

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。



ランサムウェアの被害を受けた病院

2016年1月	鳥取県立中央病院 (鳥取市) パソコンのファイルが開けなくなる
17年5月	日立総合病院 (京浜東北線) メールの送受信が不能
8月	福島県立医科大学附属病院 (福島市) CT画像が保存できなくなる
12月	新潟県立新潟大学総合病院 (新潟市) ファイルの暗号化され、使用不能
18年10月	宇都宮市立病院 (宇都宮) 電子カルテが閲覧不能
19年7月	名古屋中央病院 (川崎市) 電子カルテが閲覧不能
21年4月	電子カルテが閲覧不能
5月	市立東大塚医療センター (大塚市) CTやレントゲン、内臓検査の画像データの一部が閲覧不能
9月	豊田新成病院 (豊田) 電子カルテが使用不能
10月	富士病院 (静岡) 電子カルテが閲覧不能
	つるぎ野立平田病院 (宮城県) 電子カルテが閲覧不能

「身代金」ウイルス

ランサムウェア システムが不正侵入し、データを暗号化して読めなくするコンピュータウイルス。ランサムは「身代金」を意味する英語で、攻撃者は、復元する代わりに身代金を要求する。被害で多数の情報が流出し、2015年頃から国内でも確認されるようになった。身代金を支払わなければ、データを公開する。被害は口もみられる。警察庁によると、警察に寄せられた被害相談は今年1～6月で1万件あった。



11病院サイバー被害 救急搬送・手術停止も

遠山元議員 在宅起訴 融資仲介貸金業法違反

東京地検 遠山元議員 元衆議院議員
融資仲介貸金業法違反

【東京29日電】元衆議院議員の遠山元議員が、融資仲介貸金業法違反で在宅起訴された。東京地検は、遠山氏が2017年から2019年まで、融資仲介貸金業法違反で約1億5000万円の融資仲介を行ったと認定し、起訴した。遠山氏は、融資仲介貸金業法違反で約1億5000万円の融資仲介を行ったと認定し、起訴された。遠山氏は、融資仲介貸金業法違反で約1億5000万円の融資仲介を行ったと認定し、起訴された。

【夕刊】一週4日か
日本経済新聞によると、遠山氏は、融資仲介貸金業法違反で約1億5000万円の融資仲介を行ったと認定し、起訴された。遠山氏は、融資仲介貸金業法違反で約1億5000万円の融資仲介を行ったと認定し、起訴された。

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 (Removal Disk Exchange 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



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、万が一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

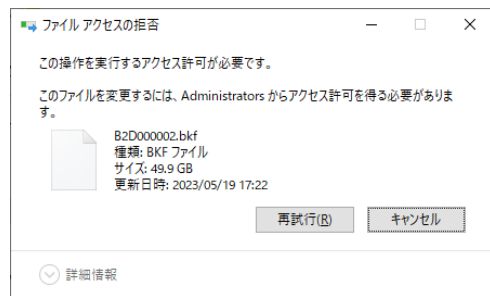
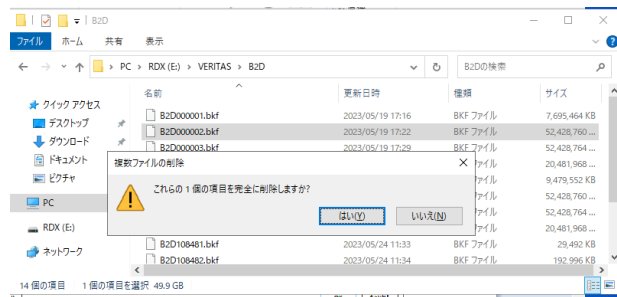
(QuikStation4,8ディスクオートローダーモードの活用)



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QuikStation4,8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)の状態でも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方法があります。



**OVERLAND
TANDBERG**

Thank You