DELL TECHNOLOGIES PARTNER PROGRAM

HEROES

データ保護(バックアップ)はセキュリティ対策です - DELLのCRSとは？

デル・テクノロジーズ株式会社
DPS事業本部　SE部
シニアシステムズエンジニア　小川 達彦

DELL Technologies PARTNER PROGRAM

Dell EMC データ保護ソリューション

目指すコアバリューは“２S”+ “ABCD”

２つのメインコンセプトで

S imple Architecture
シンプルなアーキテクチャで

S ingle Platform
単一のプラットフォームで

４つのデータ復旧を重視して

A pplication Centric Recovery
アプリケーション管理者向け

B ackup and Recovery
システム有事のデータ損失から

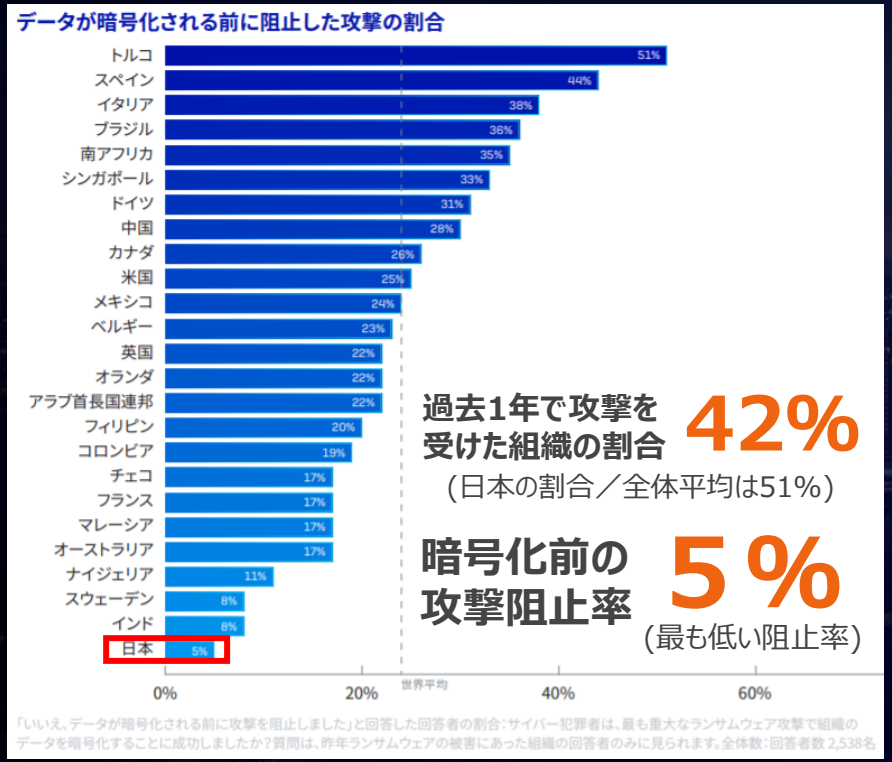
C yber Recovery
サイバー被害後のデータ損失から

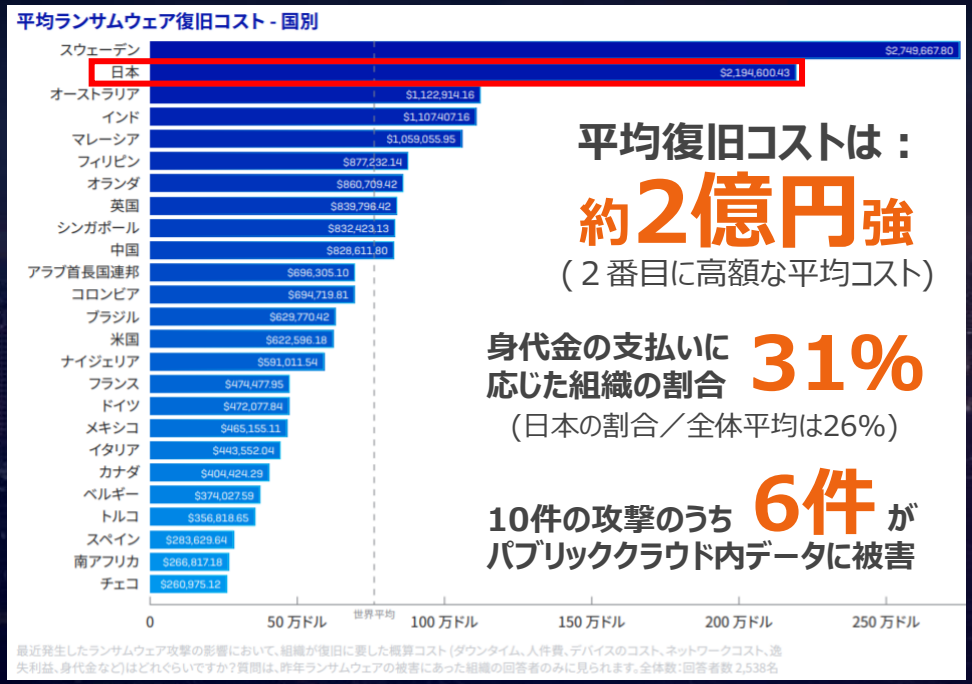
D isaster Recovery
災害時の事業継続向け

データ保護を取り巻くセキュリティの状況

攻撃非阻止率で１位、平均復旧費用額で２位

日本のデジタル環境を蝕むランサムウェアの脅威





“身代金を支払う場合は全体的な復旧コストが**ほぼ 2 倍**になる”

