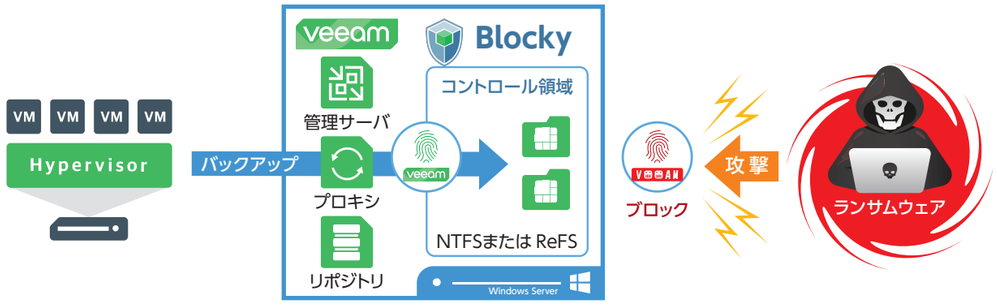
バックアップデータをランサムウェアから守る

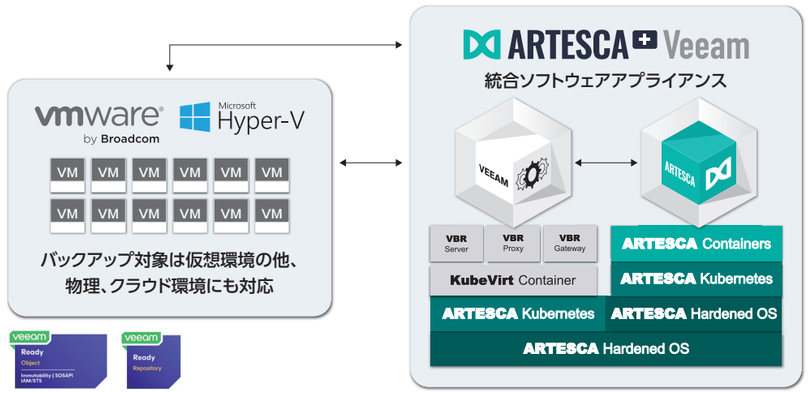
Veeam+Blockyによるランサムウェア対策

- **Windowsマシン1台のオールインワン構成可能**
  Windows上で構成できるから、スモールスタート簡単
- **Veeam以外からのバックアップデータへのアクセスをブロック**
  ホワイトリストアプローチでコントロール領域へのアクセスを制御
- **独自フィンガープリントにより、改ざんされたアプリケーションからのアクセスもブロック**
  Blockyフィルタドライバで、許可したアプリケーションであることを保証



バックアップと最強の防御をこれ1台で。「オールインワン」アプライアンス

「ARTESCA + Veeam」統合ソフトウェアアプライアンス



- 「バックアップの取得」から「ランサムウェアからの超高速復旧」まで、隙のないセキュリティを1パッケージで提供します。
- S3オブジェクトロック機能により、万が一管理者権限が奪われても、一定期間はバックアップデータを絶対に削除・変更できません。
- ハッキングのリスクを最小限に抑えた専用の「堅牢化（ハーデニング）OS」を採用。
- 多要素認証（MFA）、通信の暗号化、ファイアウォールなど、サイバー攻撃を跳ね返す機能を標準装備しています。

Climb Inc. Growing to Meet Your Needs
株式会社クライム
www.climb.co.jp

本　社／〒103-0014 東京都中央区日本橋蛎殻町1-36-7 蛎殻町千葉ビル4F
Tel：03-3660-9336 Fax：03-3660-9337 E-mail：soft@climb.co.jp
大阪営業所／ Tel：06-6147-8201
福岡営業所／ Tel：092-419-2519
名古屋営業所／ Tel：052-462-1282

クライムが提供する Veeamによるランサムウェア対策

Climb Inc. Growing to Meet Your Needs

データの一生をランサムウェアから徹底的に守る
Veeamが実装する「強固なデータ保護アーキテクチャ」

セキュリティ統合が施されたVeeamは、データの「取得」「保管」「復旧」という時系列に沿った高度なトリプルスキャン機能に加え、イミュータブル（不変性）な堅牢化技術と安全なクラウドアーカイブにより、企業の最重要データを脅かすあらゆるリスクを排除します。

バックアップインフラの常時24時間警備

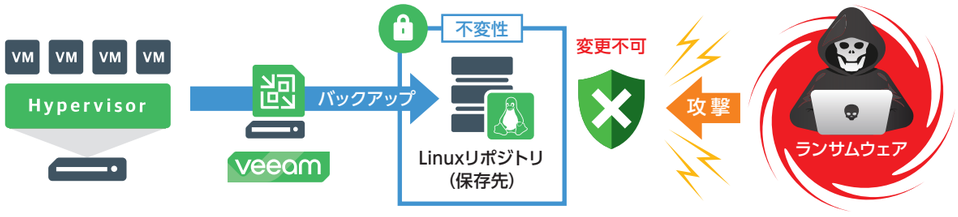
Recon for Veeam Infrastructure

Veeamバックアップ環境に特化した、セキュリティ脆弱性や不審な挙動をリアルタイムに検知・診断する専用アナリティクスエンジン。攻撃者が本格的なデータ暗号化を行う前に、バックアップデータや設定の変更・削除を試みる「前兆動作（Reconnaissance = 偵察行動）」をいち早く捉え、防御します。

