Veeam® Data Platform Foundation

万一のときはスピードが命!!
いち早く復旧できる
ソフトウェアはヴィームだけ

ランサムウェア対策に単純なバックアップだけでは**不充分！**

感染しない対策だけでなく、攻撃を受けてしまった際を想定した対策も

対策のポイント	Veeamによる対策
書き込み不可で保持	バックアップデータをロック！
複数世代、複数箇所確保	バックアップデータを複数箇所/媒体で保管
ランサムウェア混入も想定	ランサムウェア混入をチェックしてから復旧！

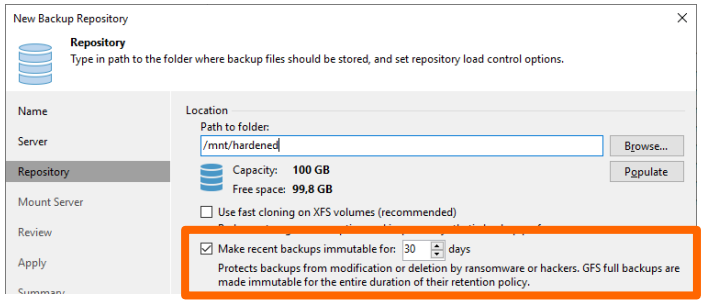
“電子保存の要求事項について”の対応も！

見読性の確保について	◇システムが停止した時は、バックアップデータから代替環境で仮想マシンとして迅速に起動して日常診療に必要な情報を見読できるようにします。 ◇災害対策として、クラウドオブジェクトストレージにもバックアップして、有事にはクラウド上へサーバを丸ごと復旧し、代替運用を開始して必要な情報を見読できるようにします。
保存性の確保について	◇バックアップストレージの空き容量、ゲストVM毎の保有バックアップ世代数、最も古いリストアポイント、最新のリストアポイント等を統合的に管理可能です。 ◇バックアップファイルを隔離された検証環境にリストアし、ウィルススキャンをかける等により当該ファイルが正常に利用できるかどうかを検証することが可能です。

ランサムウェアに備えてVeeamでバックアップ

Point1: ランサムウェアが攻撃できないようにバックアップデータをロック！

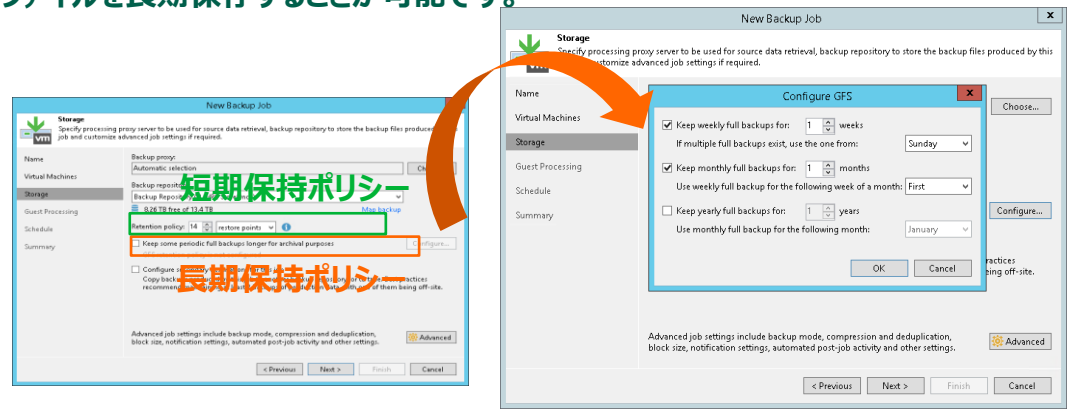
強化Linuxリポジトリ：Linuxと連携してバックアップデータの更新処理不可の設定をすることで、ランサムウェアによる暗号化等からバックアップデータを保護します。



※この他、AWS S3(クラウドオブジェクトストレージ)へ増分転送したバックアップデータをロックして保護することも可能です。
また、テープへの2次バックアップも可能です。

Point2: 潜伏期間が数ヶ月のランサムウェアも・・・短期だけでなく長期保存を可能に！

長期保持ポリシー(GFS)：7～14日等の短期保存バックアップと合わせて、週単位、月単位、年単位のバックアップファイルを長期保存することが可能です。

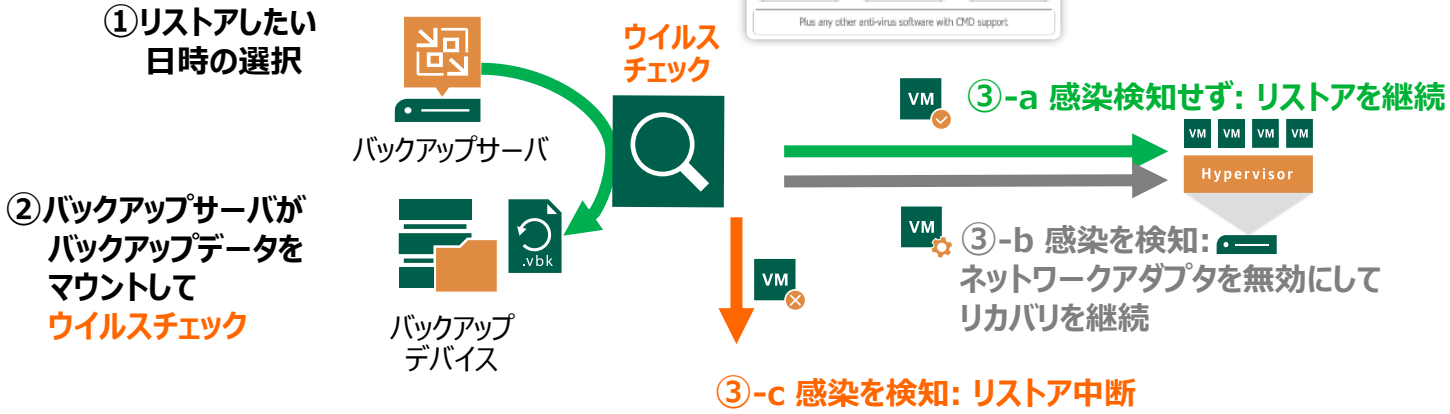


<u>長期保持の目的で新しいバックアップファイルは作成しません。</u>
GFS(grandfather/father/son)と呼ばれる長期の保持ポリシーでは、既存のフルバックアップファイルにGFSフラグを割り当て保持します。

Point3: 再感染、被害拡大を回避・・・ランサムウェアの混入をチェックしてから復旧！

Secure Restore：リストア時にバックアップファイルをチェックして、安全を確認した上でリストアし、システムを復旧させることが可能です。

アンチウイルスソフトウェアと連携
※デフォルトで*Windows Defender*を使用



Veeam公式問い合わせ窓口

製品購入前の各種お問い合わせ：
0120-394-029
平日 9:30-12:00/13:00-17:30
（土日祝、年末年始を除く）
メールでのお問い合わせ：
Sales.Japan@veeam.com

● お問い合わせ・ご用命は・・・

※このチラシの記載内容は、2023年6月現在のものです。