DELL Technologies

Dell PowerProtect Cyber Recovery

データ保護をサイバーレジリエンスへ高度化

サイバー脅威も**ニューノーマル**な時代へ

「特定の」ターゲットからデータを**「窃盗」**する時代から
「不特定多数」に対してデータを**「利用不可（破壊・捕縛）」**にする時代に

1. 激変するサイバー脅威

2015～16年を境にサイバー脅威は大きな変貌を見せている。侵入後に入手（コピー）した情報の転売や悪用、情報書き換え、高負荷をかけてサービスを停滞させるといった手法から、**デジタルデータそのものを掌握（削除・暗号化）する**ことで事業活動自体・全体を機能不全に陥れる手法へと激化している。

2. 広がる被害と損失

デジタル変革が進むなか、デジタルデータは経営の重要な資源となってきており、様々な業務・サービスを動かす潤滑油となってきている。そのため、デジタル化の推進度合いに比例し、掌握されてしまった時の被害は甚大で、**長期に渡るサービス停止や多額の損失から企業の存続を危ぶませる実例**が、国内・海外ともに多くみられるようになった。

3. 巧妙化する手口

その経緯から、IPAを始めとした様々な機関が最終的な手段として「バックアップデータの確保と活用」を企業に提言 ※1。さらには一般消費者に対しても警視庁が「定期的なバックアップ」を奨励 ※2 するなど、対策として一般化しつつある。その流れを汲み、ウィルスや攻撃者の手口も変化し、**最初にバックアップデータから掌握することを、ターゲットに設定し始めている。**バックアップデータを保管するストレージや、バックアップソフトウェアのカタログ・インデックス情報の暗号化・破壊などだ。

※1 出典：IPA（情報処理推進機構）ウェブサイト
https://www.ipa.go.jp/security/txt/2016/01outline.html
※2 出典：警察庁 サイバー犯罪対策プロジェクト ウェブサイト
https://www.npa.go.jp/cyber/ransom/main2.html

何が変わってきたのか？
サイバー攻撃がもたらす脅威の変貌

- **従来の脅威**
  - サイバー**窃盗**：一部情報の瞬間的な複製入手と流用
  - サイバー**攻撃**：一部情報の改ざんによるビジネス妨害

- **昨今の脅威**
  - サイバー**破壊**：本番・災対・バックアップデータの完全破壊
  - サイバー**恐喝**：データの捕縛（暗号化など）と身代金要求

海外・国内で見られる様々な被害

激化するサイバー脅威

グローバル海運会社大手

NotPetyaマルウェアにより、2.6億米ドルの**被害（売上・機会損失、賠償等）**、および3億ドルの**収益の減少**を伴い、**数週間の運用遅延と混乱**に苦しむ。

グローバル大手製薬企業

主要な生産管理システムおよび作業者エンドポイントデバイスに影響を及ぼす**ランサムウェア**により、**製薬事業の全面的な混乱**を経験。

グローバル大手食品企業

NotPetyaマルウェアが複数の工場コンピュータシステムに感染し、**生産が完全に停止**。被害は約1.4億米ドルと測定される。

国内でも見られる被害

某国内大手自動車メーカー

主要工場内で利用の端末に**WannaCry**発症が露見。工場内総点検の為、**製造ラインの24時間停止**に追い込まれ、**主力車種約1,000台**の製造遅延を強いられる。

某国内大手食品小売業

社内に混入した**WannaCry**が店舗系システムに伝染。**約2,900店舗の電子マネー決済やポイントサービスを数日停止**させ、店舗運営の**混乱**と**機会損失**を誘発。

某国内鉄道運営企業

業務系システム内に侵入した**ランサムウェア**が**本番・バックアップデータを全て掌握**。幸いにもネットワークが分断されていた運行・料金系システムには影響なく、運行は維持。

