Veeam Data Platform

最初の100日間

IT管理者のための実践的なオンボーディングガイド

コンテンツ

1. エグゼクティブサマリ

Veeam Data Platformは、ランサムウェア回復力と運用継続性を実現する組織の基盤です。このガイドは、ITチームが環境を体系的に運用し、成熟させるのを支援するために設計されています。「最初の100日間」という言葉を使っていますが、これはタイムラインの比喩にすぎません。すべての組織は異なり、進捗のスピードもさまざまですが、目標は同じです。初期設定から、より安全で、回復力が高く、リカバリ準備が整った状態へ移行することです。厳格な導入要件ではなく、実用的なマイルストーンと推奨される成果を重視して構成されているため、ご自身の環境やエディションに最も適した手順に集中できます。

2. 本ガイドの対象者

本ガイドは、Veeam Data Platformの導入、設定、および運用に関わる**IT管理者**を対象としています。仮想化インフラストラクチャ（例：VMware vSphere、Microsoft Hyper-V、またはVeeam Backup & Replicationがサポートするその他のハイパーバイザー）および基本的なWindows Server管理に精通していることを前提とします。Linuxの専門知識は不要です。

これは、範囲やタイムラインを管理する**ITマネージャー**、強化の状況を検証するセキュリティ担当者およびコンプライアンス関係者、そして「100日間」の成功がどのようなものかを定義することで、リーダーシップや調達チームにも共通の参考資料として役立ちます。

3. 100日目までに達成できること

100日目までに、停止リスクを軽減し、何があっても迅速かつ自信を持って復元できる、安定した、堅牢で、復元性が検証可能な環境を構築できます。

すべてのお客様は、以下のチェックポイントが満たされていることを確認できるようになります。

- **導入：**Veeam Backup & Replicationが稼働しており、接続された状態で、バックアップウィンドウに合わせてサイズ調整されている。
- **保護：**優先度の高いワークロードが定められたスケジュールで正常にバックアップされている。
- **強化：**イミュータビリティがローカルおよび／またはオフサイトに適用されており、ランサムウェアから保護されている。
- **検証済みの復元性：**リストアテストが完了し、文書化され、目標復旧時間および目標復旧時点（RTOとRPO）の目標値に対応している。
- **運用の定着：**監視、アラート、レポート、およびリカバリ手順書が確立され、管理責任が明確である。

4. ロードマップ概要

本ガイドは4つの段階に分かれており、それぞれが100日間の成果に向けて構築されています。

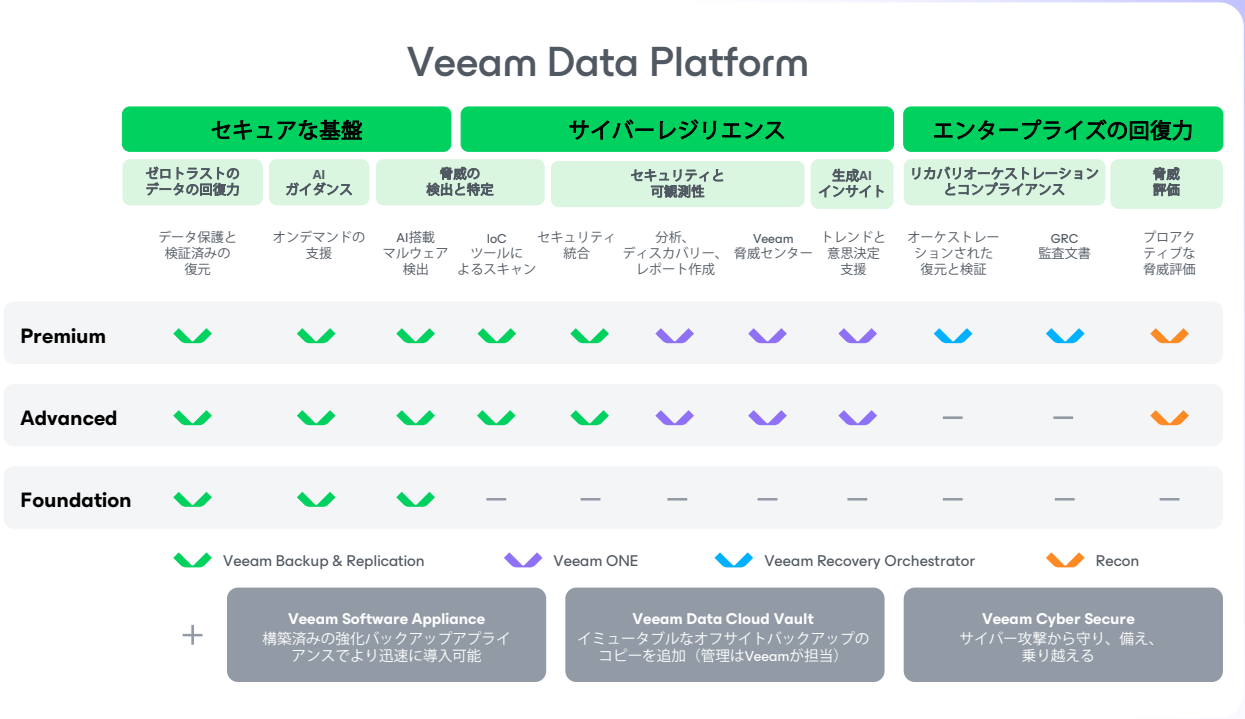
フェーズ	名前	タイムライン	重点
フェーズ1	基礎	1〜14日	環境のサイジング、Veeam Software Appliance（さらに、該当する場合はVeeam Infrastructure Appliance）の導入、初回バックアップジョブの実行、Veeam Recovery Orchestratorの準備。
フェーズ2	最適化	15〜45日	・アプリケーション認識処理。 ・バックアップコピーのジョブ。 ・Veeam Data Cloud Vaultオフサイトレベル。 ・Veeam Recovery Orchestratorセットアップ（Premium）。
フェーズ3	データとビジネスの回復力	46〜75日	保護対象範囲のギャップを解消し、Reconを有効化して、ランサムウェアへの準備を整え、チューニングを行い、オーケストレーションプランを構築（Premium）。
フェーズ4	価値の証明	76〜100日	オーケストレーションされた復元テスト、レポート作成、ドキュメントアーキテクチャ、そして継続的な健全性を維持。

