ランサムウェア対策の7つのベストプラクティス

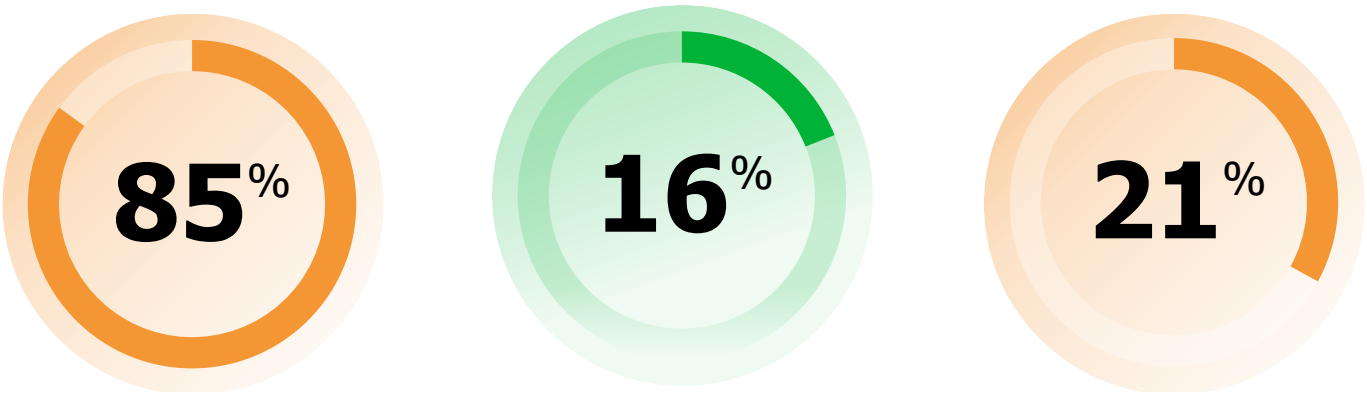
復元に最優先で取り組むために

目次

はじめに：
ランサムウェアは最大級の災害

近年、ランサムウェア攻撃はますます頻繁かつ巧妙になってきており、あらゆる規模と業界の組織にとっての脅威が増大しています。ランサムウェア攻撃の影響は壊滅的になる可能性があり、事業の中断、金銭的損失、評判の低下の原因となり、法律および規制上の影響が発生するおそれもあります。したがって、経営幹部にとって、攻撃の影響を最小限に抑え、事業活動をできるだけ速くリストアできる明確で包括的なランサムウェアからの復旧計画を用意することが極めて重要です。

Veeam の『2023 データプロテクションレポート』と『2023 ランサムウェアトレンドレポート』では、次のように報告されています。



過去１年間に少なくとも１回はランサムウェア攻撃を受けた企業の割合

身代金を支払わずに復元に成功した企業の割合

身代金を支払ったがデータを復元できなかった企業の割合

* 出典：『2023 データプロテクションレポート』、『2023 ランサムウェアトレンドレポート』

サイバー攻撃を全て防ぐことは不可能であるため、組織は復旧を優先する必要があります。バックアップは、ランサムウェア攻撃に対して最も効果的な防御策の１つであることが広く認められています。検証済みの安全な最新のバックアップがあれば、復旧が成功する可能性を高めながら、ダウンタイムを短縮し、データ消失の可能性を最小限に抑えることができます。

これまで、ディザスタリカバリ（DR）計画は全体的なインフラストラクチャ計画の一部であると見なされてきました。有事の際のデータの完全性と可用性についての想定は、この前提のもとでなされていました。リスク計算は、データのわずか **3%** ～ **5%** が毎年影響を受けている、というデータの復元に関して時代遅れになった統計に基づいて行われています。しかし、ランサムウェアの急増に伴い、このパラダイムは変化しました。組織は、１回のインシデントで全てのデータが影響を受ける可能性があるという事実を受け入れる必要があります。

ランサムウェア攻撃を乗り越えるためには、複数のベストプラクティスを実践する必要があります。このホワイトペーパーでは、脅威を早期に検出し、迅速に復元し、大規模なオーケストレーションを行うように設計された、セキュアで回復力のあるインフラストラクチャの構築に必要なフレームワークを確認していきます。

1. データ回復性

データ保護については、多くの組織が 3-2-1 ルールという業界標準のアプローチをデフォルトで採用しています。このルールは長年、絶対的な基準となってきましたが、このランサムウェアの時代においては十分ではなくなりました。組織はさらに一歩先に進んで、データのイミュータブルなコピーを確保し、さらに包括的なテストを実施してデータ内にエラーが一切ないことを確認する必要があります。つまり、新たな業界標準は 3-2-1-1-0 ルールであり、これは「可用性の郵便番号」とも呼ばれます。

3-2-1-1-0 ルールの実現

Veeam はこの 3-2-1-1-0 ルールを実現するべく、多数の可能性を提供しています。要件や機能はお客様によって異なるためです。たとえば、**Veeam Backup & Replication** は次のセットアップを使用することで、このルールを最初から確実に守れるようになっています。それは、データのコピー 3 つ（本番ワークロード、バックアップリポジトリへのコピー、テープへのコピー）が異なる 2 つのメディア（ディスク駆動のリポジトリとテープ）に存在し、そのメディアのうち 1 つはオフサイト（テープ）、1 つはイミュータブル（Write Once Read Many テープメディア）で、エラーはゼロである（SureBackup により保証）というものです。

データのライフサイクル全体に対応したイミュータビリティ

オブジェクトストレージの利用が拡大していますが、これには多くの理由があります。耐久性に非常に優れていること、クラウドプロバイダーがサービスとして提供できること、イミュータビリティ確保のための S3 オブジェクトロックという導入しやすい手法が存在することなどです。オブジェクトストレージへのダイレクトバックアップ書き込みがサポートによって、データのライフサイクル全体でイミュータビリティを活用できます。また、バックアップターゲットの管理をバックアップサーバーのコントロールプレーンから切り離すことで、さらに 1 つ、責任範囲という障壁が追加されます。イミュータビリティを有効にすれば、悪質なバックアップ管理者や攻撃者がバックアップサーバーにアクセスしたとしても、バックアップは安全な状態に維持されます。

