バックアップが狙われる時代、どう守る？

~Veeamでバックアップとランサムウェア対策の両立を実現~

2025/11/27
株式会社クライム
村岡 拓哉

Climb Inc.
Growing to Meet Your Needs

株式会社クライムとは

設　立	1984年
従業員数	約30名
主な事業内容	ソフトウェアの販売とサポート 海外ソフトウェアの日本語対応
所 在 地	本社　：東京都中央区 大阪営業所　：大阪市北区 名古屋営業所　：愛知県名古屋市 福岡営業所　：福岡県福岡市

Climb Inc.
Growing to Meet Your Needs

アジェンダ

- サイバー攻撃の概要
- ランサムウェア攻撃の現状とトレンド
- Veeamの主なデータ保護手法
- Veeamのランサムウェア対策機能

Climb Inc.
Growing to Meet Your Needs

アジェンダ

- **サイバー攻撃の概要**
- ランサムウェア攻撃の現状とトレンド
- Veeamの主なデータ保護手法
- Veeamのランサムウェア対策機能

Climb Inc.
Growing to Meet Your Needs

サイバー攻撃とは

ネットワークを介し、サーバやPC端末に対して**システムの停止**や**データの窃取・改ざん**を行う攻撃

＜攻撃の種類＞

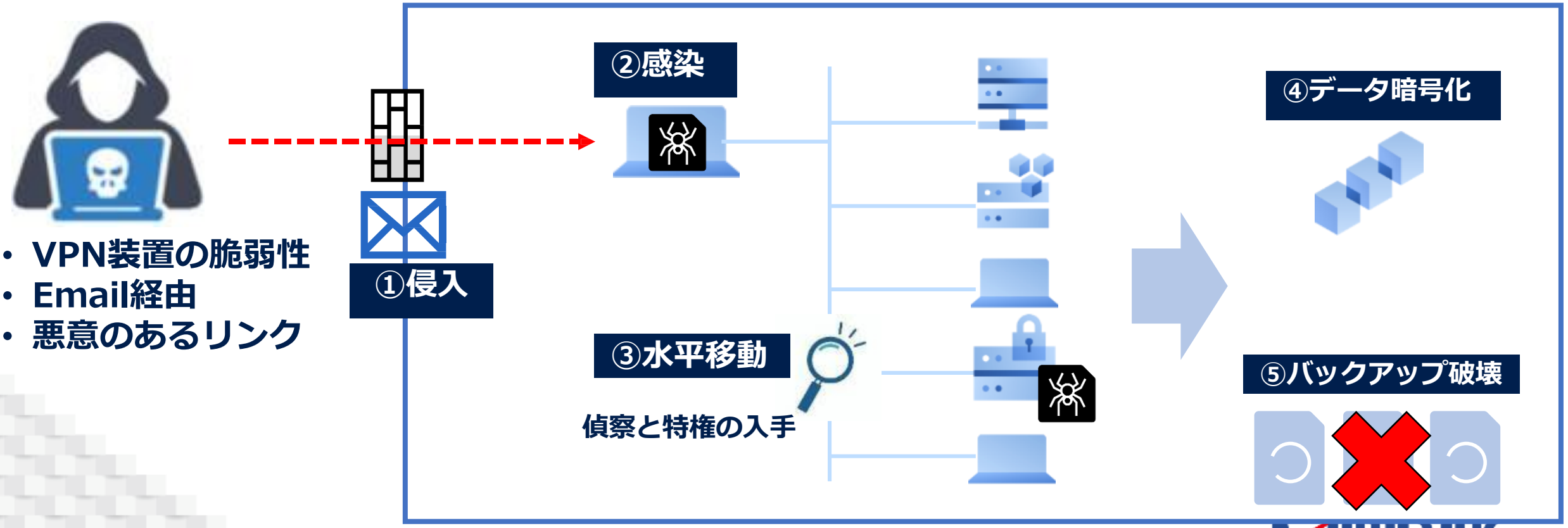
- DDoS攻撃
- マルウェア
- フィッシング

◢ 情報セキュリティ10大脅威 2025［組織］

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサム攻撃による被害	2016年	10年連続10回目
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目
3	システムの脆弱性を突いた攻撃	2016年	5年連続8回目
4	内部不正による情報漏えい等	2016年	10年連続10回目
5	機密情報等を狙った標的型攻撃	2016年	10年連続10回目
6	リモートワーク等の環境や仕組みを狙った攻撃	2021年	5年連続5回目
7	地政学的リスクに起因するサイバー攻撃	2025年	初選出
8	分散型サービス妨害攻撃（DDoS攻撃）	2016年	5年ぶり6回目
9	ビジネスメール詐欺	2018年	8年連続8回目
10	不注意による情報漏えい等	2016年	7年連続8回目

出典：IPA 情報セキュリティ10大脅威 2025
https://www.ipa.go.jp/security/10threats/10threats2025.html

