

DELL TECHNOLOGIES PARTNER PROGRAM

HEROES

Dell Cyber Recovery Solutionによる 確実なデータ隔離と復旧の実現

2021年10月14日

デル・テクノロジーズ株式会社

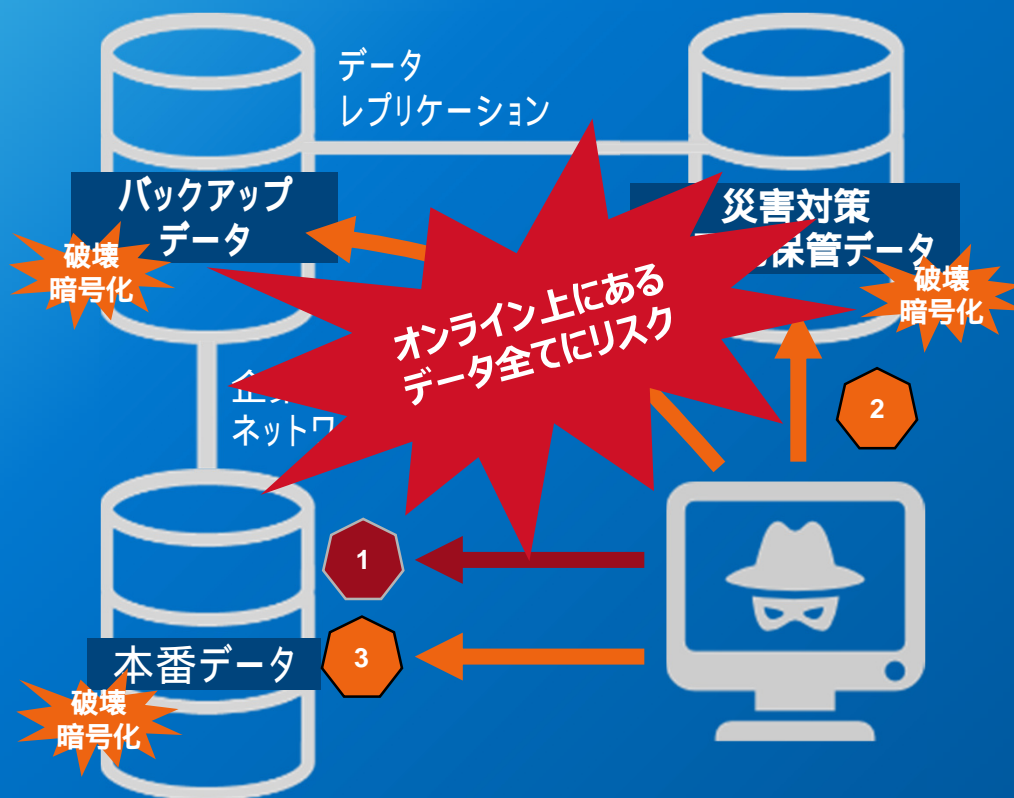
DPS事業本部 SE部

シニアシステムズエンジニア 岩井 秀樹

DELL Technologies
PARTNER PROGRAM

近年のサイバー攻撃手法の変貌

サイバー攻撃がもたらす脅威の変貌



1 サイバー窃盗・攻撃

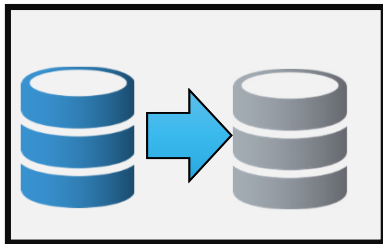
- 侵入後、本番データへアクセス
- データの複製を入手
- 本番システム上のデータを変更

サイバー破壊・恐喝

- 2 • 侵入後にインフラ全体を掌握
- 復旧できないようバックアップやDR/遠隔地データを破壊・捕縛
- 3 • バックアップやDR/遠隔地データ掌握後、または同タイミングで本番データを破壊・捕縛

従来のデータ保護方式ではサイバー攻撃には対応できない

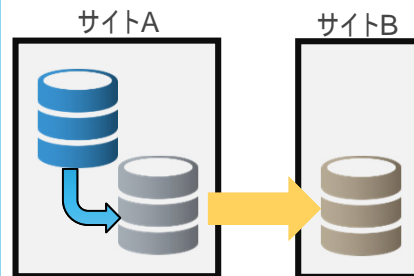
筐体内コピー (オンラインバックアップ)