オンプレミスであれクラウド内であれ、イミュータブルストレージを使用するセカンダリサイトに対して、リストアポイントを自動的にオフロードできます。長期的な保持が必要な場合は、Amazon S3 Glacier または Microsoft Azure Archive Blob Storage によるアーカイブ層のイミュータビリティがサポートされます。

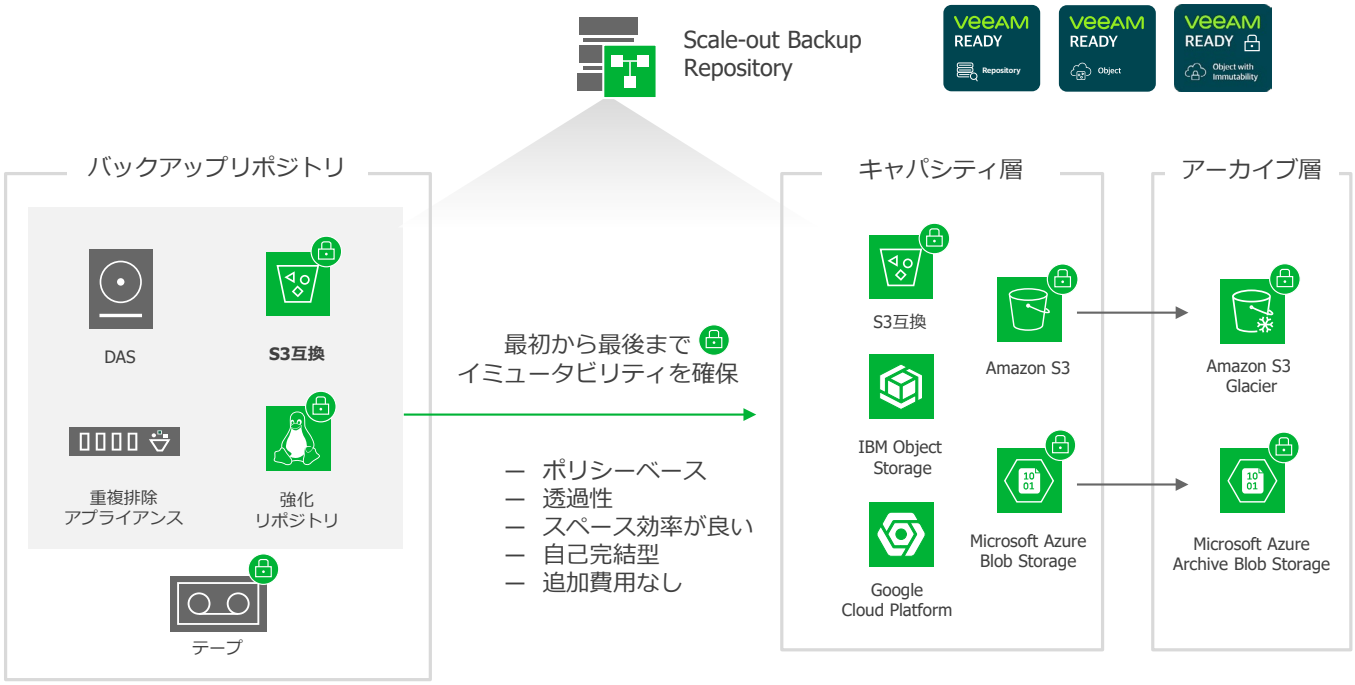
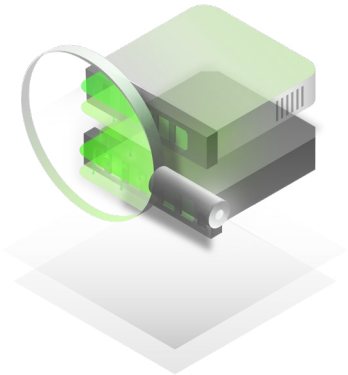


図1 — データのライフサイクル全体に対応したイミュータビリティ



オブジェクトストレージを利用できない場合は、**Veeam の強化リポジトリ**を活用することもできます。Veeam の強化リポジトリは導入時に、Linux ファイルシステム用の 1 回限りのログイン情報とネイティブの機能を使用して、バックアップファイル上にイミュータブル属性フラグを設定します。どのようなシステムでも、セキュリティ要件とベストプラクティスを考慮することが重要です。アクセスの制限（物理的、ネットワーク経由のいずれも）やホストの強化などの推奨事項に従うことが必要になります。

2. 高速復元に対応した設計

危機の際にバックアップが存在することは、復元への第一歩に過ぎません。ビジネスのダウンタイムは金銭的損失やブランドの評判低下に直結します。できるだけ早く事業活動をオンラインに戻すためには、それを実現できる回復力のあるソリューションを設計することが不可欠です。

Veeam は 2010 年に、VM を迅速に復旧する手段として**インスタント VM リカバリ（Instant VM Recovery）**をいち早く提供開始しました。現在、そのユースケースは VM に留まらず、拡大を続けています。インスタントリカバリ処理は Veeam Agent バックアップ上で実行できます。物理マシン、Microsoft SQL Server、Oracle Database、クラウドベースのワークロード（Amazon EC2、Microsoft Azure、Google Compute Engine）や、NAS 共有などに対応しています。データがマウントされアクセス可能になるとすぐに、ユーザーはリソースにアクセスできます。バックグラウンドで移行を実行して、データを本番環境にコピーすることができます。このデータには、元のバックアップとインスタンスリカバリの実行中に変更された部分との差分が含まれます。

低 RPO でのレプリカからの復元

Veeam Data Platform のレプリケーションエンジンもパワフルなツールであり、低い目標復旧時点（RPO）の達成という面で、きめ細かい設定が可能です。バックアップジョブは 24 時間ごとに実行できる一方で、レプリケーションジョブはもっと高い頻度で（2 時間ごとなど）実行するよう設定できます。これにより、復旧ポイントの間隔を大幅に短縮できます。

対象の VM のスナップショットを取得して、それを指定のランディングゾーン（通常は DR サイト）にレプリケーションすることで、レプリカが機能します。最初のレプリケーションは VM の完全なコピーですが、後続のレプリケーションには、前回のレプリケーション以降の変更のみが格納されます。初期プロセスを迅速化するために、レプリカのデータをバックアップファイルから取得することも可能です。さらに、Veeam WAN Accelerator を使用してレプリケーション時間を短縮することもできます。