サイバー攻撃の被害例



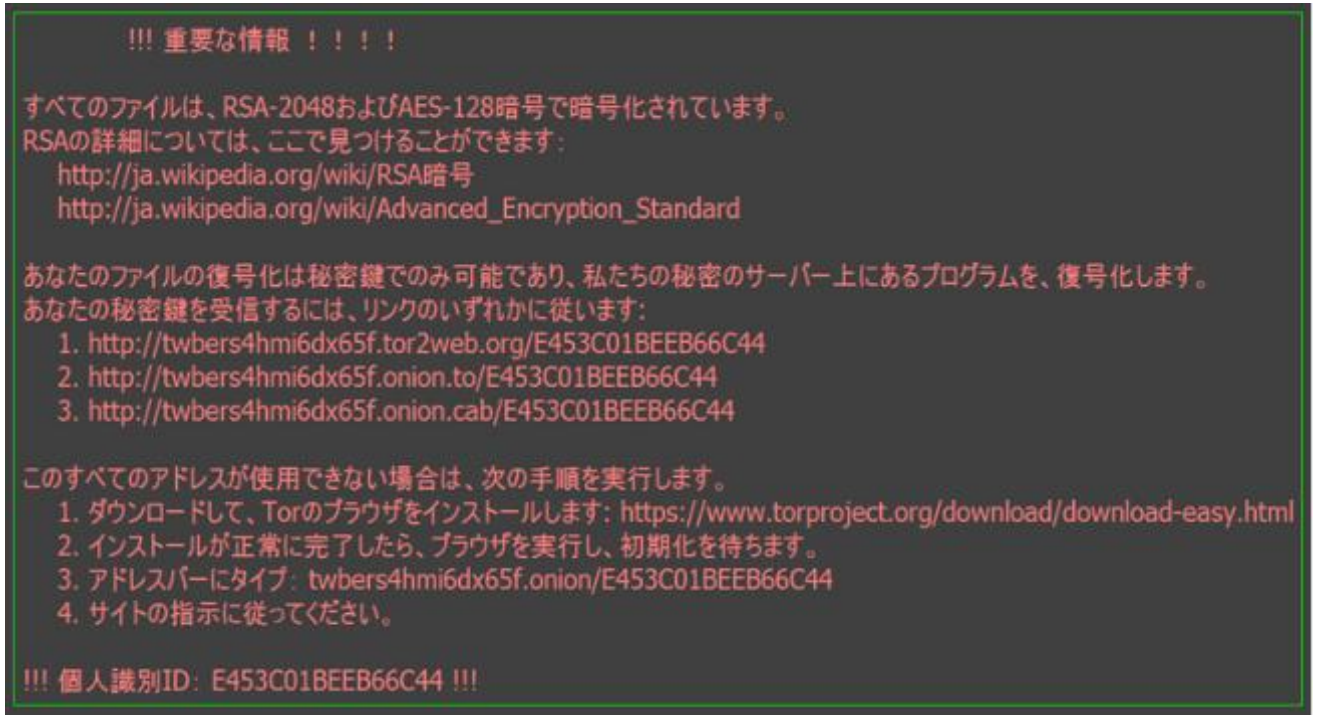
- VPN装置の脆弱性
- Email経由
- 悪意のあるリンク

アジェンダ

- サイバー攻撃の概要
- ランサムウェア攻撃の現状とトレンド
- Veeamの主なデータ保護手法
- Veeamのランサムウェア対策機能

ランサムウェアとは

端末の**システムロック**や**データの窃取**、**暗号化**を行い、これらを取引材料とした脅迫により**金銭を要求するマルウェア**の一種



Climb Inc.
Growing to Meet Your Needs

ランサムウェアの攻撃パターン

従来型

✓ばらまき型攻撃

✓ファイルのロックや暗号化

✓マスターブートレコードの書き換え

新型

✓標的型攻撃

✓二重脅迫

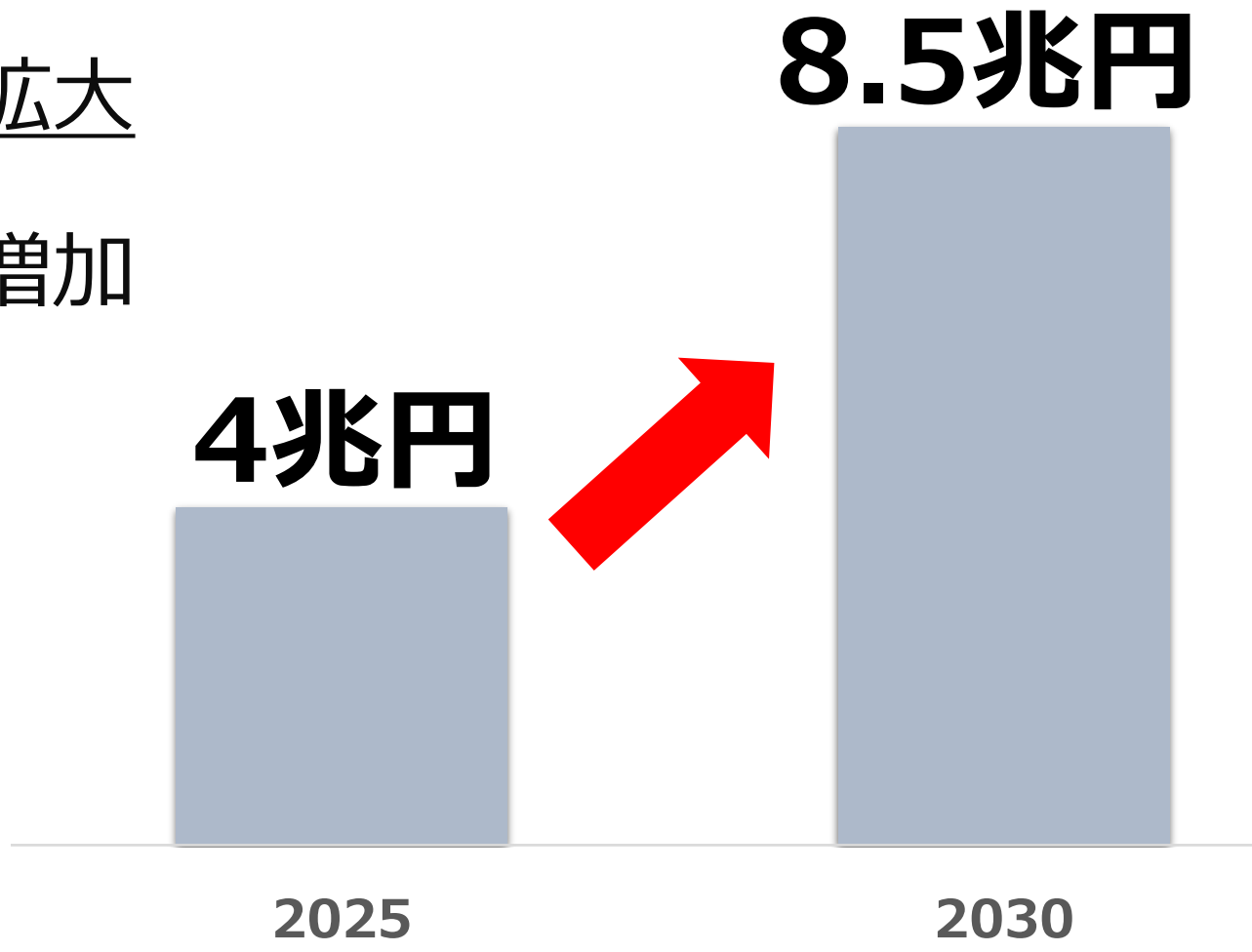
✓ノーウェアランサム

✓RaaS(Ransomware as a Service)を使った攻撃

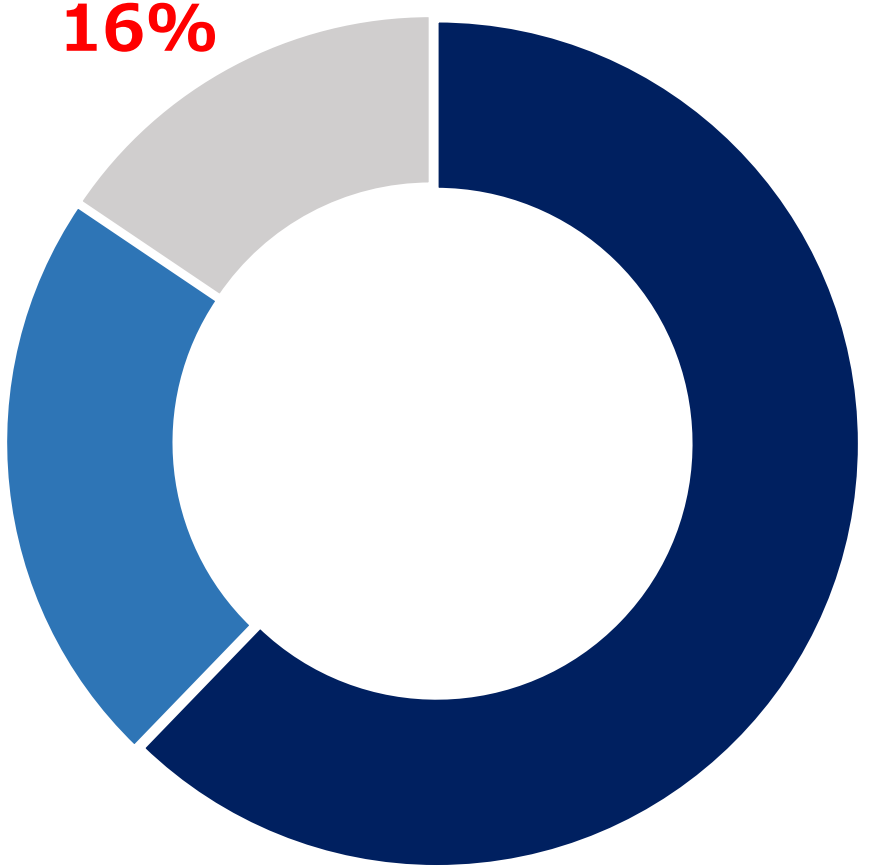
Climb Inc.
Growing to Meet Your Needs

なぜランサムウェアが流行っているのか？

- ランサムウェア市場規模の拡大
- リモートワークで働く人の増加
- RaaSの登場
- AIの悪用
- 追跡が困難



ランサムウェアの感染経路



出典：警察庁 令和７年上半期における サイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/index.html

Climb Inc.
Growing to Meet Your Needs

ランサムウェア被害の現状

222件

被害件数

2024年度に警察庁に報告されたランサムウェアの被害件数
前年比：112.6%

3億円

身代金要求額

攻撃者から要求される身代金額の中央値
平均額は約6.48億円

4.1億円

復旧コスト

2024年のランサムウェア攻撃に対する復旧コスト
前年比：150.1%

出典：警察庁 令和７年上半期における サイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/index.html

Climb Inc.
Growing to Meet Your Needs

ランサムウェア攻撃のトレンド

1 脅威アクターが法執行機関に適応

2 データ窃取攻撃の増加

3 身代金の支払いケース減少

ランサムウェア攻撃のトレンド

4 身代金支払いに対する法整備

5 運用チームとセキュリティチームの連携強化

6 セキュリティ予算の増加

Climb Inc.
Growing to Meet Your Needs

ランサムウェアの予防策

- OSやソフトウェアを最新の状態に保つ
- 不審なメールの添付ファイルや怪しいリンクを開かない
- 認証情報を適切に管理する
- ユーザ権限やアクセス範囲を限定する
- 公共Wi-Fiを使用しない
- 出所不明なUSBメモリや外付けデバイスを接続しない

