

ランサムウェア攻撃から 企業のデータを確実に保護するためには

～ セキュアなバックアップで、身代金を払わず、迅速に復旧可能 ～

企業を狙うサイバー攻撃が猛威を振るっており、特にランサムウェアによる被害が国内でも急増しています。ますます巧妙化するランサムウェアの攻撃手法に対して、侵入や感染を完全に防ぐことは非常に困難です。万が一感染した場合でも、なるべく被害を抑え、サービス復旧させるための対策として見直されているのが、回復力を高めるための統合化されたデータ保護/バックアップの仕組みです。

バックアップはセキュリティ構成要素の 1 つ

ランサムウェア被害が急増

情報セキュリティ10大脅威 2023

2023年 順位	情報セキュリティ脅威	2022年 順位
1	ランサムウェアによる被害	1
2	サプライチェーンの弱点を悪用した攻撃	3
3	標的型攻撃による機密情報の窃取	2
4	内部不正による情報漏えい	5
5	テレワーク等のニューノーマルな働き方を狙った攻撃	4

バックアップが最後の砦

ランサムウェア被害の予防のために、**バックアップの取得**をすること
(定期的な復旧リハーサルも重要)

被害を受けた後の対応は、**バックアップからの復旧**を行うこと

IPA (情報処理推進機構: 経済産業省所管) 「情報セキュリティ10大脅威 2023」
<https://www.ipa.go.jp/security/vuln/10threats2023.html>

バックアップデータもランサムウェアに狙われています セキュアなバックアップシステムが必要

IPA 情報セキュリティ白書 2019

攻撃者は攻撃対象とする組織のネットワークに侵入することから始める。侵入後は組織内のシステムを調査し、**バックアップデータ等の重要なデータを狙って、ランサムウェアに感染させる。**

IPA 情報セキュリティ白書 2019
<https://www.ipa.go.jp/security/publications/hakusyo/2019.html>

NIST サイバー セキュリティ フレームワーク

「**データ保護**」は、**セキュリティ対策の一部** 防御 (PR.IP-4) 情報のバックアップが、実施され、維持され、テストされている。**復旧 (RC.RP-1)** 復旧計画が、サイバーセキュリティインシデントの発生中または発生後に実施されている。

NIST Cybersecurity Framework
<https://www.nist.gov/cyberframework>

ランサムウェアからデータを確実に守るための バックアップシステムとは

あらゆるデータを バックアップ

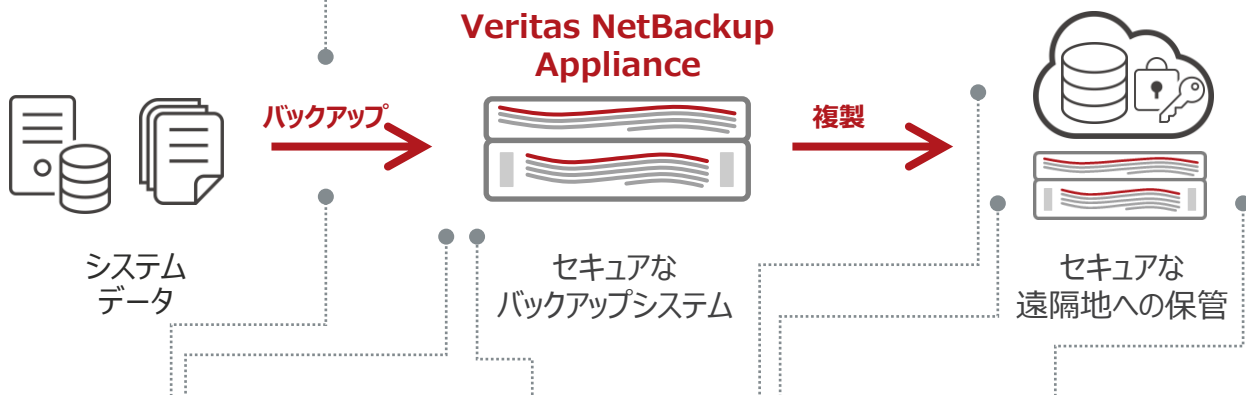
単一のバックアップシステムで、あらゆる企業のシステム、データを統合バックアップできます。バックアップ状況の全体の可視化が可能で、リストア操作を簡略化できます。

シンプル構成 最小限の初期投資

バックアップ速度が高速なため、1台のバックアップシステムでシンプルに構成できます。少ない容量からスタートでき、初期コストをおさえることが可能です。

セキュリティ強化済み 専用アプライアンス

セキュリティ強化された専用OSを搭載したバックアップシステムです。WindowsやLinuxで構成された一般的なバックアップシステムより断然セキュアです。



異常検出 マルウェアスキャン

バックアップ対象データの統計情報をAIで分析し、異常なデータ、状態を検出します。また、保存しているバックアップデータに対するマルウェアスキャンを行います。

改ざん防止 削除防止

アプライアンス、クラウドストレージのWORM*機能を活用し、バックアップデータの改ざん、削除を防止します。IT管理者の誤操作による削除も防止できます。

BCP対策 エアギャップ

バックアップデータの遠隔地への複製に、クラウドストレージを活用可能です。また、複製先のバックアップシステムへのネットワーク遮断のスケジュールを設定できます。

* WORM (Write Once Read Many) は、ストレージ内のデータ改ざん/削除を防止する機能

CTCは、NetBackup Appliance 国内実績 ダントツ No.1!!

1 導入実績・ノウハウ

- ✓ 業種を問わない多数の実績 (製造・情報通信・金融・小売・教育・サービス・公共・医療など)
- ✓ クラウド、BCPなど幅広い要件に対応



2 高品質な保守サービス

- ✓ ハードウェア・ソフトウェアの一括保守
- ✓ 25年以上のNetBackup保守実績
- ✓ 全国対応 (ハードウェア交換、稼働確認、ファームアップなど)



3 バックアップ運用

バックアップに関する定常/非常業務の効率化

- ✓ バックアップジョブ設定の自動追加
- ✓ バックアップからのシステム即時起動
- ✓ BCP発動時の一連のシステム復旧