Sophos Ltd.「ランサムウェアの現状2020年版」*2020年5月26日より*

多層化データ保護によるレジリエンス強化

堅牢

サイバーレジリエンス

最も強固

標準的なデータ保護

- あらゆる場所にあるデータを網羅（エッジ、コア、クラウド）
- データ保全が担保されたディスクベースの格納
  （X オフライン/ テープベース）
- 障害を想定した復旧訓練の実施

データ保全性の強化

- 製品に実装される標準セキュリティ機能の活用
- 保存・移送時の暗号化や多要素認証の追加
- データへの改竄防止機能実装とアクセス権の分掌

サイバー復旧を意識した強固策

- ネットワーク隔離とヴォルト（Vault）の形成
- 隔離され改変されない復旧用データの確保
- 隔離データを用いた高度なセキュリティ分析

DELL Technologies

“通常の”データバックアップ以外にも

企業の迅速な「再起動」に不可欠なデータを対象として盛り込む

認証、認可、セキュリティ情報

- Active Directory / LDAP
- DNS dumps
- Certificates
- Event logs (including SIEM data)

ネットワーク設備

- Switch / router configuration
- Firewall / load-balancer settings
- IP Services design
- Access Control configuration
- Firmware / microcode / patches

ストレージ機器

- Backup hardware configuration
- SAN / array configurations
- Storage abstraction settings
- Firmware / microcode / patches

インフラ再起動に必要なデータ

知的財産（IP）情報

- Source code
- Proprietary algorithms
- Developer libraries

ホスト情報や開発ツール

- Physical/Virtual Platform Builds
- Dev Ops tools & automation scripts
- Firmware / microcode / patches
- Vendor software
  - Binaries (golden images)
  - Configurations & settings

重要なドキュメンテーション

- CMDB / asset D/R and Cyber Recovery Run-books &checklists
- Management extracts
- HR resources & contacts lists

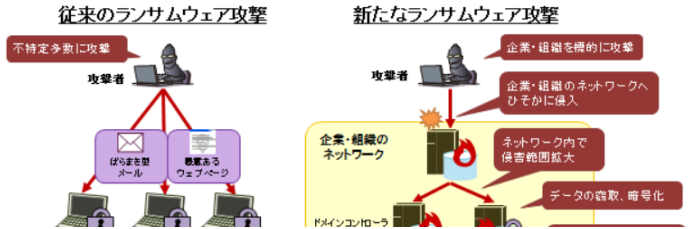
ビジネス再起動に必要なデータ

サイバー復旧を意識したバックアップシステムへ

【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について

～「人手によるランサムウェア攻撃」と「二重の脅迫」～

最終更新日：2020年8月20日
独立行政法人情報処理推進機構
セキュリティセンター



- 重要なファイルは定期的にバックアップを取得する。
- バックアップに使用する装置・媒体は、バックアップ時のみ対象機器と接続する。
- バックアップ中に感染する可能性を考慮し、バックアップに使用する装置・媒体は複数用意する。
- バックアップの妥当性（バックアップが正常に取得できているか、現状のバックアップ手法が攻撃に対して有効か）を定期的に確認する。
- データのみならず、システムの再構築を含めた、復旧計画を策定する。

出典：IPA（情報処理推進機構）
・「【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について」 https://www.ipa.go.jp/security/announce/2020-ransom.html

