クラウドを活用して
ランサムウエア被害から
迅速に復旧する方法

吉田 尚壮
ヴイエムウェア株式会社
クラウドサービス技術本部
リードクラウドソリューションアーキテクト

vmware®

アジェンダ

ランサムウエアと復旧対策の重要性

ランサムウェア対策に最適なソリューション

安全で迅速な復旧方法

まとめ

アジェンダ

ランサムウエアと復旧対策の重要性

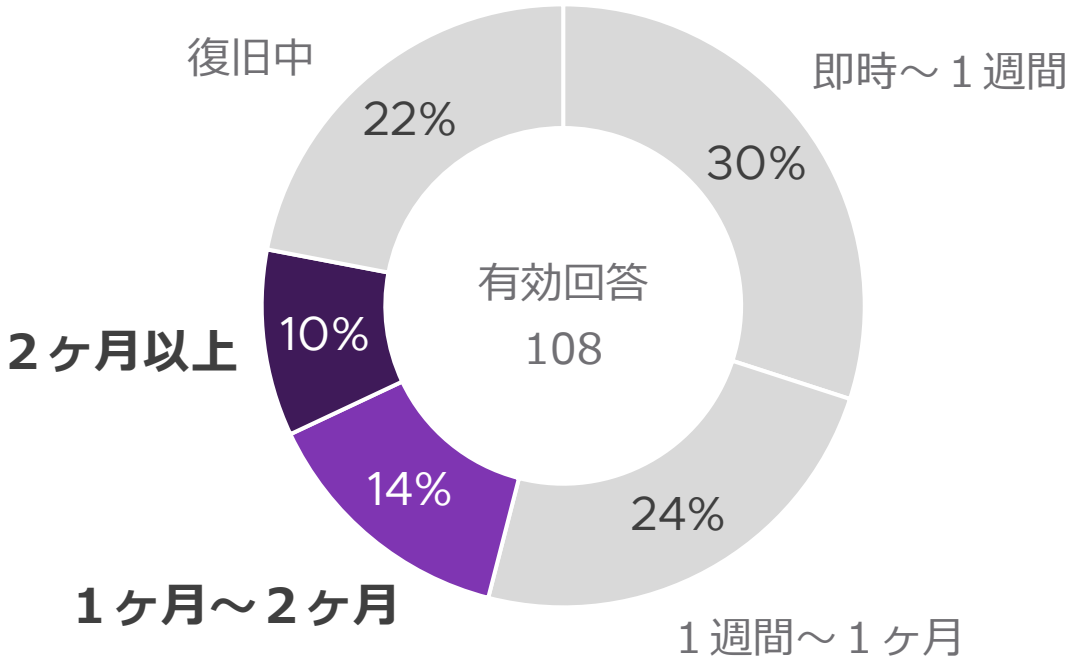
ランサムウェア対策に最適なソリューション

安全で迅速な復旧方法

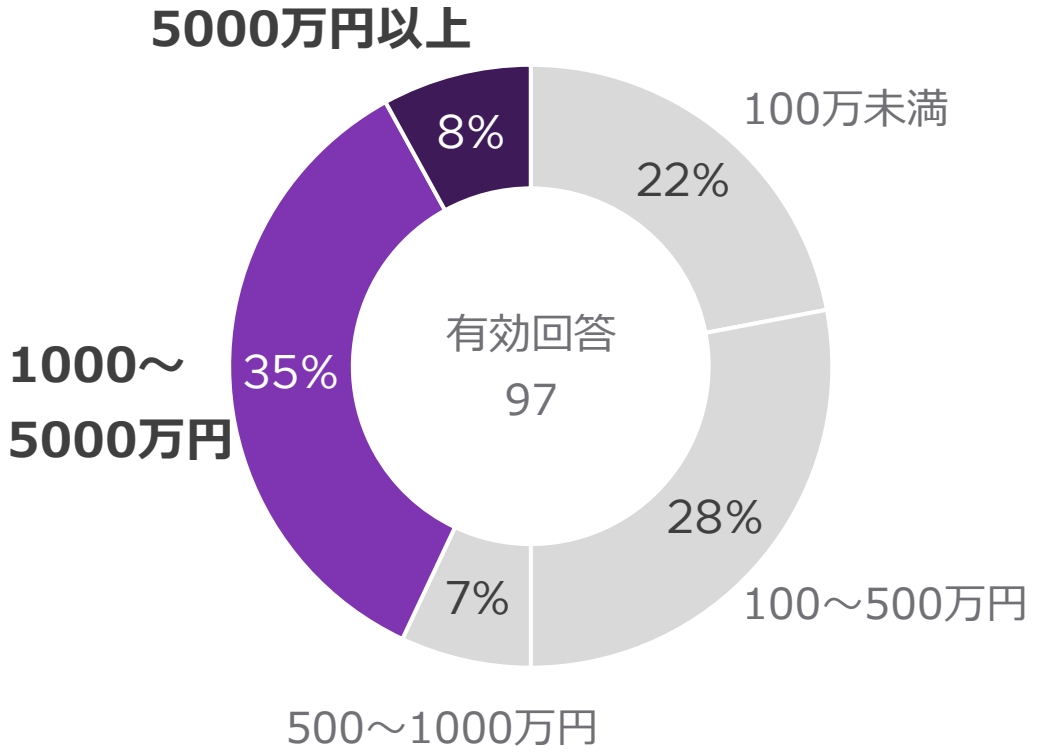
まとめ

ランサムウェアによる被害の実態

復旧に要した期間

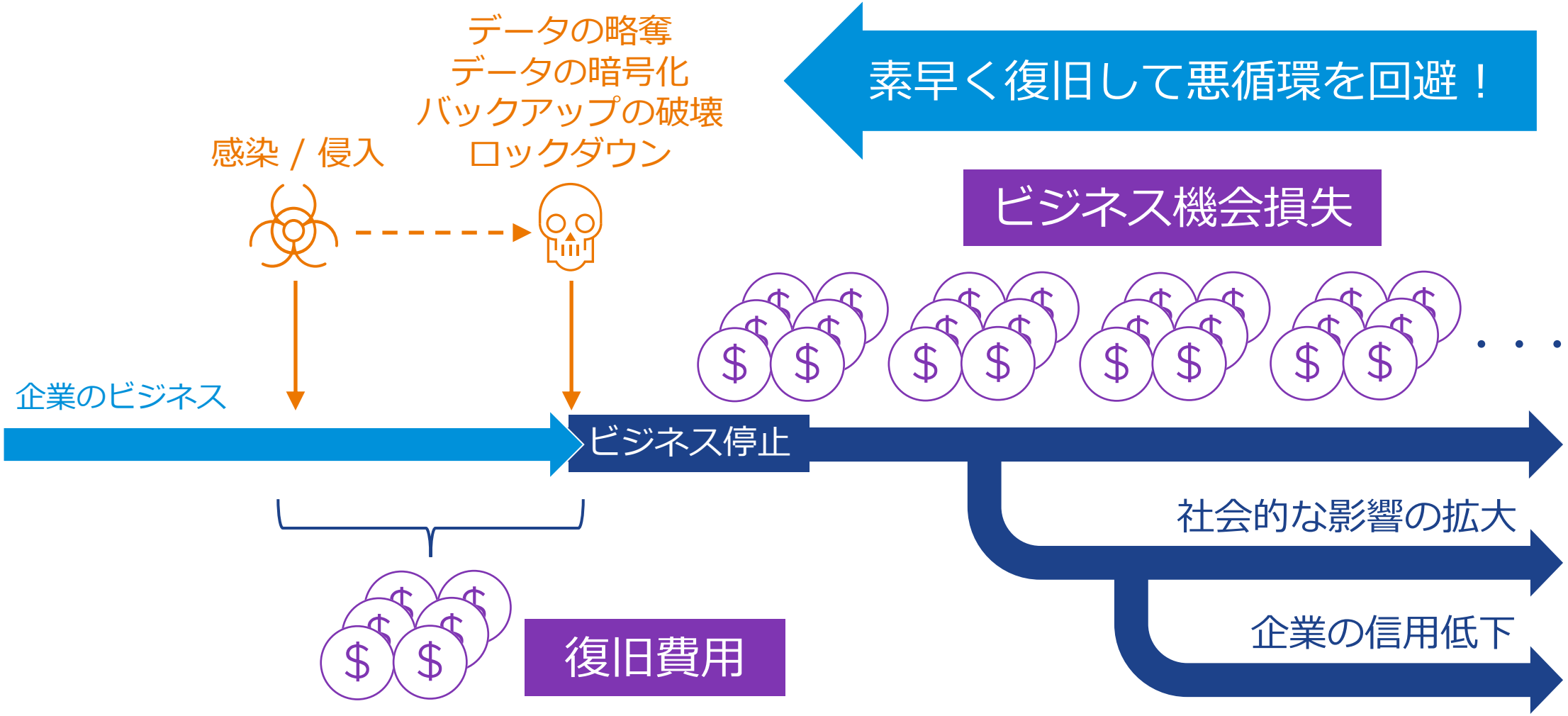


復旧費用の総額

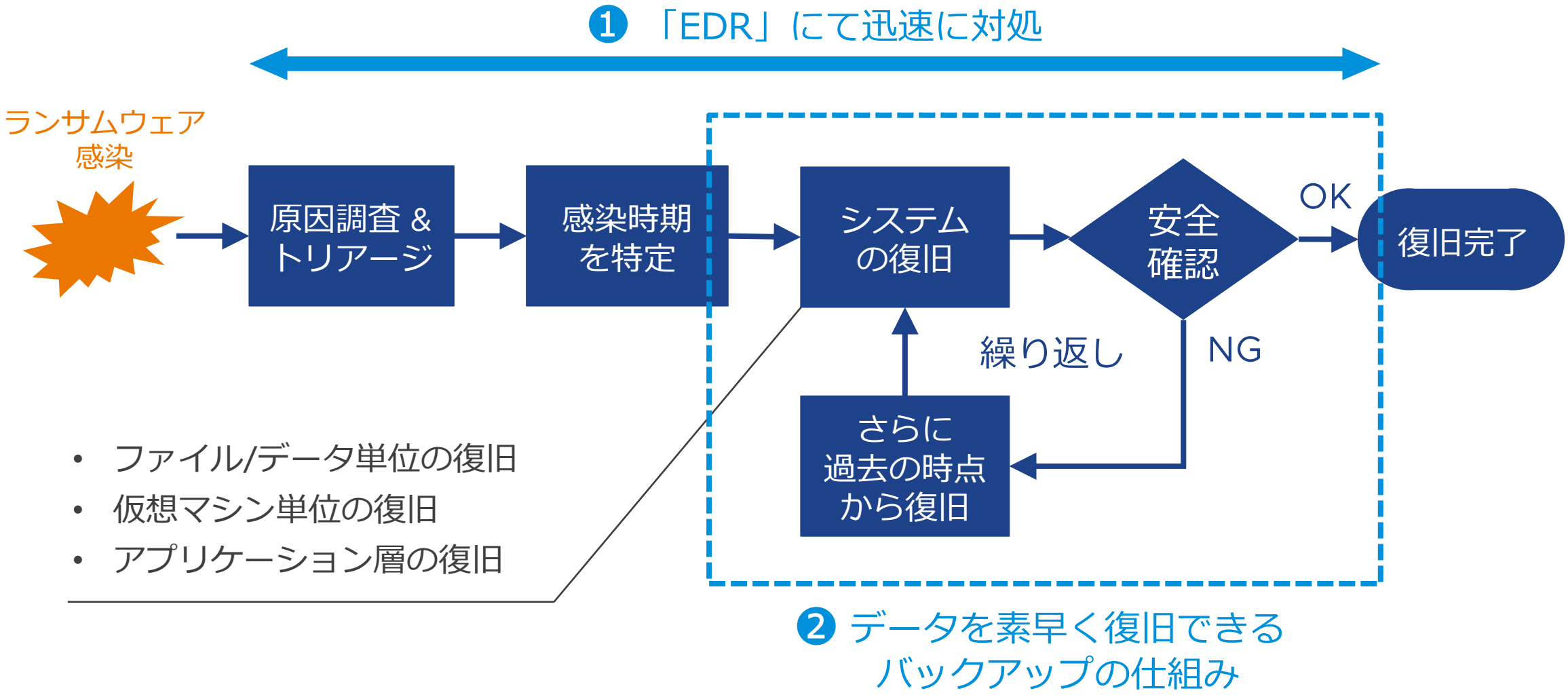


出典：警察庁「令和３年におけるサイバー空間をめぐる脅威の情勢等について」

復旧対策を強化して被害を最小限に抑えたい



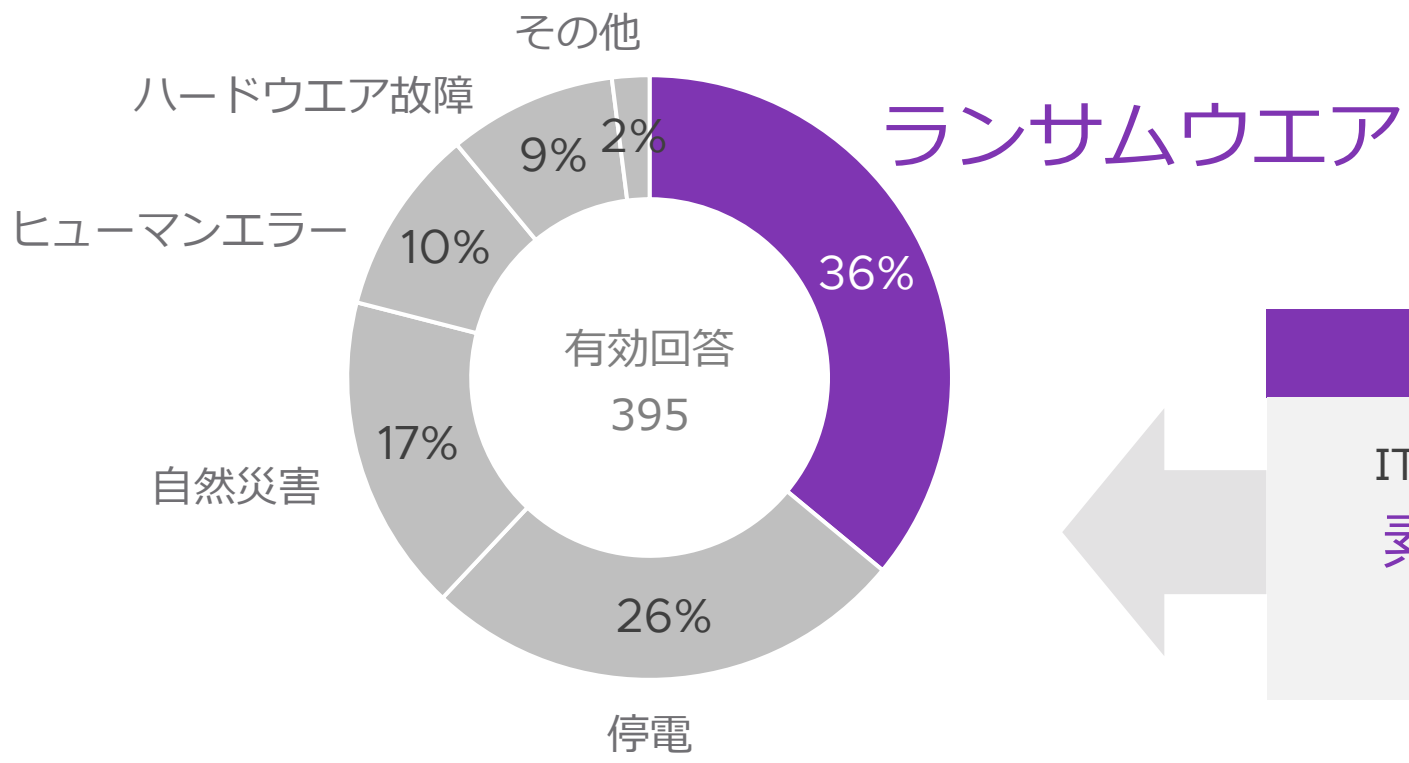
復旧期間を短縮する対策