本ガイドの使い方

- マイルストーンを順番に進めてください。特に、ローカルリポジトリやジョブが安定する前にScale-out Backup Repository（SOBR）やVaultの設定に進むと、リストア時にギャップが生じることが多くあります。
- タイムラインは柔軟です。日数はあくまで目安であり、厳密な締め切りではありません。小規模な環境では、フェーズ1を1週間以内に完了できる場合があります。より複雑な環境では、後のフェーズでより多くの時間が必要になる場合があります。
- 意思決定ポイントを活用してください。アーキテクチャの選択肢（例：導入経路やリポジトリ戦略）が発生した場合は、利害関係者と調整し、決定事項を文書化してから続行してください。
- 該当しないものはスキップしてください。その理由を記録してください。お使いのエディションにVeeam ONEまたはVeeam Recovery Orchestratorが含まれていない場合、それらのマイルストーンは明示されます。同様に、Veeam Software ApplianceとVeeam Vaultの手順はオプションの手順であり、これらのモジュールが導入されている場合にのみ該当します。

Veeam Data Platformの概要

導入やその方法に進む前に、まずはVeeam Data Platformに含まれる内容を簡単に振り返ってみましょう。Veeam Data Platformは3つのエディションで提供されており、上位エディションは下位エディションの機能をすべて網羅しています。



すべてのコンポーネントの説明については、「付録：クイックリファレンス、主要コンポーネント」を参照してください。

少し時間を取って、お使いのエディションを確認しましょう。

先に進む前にエディションを確認し、含まれている内容をすべて把握してください。データ保護において、未使用の機能は単なる価値の浪費ではなく、いずれ露呈するギャップです。

さらに、以下のモジュールはすべてのエディションで利用可能です。

- **Veeam Software Appliance：** インフラストラクチャのセットアップを簡素化し、セキュリティ態勢を強化する、強化済みでWindows不要の導入プラットフォーム。Linuxの専門知識は必要ありません。
- **Veeam Vault：**イミュータブルなオフサイトバックアップストレージがサービスとして提供され、データをランサムウェアや意図せぬ削除から保護します。
- **Veeam Agents：**Veeam Agentsは、物理サーバー、エンドポイント、および未対応の仮想マシン（VM）プラットフォームに、Veeam品質のイメージレベルのバックアップと復元を提供するソフトウェアエージェントです。これらはVeeam Backup & Replicationコンソールから一元管理されます。

回復力への道はここから始まります

今後100日間で、導入から堅牢かつ確実に復元可能な環境の構築まで、マイルストーンごとに推量の余地なく着実に進めていきます。

フェーズ1 **基礎** **1日〜14日**	フェーズ2 **最適化** **15日〜45日**	フェーズ3 **データおよびビジネスの回復力** **46日〜75日**	フェーズ4 **価値の証明** **76日〜100日**
M1：サイジングと計画	M4：アプリケーション認識処理	M7：対象範囲のギャップ解消	M10：復元テスト
M2：Veeam Software Applianceの導入とインフラストラクチャの展開	M5：バックアップのコピー、SOBR、Vault	M8：ランサムウェアへの備え	M11：レポート作成と文書化
M3：最初のバックアップジョブ	M6：監視、アラート、オーケストレーターのセットアップ	M9：パフォーマンスチューニングとオーケストレーションプラン	M12：継続的な健全性の維持

フェーズ1 • 1〜14日

基礎

目標：インフラストラクチャのサイジング、導入、最初のワークロードの保護。

マイルストーン1：サイジングと計画

何かを展開する前に、サイジングに時間を費やしてください。サイジング不足のインフラストラクチャは、最初の100日間におけるバックアップウィンドウの遅延やRPO未達の最も一般的な原因です。

ワークロードインベントリ

- VMおよびワークロードの総数、データフットプリント（総プロビジョニング容量と使用容量）、および推定日次変更率を記録します。
- 最も重要なワークロードを特定してください。これらがRPOおよびRTOの目標を左右します。
- Veeam Agentが必要となる物理ワークロード（例：Windows/Linuxサーバー）を記録してください。

Veeam Software Applianceのサイジング

- Veeam Software Applianceは、Veeam Backup & Replicationがあらかじめインストールされた状態で提供されるため、主なサイジングの決定事項は、どのホスト上で実行するかです。
- 中小企業（SMB）の最小要件：8 vCPU / 16 GB RAM（各同時ジョブにつき500 MB RAMを推奨）
- Veeamサイジング計算ツール（calculator.veeam.com/jp）を使用して、ワークロード数やデータフットプリントに対するリソース要件を検証します。
- 導入形式として、VMware vSphere用のOVAまたは物理サーバーや他のハイパーバイザー用のISOを選択してください。いずれにしても、Linuxの経験は必要ありません。

ストレージアーキテクチャ：経路を選択してください

この段階でのストレージの選択が、フェーズ1と2の進め方に影響します。SMB向けには、3つの推奨される経路があります。

経路A：Veeam Software Appliance + Veeam Infrastructure Appliance（強化リポジトリとして）+ Vault：これが推奨される基本構成です。この経路では、Linuxの専門知識を必要とせずにローカルのイミュータブルリポジトリを提供し、さらにVaultを介してオフサイトおよび物理的に隔離されたイミュータブルコピーを作成できます。

経路A：Veeam Infrastructure Applianceを介して提供されるVeeam強化リポジトリを使用する理由

Veeam強化レポジトリはイミュータブルなローカルバックアップを提供します。保持期間中は、ランサムウェアによってバックアップを暗号化したり削除したりすることはできません。