NISC が「ランサムウエアによるサイバー攻撃について【注意喚起】」を公開

内閣サイバーセキュリティセン
起】」を公開しました。様々な
ェアの特徴として、「2段階の
ます。過去に情報処理推進機構
必要です。

2020年11月26日

ランサムウエアによるサイバー攻撃について【注意喚起】

2020年11月26日、内閣サイバーセキュリティセンターは、重要インフラ事業者

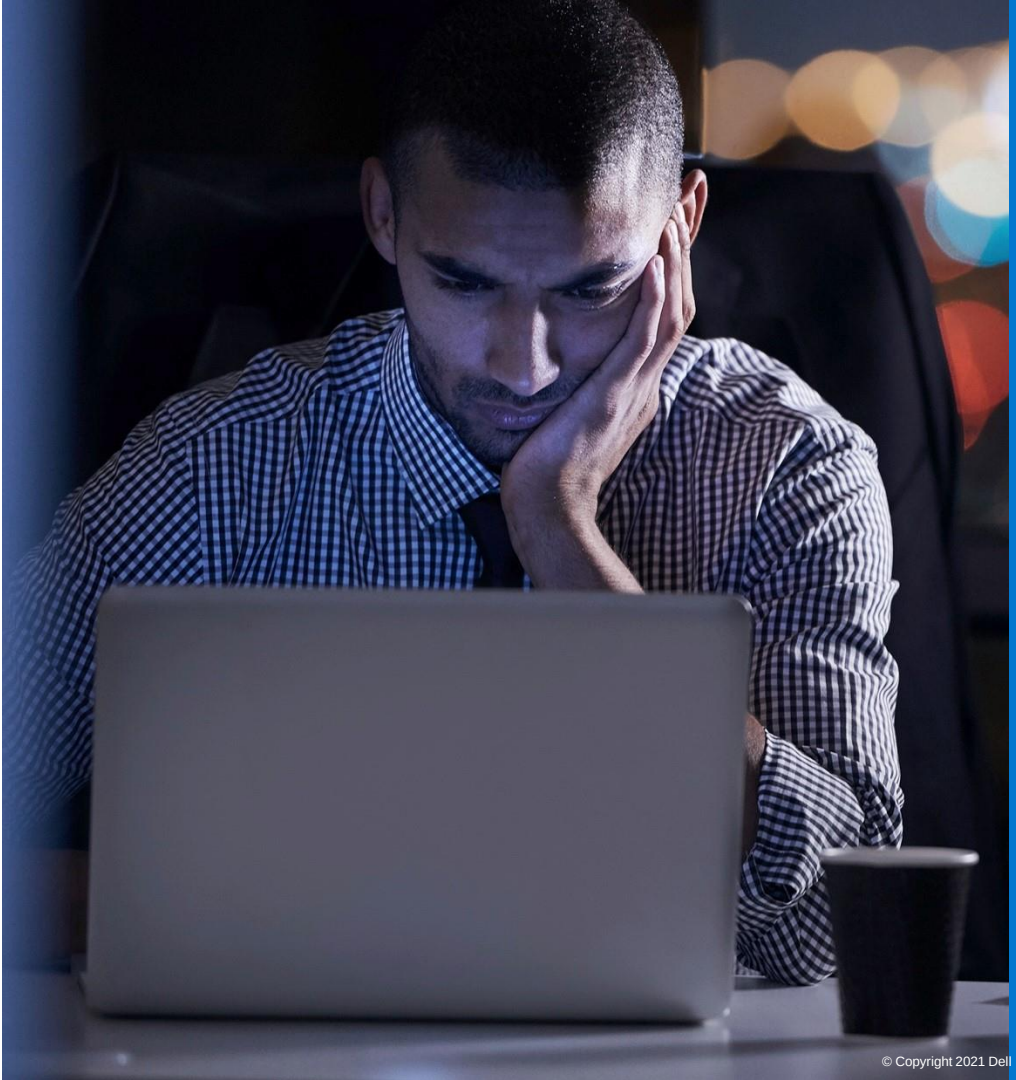
(2) ランサムウエアによるデータの暗号化に備えた対応策（予防）

従来のランサムウエア対策の常套手段であったバックアップは、引き続き有効です。しかし、2 重脅迫ランサムウエアに感染した場合は、組織の機微データ、個人情報が流出する懸念があることから、「機微データの厳格管理」については、改めて検討する必要があります。

- 重要なデータに対する定期的なバックアップの設定を確認する。バックアップの検討に当たっては、ランサムウエア感染時でもバックアップが保護されるように留意する。例えば、バックアップをオフラインで保管する、クラウド上や外部のストレージ上に重要なデータをコピーし、コピーしたデータは保護対象のネットワークからアクセスできないようにする等の対策を講じる。
- バックアップで取得したデータをもとに、実際に復旧できることを確認する。

出典：JPCERT/CC
・「NISC が「ランサムウエアによるサイバー攻撃について【注意喚起】」を公開」https://www.jpcert.or.jp/tips/2
出典：内閣サイバーセキュリティセンター (NISC)
・「ランサムウエアによるサイバー攻撃について【注意喚起】」https://www.nisc.go.jp/active/infra/pdf/ransomwa

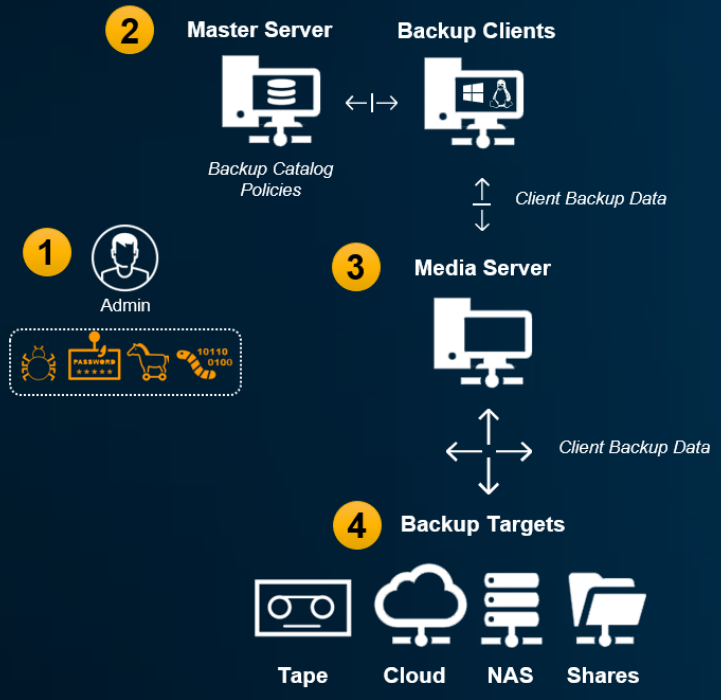
データ保護による
セキュリティ対策
CRS



デジタルデータ保護における：
３つのサイバー復旧準備ポイント

- **データ防御**
  バックアップデータの暗号化や改ざん防止などによる更なる防御
- **データ隔離**(隔離・管理)
  攻撃から「見えない」場所への復旧用データ隔離とその管理
- **データ衛生**(分析・検証)
  隔離したデータの汚染状況分析による安全な復旧用データの確保とリスクのフィードバック