仮想ワークロードでのデータ消失がほぼ許されない状況では、**Veeam CDP（継続的データ保護）**を使用できます。VMware の vSphere API for IO（VAIO）を使用して、対象の VM へのパフォーマンス面での影響を避けながら、レプリケーションを秒単位で計測できます。

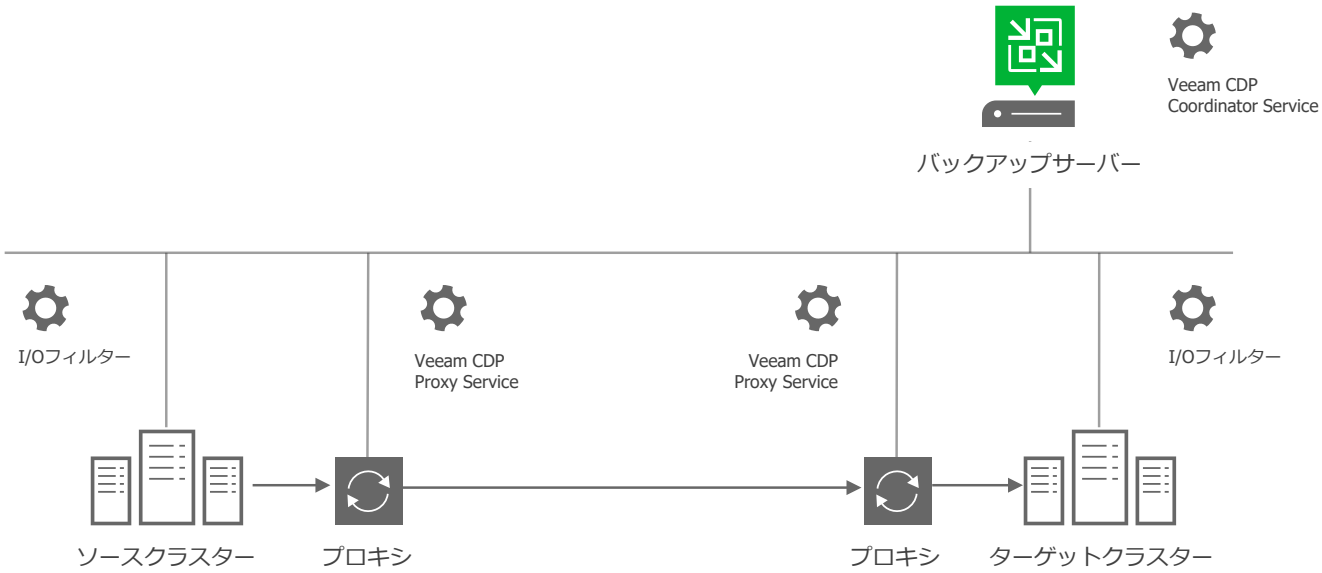
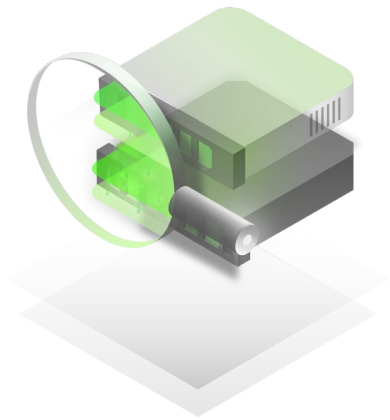


図 2 — Veeam CDP のアーキテクチャ

パワフルなストレージスナップショット統合



Veeam は多くのベンダーやストレージシステムと緊密に統合されており、Universal Storage API 統合システムを提供しています。この独自の API によって、データの保護とスナップショットからのデータのリストアのタスクが容易になり、ストレージアレイについて対象分野の専門家レベルの深い知識は不要になります。

バックアップをアレイベースのスナップショット経由で実行して、本番環境への影響を最小限に抑えることができます。さらに、**Veeam Explorer *for Storage Snapshots*** と、***ストレージスナップショット***からの**インスタント VM リカバリ**により、ユーザーは VM 全体から個々のファイルやアプリケーションアイテムまで、あらゆる範囲の復元を迅速かつ容易に実行できます。従来型のバックアップジョブのスケジューリングに加えて、スナップショットのオーケストレーションによって RPO を確実に達成することができます。

バックアップを信頼するが検証もする

SureBackup は、バックアップをテストし、そこからデータを復元できるかどうかを確認するための Veeam テクノロジーです。たとえば、システムの次の起動時に脅威が発覚するような場合に、SureBackup は、システムの起動を妨害しうる問題や、期待どおりに開始しないと思われるアプリケーションを特定することができます。SureBackup ジョブにより、アプリケーションがバックアップ（または VMware 環境のレプリカ）から期待どおりに起動することを確認でき、また、そのリストアポイントが確実にリストア可能であることがレポートで示されます。テストの実施は常に推奨されますが、ランサムウェアの脅威からの修復という面では、検証の自動化の方がはるかに重要です。