従来、イミュータブルなLinuxリポジトリを実現するには、専用のLinuxサーバーと手動によるOSの強化が必要でした。Veeam Infrastructure Applianceはその障壁を完全に取り除きます。強化済みの状態で出荷され、OVAまたはISOから展開されて、起動や保守にLinuxの専門知識は必要ありません。

Veeam Infrastructure Applianceは、シングルロールのアプライアンスです。各インスタンスは、Veeam強化リポジトリまたはバックアッププロキシのいずれかとして動作します。専任のLinux管理者や既存のイミュータブルストレージを持たないSMBの場合は、Veeam Infrastructure Applianceが提供するVeeam強化リポジトリがローカルのイミュータビリティを実現するうえで推奨される経路となります。

最大限の保護を実現するには、Veeam Infrastructure Applianceを物理ハードウェアに導入することが推奨されます。Veeam Infrastructure Applianceを仮想アプライアンスとして実行した場合は、ハイパーバイザーの攻撃対象領域を継承します。ファイルシステムレベルのイミュータビリティはバックアップファイルをOS内の攻撃から保護しますが、ハイパーバイザー管理者はイミュータブルファイルの保護下でもVMを削除することができます。

経路B：Veeam Software Appliance + Veeam Data Cloud Vault：
Veeam Backup & Replicationは、バックアップをVeeam Software Appliance上のローカルリポジトリに直接書き込み、Veeam Vaultにオフサイトコピーを保存します。これは、ローカルストレージ管理を最小限に抑えたい小規模企業や支店オフィス、さらにVaultを利用してオフサイトで論理的かつ物理的に隔離されたイミュータブルコピーを確保したい場合に最適です。念のため、Veeam Software Applianceを仮想インフラストラクチャ上に導入した場合、オンサイトイミュータビリティの代わるものとしては不十分であることに注意してください。

経路B：Veeam Software ApplianceとVaultを使用する理由

経路Bは、ストレージ管理を最小限に保ちます。Veeam Backup & Replicationは、バックアップをVeeam Software Appliance上のローカルリポジトリに保存し、その後バックアップコピーのジョブによってオフサイトのVaultに複製します。

Veeam Software Applianceのローカルストレージはデフォルトでイミュータブルなため、経路Bでもオンプレミスのランサムウェア対策が可能です。製品として正式なVeeam強化リポジトリではないため、Veeam Infrastructure Appliance専用のハードウェアがある場合は経路Aが最も堅牢な選択肢ですが、ハードウェアがない場合は経路Bが適切です。経路Aと同様に、Veeam Software Applianceを仮想アプライアンスとして稼働させる場合、ハイパーバイザー層で削除される可能性があります。そのため、可能な限り物理ハードウェア上に導入してください。

経路BではVeeam Infrastructure Applianceのステップを完全にスキップします。この経路を選択した場合は、マイルストーン2（Veeam Software Applianceの導入）から、マイルストーン5（Vaultへのバックアップコピーのジョブ）に直接進んでください。

経路C：Veeam Software Appliance ＋ 既存のNAS/Windowsリポジトリ ＋ Vaultまたはサードパーティオフサイトストレージ：
既存のストレージインフラストラクチャを活用しますが、追加の設定なしではローカルの堅牢性が低くなります。これは、顧客が既存のVeeam Cloud & Service Provider（VCSP）パートナーや、すでに利用可能な代替オフサイトストレージの活用を希望する場合に有用です。

すべての経路に共通：

- バックアップトラフィックを専用のVLANまたはNICに分離して、バックアップデータを本番ネットワークから切り離すことを検討してください。
- 導入前にソケット/ワークロードのライセンス範囲を確認してください。

マイルストーン2：Veeam Software Applianceの導入とインフラストラクチャの展開

Veeam Software Applianceを導入する

- Veeamカスタマーポータル（my.veeam.com）から、Veeam Software ApplianceのOVA（VMware vSphere用）またはISO（物理サーバーや他の対応ハイパーバイザー上のVM用）をダウンロードします。
- OVAの場合：VMware vSphereにインポートし、起動します。Veeam Backup & Replicationは、初回起動後に管理インターフェイスからアクセス可能になります。
- ISOの場合：ISOからターゲットサーバー（物理サーバー、またはその他のサポート対象ハイパーバイザー上のVM）を起動し、セットアップウィザードに従ってください。Veeam Backup & Replicationは自動的にインストールされます。
- Veeam Software Applianceの初期設定ウィザードを完了し、ホスト名、ネットワーク設定、管理者ログイン情報を設定します。

インフラストラクチャをVeeam Backup & Replicationに接続する

- 仮想化プラットフォームをVeeam Backup & Replicationのインベントリ（「バックアップインフラストラクチャ」>「管理対象サーバー」）に追加します。
- 少なくとも1つのバックアッププロキシを追加します。小規模な環境では、Veeam Software Applianceを初期プロキシとして機能させることができます。
- VMware環境の場合は、ホットアド転送モードを構成します。プロキシVMはSCSI経由でソースディスクをマウントし、直接読み取ることで、ESXi管理ネットワーク経由の遅いNBD経路を回避します。

Veeam Infrastructure Applianceを導入する（経路A）

- VeeamカスタマーポータルからVeeam Infrastructure ApplianceのOVAまたはISOをダウンロードします。
- Veeam Software Applianceと同じOVA/ISOプロセスを使用して導入します。設定ウィザードで、ターゲットロールとして強化リポジトリまたはバックアッププロキシを選択します。
- 導入後、Veeam Infrastructure ApplianceをVeeam Backup & Replicationに管理対象サーバーとして追加し、バックアップリポジトリまたはプロキシとして設定します。
- 強化リポジトリの役割の場合は、Veeam Backup & Replication（「バックアップインフラストラクチャ」>「バックアップリポジトリ」）でリポジトリを追加し、イミュータビリティの保持期間を設定します。
- 経路Bまたは経路Cを使用している場合、Veeam Infrastructure Applianceは不要なため、このセクションをスキップしてください。

