータ）へのアクセスを制御しなければなりません。

バックアップ管理システムからバックアップストレージへのアクセスもPEPによって制御され、適切に強力な認証によってネットワークの残りの部分からセグメント化しなければなりません。この要件については、下のアーキテクチャ図で改めて説明します。バックアップストレージシステムをバックアップ管理システムからセグメント化しなければならない重要な要件であるためです。

イミュータビリティ（不変性）

ランサムウェアの蔓延と巧妙化に伴い、イミュータブルバックアップデータの概念と要件が近年広く採用されるようになっています。イミュータブルバックアップとは、「一度書き込まれると変更できないストレージメカニズムを使用してバックアップされたデータ」と定義されます。前提として、仮に悪意のある攻撃者がネットワーク上に存在し、バックアップシステムを制御してバックアップストレージにアクセスできたとしても、バックアップされたデータを削除または変更（暗号化）することはできません。一部のイミュータビリティ（不変性）は、Write-Once-Read-Many光ディスクなどのストレージメディアの物理的特性に由来しますが、新しいテクノロジーでは、イミュータビリティがハードウェア層、ファームウェア層、またはソフトウェア層に適用されたメディアが使用されます。最近では、大手のクラウドサービスプロバイダーが、エンタープライズのコンプライアンス要件やアーカイブ要件を満たすために、イミュータブルストレージ機能を追加しています。

注

イミュータビリティの要件は、保存されているデータにとどまらず、データの保持期間も含める必要があります。不変データには、無期限の保存が設定されているものもあれば、1年や5年などの保持期間が定義されているものもあります。保持期間を過ぎたデータは削除される可能性があるため、データ・ストレージ・システムではデータの保持期間をイミュータブルにする必要もあります。これにより、保持期間を故意に短縮することがなくなります。

システムレジリエンス

当社はシステムレジリエンスについてかなり広い視野を持っており、バックアップインフラストラクチャそのものだけでなく、データのバックアップと復元に関連するツール、テクノロジー、プロセスのエコシステム全体に適用しなければならないと考えています。特に、バックアップインフラストラクチャは、コンポーネントやネットワークが利用不能になったり、悪意を持ってバックアップデータを期限切れにするようなネットワークタイムサーバー（NTP）操作など、障害や攻撃に対する回復力を備えていなければなりません。また、場所やインフラストラクチャの種類を問わず、分散された異種のバックアップデータストレージの使用を容易に設定できなければなりません。回復力は、バックアップデータをバックアップ管理システムから分離することでも向上しますが、これはバックアップシステムのセキュリティが侵害されても、データストレージが危険にさらされることがなくなるからです。実際に、侵害や障害が発生しても、バックアップされたデータにアクセスしてリストアする機能に影響を与えることなく再設定できるバックアップ管理システムを探しましょう。

また、システムは、エンタープライズ環境で予想される変更と予期しない変更の両方に対する回復力を備えている必要があります。予想される変更には、ハイブリッドまたはクラウドベースのアプリケーションやデータの導入など、インフラストラクチャコンポーネントの計画的な追加または除去が含まれます。つまり、バックアップシステムは、ソースの場所やテクノロジーに関係なく、エンタープライズデータを効率的にキャプチャして保存できなければなりません。予期しない変更は通常、インシデント対応やディザスタリカバリ（DR）時に発生し、ほとんどの場合、異なる環境への復元のサポートとして分類されます。組織がデータを復元する場合、復元環境が別の場所や異なる種類のインフラストラクチャで実行される可能性は十分にあります。たとえば、オンプレミスのデータセンターが浸水した場合、長期間にわたりクラウドベースの環境で継続業務を行うための復元が必要になる場合があります。したがって、バックアップシステムは、この異なる環境への復元と、この本番環境からの新たなバックアップの両方をサポートしなければなりません。

バックアップ・データ・ストレージ・システム自体は、イミュータブルなデータストレージを提供するだけでなく、容易に強化できる必要があります。これは、強化済みのアプライアンスまたは明確な強化の推奨事項を備えた管理者が設定可能なシステムの形を取ることがあり、複雑化したエンタープライズには、これらの方が適しています。