不変バックアップで水際対策

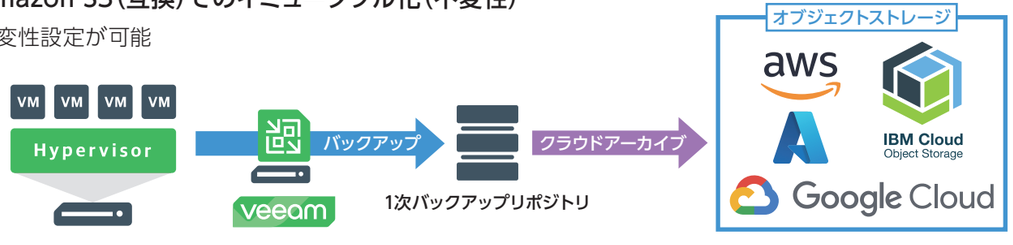
Veeamによるイミュータブルな堅牢化リポジトリ

- **Linuxリポジトリ（保存先）の不変設定**
  ランサムウェア等による暗号化や削除を防ぐ
- **シングルユース（使い捨て）認証情報の使用**
  リポジトリへ接続する認証情報をVeeamで保存しない
- **SSHプロトコルへの依存なし**
  導入時とアップデート時のみSSH接続を使用



Veeamによるクラウドへのアーカイブ

- **クラウドオブジェクトストレージへバックアップをアーカイブ**
  オンプレミス環境に何かあってもクラウド保存データから復旧
- **VPN等の構成不要**
  クラウドアーカイブはHTTPS通信で実施可能。インターネット接続さえできればOK
- **Amazon S3（互換）でのイミュータブル化（不変性）**
  不変性設定が可能



データの通り道での早期検出

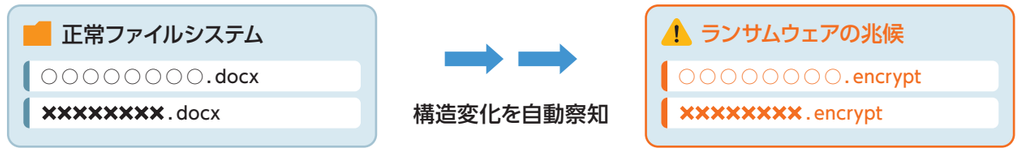
インラインスキャン（バックアップデータ取得時）

バックアップ時にデータを読み込み、バックアップリポジトリへ書き込みを行う「その瞬間（通り道）」で、データブロックのエントロピー（データのランダム性・暗号化の度合い）を解析。既存のウィルス対策ソフトやEDRでは検知できず、隠れて暗号化された汚染データを検知し、ランサムウェアへの迅速な対応を可能にします。

データ取得後の分析

ゲストインデックスデータスキャン（バックアップデータ取得後）

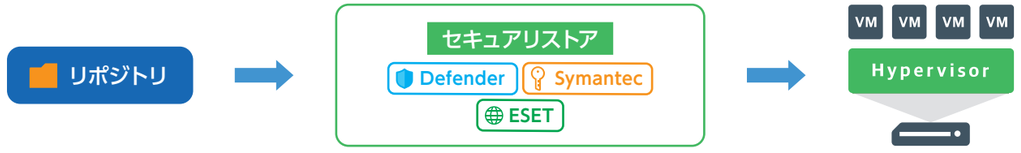
バックアップ取得時に作成したファイルシステムのメタデータ（インデックス情報）を分析し、既知の不審なファイルや脆弱性を含むファイルの検知、「.docx」から「.encrypt」のような不審な暗号化拡張子への一括変換や大量のファイル削除などの異常な振る舞いを検出、潜伏している攻撃の兆候を早期に発見します。



復旧時の再感染・二次被害をゼロ化

スキャンバックアップ / セキュアリストア（データ復旧時）

バックアップ内のデータを使い慣れた主要アンチウイルスエンジン（Windows Defender, Symantec, ESET等）や高度なYARAルールを用いて完全スキャンできます。定期スキャンすることも、本番環境へ書き戻す（リストア）前に、「セキュリティ検問所」としてスキャンを実行し、安全が確認されたクリーンで最新のデータのみを復旧することも可能です。



- **復旧フェーズの安全性をネイティブに強化**
  Threat HunterはVeeamに直接内蔵された専用エンジン。
  - 3rdパーティ製品の構築・管理コストを削減
  - Veeam独自のアルゴリズムでバックアップを解析
  - 復旧直前の「最終検疫」としてシームレスに動作