Veeam Software Appliance が担当する内容

Veeam Backup & Replicationはあらかじめインストールされており、すぐに構成できます。OSの手動セットアップ、ソフトウェアのインストール、導入前のパッチ適用は必要ありません。

Veeam Software Applianceは初期強化された状態で出荷され、不要なサービスは無効化され、OSはロックダウンされ、セキュリティのベストプラクティスがデフォルトで適用されます。

VMware vSphereにOVAとして導入するか、物理サーバーでISOを起動するか、またはVeeamがサポートするその他のハイパーバイザー上のVM内で起動します。Linuxの経験は必要ありません。

Veeam ONEをインストールする

- Veeam ONEはWindows用の個別のインストーラーです。現時点では、アプライアンスモデルには同梱されていません。
- Windows Server VMまたは物理ホストにVeeam ONEをインストールします（Veeam ONE導入ガイドの最小要件を参照）。
- セットアップウィザードでVeeam ONEをVeeam Backup & ReplicationおよびvCenter/Hyper-Vホストに接続します。
- インストール後すぐにSMTP/メール通知設定を行ってください。アラートは1日目からアクティブにする必要があります。

マイルストーン3：最初のバックアップジョブ

- プライマリハイパーバイザー向けに最初のバックアップジョブを作成してください。Veeam強化リポジトリ（経路A）、Veeam Software Applianceのローカルリポジトリ（経路B）、または既存のNAS/Windowsリポジトリ（経路C）をターゲットに指定します。
- 開始時の保持ポリシーを適切に設定します：日次リストアポイント14個、週次4個、月次3個（GFS）。
- 非ピーク時間帯にジョブを実行するようにスケジュールし、他の保守時間帯と競合しないことを確認します。
- ジョブを初回は手動で実行し、完了まで監視してください。
- 警告やエラーがないことを確認してから、フェーズ2に進んでください。

最初のリストアテスト — 必ず実施してください！

フェーズ2に進む前に、クリティカルではないVMに対してInstant VM Recoveryを実行し、復元力を確認してください。

リストア可能であることを確認するまで、保護は確立されていないと考えましょう。確認は数分で完了し、後の多大な労力と苦労を回避することができます。

Veeam Infrastructure Applianceが担当する作業

Veeam Software Applianceと同様に、Veeam Infrastructure Applianceは、割り当てられたロールに合わせて事前に強化・設定された状態で提供されます。導入後はLinuxの管理が不要です。

単一のVeeam Infrastructure Applianceは、強化リポジトリまたはバックアッププロキシのいずれか一つのロールのみを担います。両方が必要な場合は、アプライアンスを2台導入してください。

導入形式はVeeam Software Applianceと同じで、VMware vSphere用はOVA、物理サーバー用および他のサポートされているハイパーバイザー用はISOです。

フェーズ2 • 15〜45日

最適化

目標：環境全体にわたる一貫した保護、オフサイトコピー、可視性。

マイルストーン4：アプリケーション認識処理

アプリケーション認識処理により、クラッシュ整合性バックアップもアプリケーション整合性を確保できるようになります。これは、SQL Server、Oracle、Exchange、Active Directory といったトランザクションワークロードやその他の該当するワークロードにとって不可欠です。

- WindowsやLinuxのアプリケーションサーバーを対象としたバックアップジョブでゲスト処理を有効化してください。
- SQL Server、Oracle、Exchange、Active Directoryドメインコントローラーおよびその他の適用可能なワークロード向けにアプリケーション認識処理を設定してください。
- 必要に応じて、復元のニーズに合わせてトランザクションログの切り捨てポリシーを設定してください。
- 最初のアプリケーションを認識したジョブの実行後、リストアポイントがVeeam Backup & Replicationでアプリケーション整合性としてマークされていることを確認します。
- Veeam Explorer for Microsoft SQL Serverを使用して、SQLデータベースのアイテムレベルのリストア（または該当するワークロード）をテストし、エンドツーエンドのアプリケーション復元が機能することを確認します。

マイルストーン5：バックアップコピーとVault

このマイルストーンによって、3-2-1戦略が完成します。プライマリリポジトリ上のローカルコピーに加え、オフサイトのイミュータブルコピーが含まれます。これは、バックアップ環境のアーキテクチャにおける中心的な要素です。

Vaultを接続する

- Vault を Veeam Backup & Replication のオブジェクトストレージリポジトリとして追加してください（「バックアップインフラストラクチャ」>「オブジェクトストレージリポジトリ」）。
- Veeam発行のログイン情報で認証し、リージョンを選択します。
- イミュータビリティが有効になっていることを確認します。

バックアップコピージョブ

- GFS保持ポリシーを使用して、長期間のリストアポイントをオフサイトで維持するバックアップコピーのジョブを設定してください。
- オフサイトコピージョブが完了・成功したことを確認し、Veeam Backup & Replication上でVaultオブジェクトにイミュータビリティフラグが表示されていることを確認します。
- フェーズ2の完了を宣言する前に、Vaultからテストリストアを実行して、オフサイトコピーが読み取り可能であることを確認します。

経路C：オフサイトターゲットオプション

経路Aと経路Bはどちらもオフサイトコピー先としてVaultを指定しています。経路Cでは、Vaultまたは既存のVCSPやサードパーティ製のオフサイトリポジトリを使用することもできます。Vaultに保存されているすべてのバックアップデータには、デフォルトでイミュータビリティが適用されます。Vault以外のオフサイトを利用する場合は、そのリポジトリでイミュータビリティまたはオブジェクトロックが設定されていることを確認してください。