プロアクティブな検証

システムの適切な動作を保証するには、システムを監視し、すべての機能的側面とプロセスを検証する必要があります。これには2つの側面があります。まず第一に、バックアップシステムの監視は、ネットワーク、パフォーマンス、およびセキュリティを対象に行う必要があります。つまり、このシステムは、他の高価値の本番システムと同様に扱う必要があります。

第二に、そして最も重要なことですが、バックアップされたデータの有効性、および復元プロセスの信頼性と有効性を定期的に検証する必要があります。バックアップしたデータの復元は、定義上、予期しないタイミングで、高ストレスの環境で行われる可能性が高くなります。よく理解され、適切に文書化され、繰り返しリハーサルされたプロセスを組織が持っていることが重要です。また、スタッフの休暇、不在、人事異動を考慮して、これを実行できる複数の担当者を確保しておくことも必要です。

これには時間とエネルギーの投資が必要ですが、これは運用の成熟度を示すものであり、災害の場合の「保険」であることに注意してください。また、「災害」とは、必ずしも文字通りの災害、またはデータセンターの洪水などの大規模イベントを意味するものではありません。たとえば、当社が協力したあるエンタープライズでは、プログラミングエラーのために自動化されたワークフローが暴走し、財務管理システムの本番データが大量に削除されました。これは文字通りの自然災害ではありませんでしたが、（検証済みの）データ復元プロセスを使用することで、比喩的な意味での災害になることも防ぐことができました。

また、バックアップ管理システムには、マルウェア感染のタイムラインに沿ってバックアップを編成する直接的または間接的な機能が必要です。つまり、マルウェア感染を検知する（または通知を受ける）能力が必要であるだけでなく、キャプチャされた時期に応じてバックアップを「クリーン」、「疑わしい」、または「侵害された」と分類できなければなりません。

注

データの検証と復元のプロセスでは、データのプライバシーとデータ所在地の要件も考慮する必要があります。これにより、複雑さとリスクが増す可能性があるため、データの内容と組織の法的およびコンプライアンス義務の両方を理解した上で、慎重に行う必要があります。

運用のシンプルさ

最後の原則は「運用のシンプルさ」です。これは、組織が自信を持って運用できるほど簡単でありながら、企業のニーズを完全に満たすのに十分な機能、スケーラビリティ、洗練さを備えたシステムと定義しています。つまり、貴組織に適したシステムです。

これは重要なことです。当社はこれまでに、その規模、チーム、スキル、ニーズに対して複雑すぎるシステムを利用し、運用化しようと奮闘するエンタープライズを目の当たりにしてきました。その結果、メリットが限定されてしまい、フラストレーションが溜まり、セキュリティの成熟度もビジネス価値も提供できないことになります。バックアップベンダーに見るべき一連の属性は、オーケストレーションと自動化における相対的な強みです。プラットフォームに強力な機能を持つベンダーは、運用化をより速く、より簡単に実施できます。

このセクションの締めくくりとして、これらの各原則は、このドキュメントで後述する新しい成熟度モデルの拡張機能に織り込まれており、次に説明するリファレンスアーキテクチャでも明らかになります。

ゼロトラストのデータレジリエンス：リファレンスアーキテクチャ

データバックアップのアーキテクチャは、エンタープライズごとに異なりますが、特にネットワーク、アプリケーション、データインフラストラクチャが大いに異なるため、それも当然でしょう。とは言え、一般的なゼロトラスト原則による共通のアーキテクチャ要素もいくつかあり、これはあらゆるゼロトラストのデータレジリエンスのアーキテクチャ内に存在しなければなりません。

当社のリファレンスアーキテクチャを図2に示し、この種のシステムにおける主要な要件を示しています。この図は、バックアップ管理システムの観点から環境を表していることに注意してください。ユーザーやシステムによる本番システムへの定期的で日常的なアクセスも、ゼロトラストPEPによって制御されますが、わかりやすくするためにこの図では省略しています。

図2：ゼロトラストのデータレジリエンス：リファレンスアーキテクチャ

まず、ゼロトラストアーキテクチャの中核となる部分である、一元化されたポリシー決定ポイント（PDP）に注目してください。これは、身元認証をエンタープライズのIdentity and Access Management（IAM）システムに委任します。PDPはポリシーストアに依存して、人間と非人間（システム）両方の身元を含む、認証された身元のアクセス権を決定します。