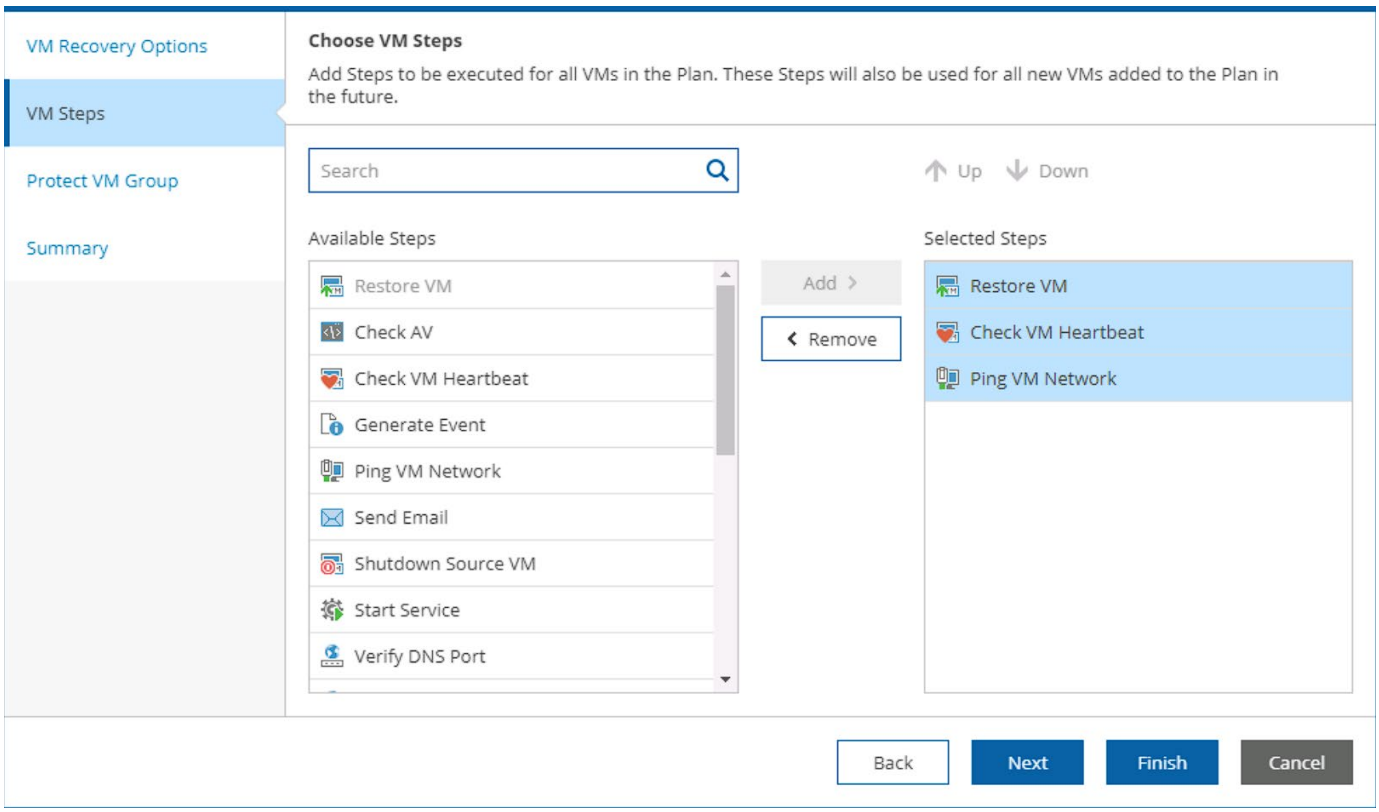
SureBackup ジョブの汎用性の高さを表す特徴の 1 つが、起動後にジョブを実行したままにしておけることです。SureBackup ジョブはデフォルトで稼働し、ユーザーが設定したチェック処理を実行します。稼働状態を維持するようにジョブを設定している場合は、バックアップのリストアポイントから、さらに追加のチェック処理をシステム上で実行できます。これには、ランサムウェアの脅威が依然として存在するのか調べるための自動または手動の検査が含まれます。この検査では、特定ファイルに異常がないかのチェックや、暗号化されたデータのチェック、詳細分析のために選択したデータの抽出などが実行されます。

復元の自動化とオーケストレーション

ランサムウェア攻撃を実際に受けた場合に、リストアを 1 回だけ実行すればよいというケースはほとんどありません。通常は多くのワークロードが影響を受けます。しかも、直接攻撃されていないワークロードにも、依存関係によって障害が発生する可能性があります。大規模な復元に際しては、スピード、自動化、オーケストレーションが必要不可欠です。Veeam Data Platform なら、迅速な復元に必要なツール一式を利用できます。

どのような DR 計画も、必要なときに機能してこそ価値があります。**Veeam Recovery Orchestrator** は、立証済みの結果を示すことで、企業が求める安心感をもたらします。カスタマイズされた動的な文書化とレポートにより、企業がリスク管理の際に必要とする記録と確実性を得ることができます。さらに、計画の策定後は、管理者が自動テストをスケジューリングして復元が期待どおりに動作することを確認できます。セキュリティ向上のため、管理者はリストアポイントにランサムウェアがないか自動テストによってスキャンでき、感染が再発しないという安心をユーザーにもたらします。

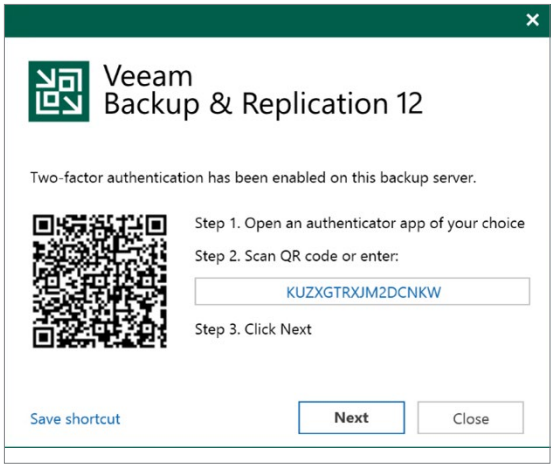
企業が本番環境へのリストアを実行できないというのは比較的よくあることです。それが人材不足のためであっても、フォレンジック調査のためであっても、サイバー保険の要件であっても、リストア先がどこにもなければ復元できません。Veeam Data Platform は、復元を Microsoft Azure 内に直接オーケストレーションすることで、企業が要求する汎用性を確保できます。



3. 多層的なセキュリティの適用

どのセキュリティ専門家も、セキュリティの第一歩は玄関口に鍵をかけることだと言うはずです。それが実際の玄関口であれ比喩的なものであれ、多層防御戦略を使用することが必要になります。Veeam は、企業が悪意のある攻撃者に対して盾を構えるために使用できる多数のツールを提供しています。

攻撃者を寄せ付けない



マルチファクター認証（MFA）は可能な限り全ての場所で有効にする必要があります。OS の視点では、プロキシ、リポジトリなどのインフラストラクチャコンポーネントや、バックアップサーバー自体へのログオン時に、何らかの形で MFA を要求することになります。さらに、Veeam Backup & Replication コンソールにアクセスする必要のあるユーザーに対しても MFA を有効にする必要があります。この機能は、バックアップサーバーがインターネットにアクセスできない場合にも、オフラインモードで動作します。これにより、設計の段階から柔軟性とセキュリティが向上します。

SQL Server を実行する Windows Server など、ゲスト OS を操作する場合には、グループ管理サービスアカウント（gMSA）などのツールが最適です。グループ管理サービスアカウントは、自動生成されたランダムな 240 バイトのパスワードを使用します。このパスワードは 30 日ごとに自動的に変更されます。これにより、総合的に見れば、ワークロードを操作するための極めて強力かつ信頼できるインターフェイスが得られます。