マイルストーン6：監視、アラート、オーケストレーターのセットアップ

- Veeam ONEでアラーム通知先を設定する：ジョブの失敗やSLAの未達成時にメールアラートを送信します。
- Veeam ONEで営業時間を設定し、SLAの計算が業務スケジュールに合うようにします。
- デフォルトのアラームしきい値を確認する：環境に関係のないアラームを無効または調整して、アラート疲れを回避します。
- 最初のVeeam ONEレポートを実行する：保護済みのVMに関するレポートとジョブセッションレポート。
- 保護されていないVMレポートを確認し、特定されたギャップがあれば対処してから、フェーズ3に進みます。

Veeam Recovery Orchestratorのインストール（Premiumのみ）

お使いのエディションがFoundationまたはAdvancedの場合は、このセクションをスキップしてください。Veeam Recovery Orchestratorは、Veeam Data Platform Premiumにのみ付属しています。

- Veeam Recovery OrchestratorはWindowsベースの独立したインストーラーです。Veeam ONEと同じWindowsホスト上で共存させることも、独立したホスト上で実行することもできます。
- Windows Server VMまたは物理ホストにVeeam Recovery Orchestratorをインストールします。Veeam Recovery Orchestratorの導入ガイドで最小要件をご確認ください。
- セットアップウィザードの途中で、Veeam Recovery OrchestratorをVeeam Backup & Replicationインスタンスに接続し、既存のバックアップチェーンを把握できるようにします。
- Veeam Recovery OrchestratorをvSphere、Hyper-V、またはMicrosoft Azureに接続し、計画された実行時にVMを起動して、ネットワークを正しく割り当てられるようにします。
- 必要に応じて、Veeam Recovery OrchestratorをVeeam ONEに接続することで、より豊富な監視データやDataLabベースの検証が利用できます。
- Veeam Data Platform Premiumライセンスを適用して、Veeam Recovery Orchestratorを有効化します。
- 計画された実行通知が1日目から機能するようにSMTP/メールを構成します。

フェーズ3 • 46〜75日目

データおよびビジネスの回復力

目標：保護のギャップを埋め、RTO/RPOを向上させ、ランサムウェア回復力を強化する。

マイルストーン7：対象範囲のギャップ解消

- 他の調整を行う前に、Veeam ONEで保護対象外VMレポートを実行し、すべての未保護ワークロードに対処します。
- 必要に応じて、Veeam Agent for Microsoft WindowsまたはVeeam Agent for Linuxを使用して、物理ワークロードへの保護を拡張します。
- ジョブスケジュールの競合を確認し、プロキシやリポジトリのリソース競合を防ぐために開始時間をずらしてください。
- RPOコンプライアンスを検証してください：すべての重要なVMが目標リカバリウィンドウ内にリストアポイントを生成していますか？
- 定義したバックアップウィンドウ内にすべてのジョブが完了していることを確認します。

マイルストーン8：ランサムウェアへの備え

- Veeam Data Platform AdvancedおよびPremiumには、補完的な2つのセキュリティツールが付属しています。1つ目はReconです。これは、Veeamの脅威インテリジェンスサービスで、実際のインシデント対応から抽出されたIOCや新たなデータを提示します。2つ目は、Veeam Backup & Replicationの製品内アクションである「バックアップのスキャン」です。「バックアップのスキャン」機能は、既存のバックアップチェーンをマルウェアの兆候について調査し、ファイルの整合性を検証します。隔離されたネットワークやVMの起動を必要としません。

バックアップのスキャンを実行する：

- Veeam Backup & Replicationの「Home」＞「SureBackup」から、SureBackupジョブを作成してください。SureBackupはスケジュールされたジョブとして動作し、隔離ネットワークやスキャン自体のVM起動を必要とせず、一連の流れでバックアップをマルウェア、署名ベースの脅威、ファイル整合性についてスキャンできます。
- 対象となるバックアップジョブをリンクして、SureBackupジョブが経時的にすべてのデータを網羅できるようにします。これにはVeeam強化リポジトリ（経路A）、Veeam Software Appliance ローカルリポジトリ（経路B）、既存のNAS/Windowsリポジトリ（経路C）、Vaultが含まれます。

2台目のVIAによるプロキシ容量の追加

バックアップジョブの実行速度が遅い場合やバックアップウィンドウを超過している場合は、プロキシロールで2つ目のVeeam Infrastructure Applianceを展開してください。

事前強化アプライアンスモデルにより、迅速な対応が可能です。OVAまたはISOを導入し、Veeam Backup & Replicationに登録すると、ジョブは両方のプロキシ間で自動的に負荷分散され、手動でのプロキシ設定は不要です。

- 検証オプションで、Veeam Threat Hunter（またはサードパーティ製のアンチウイルスソリューション）によるマルウェアスキャンを有効化し、バックアップ内容を最新の脅威署名データベースと照合してください。
- 同じ検証オプションで、ファイル整合性チェックを有効化し、CRCチェックによってバックアップファイルを検証し、破損ブロックを特定します。
- SureBackupジョブをスケジュールし、セッション結果を定期的に確認してください。リカバリに使用する前に、フラグ付きのリストアポイントを調査しましょう。
- 「ホーム」>「バックアップ」に移動し、バックアップジョブを展開してワークロードを選択し、バックアップタブから「バックアップのスキャン」を選択します。

Reconのインストール

- Reconバイナリを、任意のWindowsベースのVeeamインフラストラクチャホストまたは任意のLinuxホストにインストールします。
- Reconは、該当するWindowsドメインコントローラーにもインストールできます。
- ReconはVeeam Infrastructure Applianceにはインストールできません。Veeam Infrastructure Appliancesは単一の役割を担うとともに事前に強化済みです。

イミュータビリティ監査

- Veeam Infrastructure Applianceの強化リポジトリのイミュータビリティ期間が、適切な保持期間に設定されていることを確認します。
- バックアップの暗号化設定を確認し、バックアップジョブの静止時の暗号化を未設定の場合は有効にします。
- Veeam ONEの「イミュータブルワークロード」レポートを実行し、ワークロードのバックアップイミュータビリティターゲットを測定・特定します。