Climb Inc.
Growing to Meet Your Needs

ランサムウェアに感染してしまったら…

- **ネットワークから切り離す**

  有線LANの場合はケーブルを抜き、無線LANの場合は端末の無線LANをオフ

- **ランサムウェアの種類を調べて復号**

  外部の無料Webサイトで、感染したファイルをアップロードすることで、対処方法を提示

- **バックアップから復元**

  定期的にバックアップしていれば、そこから戻すことが可能

Climb Inc.
Growing to Meet Your Needs

ランサムウェアに感染してしまったら…

・ネットワークから切り離す

有線LANの場合はケーブルを抜き、無線LANの場合は端末の無線LANをオフ

・ランサムウェアの種類を調べて復号

外部の無料Webサイトで、感染したファイルをアップロードすることで、対処方法を提示

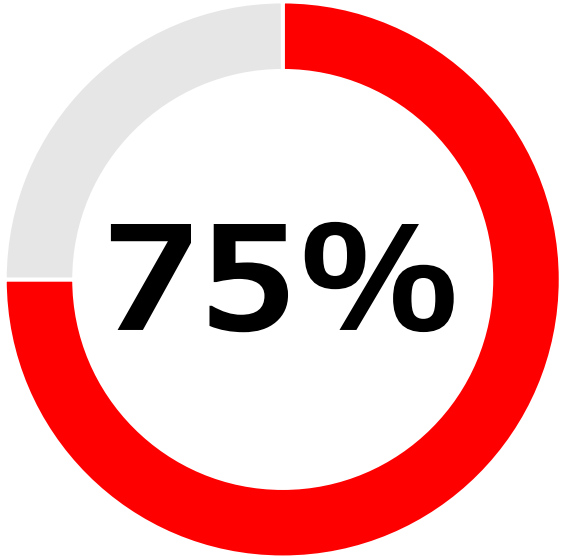
・バックアップから復元

定期的にバックアップしていれば、そこから戻すことが可能

身代金の要求に応じない!

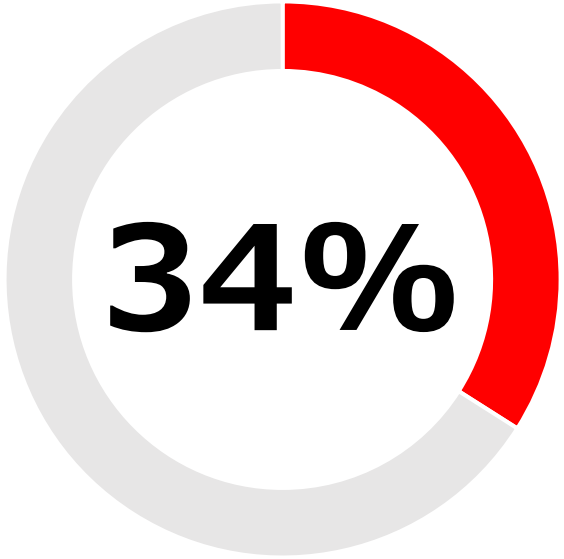
Climb Inc.
Growing to Meet Your Needs

ランサムウェア被害の傾向



過去1年間にランサムウェア被害を受けた企業の割合

バックアップデータの保存先を標的とした攻撃の割合

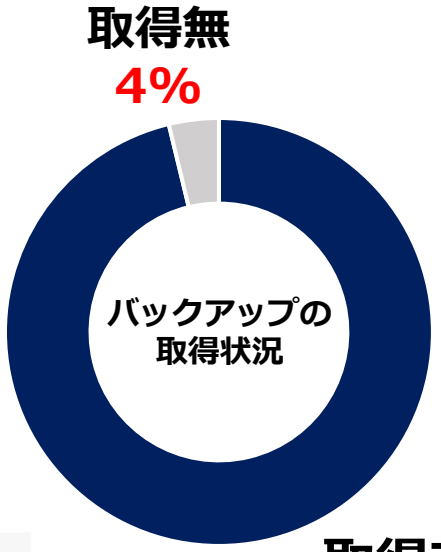


実際にバックアップデータを改ざん/削除された割合

Climb Inc.
Growing to Meet Your Needs

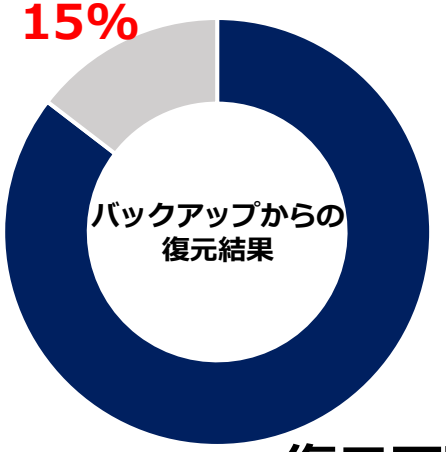
バックアップの暗号化

出典：警察庁 令和７年上半期における サイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/index.html



取得無
4%

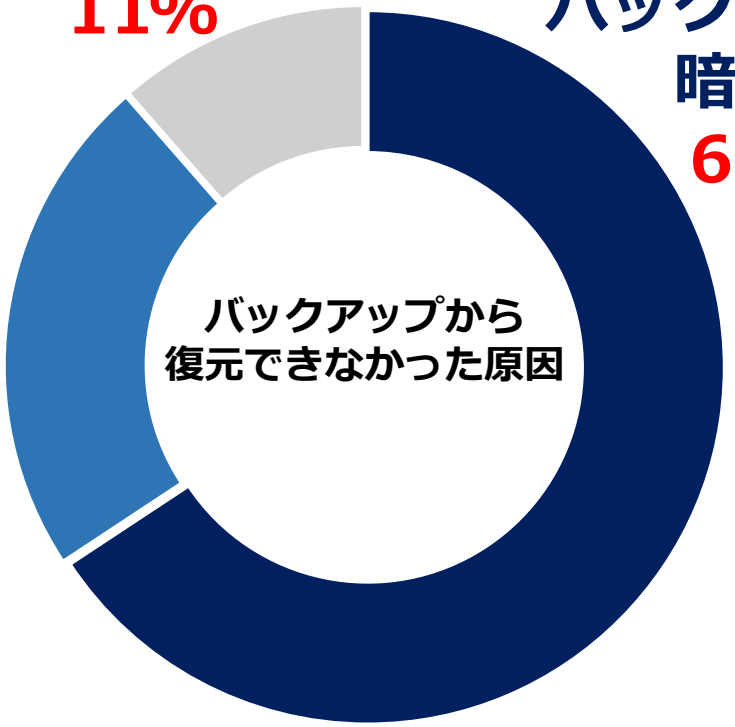
取得有
96%



復元可
15%

復元不可
85%

運用不備
23%



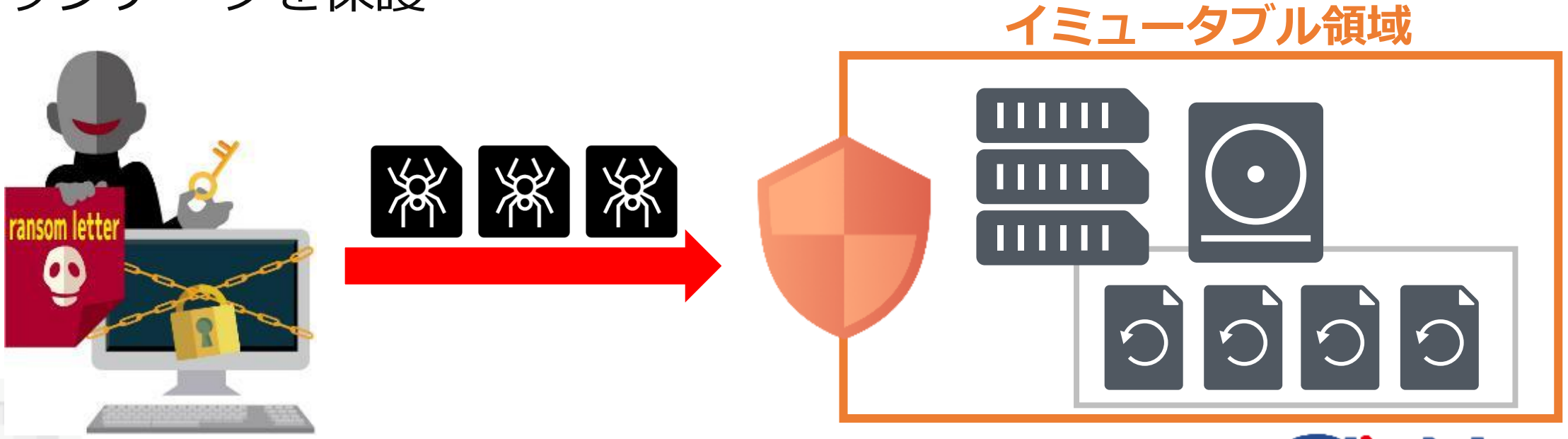
その他
11%

バックアップも
暗号化
66%

ランサムウェアに負けないバックアップ

イミュータブル(変更不可)バックアップが必要

データを変更不可能にして削除や改ざん、暗号化を防ぎ、バックアップデータを保護



Climb Inc.
Growing to Meet Your Needs

アサヒグループHDでランサムウェア被害

2025/9/29にランサムウェアによるシステム障害が発生

- 国内グループ各社の受注・出荷業務が停止
- お客様相談室などのコールセンター業務が停止
- 財務文書などの内部情報が窃取
- 個人情報が流出した可能性あり

企業への影響

- 復旧に多大な**時間とコストを消費**
- 機密データを人質に**身代金を要求される**
- 顧客や従業員の**個人情報が流出**

復旧に2億円

異例の決算発表困難

トヨタ系も

情報搾取と晒し

ランサムウェア対策における課題

課題 1.
ランサムウェアの侵入

課題 2.
データ保護

課題 3.
感染後の対策

解決 1.
感染予防

解決 2.
バックアップ
ウイルス検知

解決 3.
データの復旧

Growing to Meet Your Needs


veeam

ランサムウェア対策における課題

課題 1.