ランサムウェアがバックアップシステムをターゲットに



1. **IT管理者とバックアップ管理者が侵害の主な標的です。**

2. **マスターサーバー (バックアップカタログ):** バックアップマスターサーバーが標的にされて感染しているため、バックアップカタログが暗号化/消去されたり、ポリシーの有効期限が切れたりします。

3. **メディアサーバー:** メディアサーバーにマウントされているすべてのファイルシステムが対象となり、暗号化/消去されます。

4. **バックアップターゲット:**

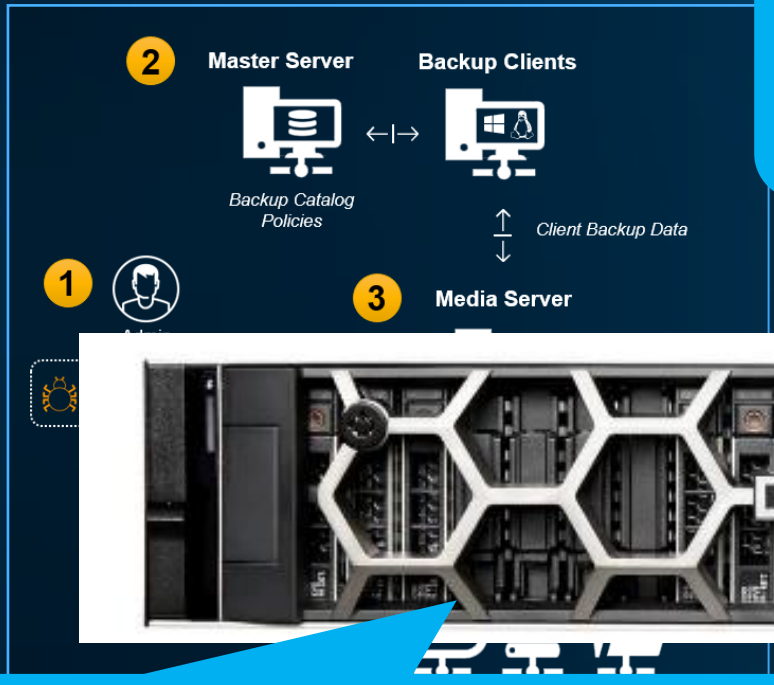
   ディスク/NAS: メディアサーバー上のファイルシステムは、ターゲットにされ暗号化/消去されます。バックアップリポジトリは、ネットワークファイル共有を迂回するランサムウェアから暗号化/消去される可能性があります。

   テープ: 攻撃の前にバックアップ環境からメディア排出された場合、破壊的なイベントから回復するこでが可能です。しかし、バックアップカタログを隔離、破壊されたりすると、テープからの復旧は非常に難しくなります。

   クラウド: プライベートまたはパブリッククラウドは、リモート保護の利点を提供しますが、インターネット(常時アクセス)または安全でないネットワークへに接続している場合、バックアップデータ、カタログが公開されるため、実際には安全性が低くなります。

ランサムウェアがバックアップシステムをターゲットに

PowerProtect DDなら、独自のプロトコル DD Boostによる専用のデータ保管領域で より安全にバックアップデータを保管



感染 タログが暗号化/消去されたり、ポリシーの有効期限が切れたり

3 メディ …メディアサーバーにマウントされているすべてのファイルシステムが対象となり 号化/消去されます。

クラウド: プライベートまたはパブリッククラウドは、リモート保護の利点を提供しますが、イ ット(常時アクセス)または安全でないネットワークへに接続している場 アップデータ、カタログが公開されるため、実際には安全性が低くなります。

でも、更なる堅牢性を求める場合には、

Dell EMC PowerProtect Cyber Recovery 概要

サイバー被害後の確実なデータ復旧を可能にする最後の防波堤

- 外部ネットワークから隔離されたヴォルト(Vault)を準備
- エアギャップを用いたデータ転送
  - Vault へのデータ転送に一時的なデータリンクを確立
  - 転送終了後にデータリンクを遮断
- 改ざん防止加工を施した「復旧データ」の生成
- ヴォルト内(In-Vault) データに対するフォレンジック分析
- オプションとして以下を配備
  - 復旧データを用いた検証（復旧テスト/etc.）
  - 3rd Party 製品分析用のデータ出力

DELL Technologies
サイバー復旧（レジリエンス）分野におけるプレゼンス

2015 – カスタマイズ導入で初の「隔離された」リカバリ環境を顧客に提供

2016 – 同仕組みを Dell EMC Isolated Recovery Solution (IRS) として一般提供を開始

2018 – IRS を機能強化した PowerProtect Cyber Recovery の提供を開始

2019 – テクノロジーベンダーとして初めてSheltered Harbor Alliance Partner Programに参加

2020 – 専用分析エンジン CyberSenseの提供を開始

– Sheltered Harbor 向けソリューションとしての認定を取得

Cyber Recovery 導入顧客数 350+ 社

独自の多彩なパートナーアライアンスを展開

EY Building a better working world　Deloitte.