ランサムウェアリカバリの備え

どのVMを優先的にリストアするか、どのリストアポイントから、どのターゲットへリストアするかを含めた簡易的なリカバリ手順書を作成してください。

Vaultで、少なくとも1つのクリーンな感染前のリストアポイントを復旧基準として特定してください。

イミュータブルコピーは、イミュータビリティ期間中に上書きや暗号化されることはありません。これがセーフティネットです。

経路A：Veeam強化リポジトリ + Vault

経路B：Veeam Software Applianceのローカルストレージ + Veeam Vault。

経路C：Vault + ローカルリポジトリ（イミュータビリティが設定されている場合）

マイルストーン9：パフォーマンスチューニングおよびオーケストレーションプラン

- Veeam Backup & Replicationのジョブ統計情報でプロキシのスループットを確認します。ジョブがボトルネックになっている場合は、プロキシロールで2台目のVeeam Infrastructure Applianceを展開します。
- バックアップ転送モードが最適であることを確認してください。利用可能な場合は、VMwareのホットアドまたはダイレクトストレージアクセスを選択してください。
- すべてのバックアップジョブが、定義した保守ウィンドウ内に完了したことを検証します。
- Veeam ONEのパフォーマンスチャートを確認し、変更率が異常に高いVMを特定します。専用ジョブやスケジュール調整が必要となる可能性があるVMを見極めましょう。

初期オーケストレーションプランの構築（Premiumのみ）

お使いのエディションがFoundationまたはAdvancedの場合、またはVeeam Recovery Orchestratorでサポートされているハイパーバイザーを使用していない場合は、このセクションをスキップしてください。

Veeam Recovery Orchestratorは、手動による復元ランブックを実行可能な計画に変換します。計画を策定することで、フェーズ4では手動リストアを再実行することなく、自動的に復元力を証明できます。

- オーケストレーションされた復元が必要なレベル1アプリケーションスタックを特定します（例：ドメインコントローラー、主要なデータベース、主要なアプリケーションサーバー）。
- Veeam Recovery Orchestratorで、これらのスタックの1つを対象とする最初のリストアプランを作成します。
- VMの起動順序と依存関係を定義し、前提条件（例：DC、DNSなど）が依存サービスより先に起動するようにします。
- 復元ターゲット（ホスト、クラスター、データストアなど）を設定し、実際のフェイルオーバーのために本番ネットワークをマッピングし、テスト用に隔離されたネットワークをマッピングします。
- 計画のRTOおよびRPOの値を設定し、Veeam Recovery Orchestratorが時間の経過によるズレを警告できるようにします。
- 計画を保存し、フェーズ3の完了を宣言する前に、利害関係者と自動生成されたドキュメントを確認します。

フェーズ4 • 76〜100日

価値の証明と実運用

目標：復元力を検証し、運用の健全性を確立し、ROIを実証する。

マイルストーン10：復元テスト

重要なのは、リストアできるバックアップのみです。フェーズ4は、文書による証拠を用いて、環境がRTOおよびRPOの要件を満たしていることを証明する段階です。

SureBackupとバックアップのスキャン

- 最も重要なVM（例：ドメインコントローラー、主要なアプリケーションサーバー）を対象とするSureBackupアプリケーショングループを設定します。
- SureBackupジョブを実行して起動検証を自動化し、VMが正常に起動し、ハートビート、ping、アプリケーションレベルのテストに正常に動作することを確認します。
- 簡易な検証の場合は、Scan Backupを実行してください。VMを起動することなくファイルの整合性を検証し、脅威をチェックする機能は、小規模環境ではSureBackupを補完または代替する手段として実用的です。

きめ細かいリストアおよびフルリストアのテスト

- ファイルレベルのリストアをテストし、個別のファイルをバックアップからテスト場所に復元します。
- Veeam Explorersを使用して、SQLデータベースオブジェクトやActive Directoryユーザーをリストアし、アプリケーションアイテムの復元テストを実施します。
- VaultからVMの完全リストアをテストし、オンプレミスの全消失をシミュレーションしてオフサイトコピーを検証します。
- 実際の復旧時間を記録し、RTO目標と比較し、結果を文書化します。

復元テストのベストプラクティス

必ず本番環境以外のターゲットにリストアし、テスト中は決して稼働中のワークロードを上書きしないでください。

何がリストアされたか、どのリストアポイントからリストアされたか、どのターゲットにリストアされたか、そしてリストアにかかった時間を文書化します。

これらの結果が復元力の証拠となります。それらをコンプライアンスレビューや監査、管理報告のために保存してください。

オーケストレーションプランの実行（Premiumのみ）

お使いのエディションがFoundationエディションまたはAdvancedエディションの場合、またはお使いのハイパーバイザーがVeeam Recovery Orchestratorに対応していない場合は、このセクションをスキップしてください。フェーズ3で最初のリストアプランを作成しましたが、フェーズ4でその本領が発揮されます。

- 計画に対して無人準備テストを実行してください。Veeam Recovery Orchestratorは、VMを起動することなく、リストアポイントのアベイラビリティ、ターゲット容量、設定のズレを確認します。
- 計画に対してDataLabテストを実行してください。Veeam Recovery Orchestratorはアプリケーションスタックを隔離ネットワークにリストアし、ライブVMに対してアプリケーションレベルの検証を実施します。
- DataLabの実行から実際の復旧時間を記録し、フェーズ3で設定したRTO目標と比較します。
- Veeam Recovery Orchestratorのリカバリ準備レポートを生成し、他のリカバリテストの結果とともにアーカイブします。
- Veeam Recovery Orchestratorプランで対象とされないワークロードについては、前述の手動リストアテストを実施してください。