ランサムウェアの侵入

解決 1.

感染予防

課題 2.

データ保護

解決 2.

バックアップ
ウイルス検知

課題 3.

感染後の対策

解決 3.

データの復旧

3-2-1-1-0ルール

3
3つの
データコピー

2

2つの異なる
メディアに保存

1
そのうち**1**つは
オフサイトに保管

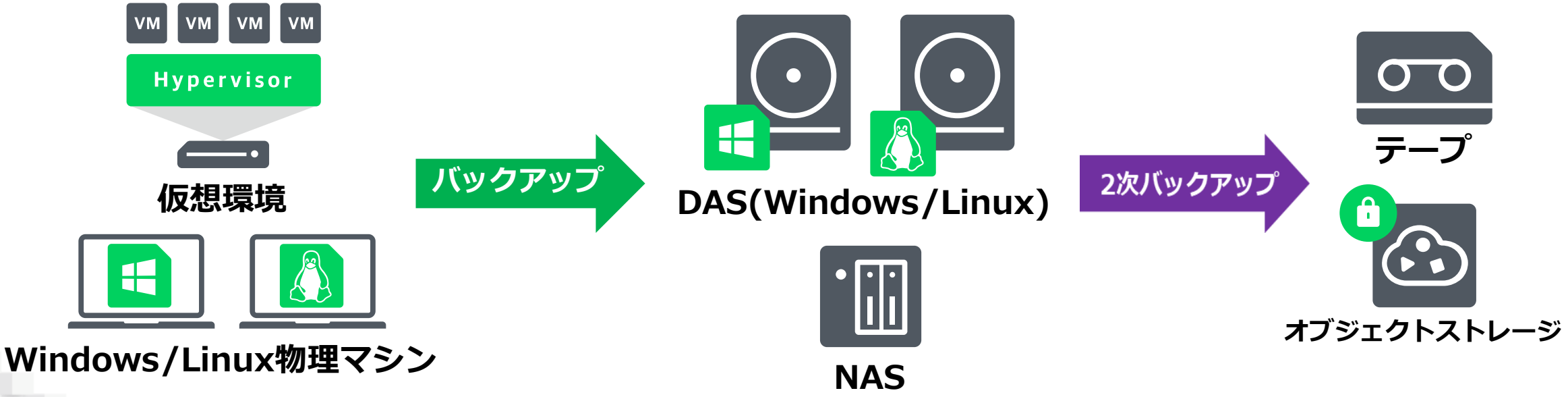
veeam

1
そのうち**1**つは
オフライン
or
イミュータブル

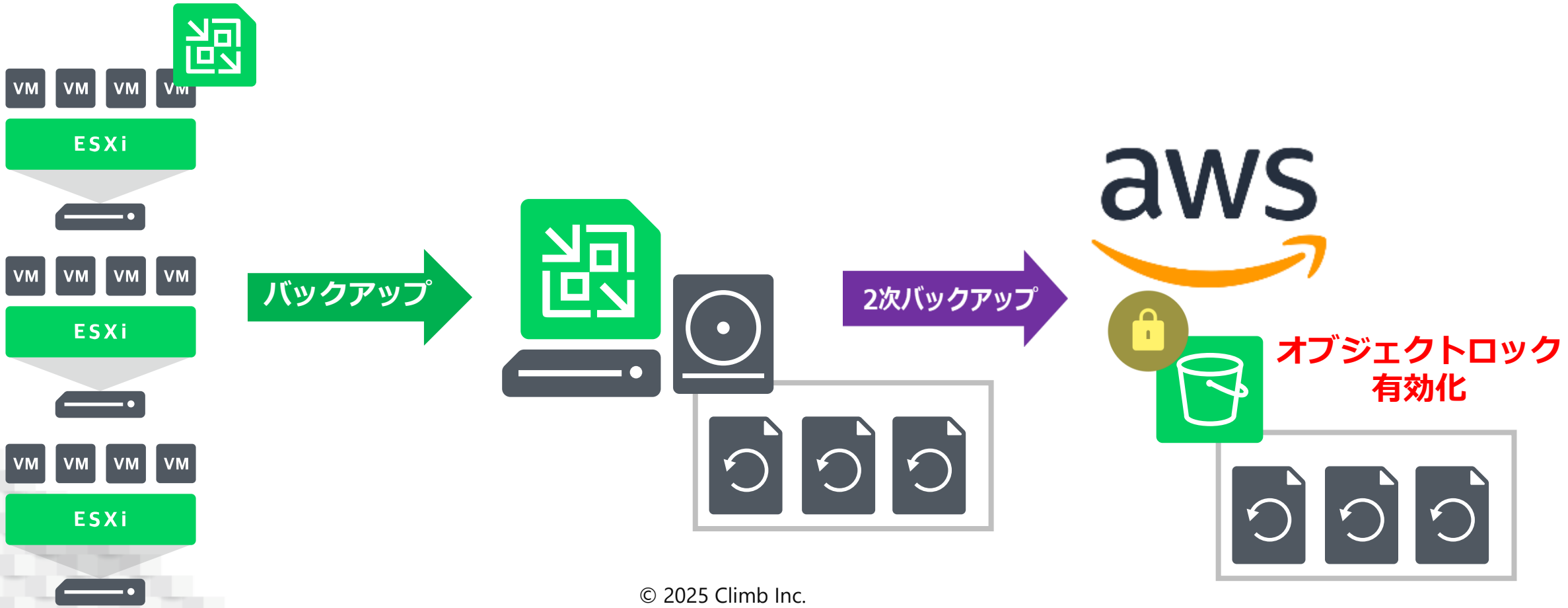
0
バックアップテスト
リカバリ検証で
エラーを**0**に

Climb Inc.
Growing to Meet Your Needs

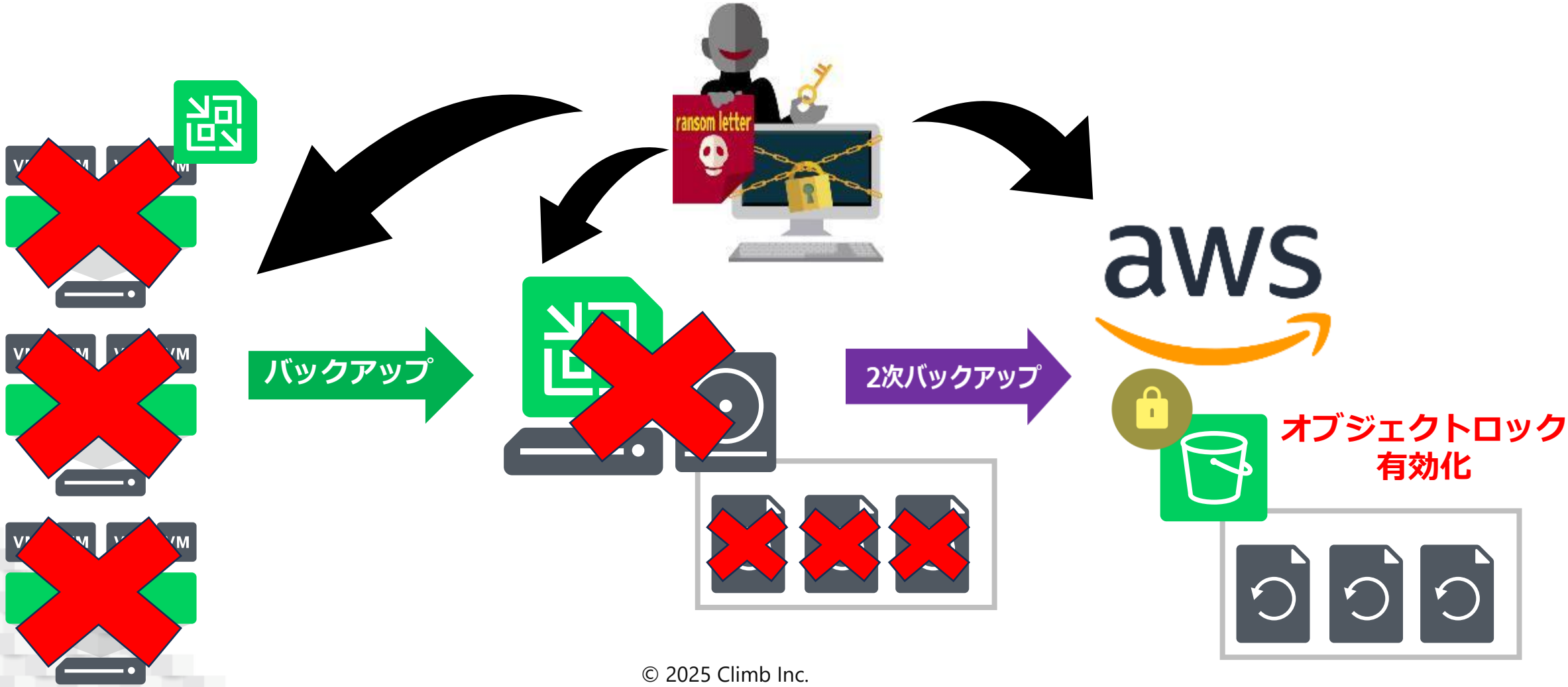
Veeamで実践する3-2-1-1-0ルール



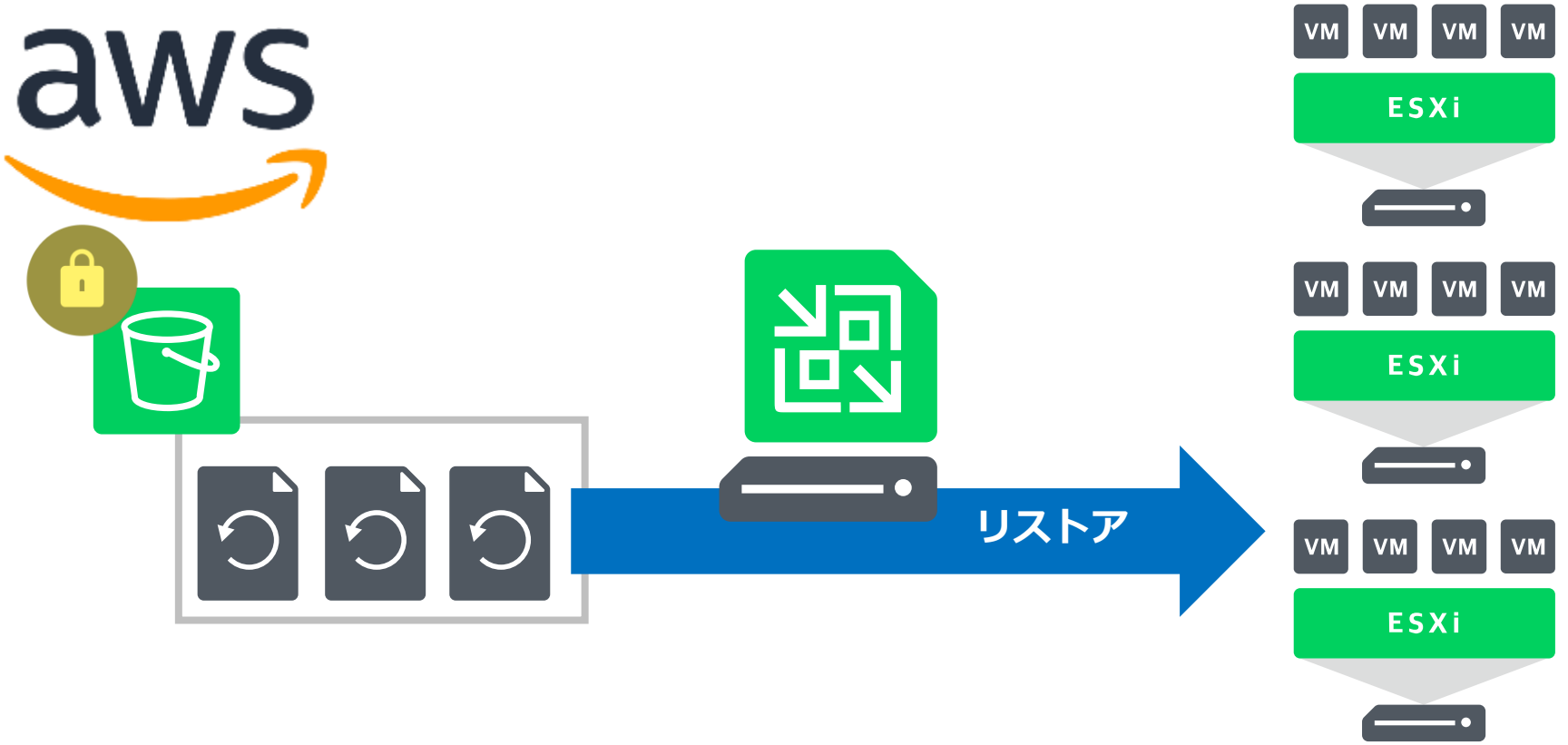
某製造業様の事例



某製造業様の事例



某製造業様の事例