バックアップ環境における現在のセキュリティ方針を確認する目的で、**セキュリティの Best Practices Analyzer** をいつでも実行できます。このツールは、Veeam Backup & Replication サーバーの設定に関連したセキュリティのベストプラクティスの概要を示すものです。環境を変更した際に、このツールを実行して影響度を再確認することができます。

送信中、転送後のデータの保護

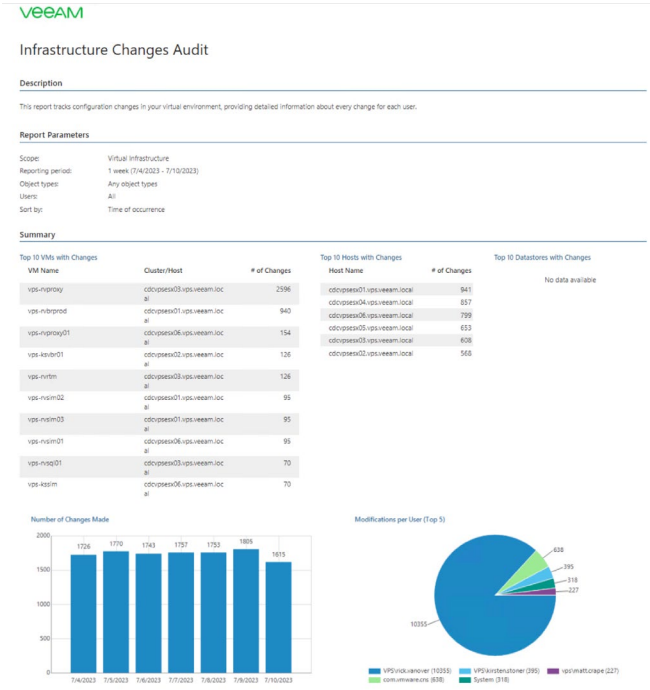
バックアップデータの保管場所にかかわらず、暗号化を検討する必要があります。イミュータビリティは悪意のある攻撃者によるバックアップ削除の阻止に欠かせませんが、そのデータのコピーや窃取を必ずしも阻止するものではありません。

Veeam Backup & Replication の暗号化テクノロジーなら、バックアップコンポーネント間で送信中のデータも、転送後に最終保存先で保管されているデータも保護できます。データ保護プロセスの全ての手順を通して、重要なデータを不正アクセスから保護するために、いずれかの暗号化手法を使用することも、両方を組み合わせて使用することもできます。

4. 新たな脅威の監視

Veeam ONE は、主にプロアクティブな監視と分析の役割を担う、Veeam Data Platform の重要なコンポーネントです。ほぼ全ての攻撃には、特定可能な前兆があります。それらに対する警戒と対策が、ランサムウェアとの闘いの勝敗を分けるかもしれません。

許可されていないアクセスや変更の特定


VEEAM

Infrastructure Changes Audit

Description

This report tracks configuration changes in your virtual environment, providing detailed information about every change for each user.

Report Parameters

Scope: Virtual Infrastructure
Reporting period: 1 week (7/4/2023 - 7/10/2023)
Object types: Any object types
Users: All
Sort by: Time of occurrence

Summary

Top 10 VMs with Changes

VM Name	Cluster/Host	# of Changes
vps-nvproxy	cdcvpsesx03.vps.veeam.local	2596
vps-nvbrprod	cdcvpsesx01.vps.veeam.local	940
vps-nvproxy01	cdcvpsesx06.vps.veeam.local	154
vps-ksvbr01	cdcvpsesx02.vps.veeam.local	126
vps-nvtm	cdcvpsesx03.vps.veeam.local	126
vps-nvsim02	cdcvpsesx01.vps.veeam.local	99
vps-nvsim03	cdcvpsesx01.vps.veeam.local	95
vps-nvsim01	cdcvpsesx06.vps.veeam.local	95
vps-nvsql01	cdcvpsesx03.vps.veeam.local	70
vps-kssim	cdcvpsesx06.vps.veeam.local	70

Top 10 Hosts with Changes

Host Name	# of Changes
cdcvpsesx01.vps.veeam.local	941
cdcvpsesx04.vps.veeam.local	857
cdcvpsesx06.vps.veeam.local	799
cdcvpsesx05.vps.veeam.local	653
cdcvpsesx03.vps.veeam.local	608
cdcvpsesx02.vps.veeam.local	568

Top 10 Datastores with Changes

No data available

Number of Changes Made

Modifications per User (Top 5)

多くの場合、攻撃者は攻撃対象の環境内に目印を残します。たとえば、ログイン情報が盗み出された場合、攻撃者はネットワーク上のさまざまなワークロードにログインし始めるかもしれません。盗み出したログイン情報が有効であることを確認し、そのログインユーザーが持っている権限やログイン先のシステムをテストしているのです。

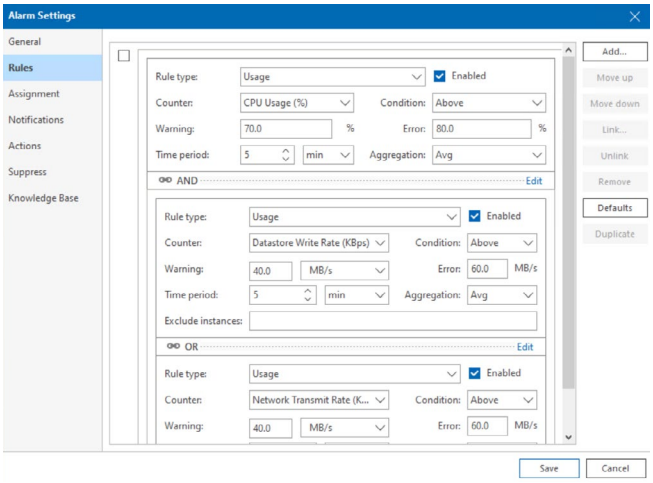
インフラストラクチャ変更監査レポートは、仮想環境内の変更の特定に役立つため、定期的に実行して確認する必要があります。VM、ホスト、データストアに対する変更を追跡でき、実行された変更の件数、変更の内容、変更の実行者、変更日時などの詳細情報が得られます。これにより、許可されていない動作を迅速に特定して停止させることができます。