マイルストーン11：
レポート作成と文書化

月次Veeam ONEエグゼクティブサマリレポートを作成し、経営陣と共有して、バックアップの正常性と保護対象範囲を実証します。

- 保護対象ワークロードのインベントリレポートをエクスポートして、対象範囲を確認します。
- ジョブ一覧、リポジトリ構成、Veeam Infrastructure Applianceの役割、スケジュール、保持ポリシーなどを含む最終的なバックアップアーキテクチャを文書化します。
- Veeam Vaultのストレージ消費量を確認し、利用状況が予定された予算と一致しているか確認します。
- 復元テストの結果をアーキテクチャドキュメントと一緒にアーカイブしてください。
- Premiumのみ：Veeam Recovery Orchestratorのリカバリ準備レポートを毎月生成してください。ワークロードや依存関係の変化に合わせて経時的に準備スコアを追跡してください。
- Premiumのみ：Veeam Recovery Orchestratorで生成された計画ドキュメントをアーキテクチャドキュメントと一緒にアーカイブします。計画に変更があればVeeam Recovery Orchestratorがこれを自動的に再生成するため、計画が更新された際は再アーカイブしてください。

マイルストーン12：継続的な健全性の維持の頻度

100日目までに、環境は安定しており、完全に文書化されている必要があります。これらの習慣を通じて以下の状態を維持できます。

- **週次：**Veeam ONEのジョブヘルスダッシュボードを確認し、障害や警告があれば速やかに対処してください。
- **週次：**Veeam ONEの未保護VMレポートを確認し、新しいものがあれば保護対象に加えてください。
- **月次：**エグゼクティブサマリおよび保護済みVMレポートを作成し、結果を共有します。
- **月次：**Vaultのストレージ使用量と増加率を確認します。予算内のフットプリントを超える傾向や、今後の保持の増加が見込まれる場合は、警告を出します。
- **月次：**保持期間が現在も有効で、変更されていないことを確認します。
- **四半期次：**文書化されたリカバリテストを実施し、ワークロードの種類をローテーションします。
- **四半期次：**各リポジトリに対してバックアップのスキャンを実行し、マルウェアの署名やファイル整合性の異常をチェックします。
- **四半期次：**Veeam Backup & Replication、Veeam ONE、およびVeeam Recovery Orchestrator（Premiumのみ）の管理者権限を持つユーザーを見直します。役割を変更したユーザーや退職したユーザーのアクセス権を削除します。
- **四半期次（Premiumのみ）：**Veeam Recovery OrchestratorのDataLabテストを実施し、実行するオーケストレーションプランを定期的にローテーションします。
- **四半期次（Premiumのみ）：**前回のレビュー以降に計画が変更された場合は、Veeam Recovery Orchestratorの計画ドキュメントを再生成してアーカイブします。
- **月次：**Recon脅威インテリジェンスの更新を確認し、関連する署名またはルールを環境に適用します。

- **年次：**バックアップアーキテクチャと保持ポリシーを、現在のビジネス要件や新たなコンプライアンス義務に照らして見直します。
- **年次：**Vaultから完全なリストアを実行し、オフサイトコピーが包括的に復元可能であることを検証します。結果を文書化します。
- **年次：**送信中および転送後の暗号化設定を確認し、セキュリティポリシーに従ってキーをローテーションします。
- **必要に応じて：**Veeamコンポーネント（例：Veeam Software Appliance、Veeam Infrastructure Appliance、Veeam ONE、Veeam Agent、該当する場合はVeeam Recovery Orchestrator）の更新計画を策定し、リリース通知を購読してください。
- **更新前：**ライセンスの使用状況、成長予測、エディションの適合状況を見直します。ご利用中のエディションの機能では対応しきれなくなった場合は、この機会にVeeamの営業担当者にアップグレードについてご相談ください。

最終推奨事項

これで完了です！

100日間で、導入から本格的なデータ保護環境の運用へと移行しました。ワークロードは保護され、バックアップが強化されてイミュータブルになり、理論上だけでなく実際のレコードとして復元できることが証明されました。

決して些細なことではありません。

これからは、構築から保守へと焦点が移ります。リストアを定期的に検証し、環境の変化に応じてポリシーを最適化し、監視・レポートの定期運用でギャップを早期に発見してリスクを防ぎます。マイルストーン12で確立した、週次・月次・四半期次・年次の運用健全性維持のための定期的な作業サイクルは、100日目以降も環境の健全性を維持する基盤となります。これらを継続し、主体的に管理し、組織の成長に合わせて進化させてください。

100日目がゴールではないことに留意してください。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。

管理者ロールを常に最新の状態に保ち、適切な担当者が適切なアクセス権を持てるようにしましょう。また、Veeamのリリースノートやセキュリティアドバイザリを引き続きご購読になり、最新の情報を常に確認してください。

あなたは一人ではありません

Veeamのコミュニティ、学習リソース、技術チームが皆様の前進を支援します。環境の成長と拡大に合わせて、コミュニティやリソースをぜひご活用ください。厳選されたリソースのリストは、本ガイドの付録に記載されています。

ご質問や次のステップについては担当のお客様サクセスアカウントマネージャーまで、技術的なご質問はVeeamテクニカルサポートまでご連絡ください。

付録：クイックリファレンス

主要コンポーネント：
Veeam Data Platform

- **Veeam Software Appliance：**Veeam Backup & Replicationがプリインストールされた強化済みのアプライアンス。OVA（VM）またはISO（物理）として導入できます。これは、すべてのSMB導入で推奨される開始点です。
- **Veeam Infrastructure Appliance：**強化済みのアプライアンスで、専用のバックアッププロキシまたは強化リポジトリとして導入されます。Linuxの専門知識がなくても、アプライアンスごとに1つのロールでローカルのイミュータビリティを実現します。
- **Veeam Backup & Replication：**Veeam Software Applianceでホストされるコアバックアップエンジン。ジョブ、リポジトリ、プロキシ、およびリカバリ操作を管理します
- **Veeam ONE：**監視、アラート、レポート作成を行います。個別にWindows環境へインストールされ、Veeam Backup & Replicationおよびハイパーバイザーと連携し、全スタックの可視化が可能です。
- **Recon：**Veeamの脅威インテリジェンスサービスです。実際のインシデント対応から得られた、侵害の兆候（IOC）、脅威のシグネチャ、新たなキャンペーンデータを検出・提示します。Veeam Data Platform Advancedエディションに含まれています。
- **バックアップコンテンツのスキャン：**これは製品内機能であり、既存のバックアップチェーンを既知のマルウェアの署名でスキャンし、隔離されたネットワークやVMの起動を必要とせずにファイルの整合性を検証します。Veeam Data Platform Advancedエディションに含まれています。
- **Veeam Recovery Orchestrator：**アプリケーションレベルのディザスタリカバリ（DR）を自動化するオーケストレーションプラットフォームです。実行可能なリストアプランの作成、準備状態テストの実行、DataLabベースの検証の実行、および復元ドキュメントの生成が可能です。Veeam Data Platform Premiumエディションに含まれています。
- **Veeam Data Cloud Vault：**オフサイトコピー用のイミュータブルなクラウドオブジェクトストレージを提供します。Veeamが管理し、別途クラウドアカウントは不要です。