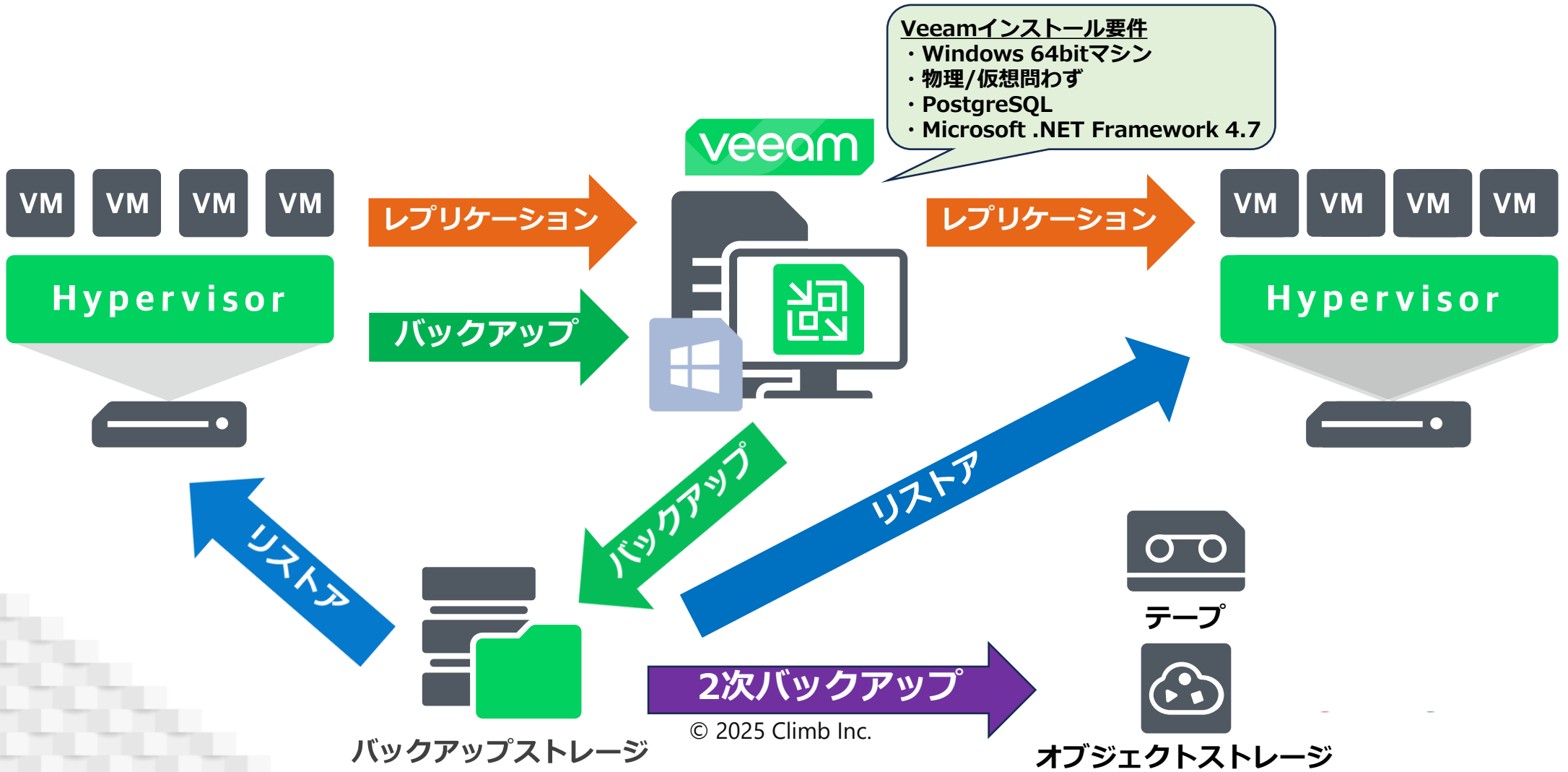


Climb Inc.
Growing to Meet Your Needs

アジェンダ

- サイバー攻撃の概要
- ランサムウェア攻撃の現状とトレンド
- Veeamの主なデータ保護手法
- Veeamのランサムウェア対策機能

Veeamのデータ保護



Veeam対応環境

仮想環境

vmware
PROXMOX
Microsoft Hyper-V
ORACLE KVM
Red Hat Virtualization
NUTANIX

物理環境

Windows
solaris
Linux
AIX

クラウド環境

aws
Google Cloud
Azure

その他

Microsoft 365
kubernetes
NAS/ファイルサーバ

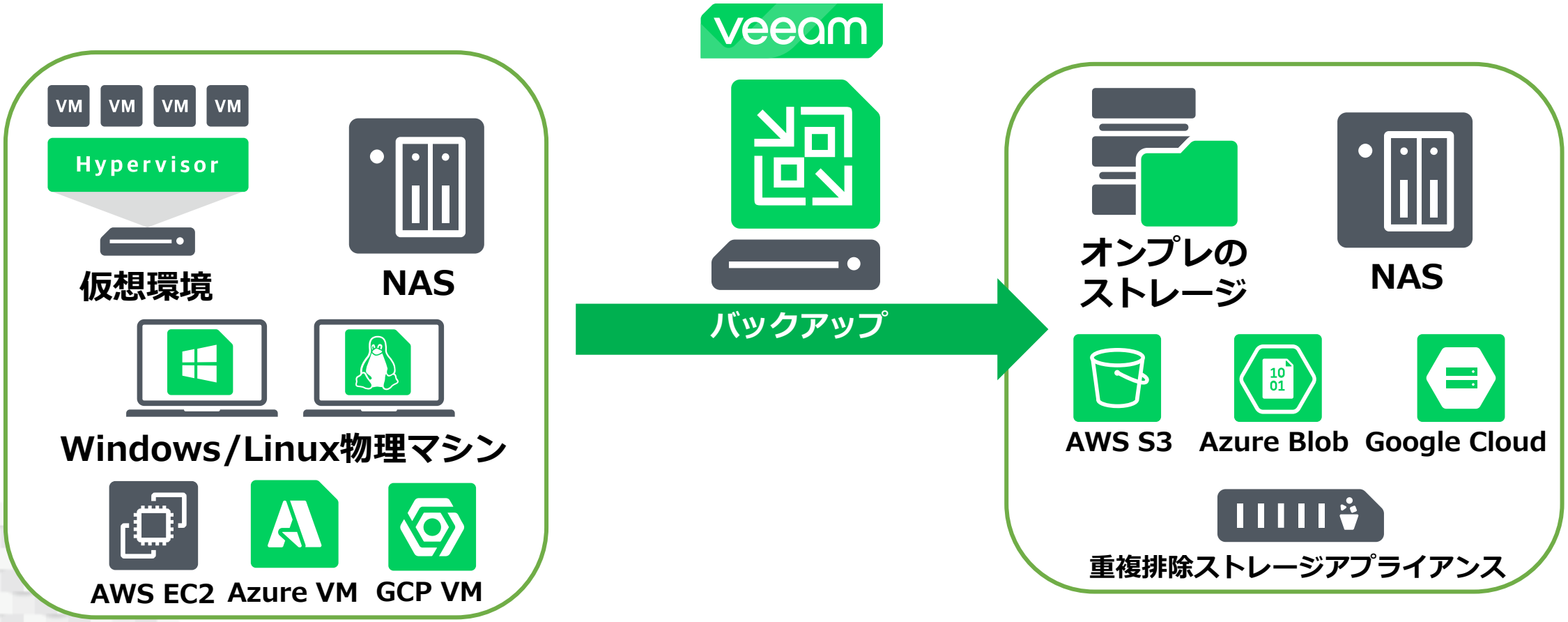
バックアップ

- **イメージベース**でのバックアップ
- **エージェントレス**で利用可能
- データを**圧縮・重複排除**して転送

Climb Inc.