サイバー攻撃対策：×

ネットワークに繋がっている
データを筐体内コピーをする為、
暗号化・改竄されてしまう

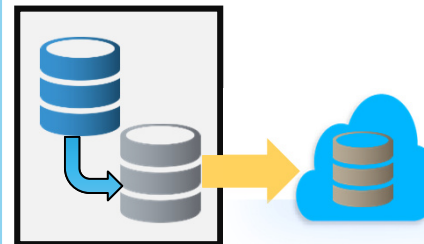
筐体間レプリケーション (オンラインバックアップ)



サイバー攻撃対策：×

サイトを分けたとしても、
ネットワークに繋がっている
データをレプリケーションをする為、
暗号化・改竄されてしまう

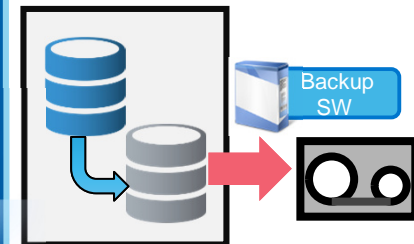
Cloudへの保管 (オンラインバックアップ)



サイバー攻撃対策：×

Public Cloud保管を実施しても、
ネットワークに繋がっている
データをレプリケーションをする為、
全て暗号化・改竄されてしまう

筐体外Tape保管 (オフラインバックアップ)



サイバー攻撃対策：

- ・Tapeから戻す為、復旧に時間がかかる/運用工数がかかる
- ・Tapeに保管したデータの整合性が取れてないリスク有
- ・確実にリストアできるかは、有事の際に戻してみないとわからないリスク有

ネットワークから切り離れた隔離領域を準備し、復旧時間と工数を最小限で実現する事が、サイバー攻撃からの被害を最小限に食い止める

サイバーレジリエンス:海外の法的規制の動向

欧米では単なるバックアップ以上のデータ復旧確保を求める傾向に



欧州銀行監督局
(European
Banking Authority)

“管轄当局は、施設が包括的かつ**実証済みのビジネス回復力および継続計画**を適切に実施しているかどうかを評価する必要があります”



アメリカ連邦準備制度
(US Federal Reserve)

“金融機関は、次の手順を踏むことを検討する必要があります... 最重要システムに対する**ハード・バックアップ、エア・ギャップ、クリティカル・システムの物理的セグメンテーション**などを...”

アメリカ連邦金融検査協議会
(US Federal Institutions Examination Council)



“...本番環境データが攻撃に晒された際、レプリケーションされたバックアップデータが破損・破壊されないよう、必要なステップを講じておく必要がある。
...エア・ギャップ型バックアップアーキテクチャであれば、サイバー攻撃への露呈を制限し、攻撃が開始される前のある時点へデータの復元が可能になる”

- FFIEC, Appendix J, 2/6/15

DELL Technologies
PARTNER PROGRAM

ランサム対応実装に向けた “3 STEP”