デジタルデータのレジリエンシを高める**3つのポイント**とは？

データ防御

バックアップデータの暗号化や改ざん防止により、高権限（admin/etc.）乗っ取りやデータを特定されても掌握されない状態に。

データ隔離（隔離・管理）

攻撃者から「見えない」場所へ復旧用データを隔離することで、攻撃時でも重要なデータが特定できない状態に。

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り、安全な復旧用データの確保と、入口対策をすり抜けたリスクの発見とフィードバックを可能に。

データ防御：見つかったデータを利用不可にさせない

Retention Lock

サイバー攻撃に対する更なる防御壁の配備

データ「破壊」「改ざん」脅威に対する
バックアップデータ削除や変更を防止

- 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下で、システム管理業務を行う事が可能
- 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更なる保護を提供

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

Retention Lock

ガバナンス機能

コンプライアンス機能

PowerProtect 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」

データ隔離：大事なデータを脅威から隠す

Cyber Recovery Management Software

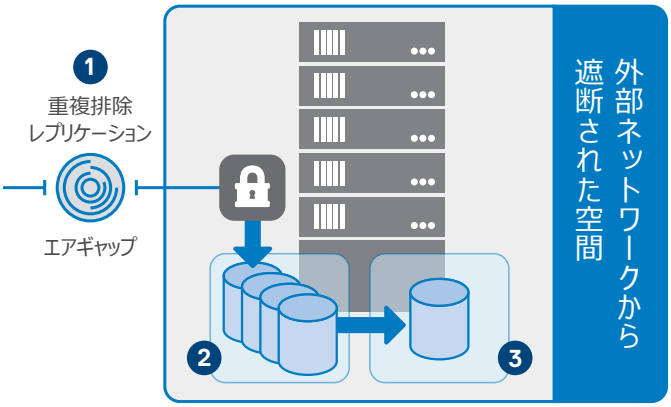
ネットワーク隔離（エアギャップ）と復旧データ管理

1. ネットワーク分離（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・保持と改ざん防止ロック適用のポリシー管理による「隔離」「防御」プロセスの自動化
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

データ隔離（隔離）（管理）

Cyber Recovery Vault



データ衛生：確保したデータの確実性を高める

Dell CyberSence

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

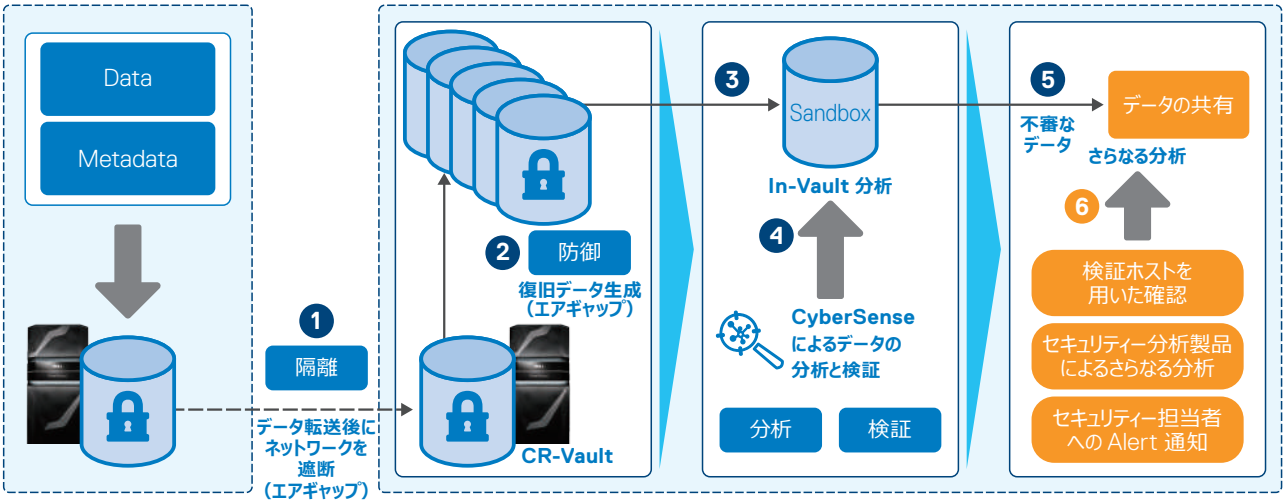
- より確実に、最適な復旧用データを準備するため、サイバー復旧データ専用の分析機能を提供
- 隔離」「防御」したデータを「分析」「検証」しデータの確実性を高める
- 隔離データから感染兆候を発見することで、入口対策で検知できなかったリスクをフィードバック