主な用語

- **目標復旧時点（RPO）**：許容可能な最大データ消失量（時間で測定）。バックアップスケジュールの頻度を左右します。
- **目標復旧時間（RTO）**：ワークロードが復旧されるまでに許容される最大ダウンタイム。
- **GFS（grandfather/father/son）**：日次・週次・月次のリストアポイントを維持する保持方式です。
- **イミュータビリティ**：一定保持期間、変更や削除ができないバックアップデータ。バックアップファイルのランサムウェアによる暗号化から保護します。
- **Instant VM Recovery**：データを最初にコピーすることなく、VMを数秒内にバックアップから直接リストアします。検証後に必ず本番ストレージに移行してください。
- **オーケストレーションプラン（Veeam Recovery Orchestrator）**：リストアする複数のワークロードの順序、依存関係、保存場所、ネットワークマッピングを定義する実行可能なランブックです。手動の復元ランブックを、自動的に文書化されテスト可能な自動化に置き換えます。
- **DataLabs**：本番環境に影響を与えずに、Veeam Recovery Orchestrator（またはSureBackup）を用いてバックアップをリストアし、アプリケーションレベルの検証を行うための分離されたテスト環境です。任意の頻度でフルプランテストを実施できます。
- **アプリケーション認識処理**：SQL Server、Oracle、Exchange、Active Directory、SharePoint、PostgreSQL、MySQLのアプリケーション整合性バックアップポイントを作成するゲスト処理。Windowsの場合はVSSを使用し、Linuxの場合はプレスクリプト／ポストスクリプトおよびデータベースネイティブの休止点作成を使用します。
- **Veeam強化リポジトリ**：ファイルシステムレベルでイミュータビリティが強制されているLinuxベースのバックアップリポジトリ。Veeam Infrastructure Applianceは、Linuxの管理が不要な、事前設定済みのVeeam強化リポジトリを提供します。オブジェクトストレージとオブジェクトロックは、別個のイミュータビリティメカニズムであり、Veeam 強化リポジトリではありません。ファイルシステムレベルのイミュータビリティはOS内の攻撃には防御できますが、VMレベルの破壊には対応できません。仮想アプライアンスとして動作しているVeeam強化レポジトリはハイパーバイザーレイヤーで削除される可能性があるため、最大限の保護を実現するにはVeeam Infrastructure Applianceを物理ハードウェア上に導入してください。
- **ホットアド転送モード**：VMware固有のバックアップ転送です。プロキシVMはソースVMの仮想ディスクをホットアドし、SCSI経由で読み取ることで、ESXi管理ネットワークを経由するNBD経路を回避します。

付録：役立つリンク集

マイアカウント

Veeamアカウントは、導入管理における中心的なハブとして機能します。ログイン後は、製品やライセンスキーのダウンロード、ケース管理者の管理、Veeamサポートへの連絡、契約の更新やライセンスの追加が可能です。

- Veeamアカウントにログインするか、新規作成する
- アカウントの作成方法
- サインインに関するFAQ
- ライセンス／ケース管理者のロール管理

ドキュメントとダウンロード

- ヘルプセンター（技術マニュアル、導入ガイダンス、ユーザーガイド）
- 製品のダウンロード（ソフトウェアアップデート、パッチ、リリースノートを含む）
- サポートナレッジベース（一般的な問題、トラブルシューティング手順、推奨される解決策を記載。Veeamサポートチームおよびエンジニアリングチームによって定期的に更新）

学習とベストプラクティス

- ライブオンボーディングオンラインセミナー：定期的に開催されるライブオンボーディングオンラインセミナーでは、リアルタイムで質問したり、技術スペシャリストから直接話を聞いたりできます
- Veeam University Free：自分のペースで進められるコースや認定資格を無料で受講できます
- Veeamサイジング計算ツール：オンラインのサイジングおよび見積もりツールで、Veeam導入のためのインフラストラクチャ、ストレージ、容量要件を算出します
- Veeamソリューションアーキテクトによるベストプラクティス：実際の導入から得られたインフラストラクチャ設計および設定のガイダンスであり、環境の成長と拡大に合わせて活用してください
- Veeam Intelligenceのための実用的なプロンプト集：Veeam Intelligenceを最大限に活用するための、実用的なプロンプトを厳選したコレクションです
- Veeam Search：Veeamのリソース全体を1か所から検索するための集中型検索ポータルです

Veeamコミュニティ

- Veeamコミュニティフォーラム：他のユーザーとつながり、ベストプラクティスの共有、ユーザーグループやコミュニティイベントへの参加、実際のユースケースについての議論などを行えます
- Veeam R&Dフォーラム：Veeam R&Dに直接連絡できる窓口です。製品に関するディスカッション、技術的な質問、機能に関するフィードバックのためにご利用いただけます

Veeam Softwareについて

Veeamはデータ 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。

米国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、世界中で55万社以上のお客様を保護しており、その中にはFortune 500企業の82%が含まれています。

詳細については、www.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。