IBM　UNISYS　Cognizant

DXC.technology　HCL

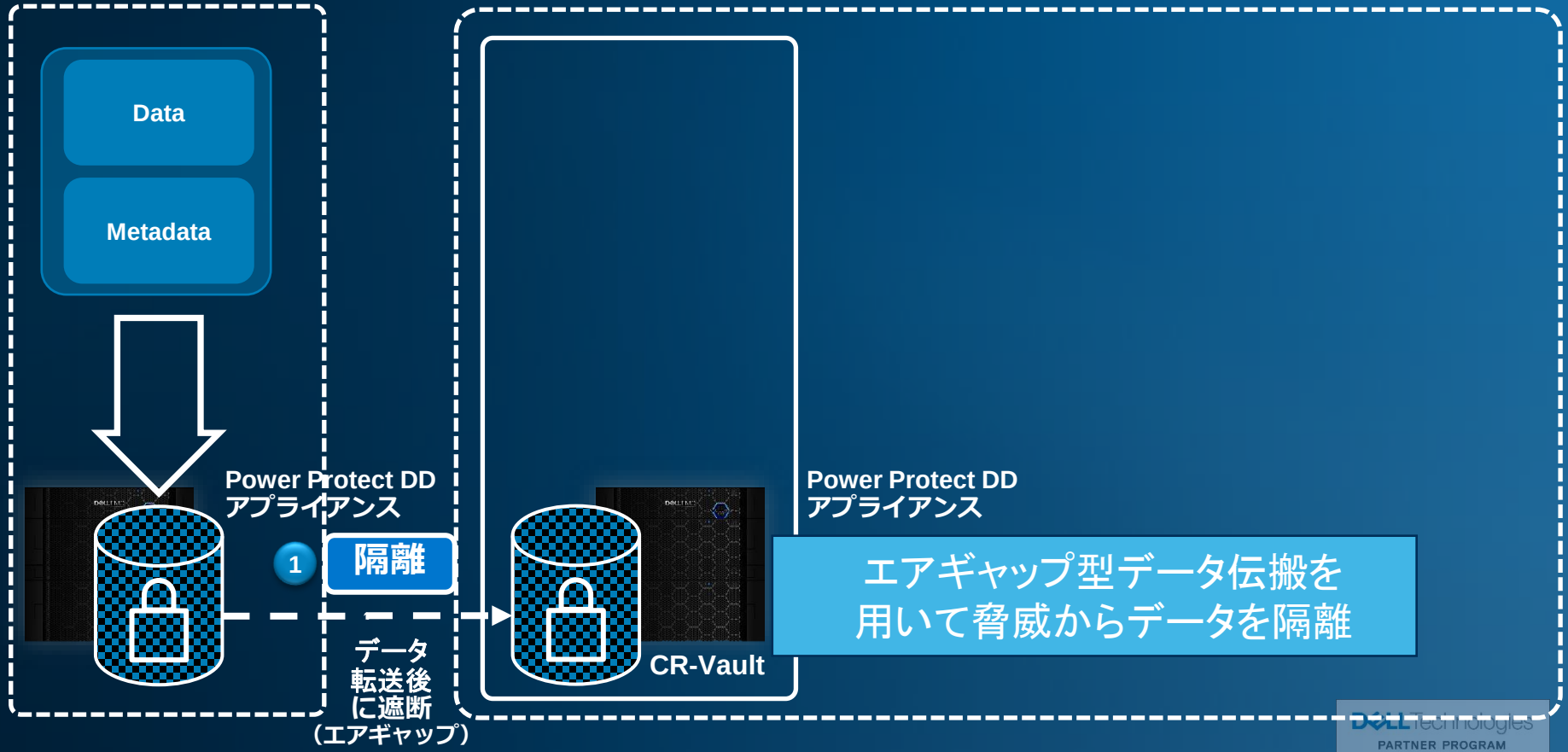
RSA　vmware Carbon Black　Secureworks

セキュリティ・トランスフォメーションを実現するグループ／連携企業

DELL Technologies PARTNER PROGRAM

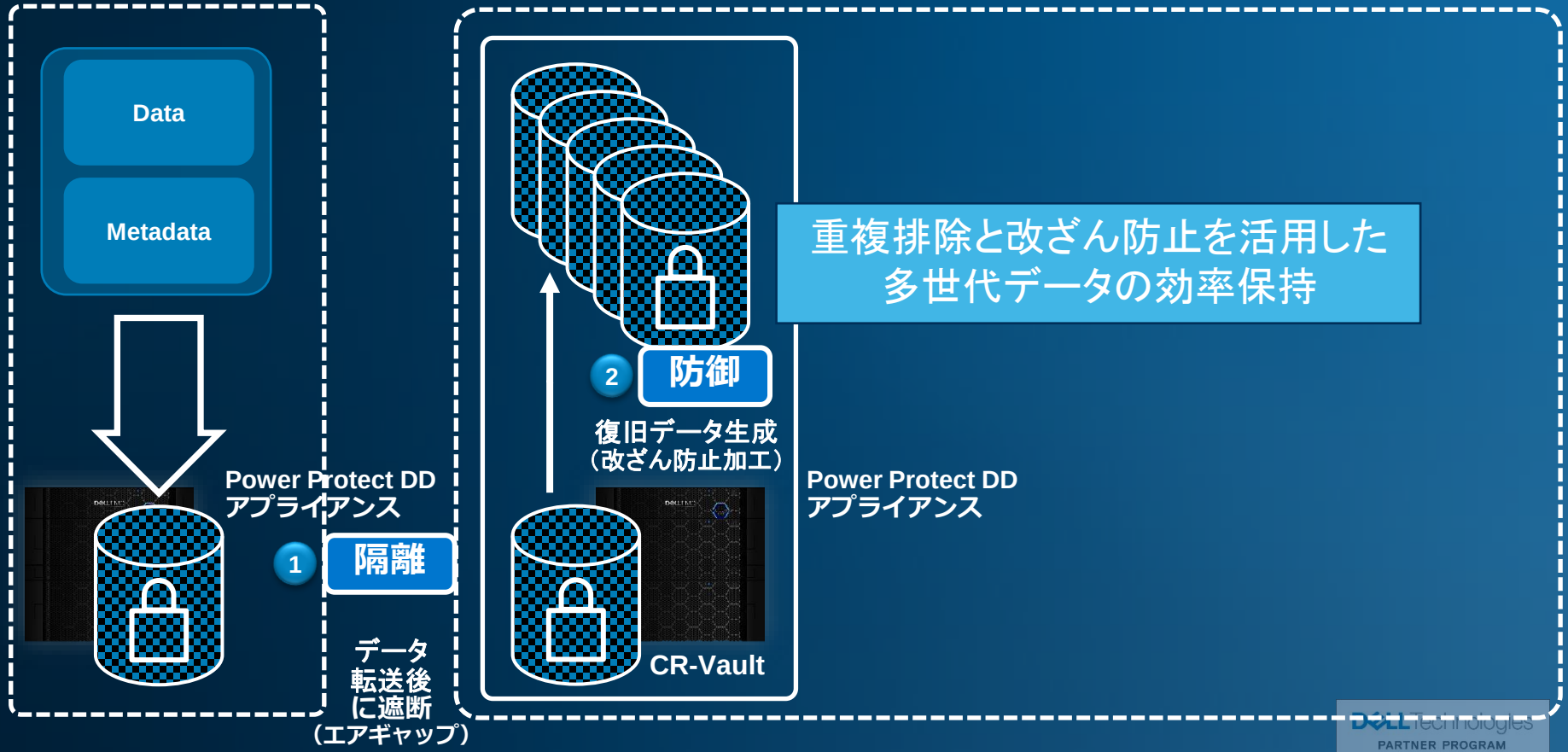
PowerProtect Cyber Recovery 概要

ソリューション機能として提供



PowerProtect Cyber Recovery 概要

ソリューション機能として提供