データ衛生（分析）（検証）

バックアップの延長で実現できる、一挙両得のサイバーレジリエンス

PowerProtect Cyber Recoveryの全体像

● ソリューション機能として提供　● 追加オプション（関連ソリューション*と組合せて実装）



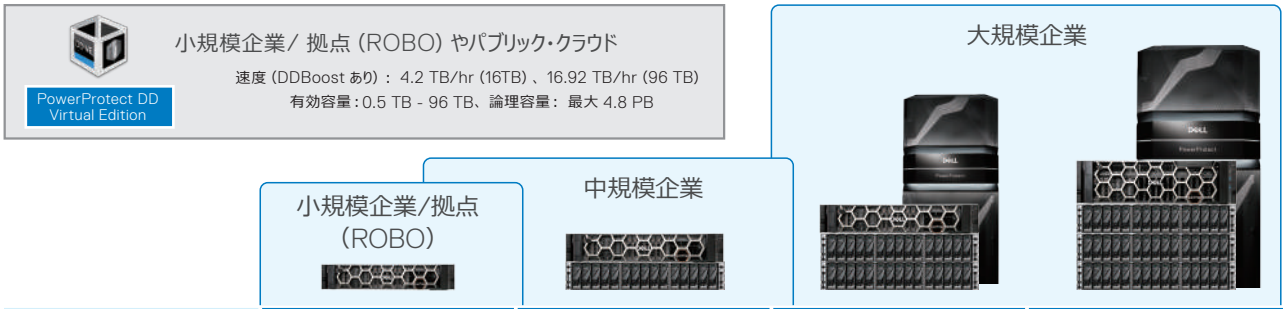
平常時運用の延長線で非常時復旧が可能

エアギャップと改ざん防止で脅威から復旧データを保全

AI/ML/フォレンジックを活用した分析による安全性担保

*関連ソリューション： Secureworks、VMware Carbon Black、RSAなど

サイバーレジリエンスを高めるデータ保護アプライアンス －Dell PowerProtect DD アプライアンス



	DD3300	DD6900	DD9400	DD9900
速度（DDBoostあり）	7TB/hr	33TB/hr	57TB/hr	94TB/hr
速度（DDBoost以外）	4.2TB/hr	15TB/hr	26TB/hr	41TB/hr
論理容量[1]	0.2 - 1.6 PB[2] 0.6 - 4.8 PB[3]	1.5 - 18.7 PB[2] 6.4 - 56.1 PB[3]	12.5 - 49.9 PB[2] 20.0 - 149.5 PB[3]	37.4 - 81.2 PB[2] 46.5 - 211.2 PB[3]
有効容量	4 - 32 PB[2] Up to 96 PB[3]	24 - 288 PB[2] Up to 864 PB[3]	192 - 768 PB[2] Up to 2.3 PB[3]	576 - 1.5 PB[2] Up to 3.25 PB[3]

[1] 論理容量は理論値上の重複排除率（DD3300 50x / DD6900/9400/9900 65x）をベースに算出
[2] アクティブ階層のみの最大容量
[3] Cloud Tier を使用した場合の長期保存用の最大容量

デル・テクノロジーズ株式会社
〒100-8159 東京都千代田区大手町一丁目2番1号 Otemachi Oneタワー17階
https://www.delltechnologies.com/ja-jp/index.htm

●セールスおよび製品に関するお問い合わせ
https://www.delltechnologies.com/ja-jp/contactus.htm