EDR：Endpoint Detection & Response

ランサムウェア被害の復旧に「災害対策」も利用されている

災害対策を発動した理由



背景

IT の災害対策には、多数の仮想マシンを
素早く同時に復旧する機能
が採用されているため

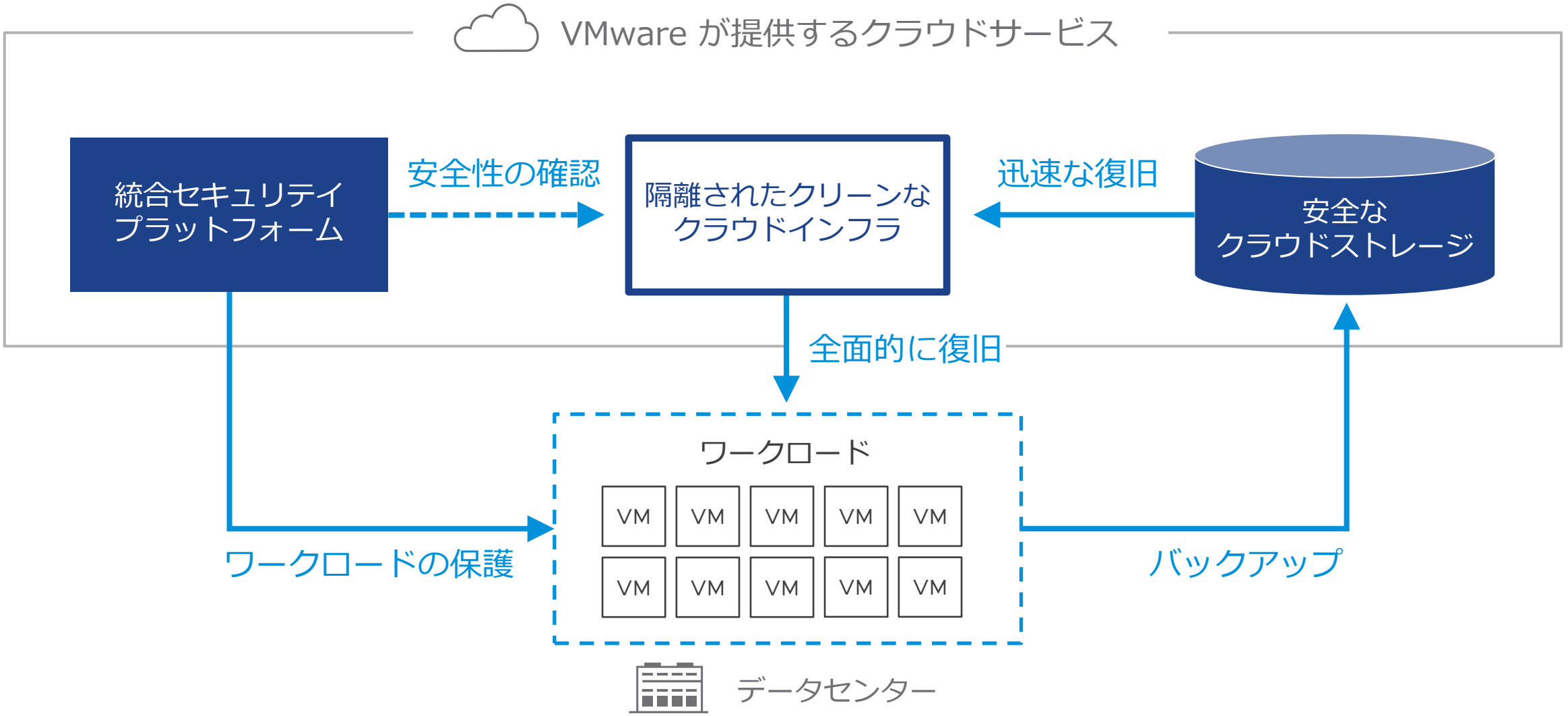
出典：Datrium : The State of Enterprise Data Resiliency and Disaster Recovery (2019)

復旧手段の違い

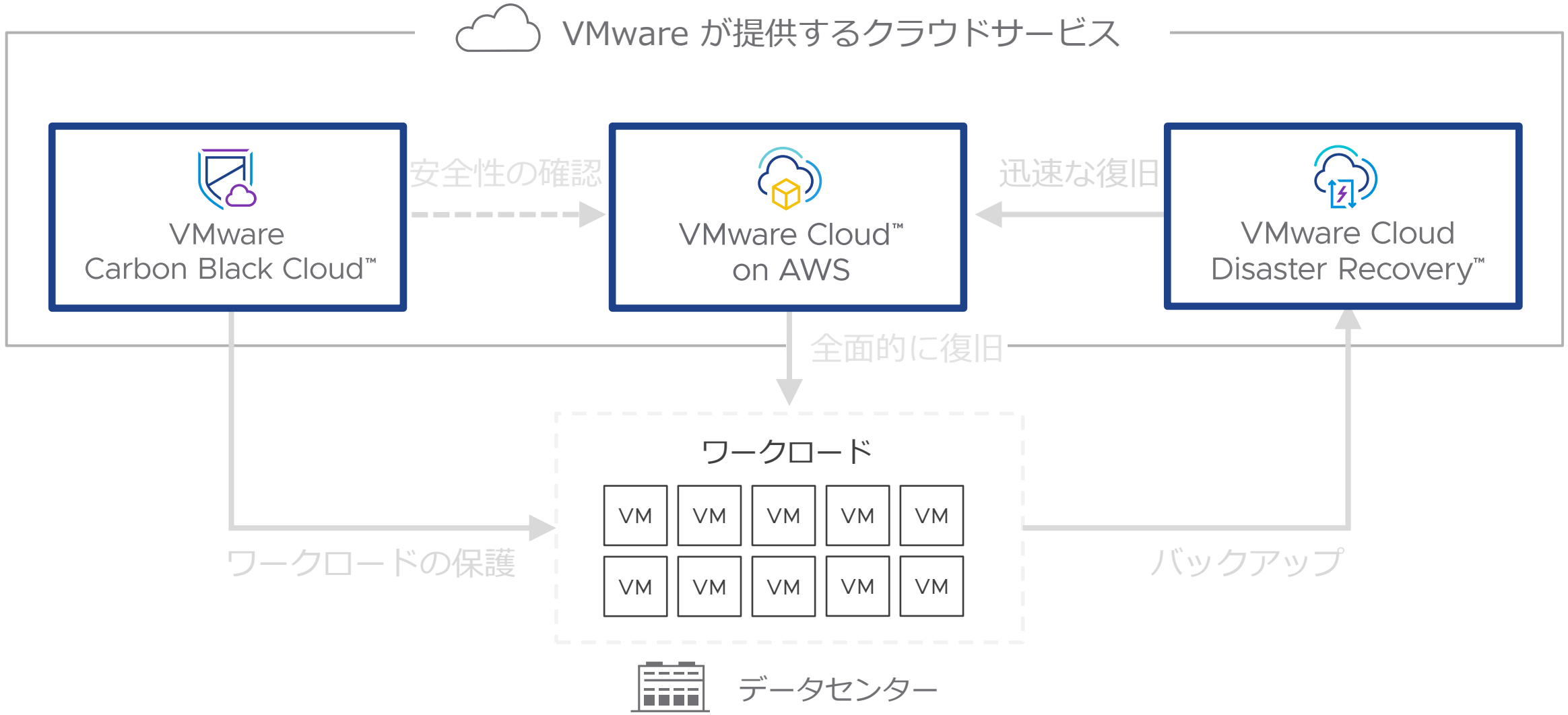
ランサムウェア被害の特徴に適した復旧手段を選びたい

	スナップショット	バックアップ	災害対策	VMware の クラウド災害対策
テクノロジー	スナップショット (VSS)	バックアップ	レプリケーション	レプリケーション ＋スナップショット
保護データの場所	端末内	バックアップ ストレージ	災害サイト (データセンター)	クラウド
ファイル単位の復旧	○	○	×	○
VM 単位の復旧	×	○	○	○
多数 VM の即時復旧	×	▲	○	○
数ヶ月前の状態に復旧	▲	○	▲	○