Growing to Meet Your Needs

バックアップの保存先

バックアップ



Climb Inc.
Growing to Meet Your Needs

2次バックアップ

1次バックアップデータを**任意の別ストレージへコピー**

- 3-2-1-1-0ルールを実現
- GFS設定による長期保存

<アーカイブ先>

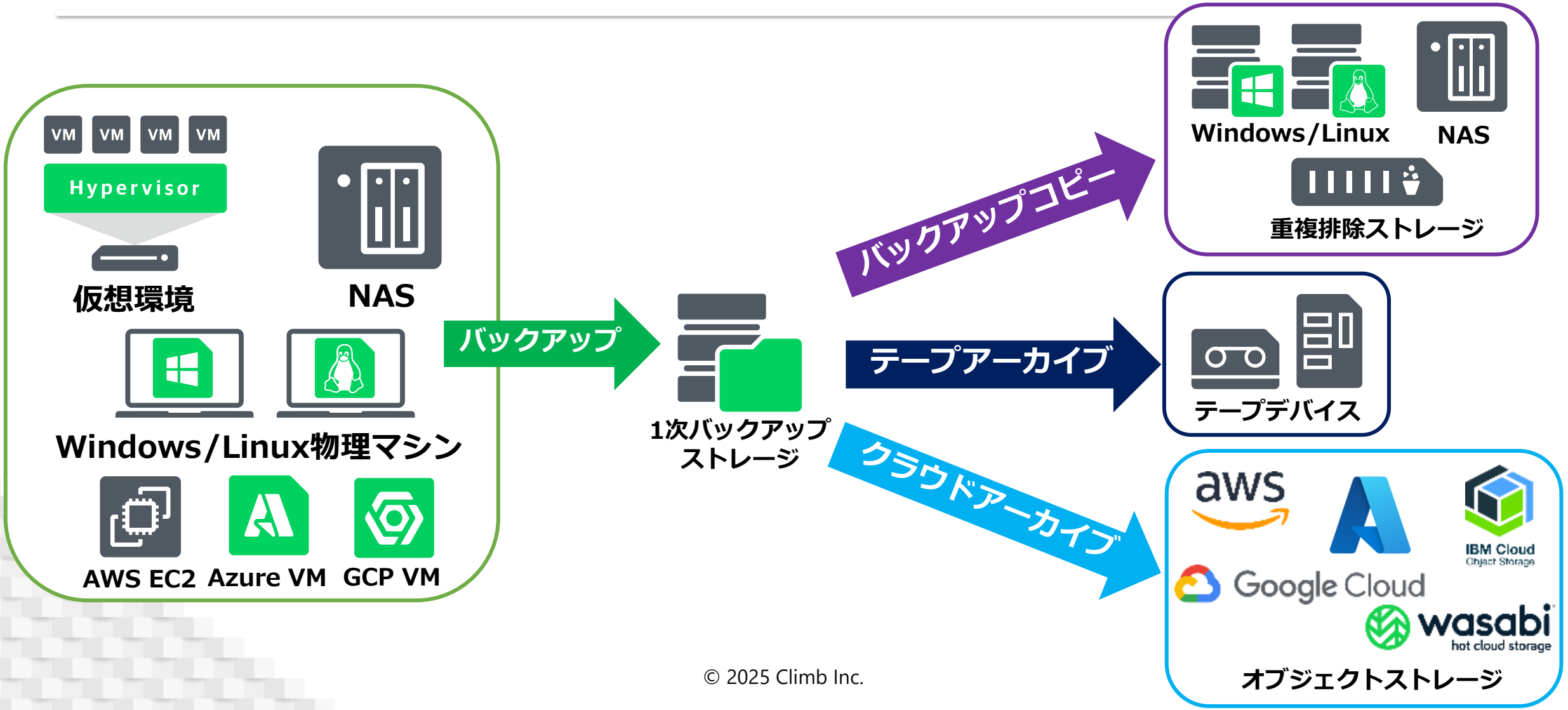
➢別ストレージ（DAS/NAS/重複排除ストレージ）

➢テープ

➢オブジェクトストレージ

Climb Inc.
Growing to Meet Your Needs

2次バックアップ



リストア

- **イメージベースのリストア**
  - マシン全体を元の or 別の環境へリストア
- **インスタントリカバリ**
  - バックアップデータから直接VMを起動
- **ゲストOSファイルのリストア**
  - ゲストOS上の特定のファイルやフォルダのみリストア
- **アプリケーションアイテムのリストア**
  - 特定のアプリケーションデータをリストア