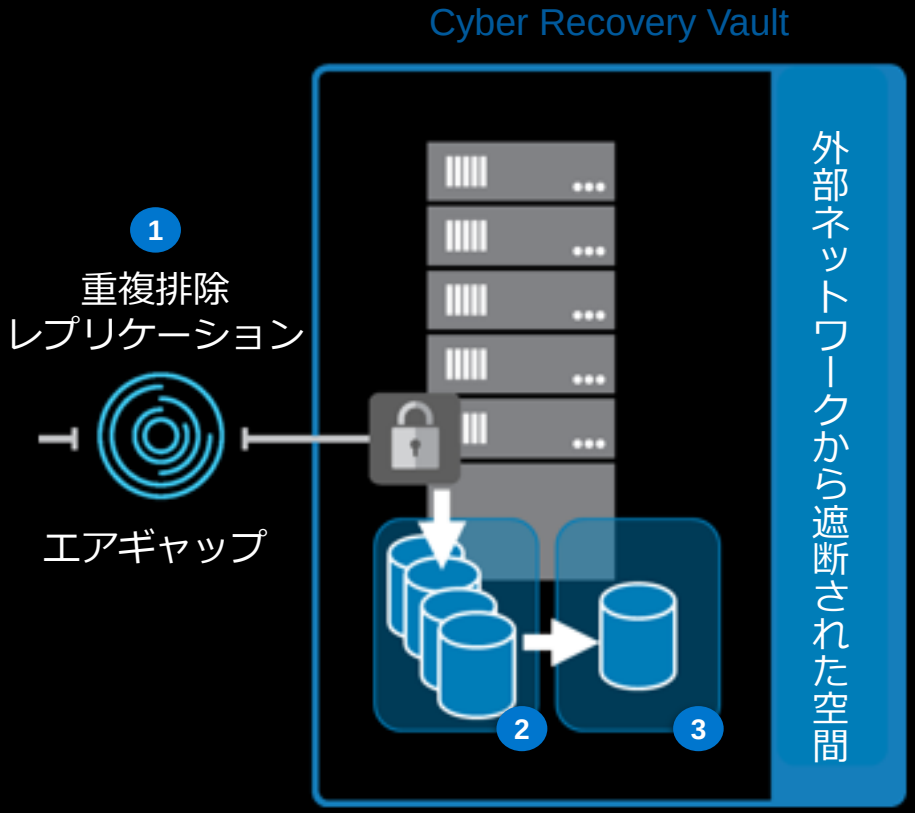


重複排除と改ざん防止を活用した
多世代データの効率保持

Cyber Recovery Management Software

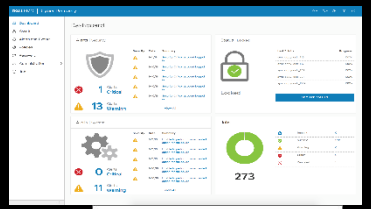
ネットワーク隔離(エアギャップ)と復旧データ管理

データ隔離
（隔離）（管理）



1. エアギャップを実現するデータリンク接続・切断の設定とポリシー管理による自動化
2. 「復旧データ」の確保：データの多世代生成・保持と改竄防止ロック適用のポリシー管理による自動化
3. 分析用のサンドボックスデータ生成とエクスポート