クラウドを活用したランサムウェア復旧対策



クラウドを活用したランサムウェア復旧対策



アジェンダ

ランサムウエアと復旧対策の重要性

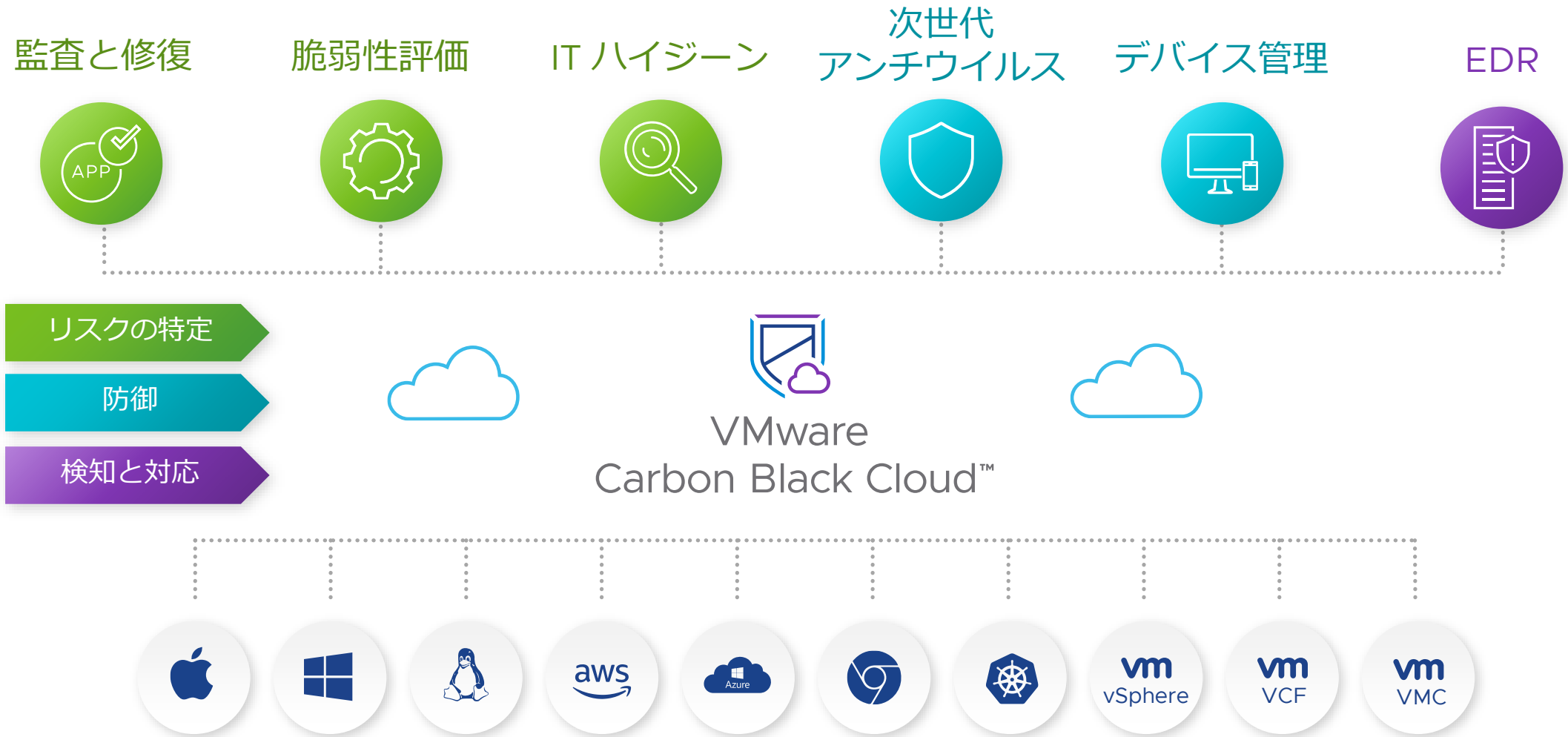
ランサムウェア対策に最適なソリューション

安全で迅速な復旧方法

まとめ

VMware Carbon Black Cloud Workload

次世代アンチウイルスと EDR を実装した包括的なワークロード保護ソリューション

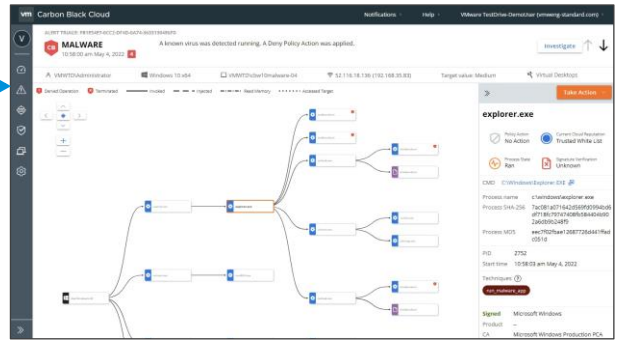


VMware Carbon Black Cloud Workload の構成と管理

セキュリティ管理者

- ワークロード全体の状態把握
- 脆弱性評価
- 調査と対処（遠隔操作など）

Carbon Black Cloud 管理コンソール

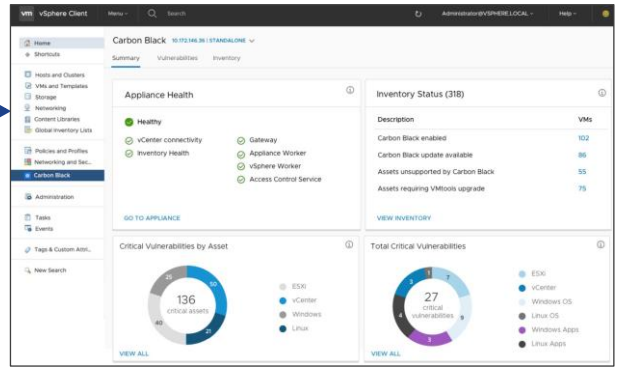


連携と協働を促進

クラウド/インフラ管理者

- vSphere 上の脆弱性管理
- インベントリ管理
- ライフサイクル管理など

vSphere Client



VMware Carbon Black Cloud™

全プロセスログを取得（エージェント経由）

VM VM VM VM VM

vSphere | SDDC

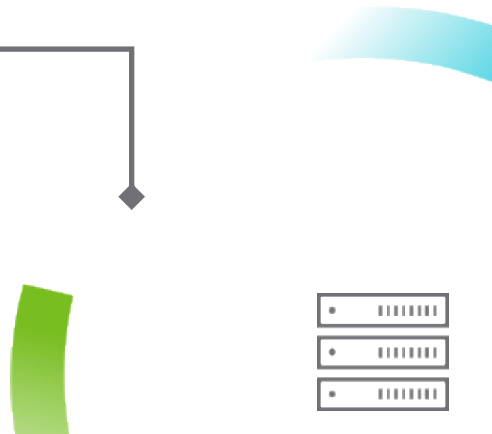
データセンターのワークロード

あらゆる攻撃を予測・検知して防御から対処まで網羅

VMware Carbon Black Workload™

脆弱性の可視化

- ワークロード全体を可視化
- パッチの適用状況を把握
- リスクスコアによる対応優先度の把握
- 脆弱性の特定と評価
- リアルタイム検索による脅威の発掘調査