バックアップサイズの変化の特定

ランサムウェアの主な特徴の 1 つは、ファイルを暗号化するという任務を帯びていることです。つまり、新しいデータが作成され、バックアップされる可能性があります。理想からは程遠いですが、これによって監視すべき新たなデータポイントが生じるのも事実です。バックアップファイルのサイズです。

バックアップの不審なサイズ増加を知らせるアラームを設定して、増分バックアップファイルのサイズに大幅な変化がないかを監視できます。アラームは、メールでのアラートの送信、タスク実行や情報収集のための事前に定義されたスクリプトの実行、SureBackup ジョブの起動などのタスクを含めるように詳細に設定可能です。

起こり得る脅威をリアルタイムで特定



新たな暗号化ファイルが作成されるときの暗号化処理は、CPU とディスク I/O に高い負荷がかかります。そのため、CPU 使用率、ディスク書き込み速度、ネットワーク送信速度などのメトリックスの急増を監視することで、活動中のランサムウェア攻撃に関する明らかな兆候を検出できます。Veeam ONE では、**ランサムウェア活動の可能性を知らせるアラーム**を有効にして、それらの観測に基づいてトリガーするように詳細に調整できます。

Veeam ONE アラームに関して推奨されるプラクティスは、このアラームをコピーして、環境に合わせて詳細に調整することです。このアラームを試しに使用すると、通常時の CPU 使用率が比較的高いデータベースワークロードがあることを発見できる場合があります。そのアラームのコピーを使用して値を微調整し、しきい値を特定の範囲のみに適用することができます。

5. 文書化、セキュリティ、テストの自動化

DR 計画を常に最新の状態に維持することは非常に重要ですが、あらゆる規模の企業に影響する課題でもあります。DR 計画を実行してみたら、ドキュメントが古い、手順が足りない、あるいは完全に間違っていることが判明しただけだったという状況は、どの IT 部門も望んでいません。Veeam Recovery Orchestrator は、作成したオーケストレーションプランごとに文書を作成するプロセスを自動化することで、この課題を克服します。

Plan Steps & Default Parameters

Restore VM

Parameter	Description	Default Value
Description	This is a default step for every machine added to a Restore Plan. It restores machines from backup files into the specified recovery location.	None
Test Action	This step will always be executed in a Test DataLab environment only.	Execute
Critical Step	Choose Yes or No to define whether this step is critical to the VM recovery. If critical step, then failure will cause the VM to be marked as failed	Yes
Restore Timeout (minutes)	Timeout (in minutes) for the restore process. As soon as this timeout expires, Orchestrator will stop both the restore process and all the restore tasks currently running on the Veeam Backup & Replication server. If you set the parameter value to 0, the timeout will be disabled, but you will still be able to interrupt the restore process by halting the plan. This setting applies to Recovery, Migrate and Rename step independently.	0
Retries	Number of retries to perform in case the step fails on the first try.	2
Restored VM Name	A name for the newly created VM	%source_machine_name%

Check license and availability

Parameter	Description	Default Value
Description	This step checks whether Orchestrator is licensed to recover this system as a VM. If not, the check displays the ordinal number of the VM in the license queue.	None
Critical Step	Choose Yes or No to define whether this step is critical to the VM recovery. If critical step, then failure will cause the VM to be marked as failed	Yes
Timeout	Timeout (in seconds) for the step	300
Retries	Number of retries to perform in case the step fails on the first try.	1
Failback & Undo Failover Action	Choose Execute or Skip to define whether this step is executed during Undo Failover and Failback operations.	Execute
Test Action	Choose Execute or Skip to define whether this step is executed during plan testing in DataLab	Execute

ドキュメントは人が判読でき、実行しやすく、かつ内容変更後などの必要なときに生成できます。

データのセキュアなリストア

ランサムウェア攻撃を受けたときの最後の防衛線はバックアップですが、マルウェアには通常、環境への潜伏期間があります。ただそこにいて、アクティベートされるのを待っている期間です。そのため、バックアップには、気づかないうちに脅威のコピーが入り込む可能性があります。つまり、バックアップをリストアすることで、環境に脅威がそのまま再度取り込まれてしまうリスクが存在します。

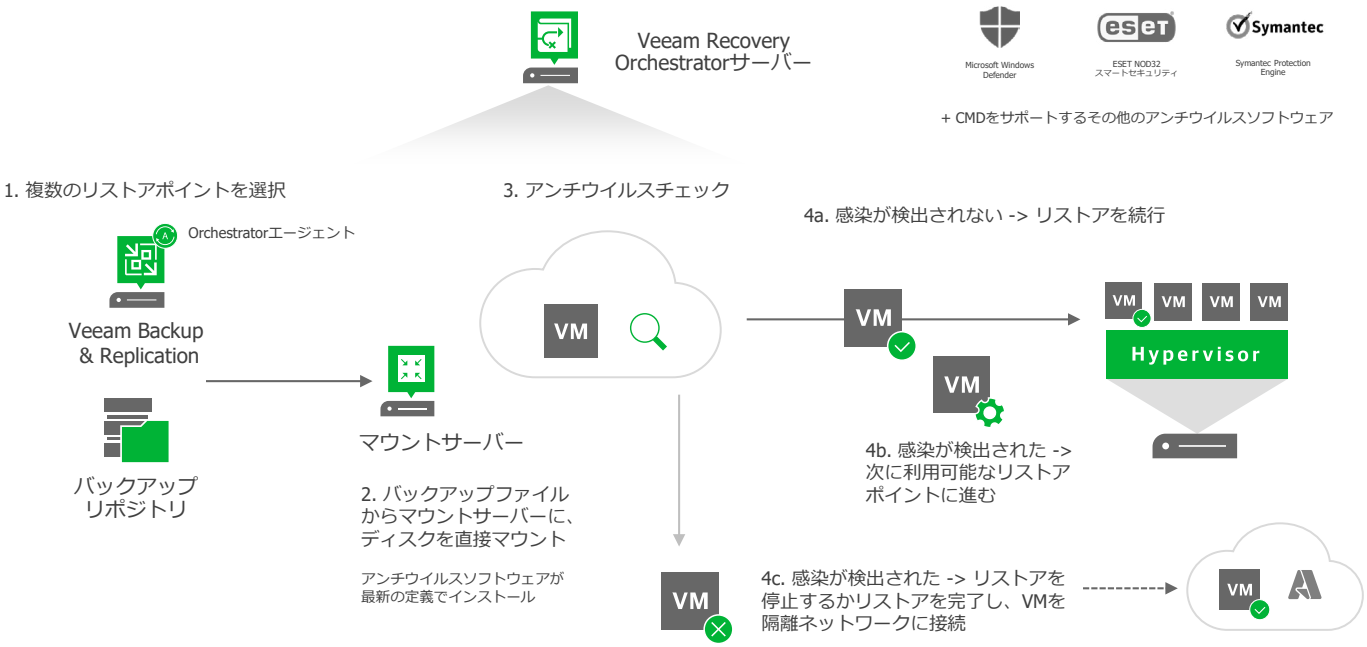
Veeam Backup & Replication の **Secure Restore** がこの脅威の解決策になります。Secure Restore を活用すれば、復元プロセスの一環としてマルウェアスキャンを実行できます。バックアップのマシン用ディスクがマウントサーバーにマウントされたときに、このサーバーでスキャンが実行されます。脅威が検出されない場合は、通常どおりリストアを続行します。一方、マルウェアが検出された場合は、リストアを中止するか、制限付き（ネットワークインターフェイスを無効にするなど）で続行するかをユーザーが選択できます。