Climb Inc.
Growing to Meet Your Needs

レプリケーション

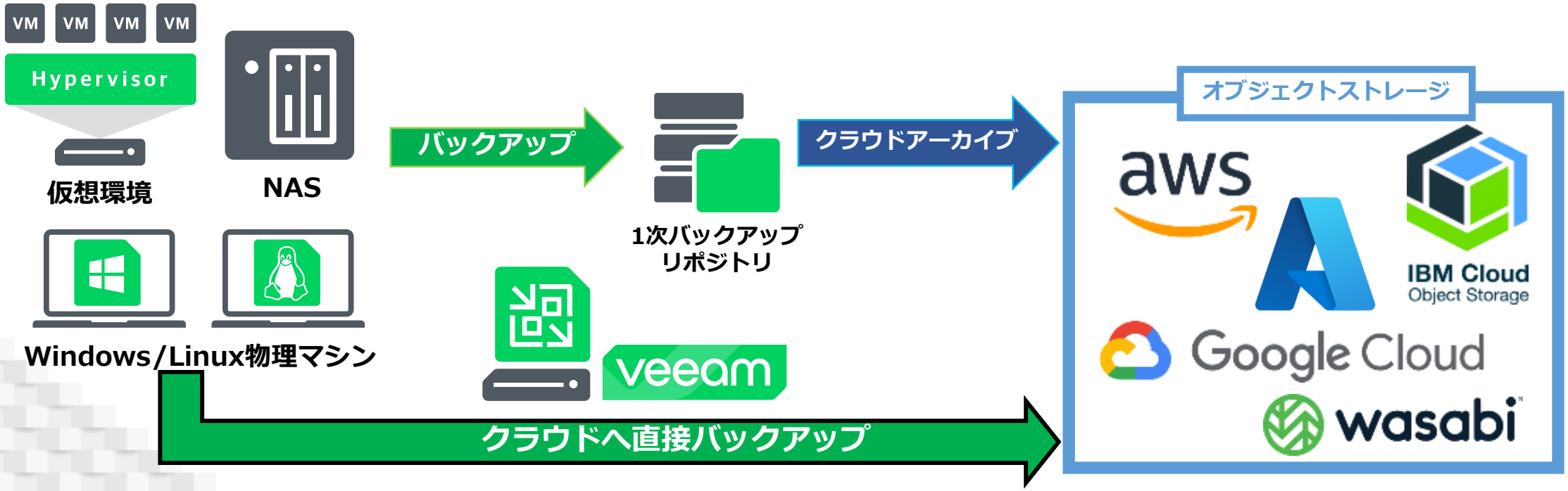
別ホストに対して**仮想マシンの複製**(レプリカVM)を作成
→ほぼ無停止での復旧が可能

アジェンダ

- サイバー攻撃の概要
- ランサムウェア攻撃の現状とトレンド
- Veeamの主なデータ保護手法
- Veeamのランサムウェア対策機能

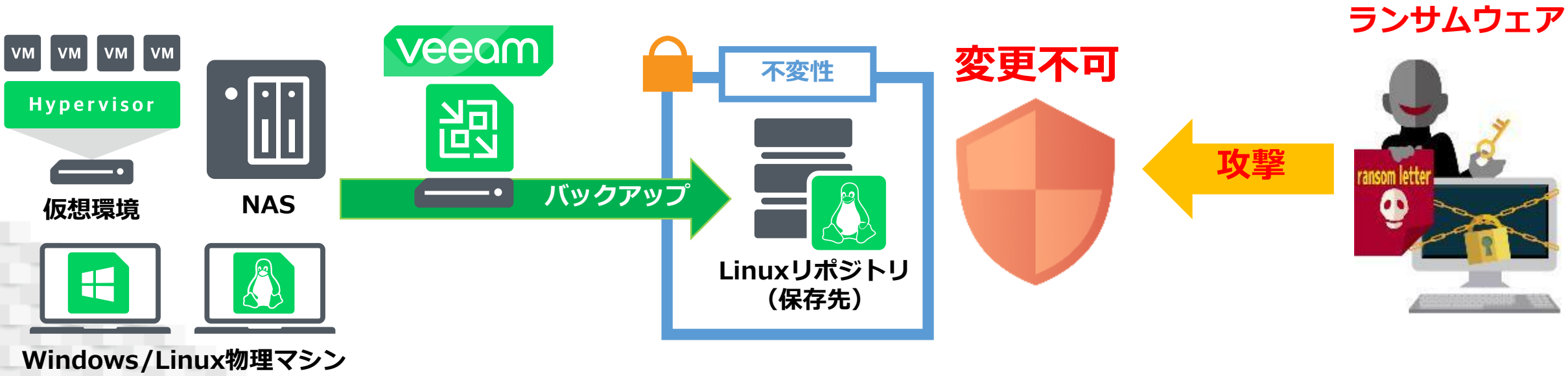
クラウドへのバックアップ

- **オブジェクトロックと連携**したイミュータブルバックアップ
- VPN等の構成不要



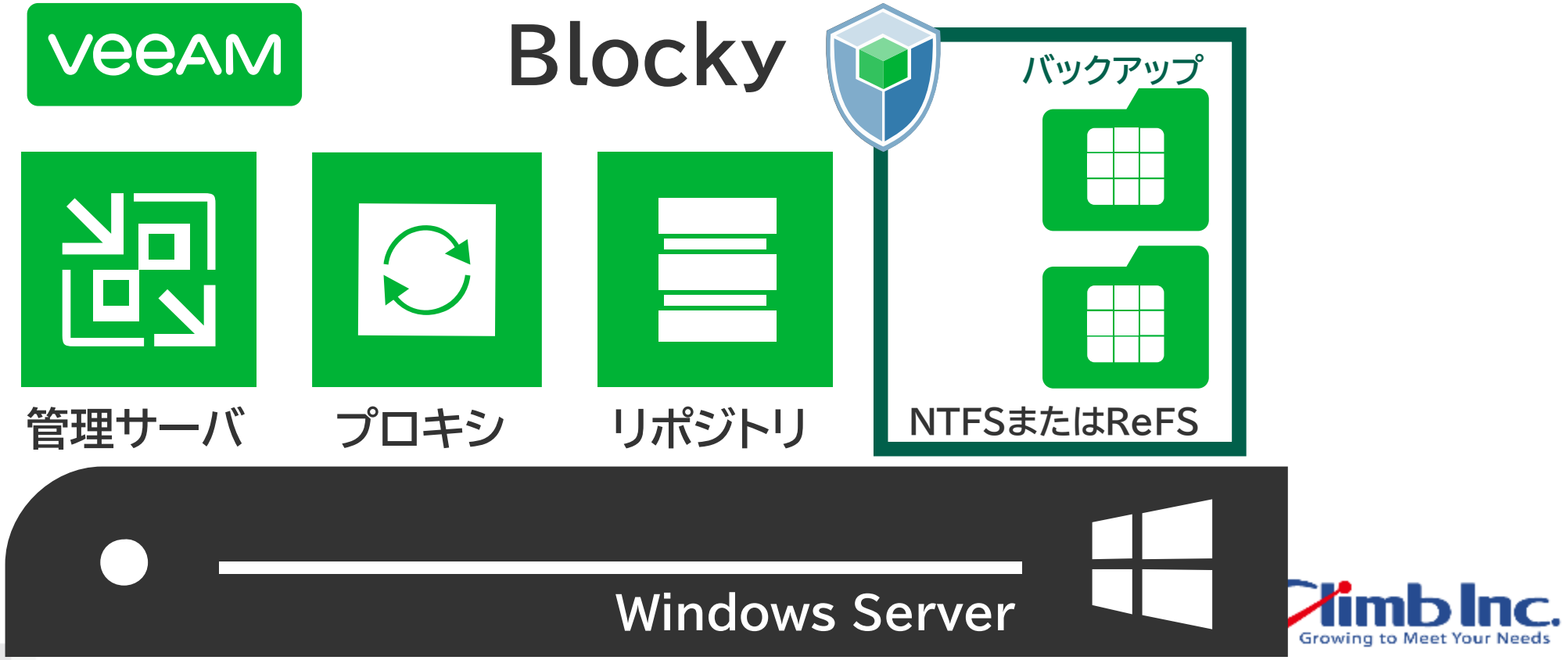
Hardened Repository(堅牢化リポジトリ)

