OVERLAND TANDBERG

RDXによるランサムウェア対策

ランサムウェアとは

ランサムウェア（Ransomware）とは、ファイルを暗号化して読めなくし、データ復旧のために身代金を要求する脅迫型マルウェアです。10年ほど前から感染による被害が拡大し、最近では日本国内でも多くの感染被害が確認され、病院で電子カルテシステムが感染し、患者の受け入れができないという被害も発生しています。

11病院サイバー被害
救急搬送・手術 停止も
「身代金」ウイルス
16年以降
遠山元議員 在宅起訴
融資仲介 貸金業法違反
夕刊は1月4日から

2021年12月29日読売新聞記事

ランサムウェアへの有効な対策

ランサムウェアによる被害に合わない、あるいは被害を最小化するためには以下のような対策が有効です。

①セキュリティソフトのインストール
②データのバックアップを取得しネットワークから隔離された状態で保管する
③マルウェアからアクセスできない形でデータを保管する

①のセキュリティソフトによる対策は既存のランサムウェアに対しては有効ですが新型の場合、検知/駆除できないケースもあります。
したがって、②③の対策がより有効/確実なものとなりますが、この手法に対しリムーバブルディスクシステムであるRDXを活用することが可能です。

RDXとは?

RDX（**R**emoval **D**isk E**x**change System)とは？

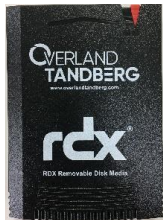
2005年にPROSTOR Systems 社が開発したリムーバブル・ディスク・システム。高い互換性、テープメディアのようなポータビリティ、ディスクドライブのランダムアクセス性を兼ね備えた製品。Tandberg Dataは、2011年5月ProStor社よりRDX製品に関する権利と開発リソースを取得しました。

SMBのバックアップデバイスの業界標準！

多くのサーバベンダーがバックアップデバイスとして採用。
DDS/DATの生産/販売終了後、事実上のSMBビジネス向けのバックアップデバイスとして、広く認知されています。

Tapeの良いところ!

- ポータビリティ
- 丈夫なカートリッジ
- 低コスト



Diskの良いところ!

- ランダムアクセス性能
- 高い転送レート
- 信頼性

erg

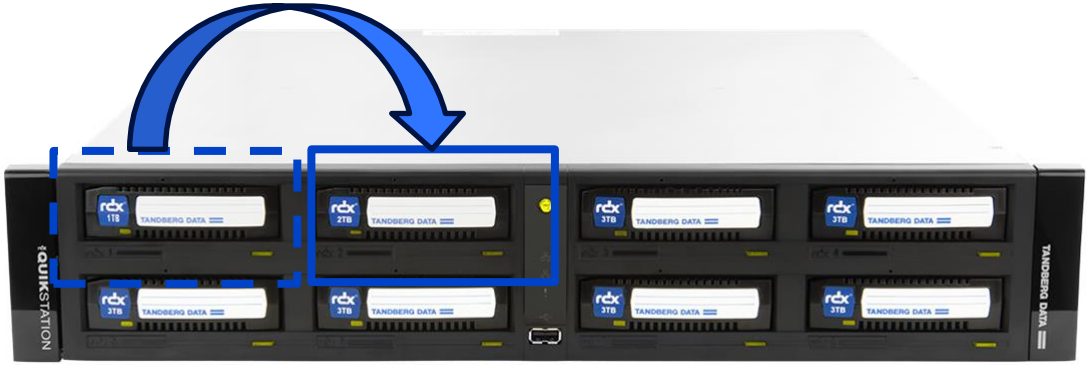
OVERLAND TANDBERG

RDXによるランサムウェア対策①（基本的な手法）

RDX + バックアップソフトウェアでイメージバックアップを取得し、複数世代管理/外部保管を組み合わせることにより、万がーサーバーが感染した場合でも、感染していないバックアップデータより容易にデータ復旧が可能です。
（③～⑤世代のデータが感染していても①②世代より復旧が可能）

RDXによるランサムウェア対策②

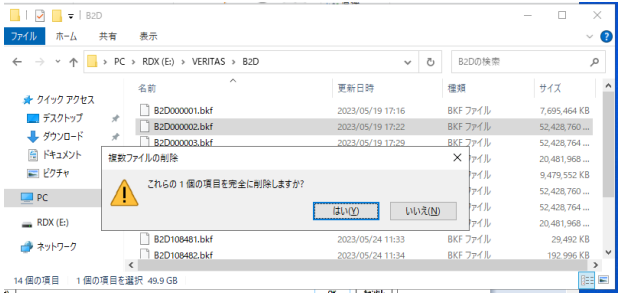
（QuikSation4,8ディスクオートローダーモードの活用）

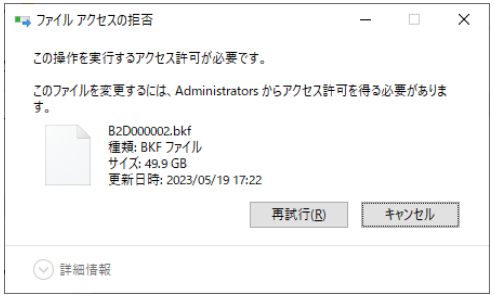


複数世代管理を行う場合、RDX集合装置QuikStation4/QuikStation8のディスクオートローダーモードを使用すれば、自動で次のカートリッジにバックアップ先が移動し、それ以外はオフラインとする運用が可能となり、自動での複数世代管理/オフライン保管が実現できます。

RDXによるランサムウェア対策③

（バックアップソフトウェア機能の活用）





Backup Execの
バックアップフォル
ダへのアクセスは
拒否されます。
※BEインストール
環境のみ有効

RDX単体ドライブやQuikSation4,8を使用し、カートリッジを挿入したまま（オンラインのまま）の状態でランサムウェア被害を回避するための方法として、Veritas社Backup Execの「ランサムウェアレジリエンス」機能を使用する方法もあります。

RDXによるランサムウェア対策④（その他）

RDX WORMカートリッジの活用
※上書きバックアップは不可

RDX WORMカートリッジ

QuikSation4,8の仮想テープモードでの使用
※オンラインの状態では100%の安全を
保証するものではありません

ランサムウェア対策に効果があるその他の手法として、WORMカートリッジの活用や、QuikSation4,8をランサムウェアの影響がより少ないと思われる仮想テープモードで使用する方法があります。


OVERLAND
TANDBERG
Thank You