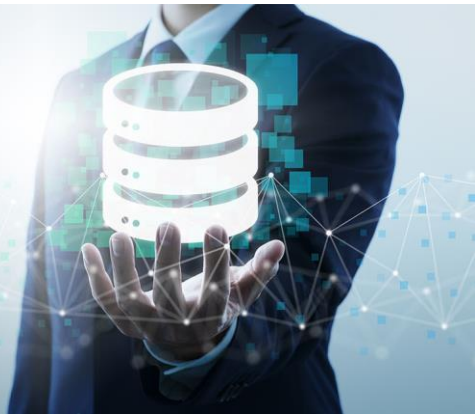
HITACHI
Inspire the Next

ランサムウェアの被害から迅速なデータ回復を支援

データ回復ソリューション

ランサムウェアなどによるデータ侵害の脅威が高まる中、災害対策や機器障害・データ損失からのデータ復旧を目的とした従来のバックアップでは昨今の巧妙なサイバー攻撃に対応することが難しくなっています。こうした状況において重要となるのが、インシデントが発生した場合にも、早急に事業を復旧するための仕組み作りです。



ランサムウェアに感染するとどうなる？

端末やサーバーのデータが暗号化され使えなくなってしまいます。復号のために身代金を支払ったとしても、**データが必ず復号される保証はありません**。また、バックアップを取得していても**バックアップデータ自体がランサムウェアに感染**していたというケースもあります。

食品製造業

複数のサーバーがランサムウェアに感染。**バックアップシステムも被害**に遭い、完全復旧まで**約2カ月**。

自動車製造業

複数のサーバー、PCがランサムウェアに感染。
取引先企業が**操業停止**となり、完全復旧まで**約1カ月**。

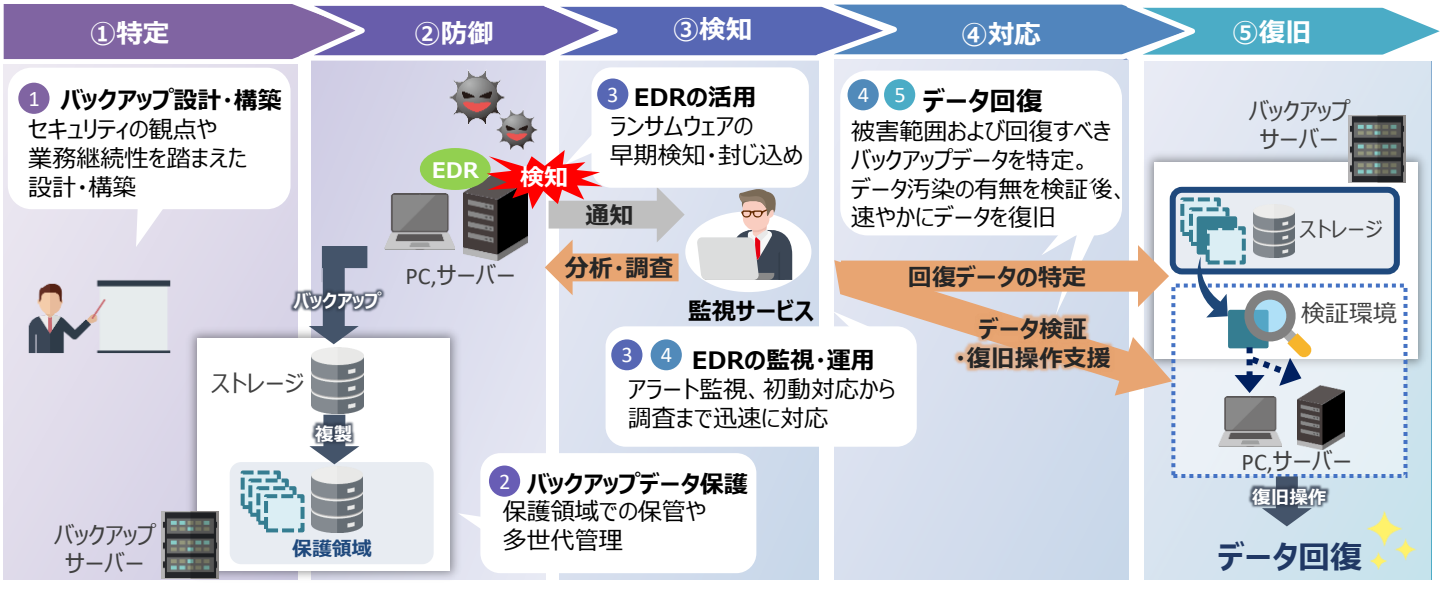
医療機関

複数のサーバー、PCがランサムウェアに感染。**バックアップシステムも被害**に遭い、事業再開まで**約2カ月**。

場合によっては事業停止といった事態に陥ってしまうケースも

データ回復ソリューションとは

豊富な知識を持ったセキュリティエキスパートが、セキュリティの観点や業務継続性を踏まえたバックアップ・リストアの設計から構築、EDR製品を活用した端末の日常的な監視運用、インシデント発生時の初動対応、データ復旧まで支援。NISTのサイバーセキュリティフレームワークで定義される、サイバーセキュリティ対策を構成する5つの要素それぞれに分類されるメニューを提供します。