このアーキテクチャでは、PDPがバックアップ管理システムのアクセスを決定します。これらの決定は、ポリシー適用ポイント（PEP）を備えたコントロールプレーン（点線で表示）を通じて伝達されます。PEPはバックアップ管理システムと、バックアップ対象データソースおよびバックアップの保存場所との間に論理的に配置されます。

このアーキテクチャには、バックアップデータのための推奨構造も含まれています。データのイミュータビリティ要件に加えて、エンタープライズは、少なくとも1つのコピーを目的のリストア先へのネットワーク接続レイテンシがあまりない第1の場所に保持することを目指す必要があります。これにより、バックアップスナップショットが高速化され、復旧時点の頻度が増加し、復旧時間が短縮されます。もちろん多くの場合、第1の場所は本番システムと同じ場所に配置されるため、当社のリファレンスアーキテクチャでは、少なくとも2つのデータのコピーを第2の場所に保持するという目標も示しています[3]。これらは、地域の災害に対する回復力を実現するために、第1の場所から地理的に分離されていなければなりません。考えられるトレードオフは、ネットワーク接続が遅くなることであり、その結果、復旧時点の頻度が低くなり、回復時間が長くなる可能性があります。

注

バックアップ管理システムは、ストレージ層から意図的に分離されています。これにより、バックアップシステムは、イミュータブルで地理的に分散された複数のリポジトリに、バックアップされたデータをシームレスに分散できます。また、エンタープライズはパフォーマンス、価格、運用のシンプルさにおいて、独自の要件に最適な組み合わせを提供するバックアップストレージリポジトリを選択することができます。さらに、PEPを介して通信を制御することで、セキュリティの層を追加することもできます。

[3] さまざまな場所にあるバックアップの数についてはさまざまな考え方の流派があり、多くの場合、3-2-1や3-2-1-1-0などのニーモニックで呼ばれます。

ゼロトラストのデータレジリエンス：拡張成熟度モデル

ゼロトラストのデータレジリエンスのために私たちが提案した原則とリファレンスアーキテクチャは普遍的に適用できますが、ほとんどの企業に完全かつすぐに適用することはできません。ゼロトラストのほとんどの側面と同様に、それらについては計画的に進め、段階的に採用しなければなりません。これをモデル化して伝達する標準的な方法は、成熟度モデルを使用することです。冒頭で述べたように、私たちは事実上の標準のCISAゼロトラスト成熟度モデルのフレームワークに従い、私たちの原則と要件を構成する4つの新しい機能でそれを拡張しています。

これらの新機能は次のとおりです。

エンタープライズデータおよびシステムへのアクセス

バックアップストレージとデータへのアクセス

システムレジリエンス

システムの監視と検証

成熟度モデルに対するこれらのZTDR拡張機能は、図3～6に示されており、4つの新機能のそれぞれを次の標準的な成熟度レベルでどのように進めるべきかを示しています。それは、Traditional、Initial、Advanced、およびOptimalです。

各機能について、各成熟度レベルに期待される属性を特定しました。これにより、このモデルは、組織が各機能の成熟度を高めるために必要な改善と変更を示しています。次に、それが成熟度レベルを進むときの各機能を順番に調べます。