- 専用UI・ダッシュボードによる設定と運用管理の一元化



DELL Technologies
PARTNER PROGRAM

データ「破壊」「改ざん」脅威に対応

サイバー攻撃に対する更なる防御壁の配備

Retention Lock 機能による
バックアップデータの削除や変更を防止

- システム管理者権限を使用しても バックアップデータの変更、破壊、削除は不可
- より高い権限を持ったセキュリティ管理者の監視の元でのシステム管理業務を行う
- ランサムウェア、破損、およびその他の破壊的攻撃に対する付加的な保護を提供

保存期間中はいかなる人もデータを変更できない

データ防御

ソフトウェアのエディション

- ガバナンス
- コンプライアンス

Power Protect DD
アプライアンス

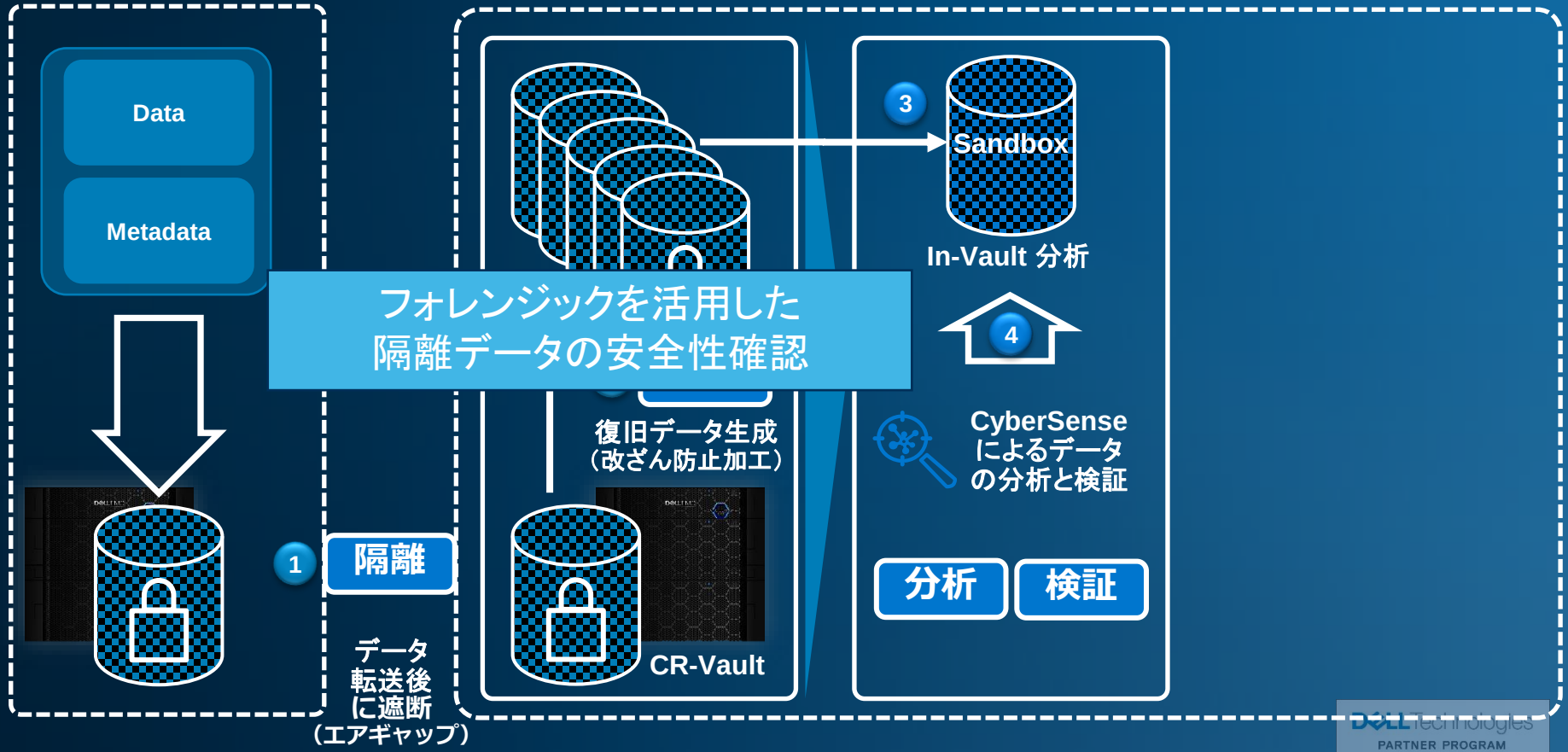
システム管理者

指定の
「セキュリティ担当者」

DELL Technologies
PARTNER PROGRAM

PowerProtect Cyber Recovery 概要

ソリューション機能として提供



Dell EMC CyberSence

PowerProtect Cyber Recovery 専用の脅威分析エンジン

データ衛生（分析）（検証）

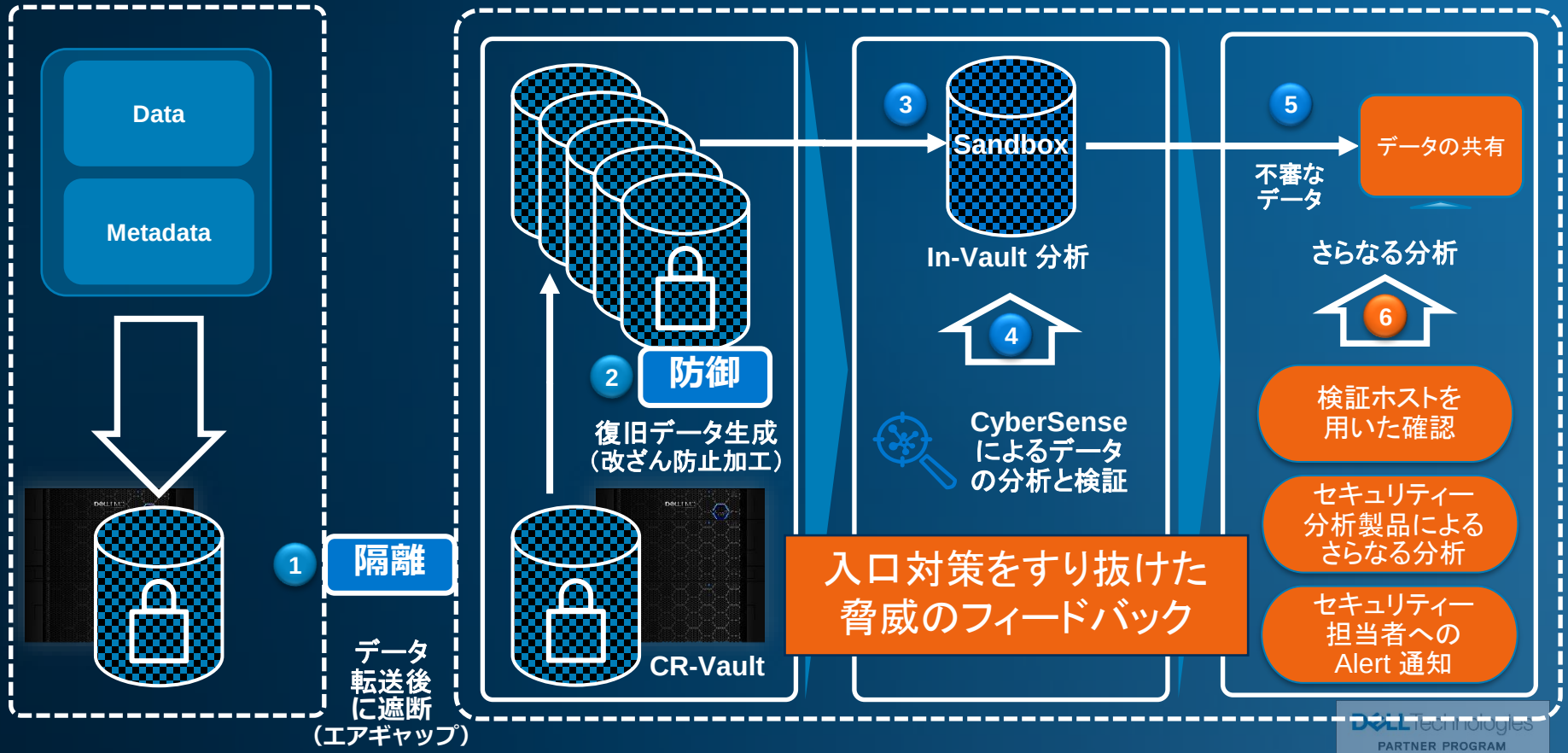
- より確実に、最適な復旧用データを準備するための サイバー復旧データ専用分析機能
- 「確保」「隔離」「管理」機能と連動した 「分析」「検証」を提供
- 隔離データから感染兆候を発見することで、入口対策で検知できなかったリスクをフィードバック

DELL Technologies PARTNER PROGRAM

PowerProtect Cyber Recovery 概要

ソリューション機能として提供

追加検討項目（別ソリューション実装）



最新事例にみるDell EMCデータ保護の効果

秋田県 湯沢市 様

増え続けるデータへの対応と**ランサムウェア等への事前対策**を講じたデータ保護基盤の構築

岡山県 真庭市 様

VDI 環境での**220倍重複排除**と**ランサムウェア対策**を実現する堅牢なデータ保護基盤の構築

三協立山 株式会社 様

テレワーク下 業務端末4,000台の**運用管理効率**と**ランサムウェア対策**を高めるデータ保護基盤の構築

データ保護の視点から 定常**運用負荷の大幅削減**による「**働き方改革**」と「**レジリエンス強化**」を支援

THANKS FOR YOUR GREAT PARTNERSHIP

intel

vmware

CISCO

BROCADE
A Broadcom Company

NVIDIA