NIST:National Institute of Standards and Technology

事業継続に必要な対応をワンストップで提供

株式会社 日立ソリューションズ

特長

01 EDRの導入、運用サポートによる被害の拡大防止

EDRのアラート分析により被害範囲（被害を受けた端末、時刻）を調査し、感染前のバックアップデータの特定・データ回復を素早く実施。
迅速な業務復旧を支援。

対応EDR製品：CylanceOPTICS、Trend Micro Apex One、FortiEDR、VMware Carbon Black、CrowdStrike

02 ランサムウェアなどの脅威からバックアップデータを保護・保全

セキュリティの観点や事業継続性を踏まえ、サイバー攻撃対策を前提としたバックアップの設計・構築を支援。
バックアップデータを守ります。

03 独自技術を活用した調査ツールで被害ファイルを特定

独自技術を活用した調査ツールにより、データのエントロピー*を評価し、ランサムウェアにより暗号化された可能性が高いファイルを検出。回復が必要なデータを絞り込むことで、事業復旧にかかる時間を削減。

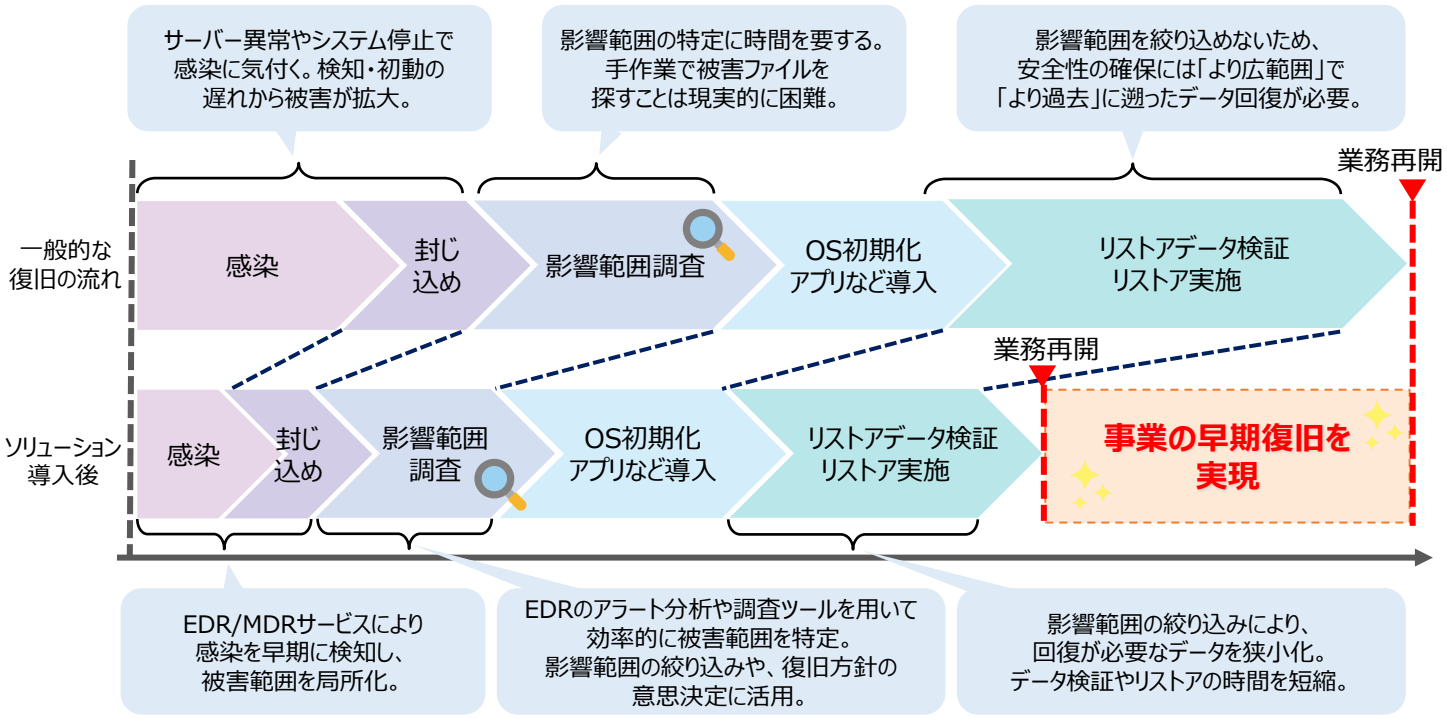
*エントロピー：ファイル内のデータの不規則性を表す尺度

04 専門家によるワンストップ支援

サイバーセキュリティに関する専門知識や高度なスキルを持つ技術者が、アラート発生の検知から感染前のバックアップデータ特定、データ回復までをワンストップで支援することで、お客様の運用負荷を軽減。

導入効果

被害範囲（端末・時刻・ファイル）特定により、ランサムウェア感染後の「リストアデータの検証」や「リストア実施」の工数を大幅に削減可能。業務の早期再開を支援します。



株式会社 日立ソリューションズ
www.hitachi-solutions.co.jp

本リーフレット掲載商品・サービスの詳細情報
https://www.hitachi-solutions.co.jp/security/sp/solution/task/data_recovery.html