大規模なクリーン DR

災害に見舞われ、データセンター全体が影響を受ける場合はどうでしょうか。Veeam Recovery Orchestrator の**クリーン DR** を使用すれば、安全でオーケストレーションされた復元を大規模に実行できます。クリーン DR のベースは Veeam Backup & Replication の Secure Restore です。このため、クリーン DR でも Secure Restore と同様にディスクが自動的にマウントされ、マルウェア検出のためのスキャンが実行されます。脅威が検出されない場合は、リストア処理を復元計画に従って続行できます。

脅威が検出された場合は、管理者は次のいずれかのアクションを実行できます。

- 次に新しいリストアポイントにマルウェアが存在しないかをスキャンする
- リストアを停止する
- 疑いがあるリストアポイントを使用してリストアを完了させ、VM を隔離ネットワークに接続する



マルウェア検出エンジンに関しては、現在ある多くの統合のいずれかを使用することも、XML 設定ファイルを作成しカスタマイズすることで独自のエンジンを追加することもできます。詳細については、Veeam KB 3132 を参照してください。

DR 計画のコンプライアンスの立証

DR 計画のテストは、多くの組織が望んでおり、実行すべきだとわかっていても達成できていないことです。Veeam Recovery Orchestrator のスケジューリングされた自動テストでは、Veeam **DataLabs** を活用することで、テストプロセス全体を合理化します。

RPO

Result	Check	Details
[i] Info	RPO	Target RPO is 24:00 (HH:mm)
✓ Success	Target RPO Met	Yes
✓ Success	VMs not meeting RPO	None
✓ Success	Worst RPO failure	None

RTO

Result	Check	Details
[i] Info	RTO	Target RTO is 01:00 (HH:mm)
[i] Info	Duration	Test duration was 00:04:56 (HH:mm:ss)
✓ Success	Target RTO Met	RTO achieved

DataLabs は、エージェントベースのワークロード、仮想ワークロードの両方について、Veeam Data Platform によるバックアップをサンドボックス環境内に完全にリストアできる独自の機能です。そのため、DR テストの実行時に、計画全体が帯域外ネットワークにより実行されます。DR 計画が期待どおりに機能することを確認できるだけでなく、実際の RPO と目標復旧時間（RTO）を取得して、コンプライアンスを立証するために使用できます。

6. API ドリブン型の脅威検出の使用

脅威検出に関して企業が直面する共通の課題は、リソースへの負荷が高い検出スキャンを本番ワークロードに対して実行することによる影響です。ファイルの脅威のスキャン、既知のアーティファクトや脅威指標の検出で CPU が過度に使用され、ディスクのパフォーマンスが低下する可能性があります。バックアップに対するオフラインスキャン機能を使用すれば、こういったペナルティを回避しながら脅威をスキャンできます。

周囲に影響のない脅威ハンティング

Veeam Backup & Replication v10 で初めて導入された Veeam **データインテグレーション API** は、オフラインでデータに無制限にアクセスできる機能を提供します。この機能により、バックアップファイルのデータをマウント済みフォルダとして公開し、Veeam Backup & Replication が作成したバックアップ内のデータにアクセスできるようになります。ランサムウェアやその他の脅威が本番環境にリストアされないようにする優れた技法です。この API では、データに他の脅威がないかを定期的にスキャンでき、セキュリティチームは隔離されたセキュアな環境で脅威ハンティング活動を実行できます。

さらに、データはアクティブに実行中のシステムではなくファイルシステムとしてマウントされるため、脅威が実行されることも、システムメモリ内にロードされることもありません。そのため、影響を最小限に抑えて他のワークロードに対する脅威を取り除きながら、安全で効果的にフォレンジック的な監査や検索を実施できます。

コンプライアンス違反のデータや変更の特定

これらのシステム上でデータを分類して、規制コンプライアンスに従っていることを確認する際にも、同じような課題に直面します。ファイルの内容や変更に対するチェックは、本番環境で実行できるようなことではありませんが、実行できれば多くの組織にとって利点があります。Veeam データインテグレーション API は **PowerShell** を利用しているため、企業は必要なタスクを実行するためのコードを開発できます。個人識別情報（PII）がある場所の特定や、機密ファイルが変更されたかの判断などを行うタスクが考えられます。

そういった分析を実行して結果を記録することで、組織はデータが保存されているシステムを自信を持って追跡できます。1 つの利点として、このデータを使用してリストアプランを作成しレビューすることができます。さらに災害の発生時ではなく事前に、データ局所性とコンプライアンスを確保できるという利点も得られます。

7. データセンターへのアクセス不能に備えた計画

ワークロードのリストア先を確保することは、事前の計画が必要となる非常に重要なタスクです。本番サーバーがフォレンジック調査のためにオフライン状態であっても、あるいは、データセンターへのリストアに対応できる人材がいなくても、できる限り早くオンライン状態に復旧する必要があります。

Veeam Data Platform Premium Edition に含まれる Veeam Recovery Orchestrator なら、自動化プランとオーケストレーションプランを作成して、SLA を遵守しながらワークロードを再稼働させるための能力と柔軟性を得られます。