次世代アンチウィルス

- 未知のマルウエアから防御
- ファイルレス攻撃から防御

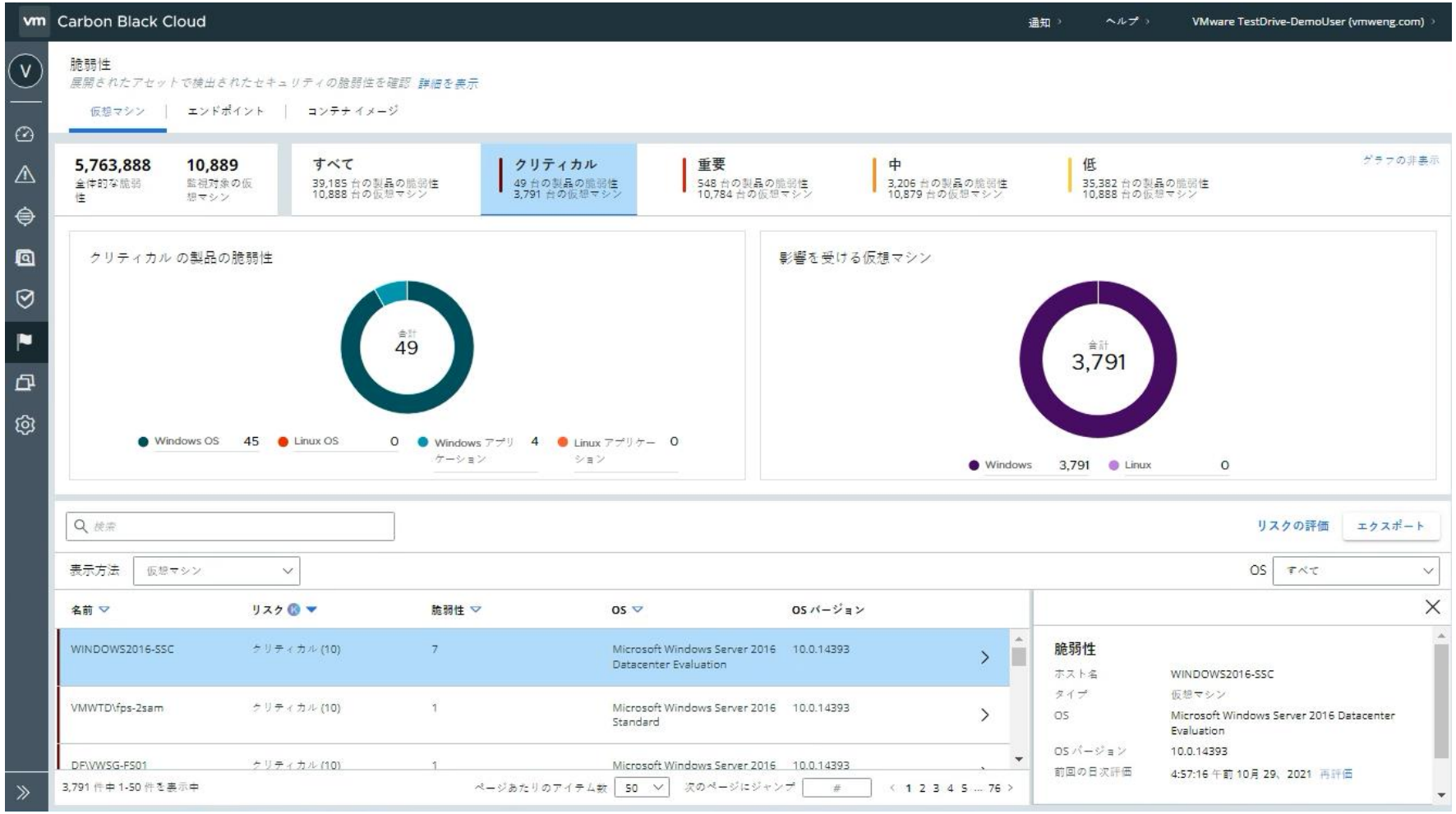
EDR

- 全てのプロセスログを記録し脅威を素早く検知
- 攻撃の可視化
- 迅速な原因特定と早期対応
- ワークロードの修復

脆弱性の可視化

環境全体の脆弱性をリアルタイムに把握・管理できる

リスクの特定



脆弱性の可視化

- ワークロード全体の脆弱性を可視化

リスクスコア

- 脆弱性リスクの評価基準
- 独自の脅威データおよび Kenna Security の高度なモデリングを組み合わせて実現

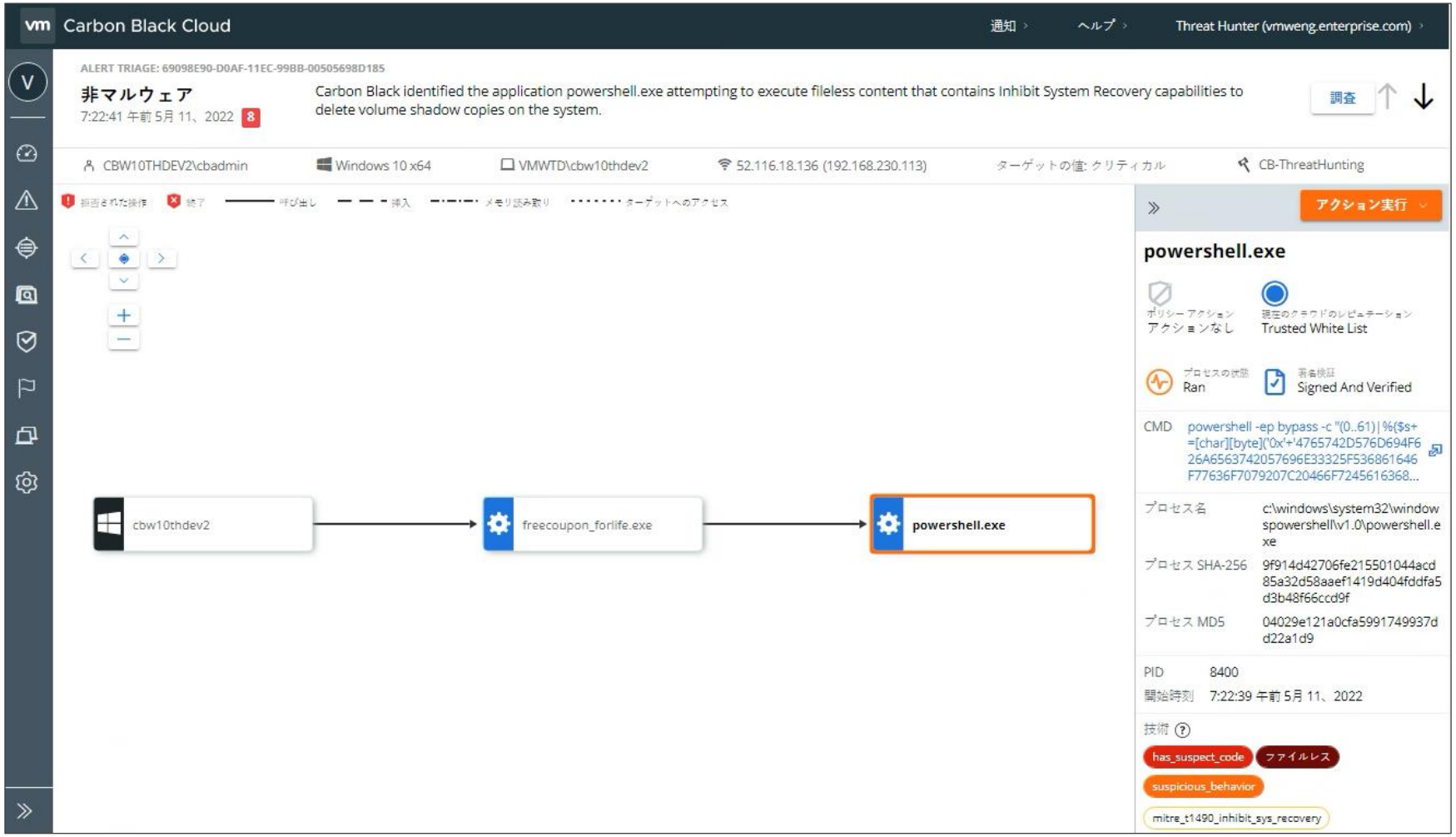
IT ハイジーン

- 調査クエリによる能動的な脅威の発見と対応
- 定期的かつ継続的にワークロードの健全性を維持

次世代アンチウィルス

あらゆる脅威から防御可能

防御

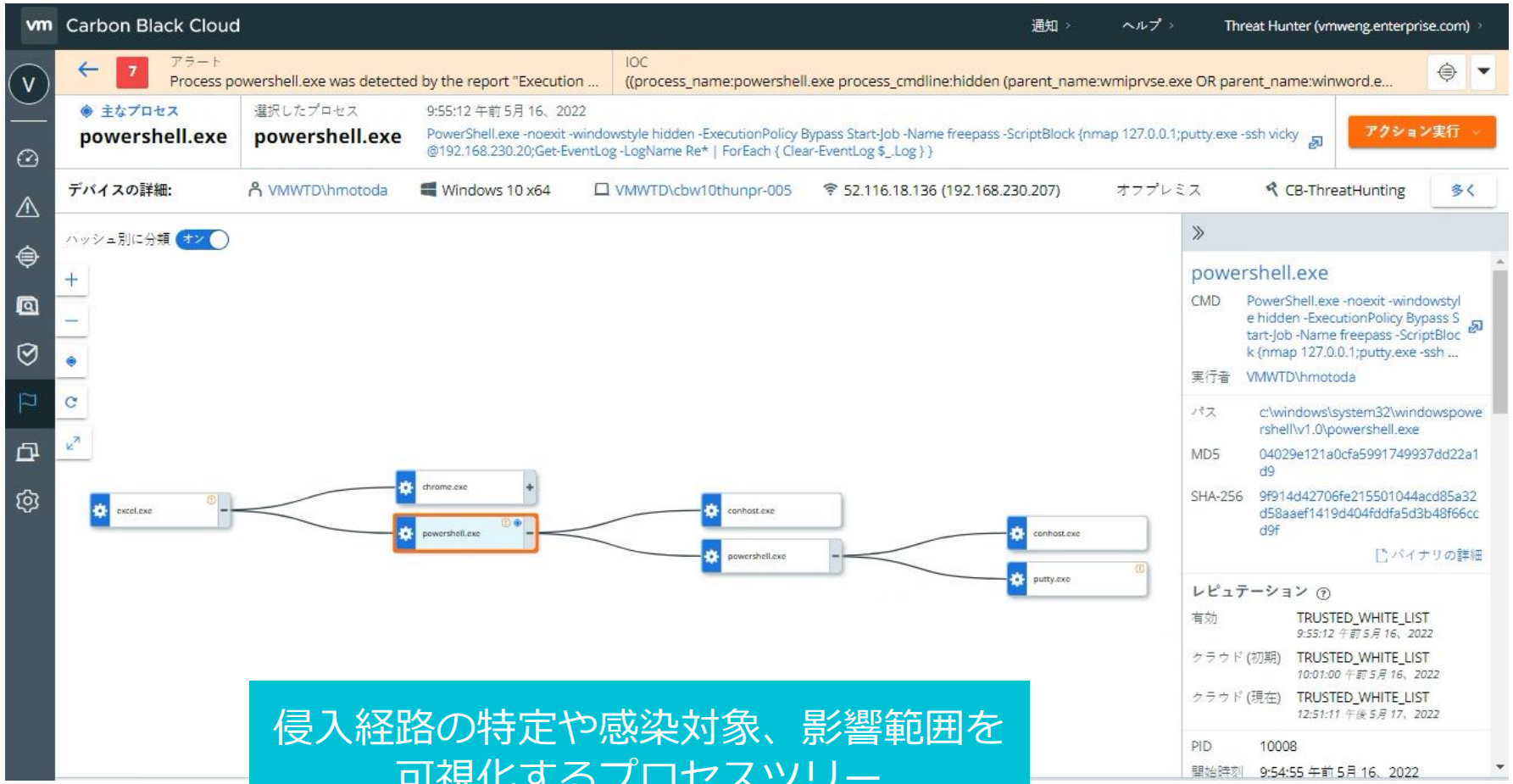


未知の脅威も検知・防御可能

- マルウエア / 非マルウエア / 未知のマルウェアを防御
- 既知 / 未知のランサムウェアも防御

EDR
端末上の動きは、脅威であるかどうかに関わらず全て記録し可視化

検知と対応



侵入経路の特定や感染対象、影響範囲を可視化するプロセスツリー

検出
- 端末内のファイルやプロセス等の動きを全て記録
- 未知の攻撃も検知して被害の拡大を抑制

封じ込め
- 感染端末を隔離

調査
- 過去に遡り原因や影響範囲を特定

復旧
- 不正ファイルの除去と感染端末の復旧

遠隔操作機能

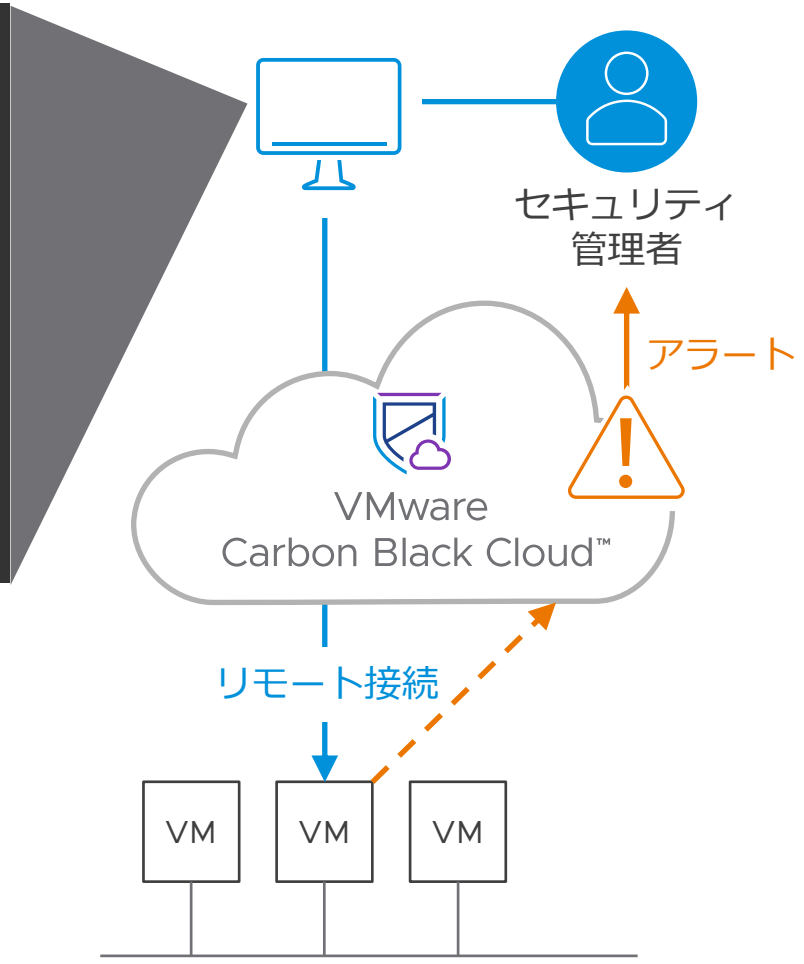
クラウドから各端末に接続し、マルウェアの削除などの修復作業を実行できる

検知と対応

```
デバイス 1624717 の Live Response

[1624717] C:\Windows\system32> help

Live Response のコマンド
cd        現在の作業ディレクトリを別のディレクトリに変更します。
clear     (cls) ターミナル画面を消去します。"cls" コマンドを使用しても同じ操作が可能です。
delete    (rm, del) 特定のファイルを削除します。
detach    現在の Live Response セッションから切り離します。
dir       (ls) 指定されたディレクトリ内のファイルの一覧を表示します。
drives    現在のリモート ホスト上の使用可能なドライブの一覧を表示します (Windows ホストのみ)。
exec      現在のリモート ホスト上でバックグラウンド プロセスを実行します。
execfg    現在のリモート ホスト上でプロセスを実行し、stdout/stderr を返します。
get       指定されたファイルをリモート ホストからローカル ホストにダウンロードします。
help      Live Response コマンド リファレンスを表示します。
kill      現在のリモート ホスト上で指定されたプロセスを終了します。
memdump   センサー マシンのメモリの内容を指定された場所でファイルに保存します。
mkdir     リモート ディレクトリを作成します。
```



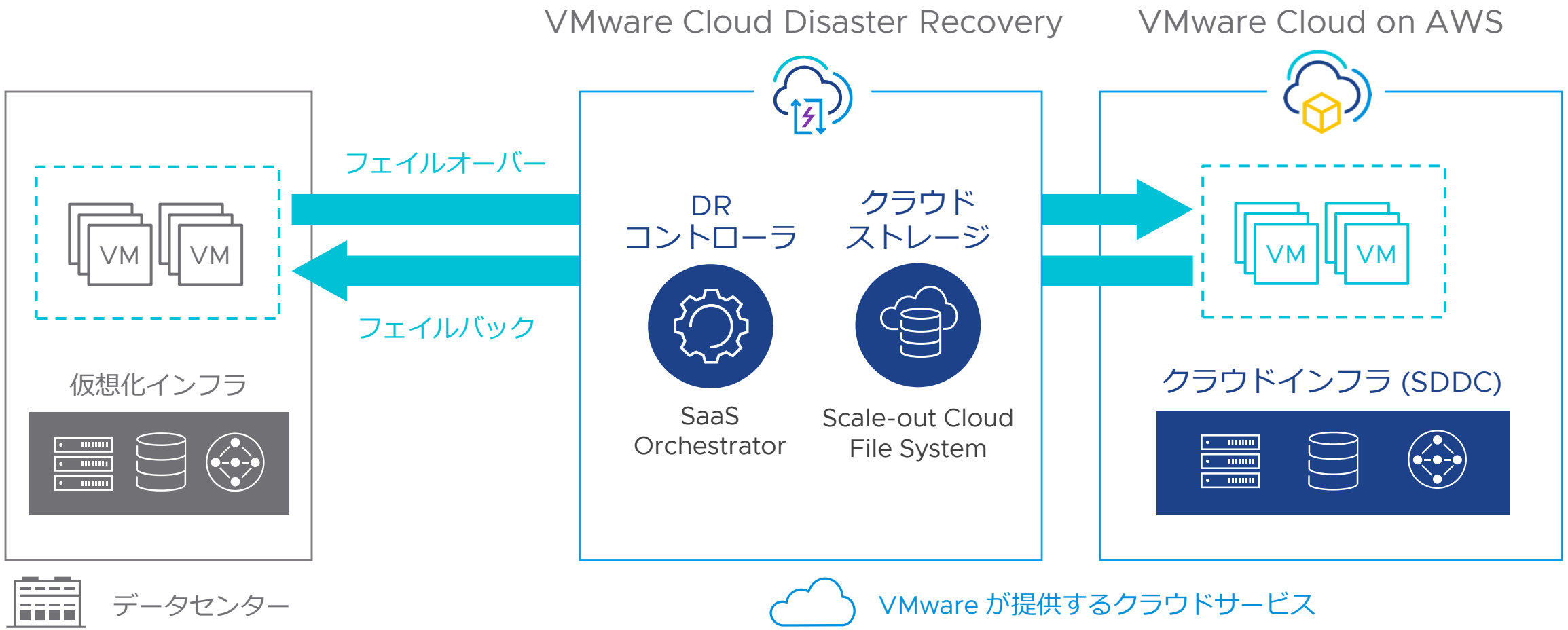
リモート接続による
初期対応が可能

- 調査目的の情報取得
- マルウエアの削除
- データの復元
- コマンド実行など

本番ネットワークから
隔離した状態でも作業
可能

VMware Cloud Disaster Recover と VMware Cloud on AWS

クラウドを活用した災害対策ソリューション



セキュアで堅牢なクラウドストレージ

VMware Cloud Disaster Recovery

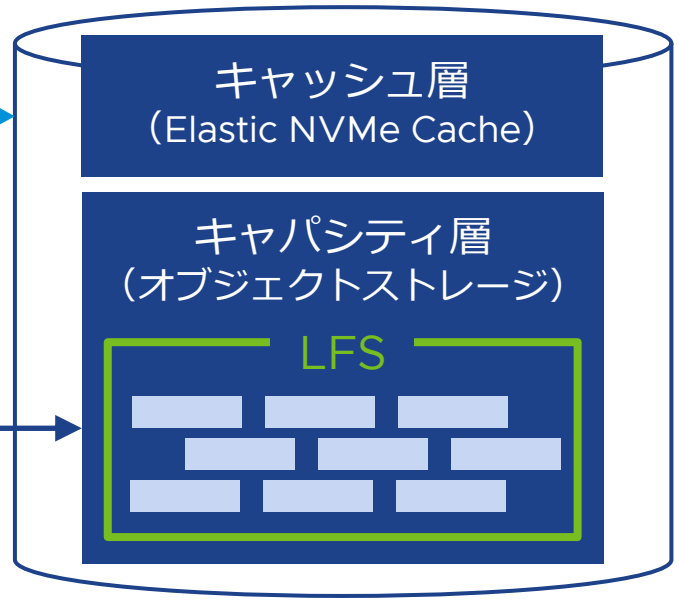
安全なレプリケーション

- NFS/CIFS による接続は不可能
- 通信は暗号化済み
- データは送信前に圧縮+暗号化

データセンター

データの改ざん不可

- データは暗号化されて保持
- 既存データの上書き変更は不可



Scale-out Cloud File System (SCFS)

