# 最初の100日間
# – Veeam Data Platform

リーダーのための測定可能な回復力ガイド

# ほとんどの組織は自分たちが保護されていると想定していますが、実際にそれを検証した組織は少数です。

最近の調査では、90%のセキュリティリーダーが設定した目標内で復旧できると回答しました。しかし、ランサムウェア被害者のうち、データを完全に復元できた組織はわずか28%でした（出典：2026年データの信頼性と回復力レポート）。自信と実証された復元機能は同じものではなく、その間に生じるギャップこそが、ランサムウェアの勝利、監査の失敗、そして停止が危機へと発展する原因となります。

**90%**

**定義した目標期間内で復元できたと回答したセキュリティリーダーの割合**

**28%**

**データを完全に復元できたランサムウェア被害者の割合**

## 回復力は証明できてこそ真の価値をもたらすためです。

本ガイドでは、Veeam Data Platformの導入を戦略的な観点で捉えます。チームが技術的な導入マイルストーンを進める中で、本ガイドではそれらをリスクの軽減、獲得した機能、そして最終的に得られる証拠といったビジネス成果の面で評価します。

リスク許容度、復元へのコミットメント、ビジネス継続性に関する意思決定は貴社の判断です。本ガイドでは、貴社の責任範囲に加え、100日目までに取締役会や監査人、保険会社に自信を持って伝えられることについて解説します。

## 本ガイドで得られる内容：

1. 想定の保護とテスト済みの回復力を分ける5つの成果
2. CIO、CISO、CFOの役割における意義
3. 投資対象とすべき7つのユースケースと、それによってROIが向上するしくみ
4. 100日目以降の回復力を確認するための、チームに問うべき質問

# リスクからエビデンスへ：重要な5つの成果

これらは、Veeam Data Platformを導入する際に組織がコミットする5つの成果です。それぞれが漏洩を証拠へと変える一連のステップを表しており、これらを組み合わせることで、検証可能な回復力のある環境がどのようなものかを定義できます。

## 01. 導入済み

何が保護され、どこに保存されているか、またどの基準で保護されているかを正確に把握できます。想定はなく、プレッシャー下でもギャップは生じません。

## 02. 保護済み

すべての重要なワークロードは、貴社のビジネス継続性戦略に裏付けられた計画で保護されています。最も重要なときに抜けや漏れは一切ありません。

## 03. 強化済み

攻撃者は貴社の復元能力を破壊できません。イミュータブルコピーはローカルとオフサイトに存在するため、インシデントがどのように展開しても、クリーンなリストアポイントが保証されます。

## 04. 検証済みの復元可能性

復元が単なる主張ではなく、実際に機能することを証明できます。復元力がテスト済みで文書化され、取締役会、監査人、保険会社に提出できる状態です。

## 05. 運用化

回復力は、特定の個人や英雄的な行動に頼るものではありません。回復力とは、明確な責任、体系的な報告、そしてチームが維持可能な明確なサイクルによって成り立つものです。

# それぞれの役割への影響

## 最高情報責任者/最高技術責任者（CIO/CTO）

取締役会から、組織が重大なインシデントから復旧できるか問われた際にも、文書化された検証済みの回答がすでに存在します。停止リスクはもはや信頼や確信の問題ではなく、記録に基づくものです。

## 最高情報セキュリティ責任者（CISO）

インシデントが危機へと変わる前に、確認済みのクリーンなリストアポイントを確保できます。脅威インテリジェンスのスキャン、イミュータブルなコピー、そして文書化されたテスト結果によって、保険会社、監査人、法務チームが必要とする証拠を提供できます。

## 最高財務責任者（CFO）

想定の復元力ではなく、実証可能な復元力があれば、サイバー保険の適格性、更新条件、保険料の交渉をいずれも有利に進めることができます。調査によると、強化されたデータの回復力への投資を行っている組織が身代金を支払った割合は33%にとどまり、投資を行っていない組織では52%に上りました。Veeamへの投資は明確に定義されており、予測可能で、計画外停止による財務リスクの低減に直結します。

**33%**

**データの回復力への投資を強化している組織が身代金を支払った割合**

**52%**

**そうした投資を行っていない組織が身代金を支払った割合**

出典：2026年データの信頼性と回復力レポート。

# 引き出される価値

Veeam Data Platformがもたらす価値は、単一のロールやインシデントをはるかに超えて広範囲に影響を及ぼします。最初の100日間以降、貴社はハイブリッドインフラストラクチャ、クラウドスプロール、規制対応のプレッシャー、進化する脅威の状況など、現代のIT環境がもたらす真の複雑さに対応できる機能を活用できます。