STEP1 : ネットワークから隔離された環境(Vault)の構築

Point 1

独自プロトコル(Boost)によるレプリケーション
AirGapによるネットワーク遮断

STEP2 : 複数世代バックアップと改ざん防止

Point 2

重複排除によるリソースの効率化
Retention Lock

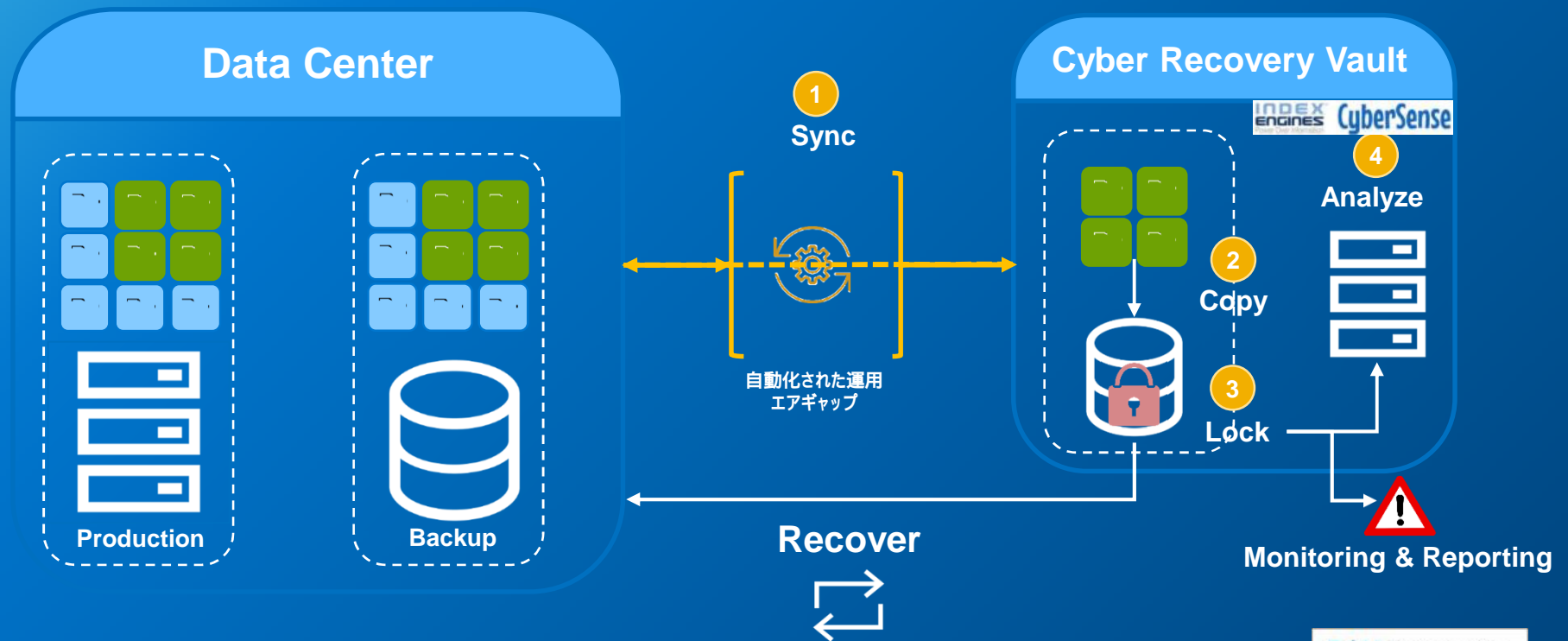
STEP3 : クリーンなデータセットを見つけ出し、確実にリストア

Point 3

バックアップカタログデータの隔離
定期的なバックアップデータの監視

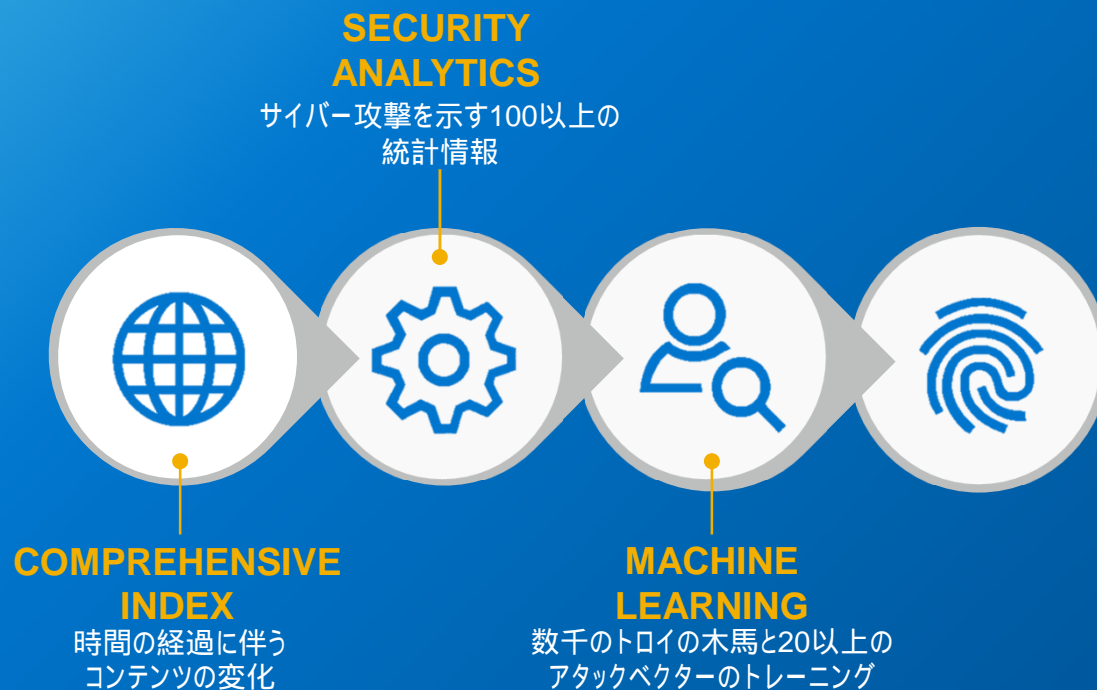
PowerProtect Cyber Recovery Solution

サイバー攻撃に対するデータ保護防御の最終ライン



CyberSense バックアップデータ分析フロー

機械学習により、サイバー攻撃の早期発見と迅速な回復が可能に



Cyber Recovery with CyberSense

- アタックベクターの通知
- ランサムウェア
- 破損したファイルの詳細
- データの変更/削除
- 侵害されたユーザーアカウント
- 違反した実行可能ファイル
- 最後の健全なコピーによる回復

DELL Technologies
PARTNER PROGRAM






CyberSense と「一般的な」分析の違い

機械学習により、CyberRecoveryポータル内での早期検出と迅速なリカバリを可能

CyberSense:



完全なコンテンツの
インデックス作成：

- 1 ファイル メタデータ 
-  2 ドキュメント メタデータ 
-  3 ドキュメント コンテンツ 

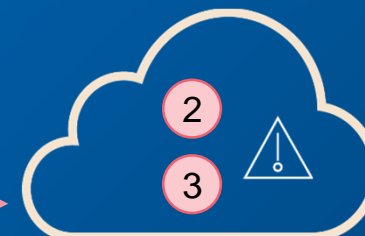
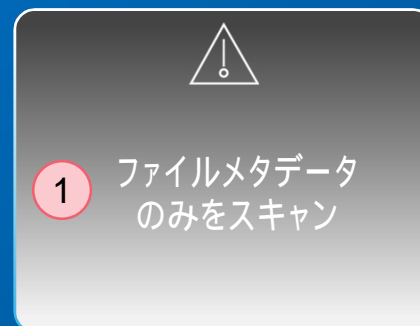
99.5%

VS.

Basic Analytics:

オンプレミス
分析エンジン

クラウドベース
分析エンジン



2回目または完全な
コンテンツ分析のために
疑わしいファイルをクラウド
に送信

88%

DELL Technologies
PARTNER PROGRAM

PowerProtect CyberRecovery Solutionの優位性