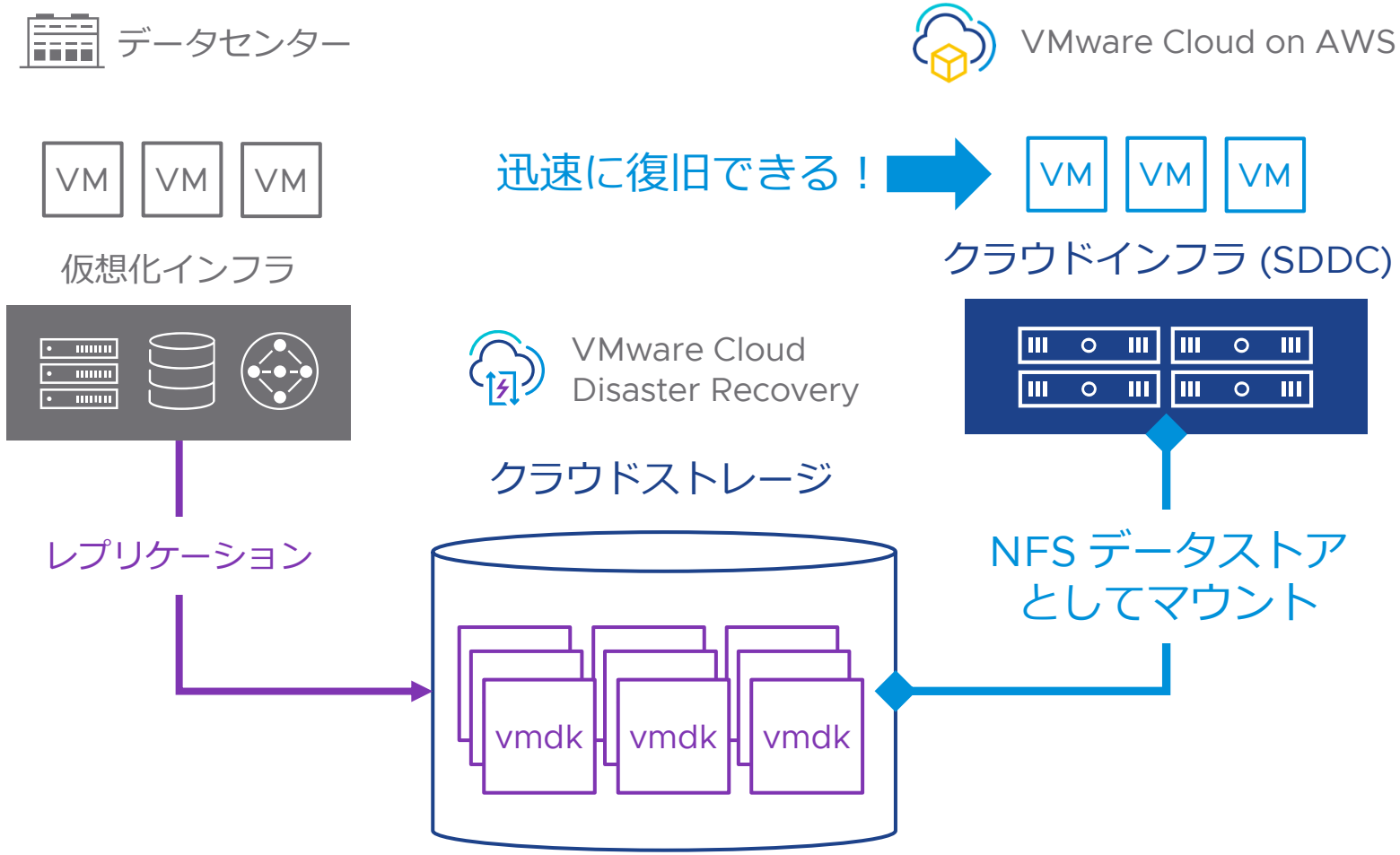
- VMware 独自の技術で構成されたクラウドストレージ
- キャッシュ層とキャパシティ層で構成（キャッシュ層を採用することにより性能向上を実現）
- VMware Cloud on AWS のホストから「NFS データストア」としてマウント可能

Log-Structured Filesystem (LFS) の採用

- 一度書き込まれたデータは上書き出来ない仕様
- データの配置場所が隠されており、外部からの直接アクセスは不可能

クラウドインフラのデータストアとして活用可能

VMware Cloud on AWS のホストからデータストアとしてマウント & VM 起動が可能

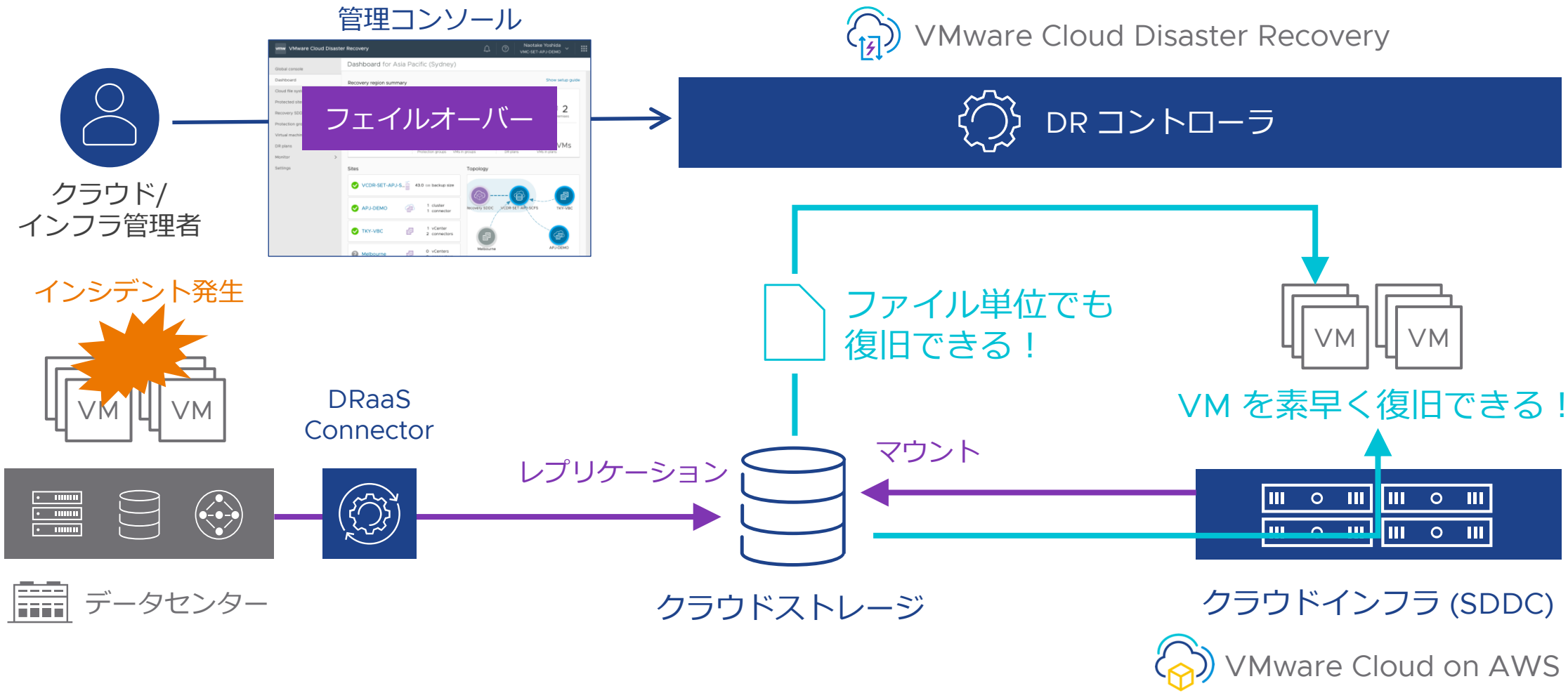


クラウドストレージをデータストアとして活用

- 復旧発動時、VMware Cloud on AWS のホストからクラウドストレージを 「NFS データストア」としてマウント
- ホストから直接マウントすることにより、迅速に仮想マシンを復元・起動することが可能