**以下は、貴社の投資で対応できる7つのユースケースです。**

## 保護と復旧

インシデントが発生した際、対応の質は事前準備の質に完全に左右されます。これは、業界やインフラストラクチャに関係なく、すべての組織に必要なベースラインです。

1. **脅威の検出と対応：**Veeamはバックアップチェーンをスキャンしてマルウェアの兆候を確認し、リストア前にファイルの整合性を検証します。これにより、脅威が再び侵入することなくクリーンな状態で回復できます。文書化されたスキャン結果はインシデント対応プロセスに利用でき、保険会社の要件も満たします。
2. **クラウドへのディザスタリカバリ：**Veeamは、オンプレミスのインフラストラクチャに障害が発生すると、お客様が定義した復元目標の範囲内でクラウドターゲットにワークロードを移行します。貴社のチームは、プレッシャー下では十分に機能しない手動のプロセスではなく、テスト済みで実行可能な計画を備えることができます。

## 制御と準拠

規制によるプレッシャーとデータの主権性要件は拡大し続けています。データ保護戦略も時代の変化に対応していく必要があります。規制対象の業界で事業を行っている場合や監査サイクルが間近に迫っている際は、まずこの点に注力すべきです。

3. **管理、リスク、コンプライアンス：**Veeamなら、コンプライアンスおよび法務チームが必要とする形で、復元テスト結果、対象範囲のインベントリ、保持ポリシーの確認などの監査対応レポートを生成できるため、監査時に手作業で証拠を収集する必要がありません。
4. **データ主権：**Veeamは、バックアップデータの保存場所や処理場所を組織が管理できるようにし、復元機能を損なうことなく、複数の管轄区域にまたがるデータ所在地要件への対応を可能にします。

## 複雑な環境下での運用

最新のインフラストラクチャは1か所に存在するわけではありません。同様に、貴社の保護戦略も1か所に限定すべきではありません。移行中や、すでにマルチクラウドやハイブリッドSaaSを運用している場合は、そこに運用上のリスクが集中します。

5. **環境間におけるワークロードのモビリティ：**Veeamでは、ワークロードをオンプレミス、クラウド、エッジ環境間で移動する際に、保護も一緒に移動します。インフラストラクチャが変わっても保護が途切れることはありません。
6. **マルチクラウド保護：**Veeamはクラウドプロバイダー全体で一貫した保護と復元機能を提供し、ツールの断片化やプラットフォーム間の盲点による運用上のリスクを排除します。
7. **ハイブリッドSaaS：**SaaSアプリケーションに保存されている重要なデータはインフラストラクチャのワークロードとともに保護されるため、インシデント発生後に初めて気付くことの多い保護のギャップを事前に解消できます。

これらは将来的な機能や追加のアドオンではありません。これらは、組織が導入と運用開始を進める中で得られるものであり、それぞれが特定のリスクカテゴリを軽減し、困難な状況下でリーダーシップチームに自信をもたらします。もはやこうしたレベルの回復力が貴社に必要かどうかという問題ではなく、いかに迅速に達成できるかが重要です。

## 100日目はゴールではありません。ここがベースラインです。

## 回復力は一度きりのプロジェクトではなく、長期にわたる実践項目です。

Veeamは、Veeam DataAI Command Platform、実績のあるデータとAI信頼成熟度モデル、そして最初の導入から完全な回復力が実証されるまで貴社を導くうえで必要な技術的専門知識を提供します。あらゆる段階でVeeamが貴社を全面的にサポートいたします。

チームが「最初の100日間」技術ガイドを参照できることを確認し、導入範囲やスケジュール、期待事項についてすり合わせを行いましょう。

このレベルの回復力は長期的な目標ではなく、適切な導入計画があれば貴社ですぐに達成できるものです。

## 次の一手を進めましょう。

# 定期的にチームに問いかけるべき質問

- すべての重要なワークロードは保護されていますか？また、保護のギャップや障害が未対応のままになっていませんか？
- 実際の条件下で完全復元のテストを最後に行ったのはいつですか？その結果は文書化されていますか？
- もし今夜ランサムウェア攻撃を受けた場合、確認済みのクリーンなリストアポイントを特定し、身代金を支払うことなく復旧できるでしょうか？
- コンプライアンスおよび法務チームは、手作業を伴わずに監査証拠を提示できますか？また、弊社のアーキテクチャは現在の規制要件に適合していますか？
- バックアップ環境に管理者アクセスできる人物は誰で、最後にそのアクセス権限を見直したのはいつですか？

## Veeam Softwareについて

VeeamはデータとAIを託す信頼のパートナー。組織が自社のデータとAIを完全に理解し、保護し、回復力を確保することで、安全なAIの大規模な活用を加速できるよう支援しています。データの回復力とデータセキュリティ態勢管理の両方における市場リーダーとして、Veeamはアイデンティティ、データ、セキュリティ、AIリスクを収束させることを念頭に設計されています。Veeamは米国シアトルに本社を置き、30カ国以上にオフィスを展開し、世界中で55万以上の顧客を保護しています。その中にはFortune 500企業の82%も含まれます。詳細についてはveeam.com/jp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