エンタープライズデータおよびシステムへのアクセス

この機能は、「バックアップ管理システム（BMS）がバックアップを担当するソースデータにアクセスするための手段およびメカニズム」と定義されます。

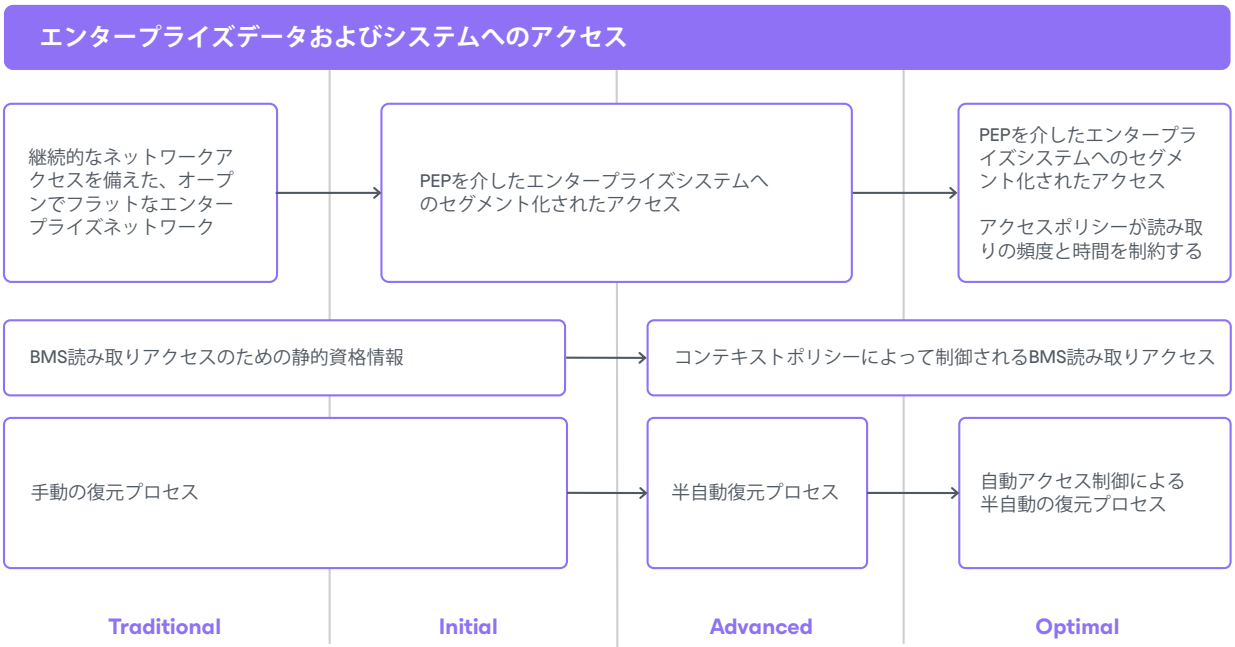


図3：エンタープライズデータおよびシステムへのアクセス：成熟度モデル

Traditional成熟度レベルでは、エンタープライズはフラットでオープンなネットワークを持ち、バックアップ管理システムにはソースシステムへの継続的かつ妨げられないネットワークアクセスがあります。BMSは、ソースデータを認証して読み取るために、APIキー、保管されたユーザー名／パスワード、証明書などの静的ログイン情報を使用します。エンタープライズがBMSを使用してシステムを復元する場合、手動プロセスに依存しています。

Initialレベルに進むには、エンタープライズはより適切なネットワークセグメンテーションの実施を開始し、ゼロトラストポリシー適用ポイント（PEP）を介してエンタープライズシステムへのBMSアクセスを制限して、最小特権の原則を導入する必要があります。

エンタープライズが**Advanced**レベルにいる場合、エンタープライズのデータとシステムへのBMSアクセスにコンテキスト依存のアクセスポリシーが導入されているため、動的なゼロトラストポリシー適用機能をより有効に活用できます。また、自動化された復元プロセスの使用も開始されます。これには、開始とプロセス検証のための手動の手順も含まれます。

Optimalレベルでは、組織はアクセスポリシーの使用を強化して、BMSアクセスを許可された期間またはアクティブな復元ベントのみに制限します。これにより、最小権限の原則がさらに強化されます。

バックアップストレージとデータへのアクセス

この機能は、バックアップ管理システムがバックアップストレージとそこに格納されたデータに対して書き込みおよび読み取りアクセスを行うための手段およびメカニズムとして定義されています。