データセンター外での復旧

Veeam Recovery Orchestrator の大きな特長の 1 つは、VMware ワークロードと Veeam Agent バックアップを、VMware 環境だけでなく、Microsoft Azure 環境にも直接リストアできることです。企業は、ダウンタイムを解消するためのオーケストレーションプランを作成することで、復元計画を策定できます。ダウンタイムがランサムウェアによるものでも、法執行機関による制限事項などの影響によるものでも関係ありません。計画を策定したら、サンドボックス環境でテストできます。これにより、全てが期待どおりに機能することを確認できるだけでなく、立証済みの RPO と RTO の情報を取得できるため、インシデントから復元するために必要な確信を得ることができます。

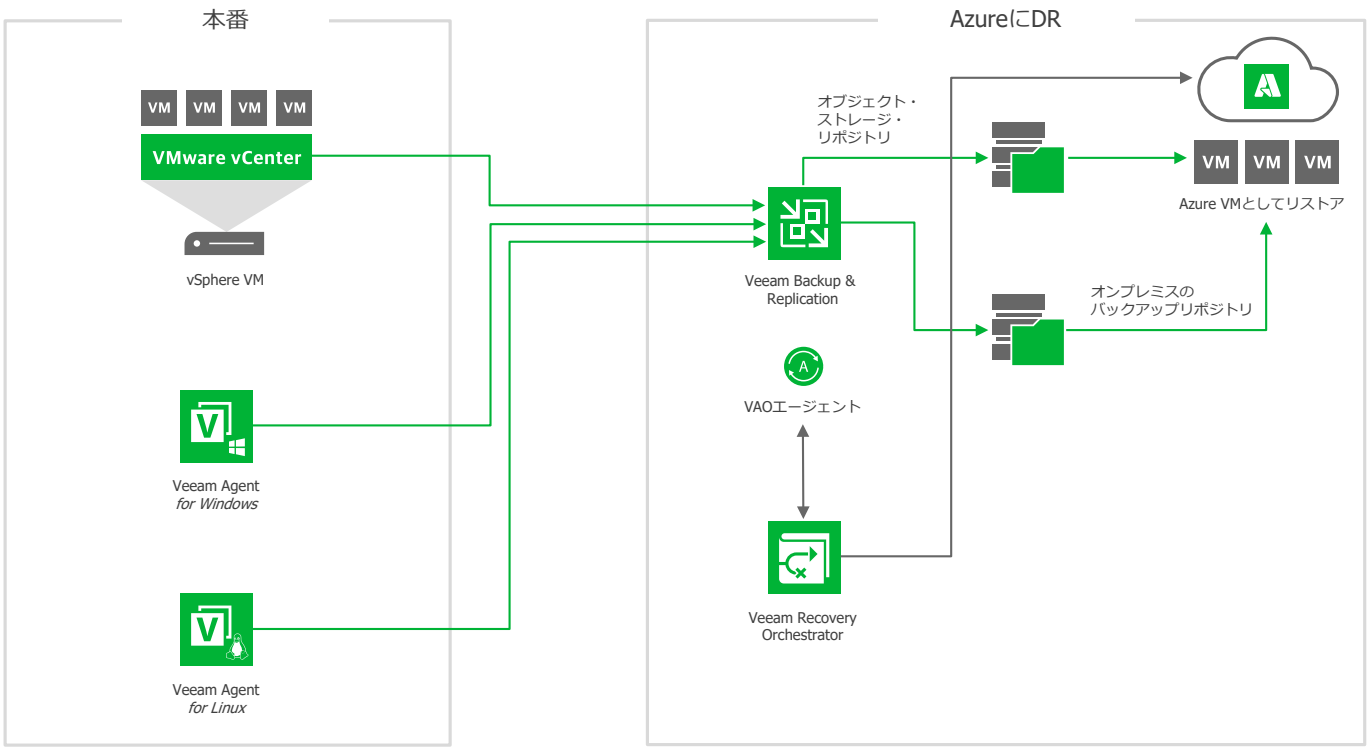


図 9 — Microsoft Azure へのオーケストレーションによる復元

まとめ：ランサムウェアからの迅速な復旧の実現

ランサムウェア攻撃は驚くべき速さで増大しており、ビジネスと組織に深刻な被害をもたらしています。こうした攻撃は重要なデータを標的としていて、身代金が支払われるまで所有者がこれらにアクセスできないようにしてしまいます。多くの場合、支払った後でさえ、データはリストアされず、犯人はデータを人質に取り続けます。ランサムウェアから保護する最善の方法は、強固なバックアップ計画を策定することです。

ランサムウェア攻撃を乗り越えるには、信頼できるバックアップの存在が不可欠です。組織には、確信を持ってあらゆる規模の攻撃から迅速に復旧できることが求められます。組織が継続してバックアップと復元を全体的なセキュリティプログラムに組み込み、データが回復力を備え保護されるよう徹底することが是非とも必要です。

包括的なセキュリティプログラムを確立するには、継続的な改善に重点を置き、組織が保守的な防御から積極的な姿勢に移行できるよう、人材、プロセス、テクノロジーを融合することが求められます。組織がどのような方法を選択しようとも、IT チームが攻撃を防御し、攻撃が成功した場合に素早く復元できる、測定可能な成果が得られる必要があります。

ランサムウェアからの復旧計画の目標は、ランサムウェア攻撃が行われたときにダウンタイムを最小限に抑え、リスクを軽減するプロセスを自動化することです。攻撃が行われる前に、組織は、潜在的な脅威に対抗するために市場で得られる最も完全な機能セットを備えていることを確信できる必要があります。

これらの手順に従うことで、経営幹部は、組織がランサムウェア攻撃に対応するための準備が十分に整っており、身代金を払うことなく素早く復元できることを確信できます。ランサムウェア攻撃を阻止するための絶対確実な方法は存在しませんが、データを保護するためのベストプラクティスとランサムウェアからの復旧の成功にかかわる手順を明確に理解できれば、攻撃対象領域が小さくなり、起こり得る脅威に対する可視性が増します。この結果、対応チームは、データを防御し、ランサムウェアの脅威からビジネスを保護する上でより優れた知識とツールを装備できるようになります。

『2023 データプロテクション レポート』

『2023 ランサムウェアトレンド レポート』

ランサムウェアを克服するための 6 つのショートデモを見る


veeam