- バックアップファイルに**不変属性を付与**
- シングルユース(使い捨て)認証情報の使用
- SSHプロトコルへの依存なし



Veeam + Blocky

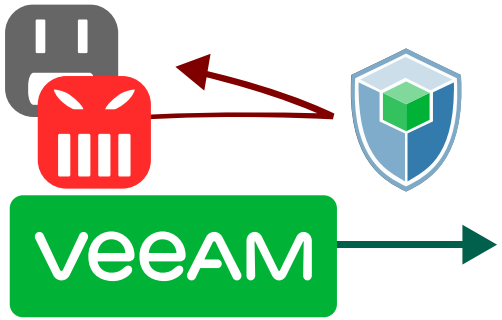
Windowsマシン1台でランサムウェア対策、ゼロトラスト構成



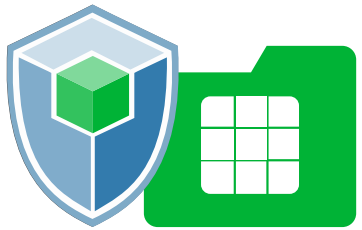
デフォルト拒否で、確実にブロック

アプリケーションホワイトリスト（AWL）アプローチ

→**Veeamだけを許可**して、システムアプリからのアクセスも拒否



許可アプリのみ
がアクセス可能



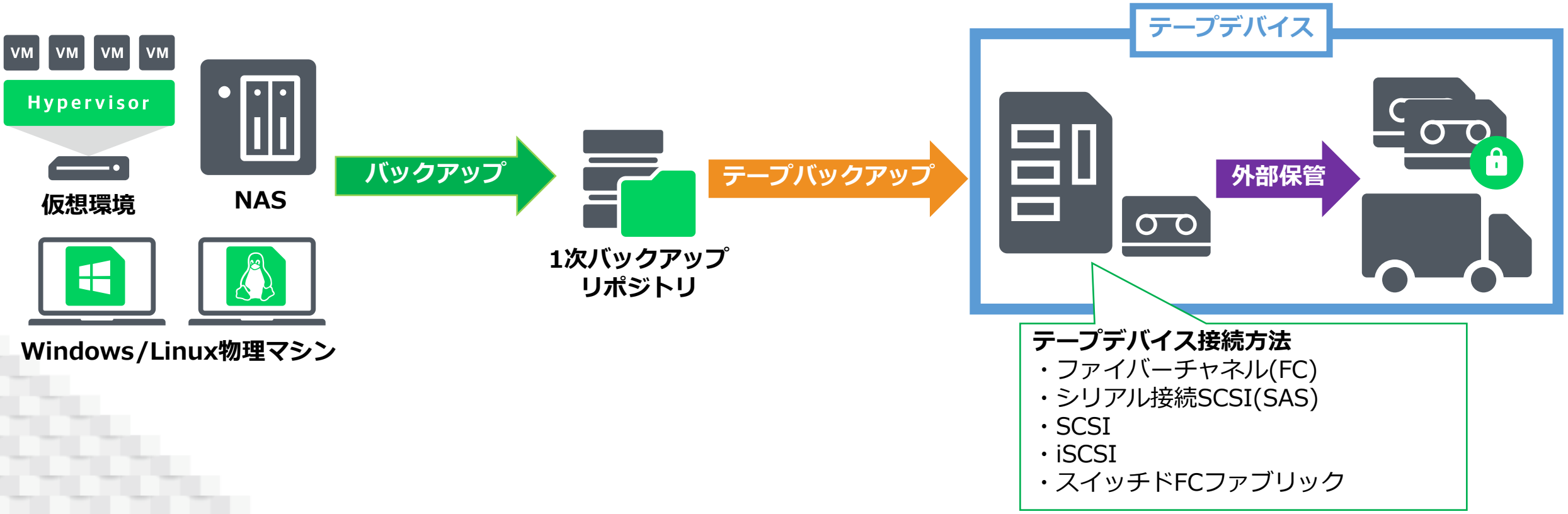
デフォルトで
アクセスを拒否

信頼中 心の
アプローチ

Climb Inc.
Growing to Meet Your Needs

テープへのアーカイブ

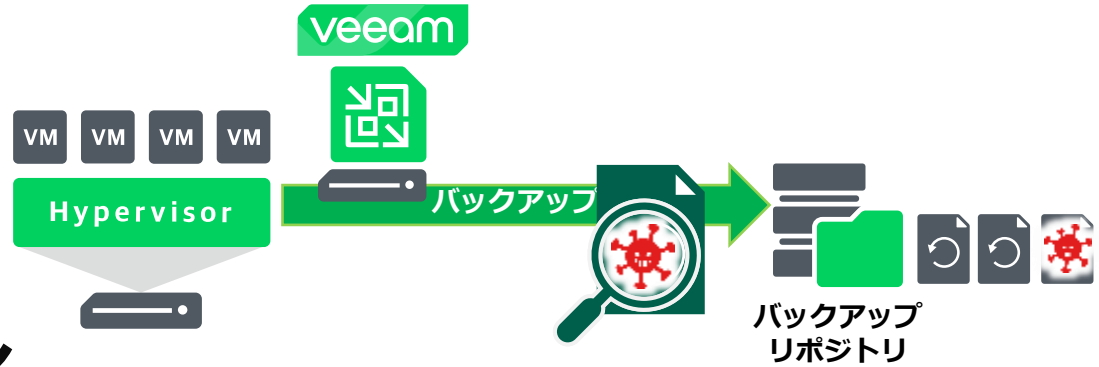
1次バックアップデータを**2次バックアップとしてテープ**へ保存



ウイルス検知機能

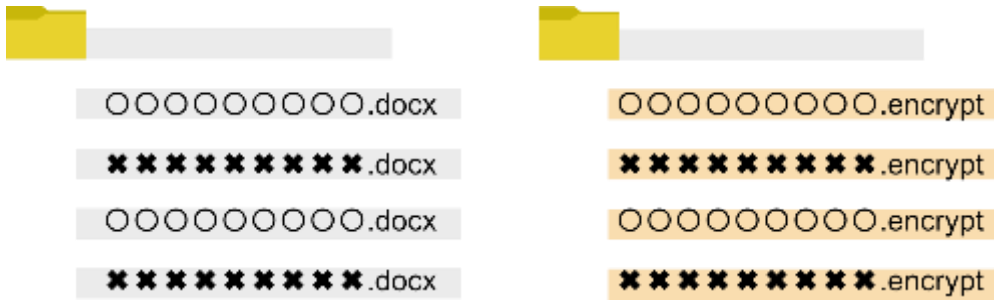
- **インラインスキャン**

  バックアップ時に処理したデータブロックをスキャンし、**マルウェアを検知**



- **ゲストインデックスデータスキャン**

  バックアップ時に作成した**ゲストOSファイルシステムのインデックスをスキャン**



健全性検証

- **SureBackup**
  隔離環境にVMを起動させることでバックアップの健全性検証

- **Scan Backup**
  取得済みのバックアップデータに対してウイルスチェックを行い、正常なバックアップを検知

- **セキュアリストア**
  リストア前にバックアップをウイルススキャン

まとめ

- ランサムウェアによる被害は増加の一途
- バックアップデータも狙われる時代に突入

→運用環境だけでなく、バックアップデータ自体の保護が必要不可欠

Veeamを利用すれば、幅広い環境の**イミュータブルバックアップ**からバックアップデータの**健全性検証**まで実現

Climb Inc.
Growing to Meet Your Needs