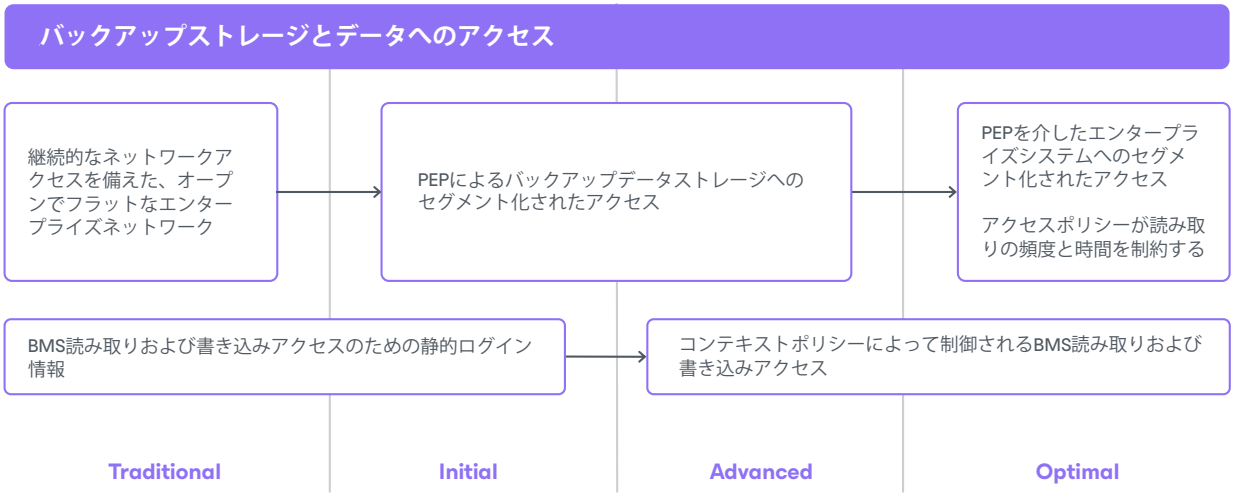


図4 — バックアップストレージとデータへのアクセス：成熟度モデル

Traditionalレベルの成熟度では、エンタープライズはフラットでオープンなネットワークを持ち、バックアップ管理システムには、バックアップストレージシステムとそこに格納されているバックアップデータへの継続的かつ妨げられないネットワークアクセスがあります。BMSは、APIキー、保管されたユーザー名/パスワード、証明書などの静的資格情報を使用して、認証とストレージへの書き込み、および保管されたデータの読み取りを行います。

Initialレベルに進むには、エンタープライズはより適切なネットワークセグメンテーションの実施を開始し、BMSアクセスをゼロトラストポリシー適用ポイントを介したバックアップストレージと保存データに制限し、最小特権の原則を適用しなければなりません。

エンタープライズが**Advanced**レベルにいる場合、バックアップストレージシステムおよび保管データへのBMSアクセスに関するコンテキストアクセスポリシーが導入されることになります。これにより、企業内で動的なポリシー適用機能をより有効に活用できます。

Optimalレベルでは、組織はアクセスポリシーの使用を強化して、ストレージへのBMSアクセスを許可された期間またはアクティブな復元ベント時のみに制限します。これにより、最小権限の原則がさらに強化されます。

