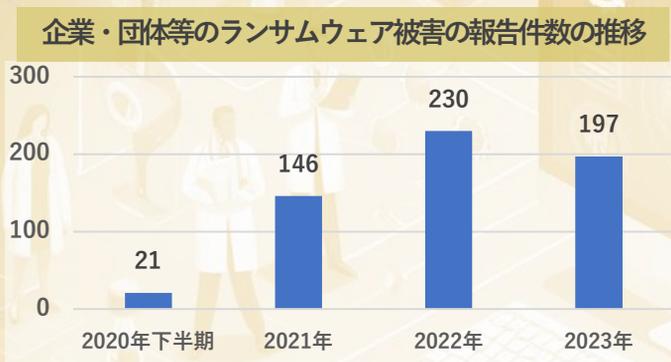
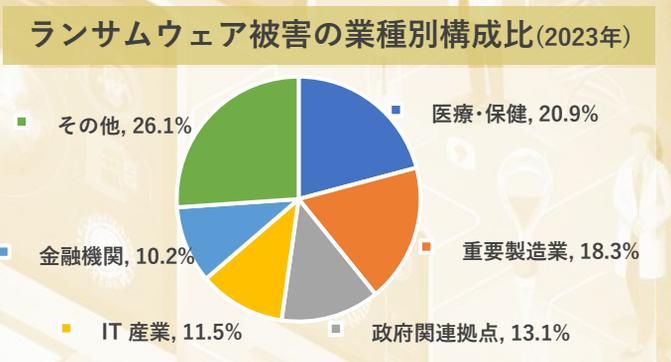


医療機関のセキュリティ強化をサポートする バックアップ・リカバリーソリューション

サイバー攻撃の現状について



出典：独立行政法人情報処理推進機構（IPA），
情報セキュリティ白書2024 図1-2-1 を基に編集



出典：独立行政法人情報処理推進機構（IPA），
情報セキュリティ白書2024 図1-1-4

日本国内でのサイバー攻撃の被害の急増
ランサムウェアのターゲットとして医療機関が狙われている・・・

被害にあってしまうと…

【被害例①】

四国の某病院（2021年10月）
復旧までに総額2億円以上かかった

【被害例②】

関西の某医療センター（2022年10月）
復旧までに数か月を要した



医療機関での必須の対策 【医療情報システムの安全管理に関するガイドライン】

安全管理を実現するために必要な要素 = 医療情報システムのバックアップを取ること

1. 大規模災害に備えて、**分散してバックアップ**を取る
2. ランサムウェア対策として、**オフライン環境**にバックアップデータを保存する
3. 障害対策として、**すぐにシステム復旧**ができるようにする

2023年5月 改定 【医療情報システムの安全管理に関するガイドライン 第6.0版】より

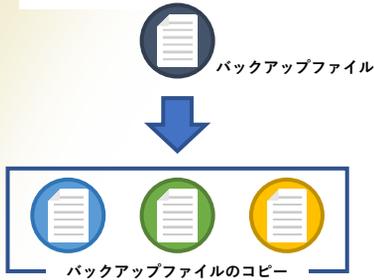
【医療情報システムの安全管理に関するガイドライン 第6.0版】に対応した
簡単なバックアップソフト

ActiveImage Protector -RE オススメ ポイント

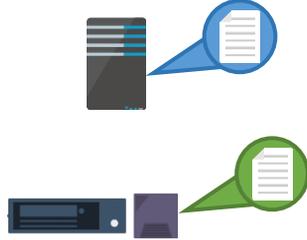
【3-2-1ルール】を活用しバックアップを分散

バックアップファイルをActiveImage Protector -REで対応しているLTOテープやRDXカートリッジなどの外部メディアにコピーすることで、バックアップを分散することが可能！

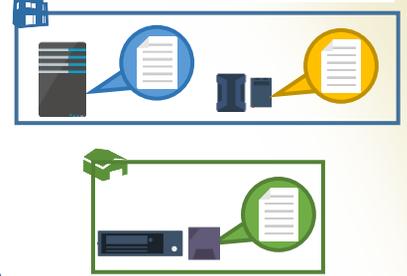
3 つのバックアップのコピーを作成



2 種類の異なるストレージメディアにバックアップを保存



1 つのバックアップは物理的に距離のある別の場所に保存



LTO・RDXに保存することでオフライン環境にバックアップを保存

LTO・RDXを活用すれば、ネットワークに接続していないオフライン環境にバックアップを保存することが可能。

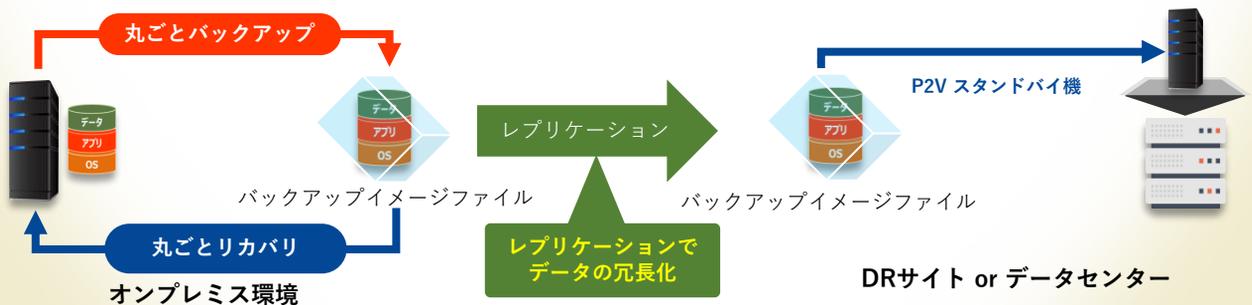
さらに標準搭載「保存先隔離オプション」を使用すれば、バックアップ後保存先の接続を自動で切断することも可能！



スタンバイ機作成で迅速なシステム復旧

スタンバイ機の作成が可能のために、医療機関で求められる早期な業務再開にも対応！

さらにスタンバイ機を遠隔地に作成することで、BCP対策にも対応可能！



<https://www.activeimage-re.com/>

【お問い合わせはコチラ！】
株式会社ラネクシー ActiveImage -RE 担当宛
⇒aipre_sales@runexy.co.jp



Webミーティングも
お気軽にご相談ください！