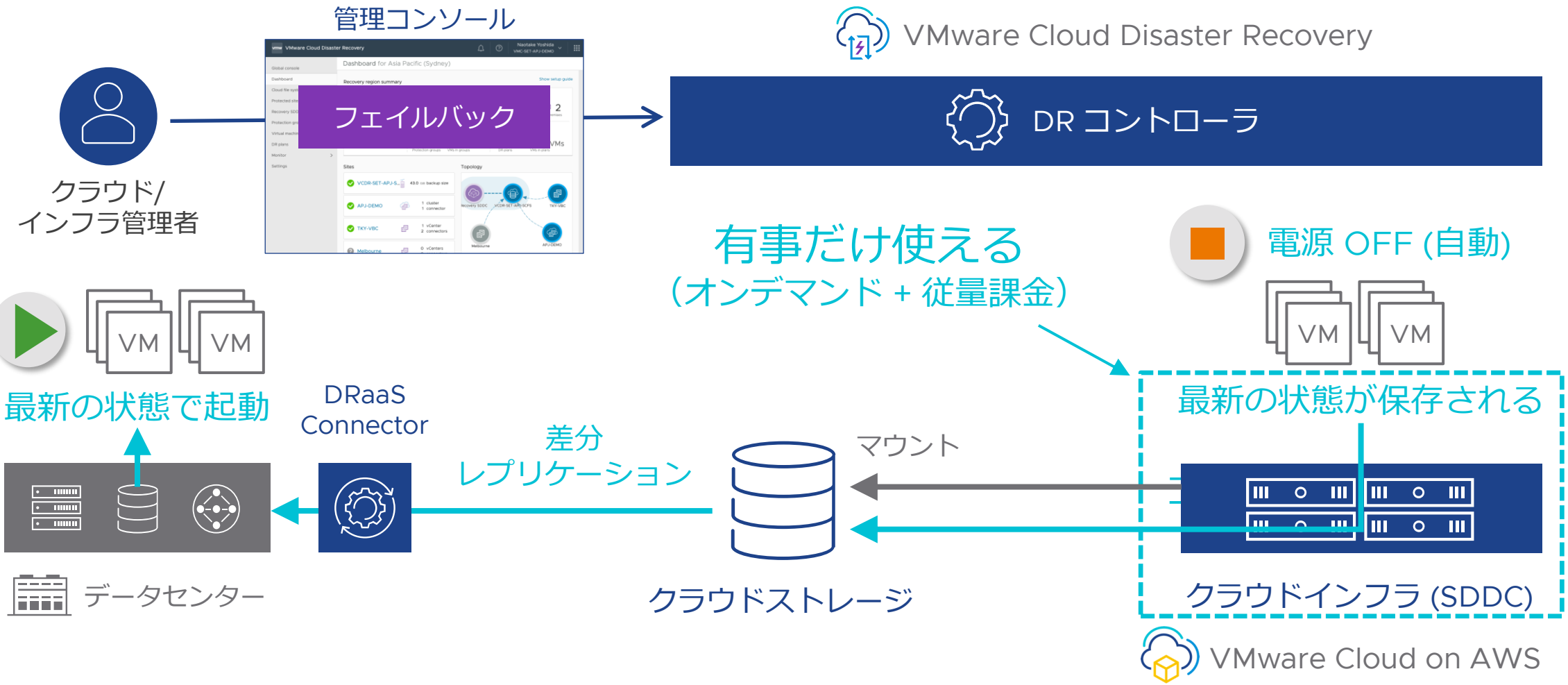
クラウドを活用した災害対策ソリューションの仕組み

クラウド上で迅速に復旧 & サービス再開できる



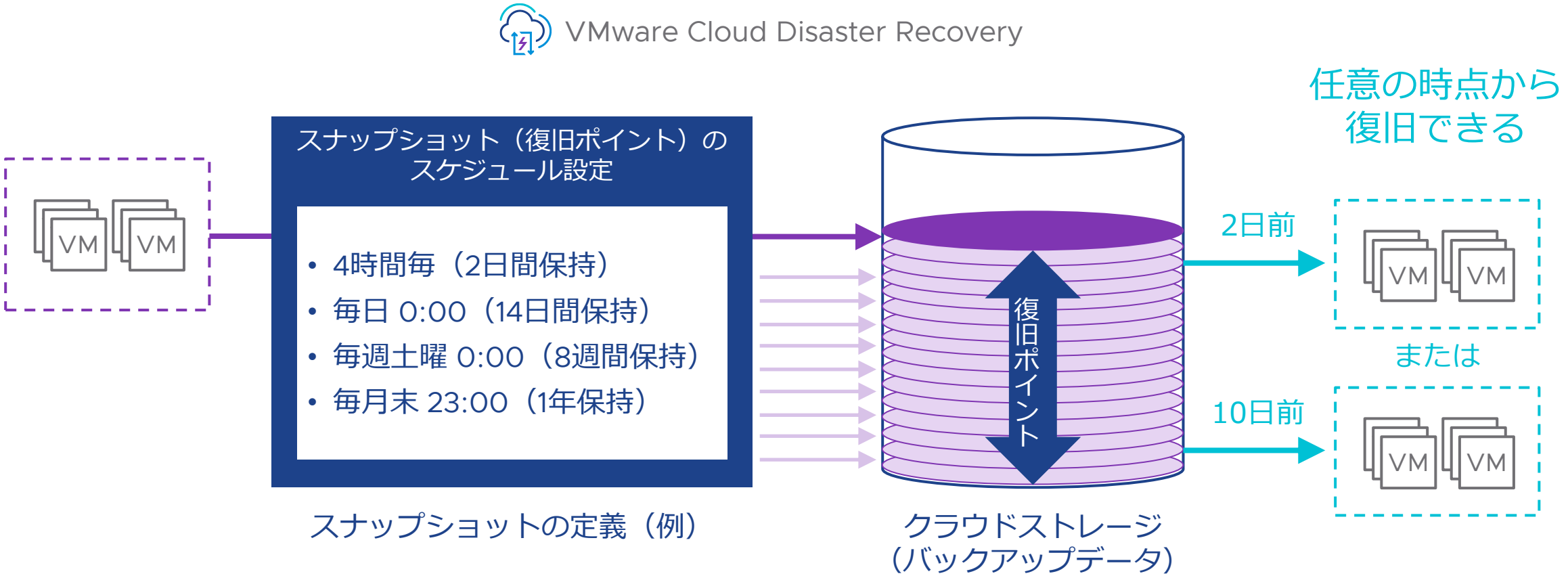
クラウドを活用した災害対策ソリューションの仕組み

最小限のデータ同期（差分レプリケーション）でオンプレミスデータセンターへ復旧できる



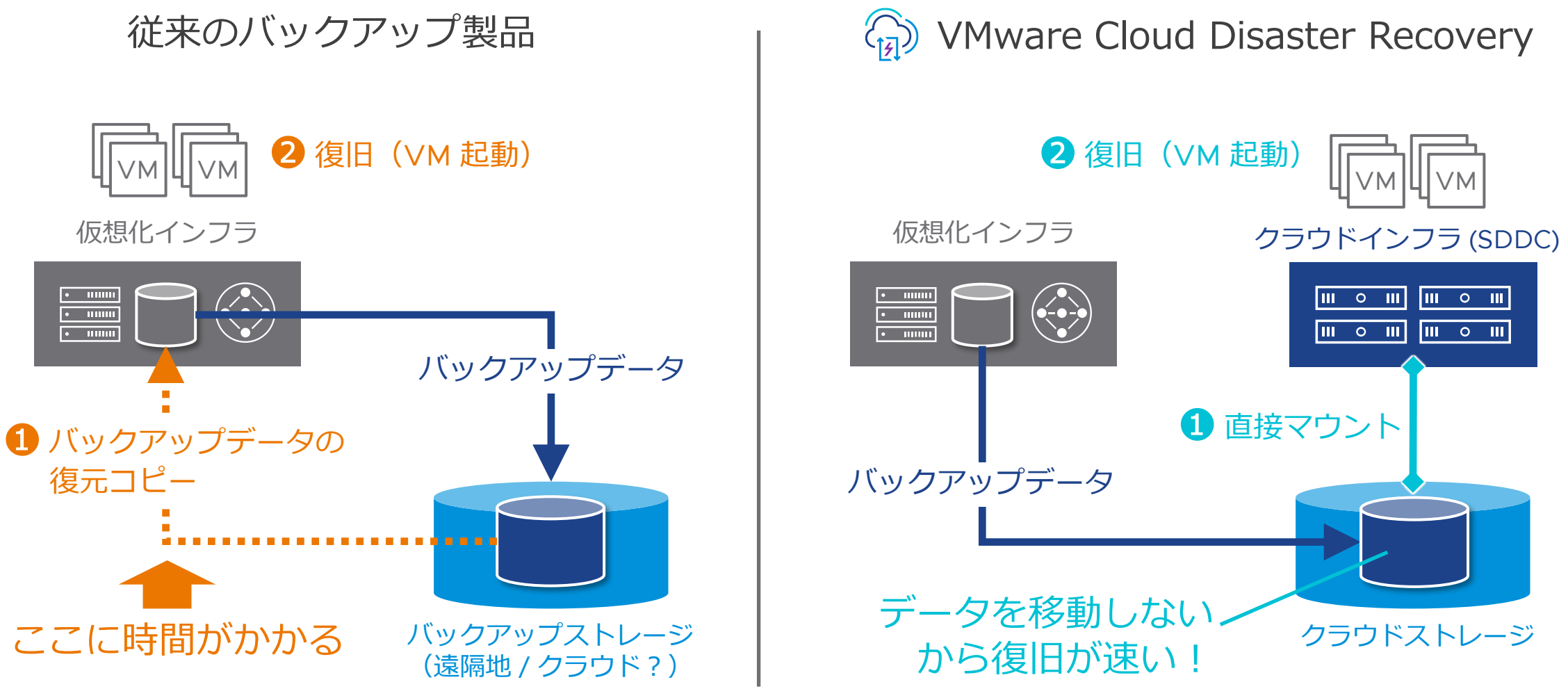
【メリット１】復旧ポイントを柔軟に定義・選択できる

バックアップするタイミングやデータ保持期間を柔軟に定義できる



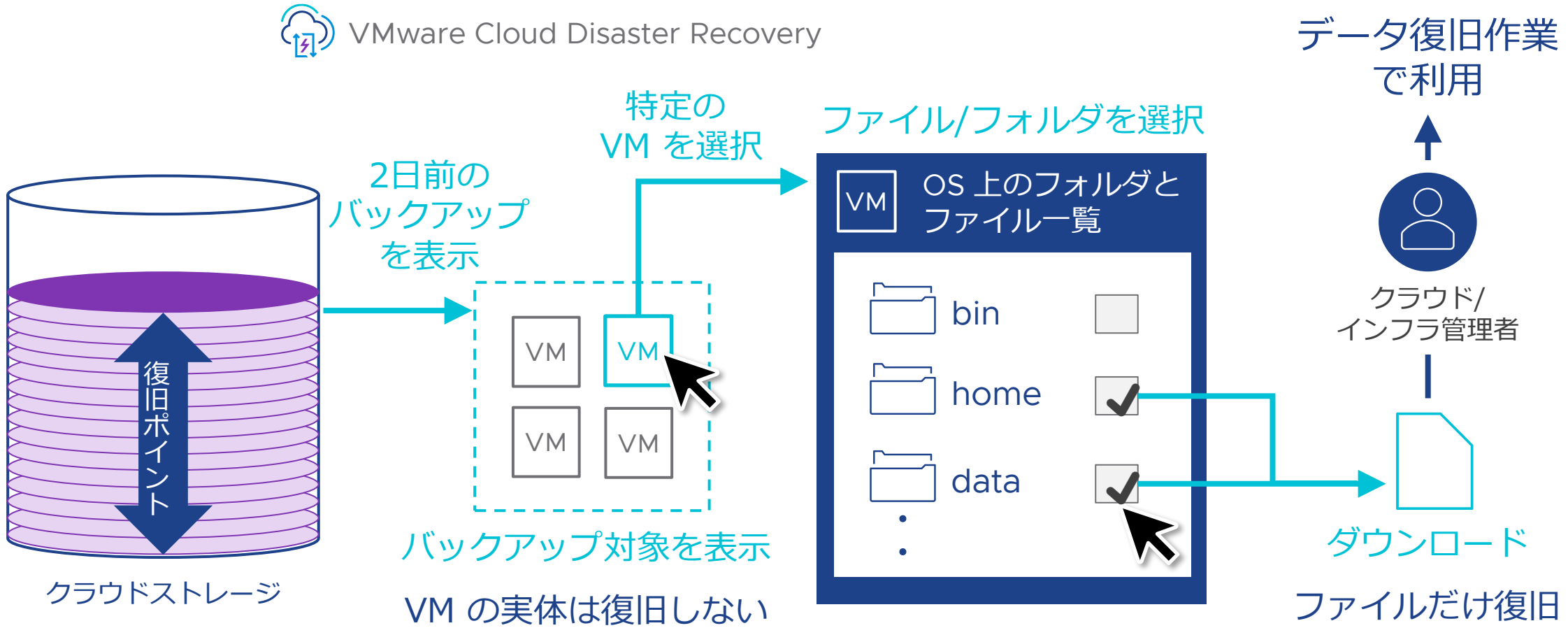
【メリット２】仮想マシンごと素早く復旧できる

バックアップデータの「復元コピー」が不要だから即時に仮想マシンを起動できる



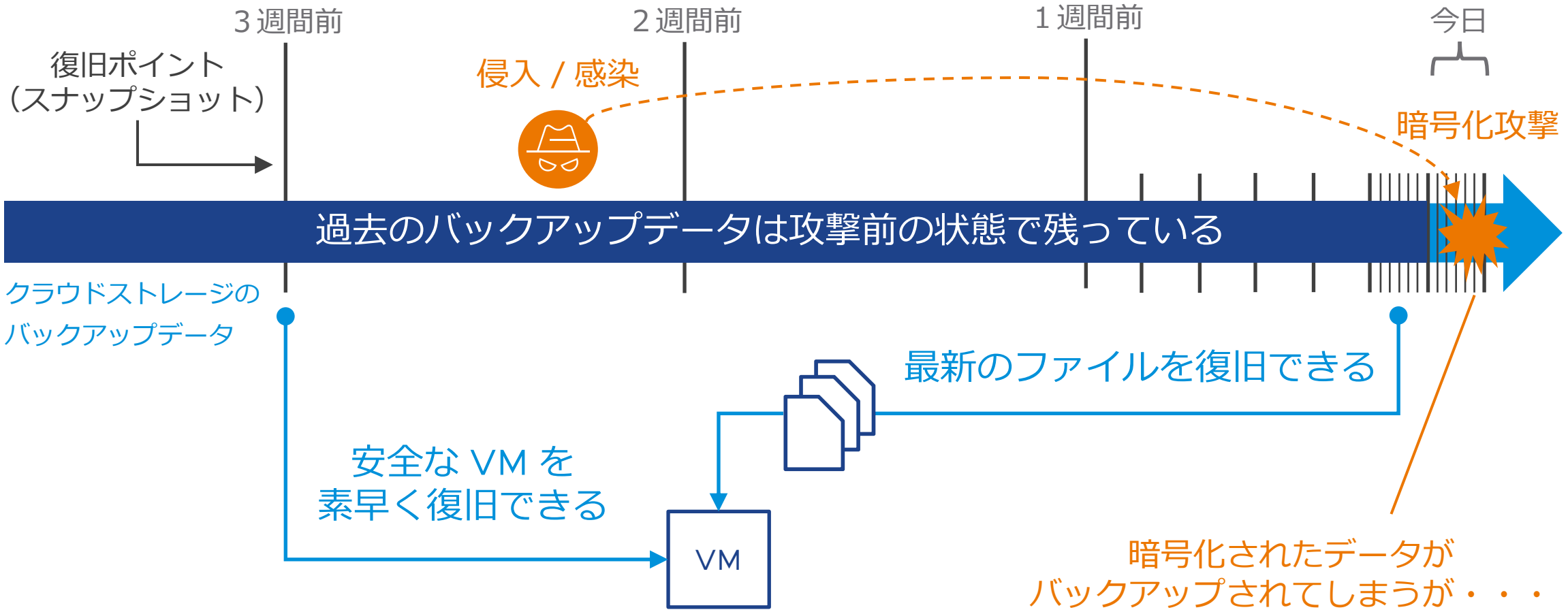
【メリット３】ファイル単位でも復旧できる

任意の時点のバックアップからファイル単位で復旧し、復旧作業を効率化できる



【活用例】迅速な VM 復旧と最新データの復旧を同時に実現

安全な VM を復旧しつつ、データは最新の状態に復旧できる



アジェンダ

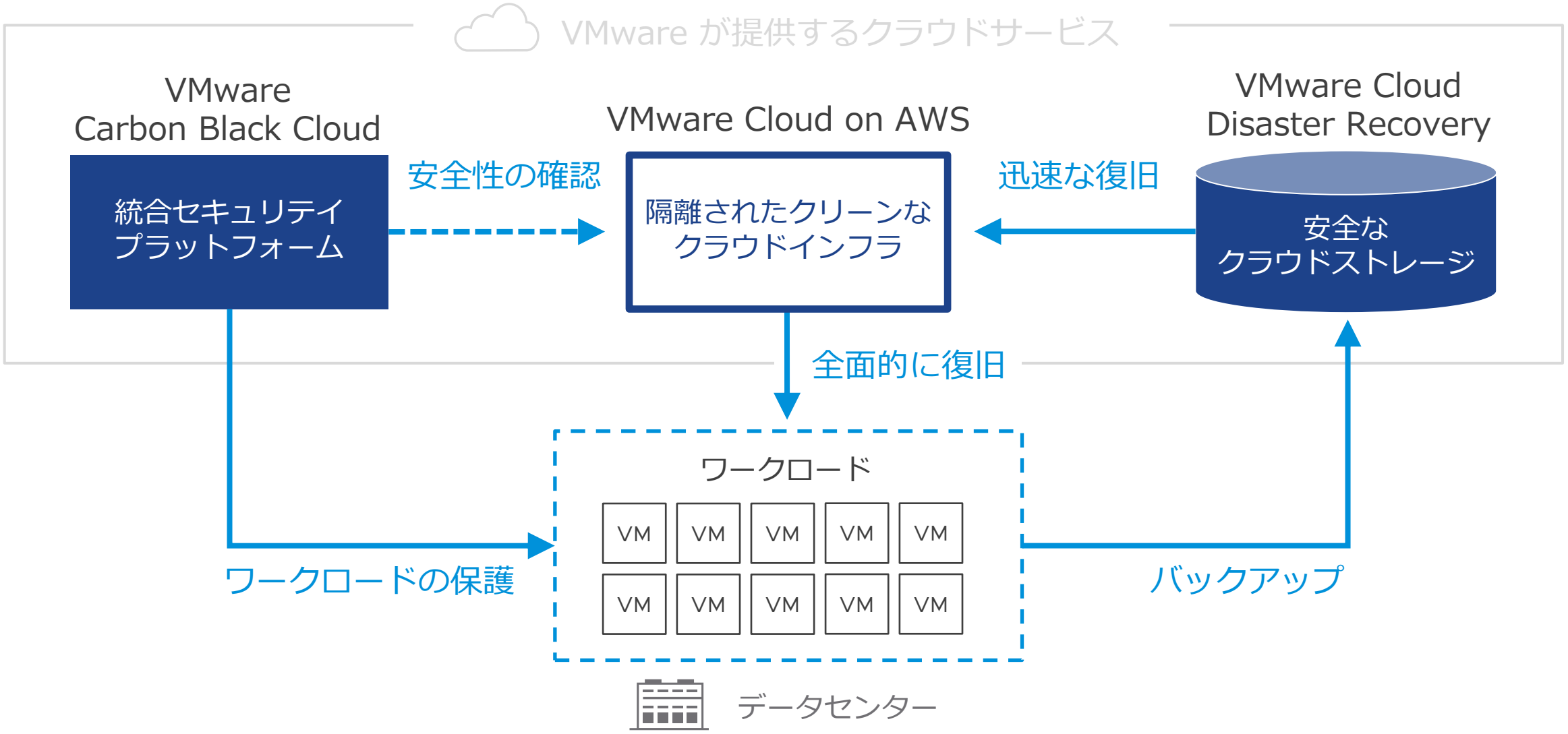
ランサムウエアと復旧対策の重要性

ランサムウェア対策に最適なソリューション

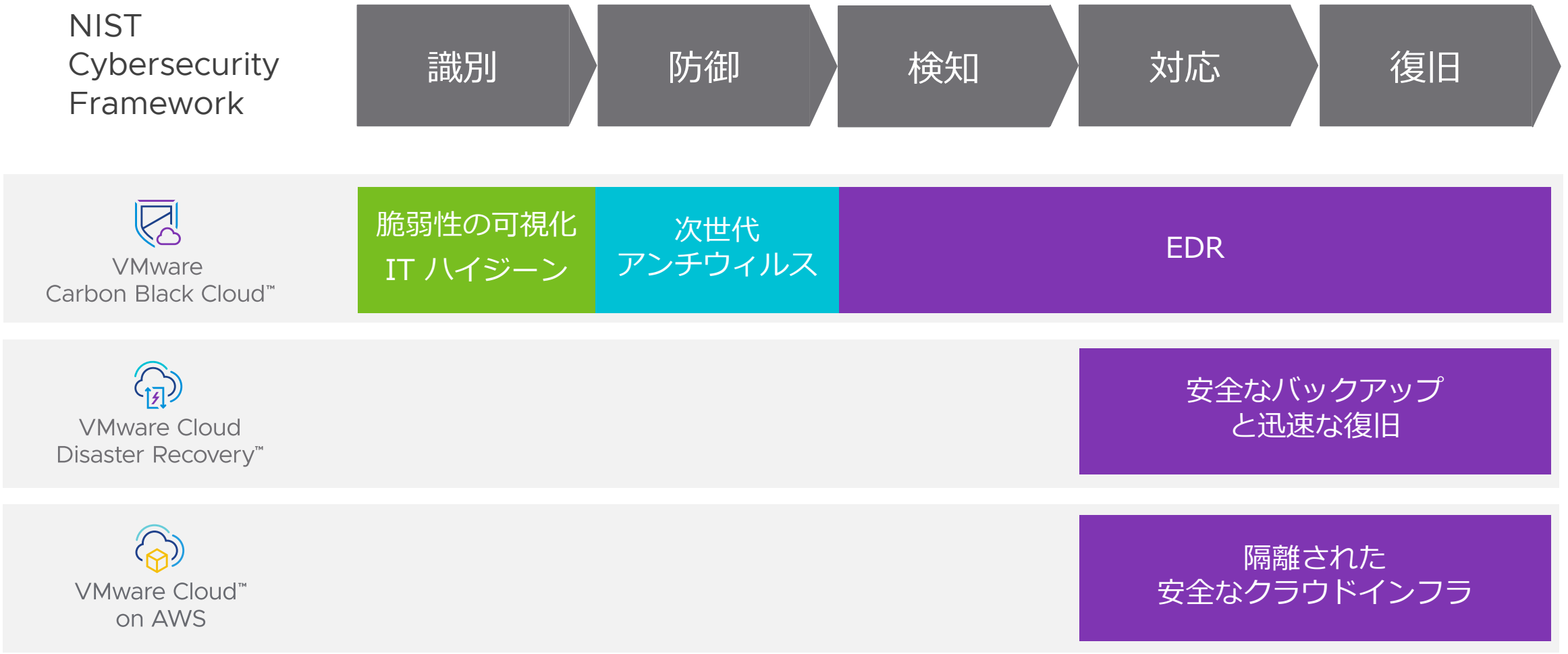
安全で迅速な復旧方法

まとめ

クラウドを活用したランサムウェア復旧対策

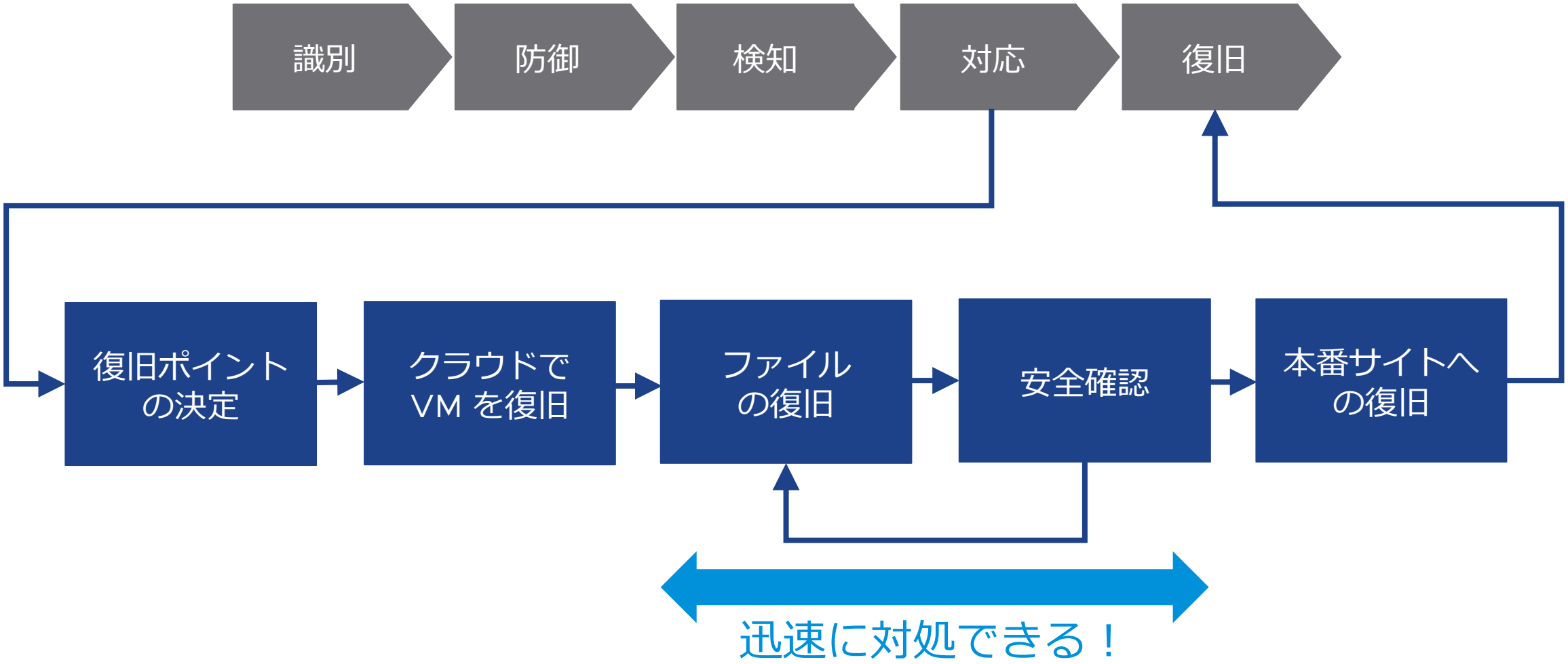


包括的にセキュリティ対策を向上し、復旧対策も万全



出典：NIST Cybersecurity Framework (https://www.nist.gov/cyberframework/framework)

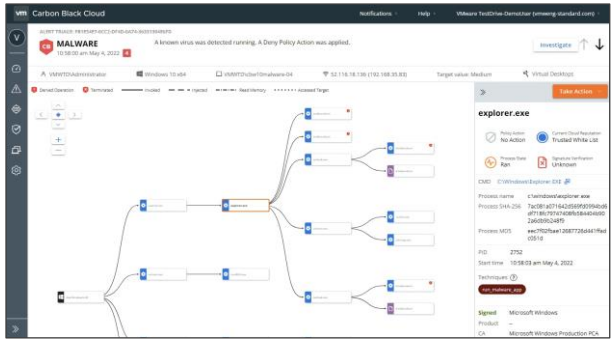
安全で迅速な復旧方法の流れ



素早く原因と影響範囲を把握して感染時期を特定する

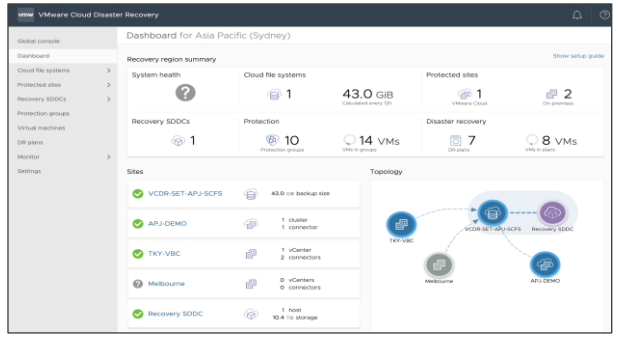
復旧ポイントの決定 → クラウドで VM を復旧 → ファイルの復旧 → 安全確認 → 本番サイトへの復旧

① 感染時期を特定



VMware Carbon Black Cloud

③ 復旧ポイントを決定



VMware Cloud Disaster Recovery

3月1日以前で復旧可能なポイントは？

セキュリティ管理者

クラウド/インフラ管理者

3月1日に感染した可能性が高い

② 感染時期を通知

復旧ポイント（スナップショット）の選択画面サンプル

VMware Cloud Disaster Recovery の管理コンソール

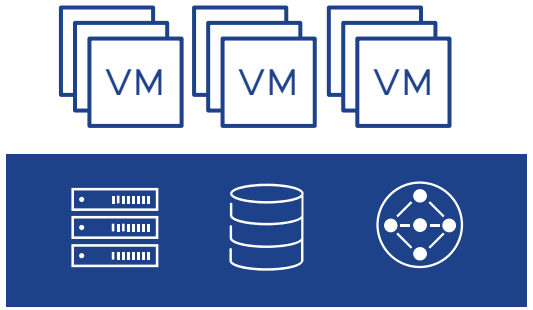
任意のポイントから復旧できる

Name	Taken timestamp	Includes	Expiration
UC-Demo - Every 4 hours - 2022-05-22T02:00 UTC	May-22 11:04 am (2h ago)	4 VMs	May-23 11:05 am (in 1d)