システムレジリエンス

この機能は、システム障害、コンポーネント障害、または悪意のあるアクティビティに対する耐性に関するバックアップシステムの特性として定義されます。

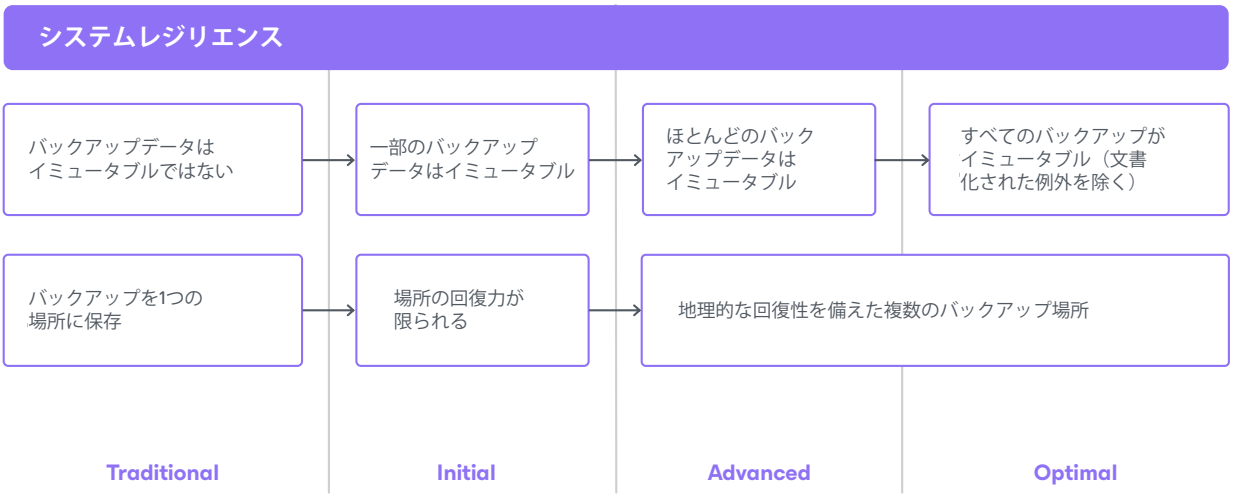


図5：システムのレジリエンス：成熟度モデル

Traditionalの成熟度レベルでは、組織はバックアップデータにミュータブルストレージを使用するので、その整合性とアベイラビリティが危険にさらされます。また、バックアップを1つの場所にしか保存していないことも多いため、地域的な災害が発生した場合に組織が全てを失う可能性があります。

組織は**Initial**レベルに移行すると、一部のデータバックアップにイミュータブルストレージの利用を開始し、それらのバックアップには限定的な場所の回復力を導入しなければなりません。

Advancedレベルでは、書き換え不能なバックアップストレージを使用することがほとんどで、データの機密性と重要度によって優先順位が付けられるのが理想的です。また、分散した場所全体で、複数のバックアップストレージの使用を導入し、運用化しています。

エンタープライズが **最適**レベルに達した時点で、書き換え不能なバックアップストレージをフル活用する方向に移行していることになります（例外は文書化され、承認されています）。新しいデータソースとアプリケーションは、デフォルトでイミュータブルバックアップを使用します。このレベルにより、組織の回復力は、地域の災害や悪意のある攻撃者に対して最大限に高められます。

システムの監視と検証

この機能は、エンタープライズがバックアップ管理システムとバックアップストレージが正常に動作していることと、必要に応じて復元プロセスを実行できるようにするためのツールとプロセスです。