最近の脅威には、最新のソリューションが必要



Isolation (隔離)

データの物理的および
論理的な分離

PowerProtect Cyber Recovery
Vault環境は、オンプレミスまたはクラウド
およびマルチクラウドのいずれかで
エアギャップによって保護



Immutability (不変)

データの元の整合性を
維持

多層のセキュリティと制御により、
保管されたデータの破壊、削除、
改ざんから保護



Intelligence (知性)

MLを活用した分析による
脅威の特定

CyberSenseは、データの確実な
回復を可能にし、CyberRecovery
Vault内からの攻撃ベクターへの
洞察を提供





Dell Technologies

サイバーリカバリとデータ保護のリーダーシップ

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
2018	PowerProtect CyberRecoveryソリューションを提供
2019	シェルトードハーバーアライアンスパートナープログラム最初のテクノロジーベンダー
2020	最初に承認されたシェルトードハーバーソリューション – PowerProtect Cyber Recovery
2021	マルチクラウド向けのPowerProtect CyberRecoveryを導入
2021	AWS向けのPowerProtect CyberRecoveryを導入

1000+

Cyber Recovery 導入顧客数

#1

Data Protection
Appliances & Software*

¹ Based on combined revenue from the IDC 3Q20 Purpose-Built Backup Appliance (PBBA) Tracker, with select Storage Software segments from the 3Q20 Storage Software and Cloud Services Qview.

² IDC 3Q20 Storage Software and Cloud Services Qview



THANKS FOR YOUR GREAT
PARTNERSHIP