UC-Demo - Every 4 hours - 2022-05-21T22:00 UTC	May-22 07:04 am (6h ago)	4 VMs	May-23 07:04 am (in 18h)
UC-Demo - Every 4 hours - 2022-05-21T18:00 UTC	May-22 03:04 am (10h ago)	4 VMs	May-23 03:04 am (in 14h)
UC-Demo - Weekly Every 4 hours... - 2022-05-21T14:00 UTC	May-21 11:05 pm (13h ago)	4 VMs	Jun-18 11:05 pm (in 1mo)
UC-Demo - Every 4 hours - 2022-05-21T10:00 UTC	May-21 07:05 pm (18h ago)	4 VMs	May-22 07:05 pm (in 7h)
UC-Demo - Every 4 hours - 2022-05-21T06:00 UTC	May-21 03:04 pm (1d ago)	4 VMs	May-22 03:04 pm (in 2h)
UC-Demo - Every 4 hours Daily - 2022-05-20T14:00 UTC	May-20 11:05 pm (2d ago)	4 VMs	May-27 11:05 pm (in 5d)
UC-Demo - Daily Every 4 hours - 2022-05-19T14:00 UTC	May-19 11:05 pm (3d ago)	4 VMs	May-26 11:05 pm (in 4d)
UC-Demo - Daily Every 4 hours - 2022-05-18T14:00 UTC	May-18 11:06 pm (4d ago)	4 VMs	May-25 11:06 pm (in 3d)
UC-Demo - Daily Every 4 hours - 2022-05-17T14:00 UTC	May-17 11:05 pm (5d ago)	4 VMs	May-24 11:05 pm (in 2d)
UC-Demo - Every 4 hours Daily - 2022-05-16T14:00 UTC	May-16 11:05 pm (6d ago)	4 VMs	May-23 11:05 pm (in 1d)
UC-Demo - Every 4 hours Daily - 2022-05-15T14:00 UTC	May-15 11:05 pm (7d ago)	4 VMs	May-22 11:05 pm (in 11h)
UC-Demo - Weekly Every 4 hours... - 2022-05-14T14:00 UTC	May-14 11:05 pm (8d ago)	4 VMs	Jun-11 11:05 pm (in 20d)
UC-Demo - Weekly Every 4 hours... - 2022-05-07T14:00 UTC	May-07 11:05 pm (15d ago)	4 VMs	Jun-04 11:05 pm (in 13d)
UC-Demo - Weekly Every 4 hours... - 2022-04-30T14:00 UTC	Apr-30 11:04 pm (22d ago)	4 VMs	May-28 11:04 pm (in 6d)