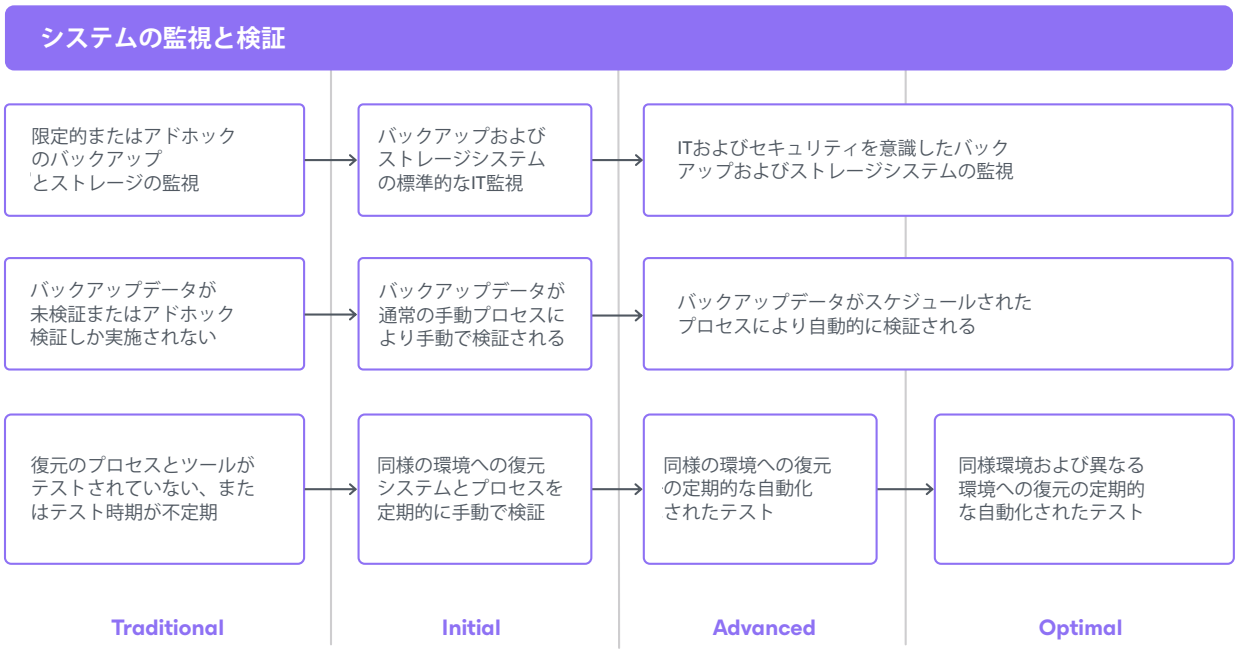


図6 — システムの監視と検証成熟度モデル

Traditionalレベルの成熟度では、エンタープライズはバックアップとストレージのインフラストラクチャの基本的な監視しか実行しません。これは多くの場合、ITと運用の全体的な成熟度が低いことを反映しています。組織は、バックアップしたデータを検証しないかもしれないし、定期的な（手動または頻度の低い）チェックしか実行しないかもしれません。さらに、企業は、復元ツールやプロセスを十分に理解し、文書化し、再現性のあるものにするために、それらを定期的にテストすることもないでしょう。

Initialレベルでは、ITと運用のバックアップとストレージシステムの監視について、標準化されたレベルを採用しています。また、手動プロセスによるバックアップデータの定期的な検証も実施します。また、復元プロセスの定期的（手動）検証を実施して、組織の知識とそれらに対する理解と認知度を確保します。

Advancedレベルでは、組織は、ITおよびセキュリティの両方の監視ツールとプロセスをバックアップとストレージシステムに対して展開します。また、バックアップされたデータは、異常な結果を報告してエスカレーションするスケジュールされたチェックによって自動的に検証されます。これには、復元のツールとプロセスを本番環境と同様の環境に組み込んで、自動化されたテストを実施することが含まれます。

Optimalレベルでは、組織は異種環境への復元力をテストするために、復元テストの精巧さを強化します。

成熟度モデルの概要

全体として、これらの新機能は、1組の機能と4つのゼロトラスト成熟度レベルにマッピングされた一連の機能と期待される一連のコンピテンシーを定義します。自社のデータのバックアップと復元のシステムをゼロトラストの取り組みに取り入れようとしているエンタープライズに、実践的なロードマップとガイドを提供します。

まとめ

ゼロトラストは、情報セキュリティにアプローチするための明らかに優れた方法であり、セキュリティリーダーとして、私たちはこの戦略を企業に導入する義務があります。現在のゼロトラストアーキテクチャと成熟度モデルは、堅実な出発点ですが、不完全です。特に、データのバックアップと復元の要件やアプローチは含まれていません。

従来、エンタープライズはバックアップと復元をITの領域のものとして扱ってきました。しかし、ランサムウェアが蔓延し、ビジネスのデジタル化がほぼ完全に浸透していることから、セキュリティリーダーは、その範囲をバックアップと復元にも広げる必要に迫られています。

このホワイトペーパーでは、ゼロトラストのデータレジリエンスの概念と、一連の基本原則、リファレンスアーキテクチャ、ゼロトラスト成熟度モデルの拡張機能を紹介しました。このゼロトラストのデータレジリエンスのアプローチを採用することで、エンタープライズはより強力な防御、より効率的な運用、より迅速な復元への明確で具体的な道筋を手に入れることができると当社は信じています。当社にとってエンタープライズデータはあまりにも重要であり、セキュリティのベストプラクティスを適用しないわけにはいきません。そのための最も効果的な方法は、ゼロトラストです。

Veeam Softwareについて

データレジリエンスにおけるNo. 1のグローバルマーケットリーダーであるVeeam®は、全てのビジネスが、必要なときに必要な場所ですべてのデータを確実に制御し、混乱の後に回復できるべきだと考えています。Veeamはこれを「根源的な回復力」と呼んでおり、お客様の実現をサポートする革新的な方法を生み出すことに力を注いでいます。Veeamソリューションは、データのバックアップ、データの復元、データの自由、データセキュリティ、データインテリジェンスを提供することで、データレジリエンスを強化することを目的に構築されています。Veeamを使用することで、ITリーダーやセキュリティリーダーは、アプリケーションやデータが保護され、クラウド、仮想、物理、SaaS、Kubernetesの環境全体で常に利用可能であることを知って安心できます。シアトルに本社を置き、30か国以上に事業拠点を構えるVeeamは、Global 2000の74%の企業も含め、全世界で55万社を超えるお客様を保護しており、これらの企業のビジネス継続性を確保しています。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をご覧になるか、LinkedIn（@veeam-software）およびX（@veeam）でVeeamをフォローしてください。

→ 詳細はこちらveeam.com/jp