隔離されたクラウドインフラにワークロードを素早く復旧する

復旧ポイントの決定 → クラウドで VM を復旧 → ファイルの復旧 → 安全確認 → 本番サイトへの復旧

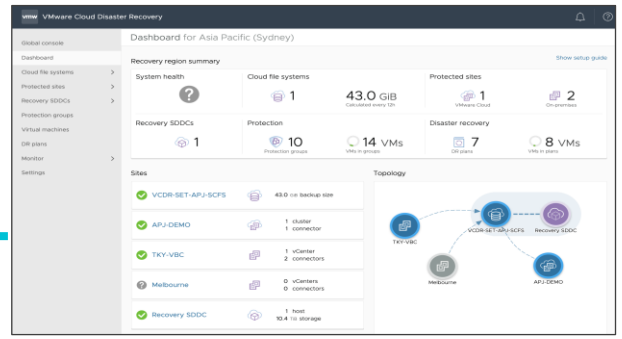
② 全ての VM が正常に起動していることを確認する



VMware Cloud on AWS

自動的にサイトを展開 + VM が復旧される

① 復旧サイトを展開

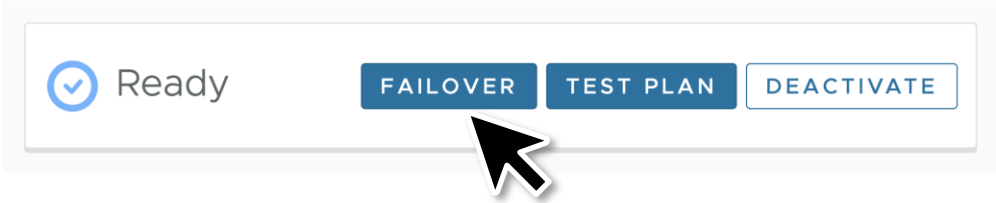


VMware Cloud Disaster Recovery

クラウドで復旧する準備を開始！

クラウド/インフラ管理者

データセンターから隔離された安全なクラウドインフラ



必要に応じて個別にデータを復旧する

復旧ポイントの決定 → クラウドで VM を復旧 → ファイルの復旧 → 安全確認 → 本番サイトへの復旧

② ファイルを復旧する

アプリ管理者

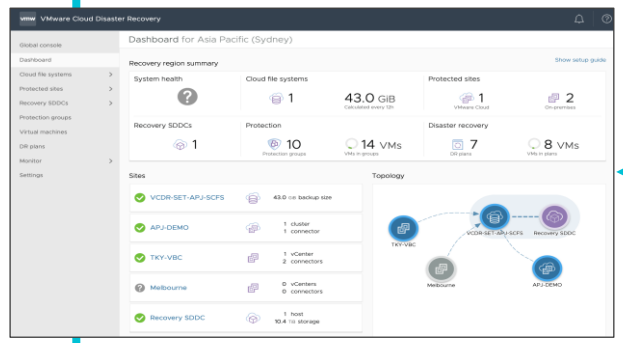
セキュリティ管理者

VM VM VM

VMware Cloud on AWS

① 特定日時のファイルをダウンロード

VMware Cloud Disaster Recovery



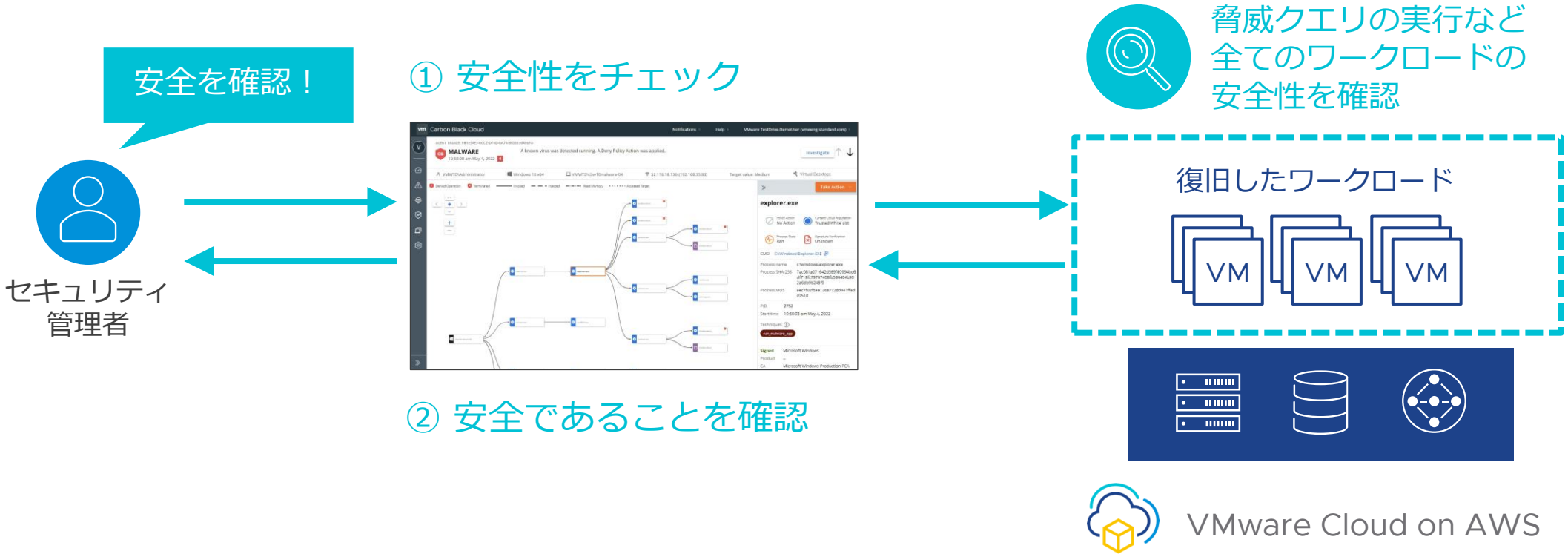
データを最新の状態に復旧しよう！

クラウド/インフラ管理者

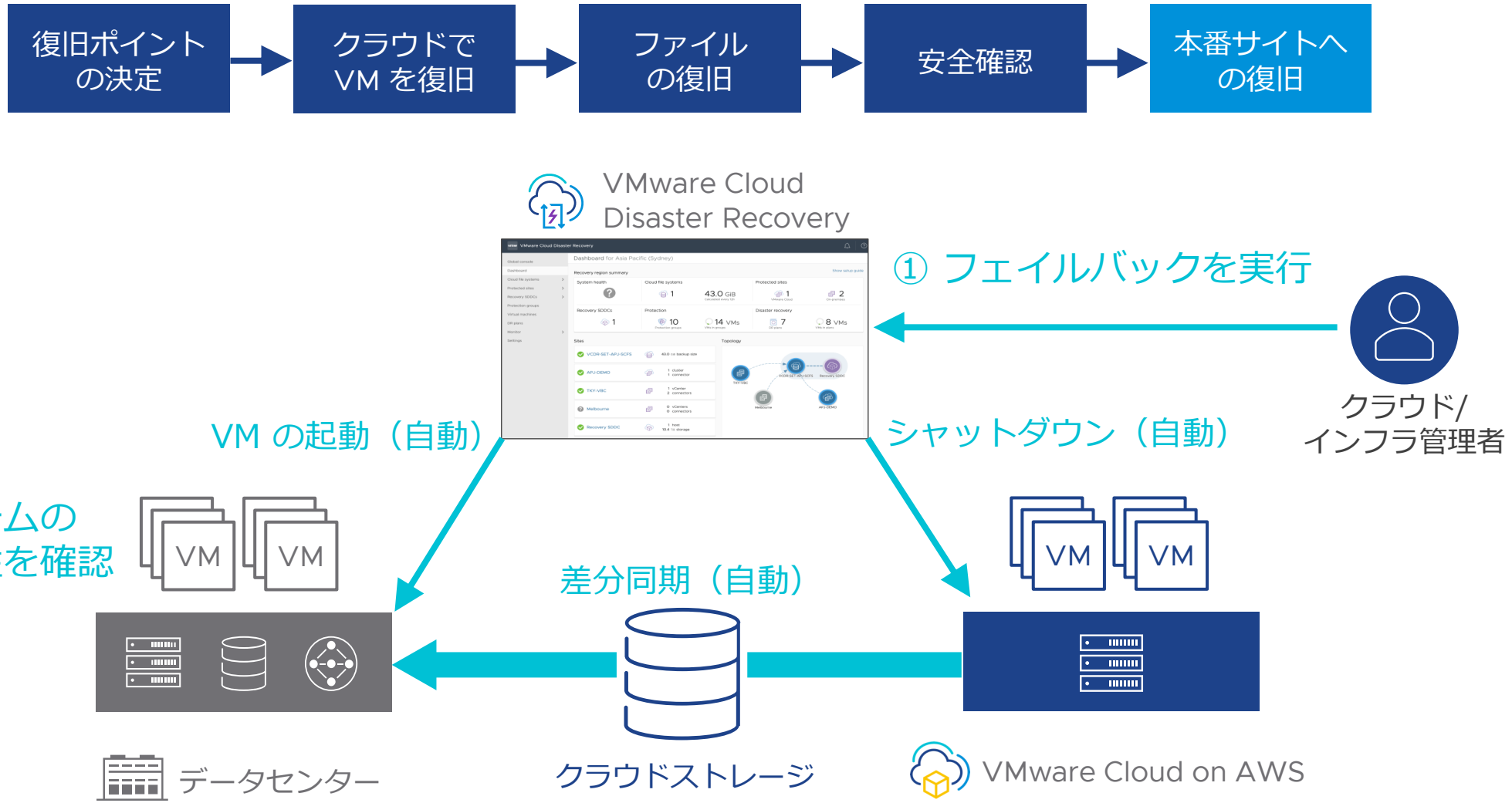
クラウドストレージ

EDR でワークロード全体の安全性を確認する

復旧ポイントの決定 → クラウドで VM を復旧 → ファイルの復旧 → 安全確認 → 本番サイトへの復旧



簡単操作で全面復旧を実行する



アジェンダ

ランサムウエアと復旧対策の重要性

ランサムウェア対策に最適なソリューション

安全で迅速な復旧方法

まとめ

ワークロードの保護から復旧まで網羅的にカバー

VMware Carbon Black Cloud™

次世代アンチウイルスと
EDR を兼ね備えた
ワークロードの包括的な
セキュリティソリューション

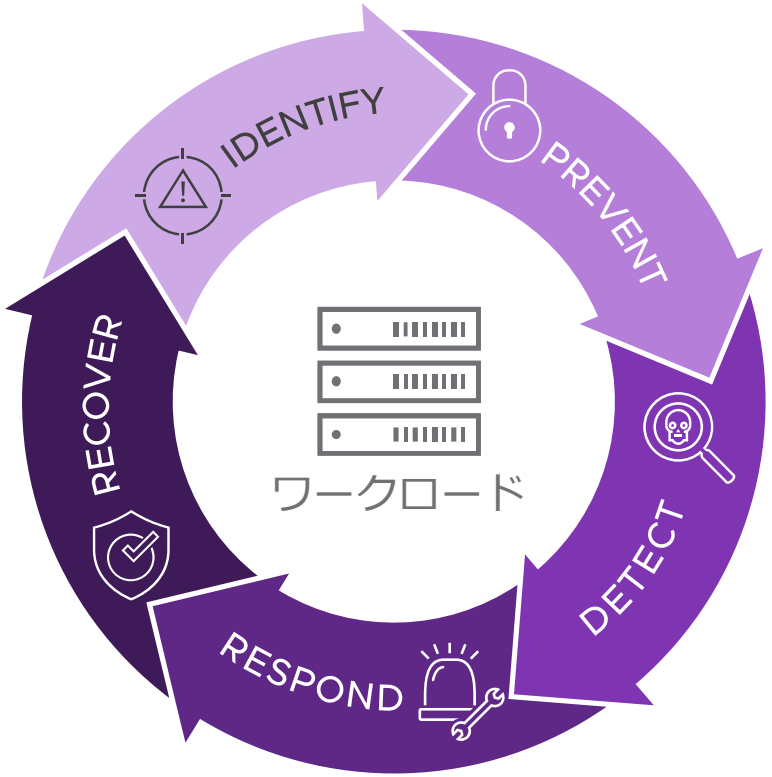
VMware Cloud Disaster Recovery™

安全で堅牢な
クラウドストレージへの
バックアップと
迅速な復旧を実現する
災害対策ソリューション

VMware Cloud™ on AWS

データセンターから
隔離された場所で
SDDC を提供する
クラウドサービス

クラウドを活用したランサムウェア復旧対策のメリット



ワークロードの保護を強化できる

- 次世代アンチウイルスと EDR によるランサムウエア対策の強化
- 脆弱性評価や IT ハイジーンによる健全性の維持

復旧期間を大幅に短縮できる

- 素早くワークロードを復旧可能
- ファイル単位で復旧可能
- ワークロード全体の一斉復旧も可能
- 安全確認フェーズの時間を短縮

Thank You