

# NetBackup がランサムウェアからあなたを守る 5 つの方法

ランサムウェアに関するニュースが続いていますが、それには十分な理由があります。2031 年までに 2 秒ごとに 1 社がランサムウェア攻撃の被害者になる見込みで<sup>1</sup>、IT セキュリティプロフェッショナルの半数は自社ではランサムウェア攻撃を撃退するための準備ができていないと考えています。<sup>2</sup>

ランサムウェア攻撃防止の最初のステップは最前線での堅ろうな防御ですが、それだけでは不十分です。すべての企業は、包括的な多層型の回復力フレームワークを開発する必要があります。このフレームワークは、総合的なサイバーセキュリティ戦略に含まれる保護、検出、および回復の各要素をサポートするためのものです。犯罪が巧妙化しており、ランサムウェア攻撃は「万が一」仕掛けられたらという問題ではなく、「いつ」仕掛けられるかという問題になっています。

Veritas NetBackup<sup>™</sup> を使用すれば、その日に備えて回復力を確保できるようになります。NetBackup は、以下の 5 つの方法でランサムウェア攻撃に対する保護、検出、回復を支援します。



## 1. ハードウェアとソフトウェアの強化を支援します。

IT システムは複雑に絡み合っているため、ランサムウェアは 1 人の従業員が受信したフィッシングメールなどの 1 つの侵入口から企業の全データへと拡大し、企業に甚大な被害を与える可能性があります。

こうした脆弱性に対する防御を高めるために、NetBackup は、包括的なハードウェアとソフトウェアの強化を通じて IT 攻撃対象を削減できるよう企業を支援します。きめ細かな役割ベースのアクセス制御 (RBAC)、2 要素認証、保管中と送信中の両方でのデータ暗号化を含む ID およびアクセス管理の強化によって、NetBackup は増え続ける脅威に対して環境を強化するためのツールを提供します。



## 2. 改ざん不可能なストレージによるバックアップの保護を可能にします。

バックアップは、ランサムウェア攻撃に対する最後の防御線となる可能性があります。攻撃者が企業のバックアップを暗号化した場合、身代金支払いに対抗する手段はほとんどなくなります。ただし、書き込んだデータを変更または削除できない改ざん不可能なストレージを備えていれば、対応方法の選択肢が広がります。

ランサムウェアが最前線の防御を突破し、オンプレミスやクラウド内の企業システムに侵入した場合に備え、NetBackup は改ざん不可能なイメージ管理およびストレージを提供してお客様のバックアップを暗号化や消去から保護します。その結果、お客様のデータはランサムウェアによる破壊や暗号化の脅威にさらされることがなくなるため、迅速に回復できるようになります。



## 3. エアギャップによるデータ保護をサポートします。

ネットワークに物理的に接続されたシステムはすべて標的となり侵入される可能性があるため、ネットワークに接続されたバックアップは脆弱です。データを保護するための 1 つの方法が、保存されたデータとネットワークに接続されたシステムとの間に物理的なスペース、つまりエアギャップの作成です。このオフラインのバックアップは、データに対する悪質なアクセスと暗号化を防ぐための安全策の 1 つです。

NetBackup はお客様のエアギャップ戦略をサポートできます。回復力機能により、ストレージメディアに対してデータを重複排除および複製し、サードパーティを必要とすることなくエアギャップを実現できます。



#### 4. 潜在的な脅威を自動的に検出します。

昨今のサイバー犯罪者は、企業のデータとインフラのあらゆる側面を標的にします。脆弱性と脅威の検出には、企業のデータ、インフラ、ユーザーアクティビティを認識し制御できることが重要です。

NetBackup があれば、環境を包括的に把握でき、人工知能 (AI) を活用して、バックアップが作成されるたびに異常を検出し、不審なアクティビティについてアラートを受けることができます。IT チームは、予期されるデータアクティビティや、システムを横断する権限など、データとインフラのベースライン動作をより適切に理解できるようになります。異常が検出されると、チームは直ちに対応して、影響するバックアップを分離し、影響を最小限に抑え、データを常に回復可能な状態にすることができます。



#### 5. リカバリプロセスの自動化およびオーケストレーションの導入を可能にします。

多くの IT チームはハイブリッドでマルチクラウドのインフラを構築して企業のニーズを満たしていますが、その複雑さのためにデータの脆弱性が高まり、回復が困難になることがあります。数百または数千台のサーバーを所有する企業は、手動でデータを迅速に回復できないため、自動化が必要になります。

NetBackup には回復プロセスの自動化とオーケストレーションを実現するための包括的なオプションが用意されており、ランサムウェア攻撃を受けたときに制御を維持するのに役立ちます。NetBackup には VMware 向けのインスタントロールバック機能があり、仮想マシンを任意の時点へと即座にロールバックできます。本番環境にロールバックするときに、必要なブロックのみが送信されるため、従来、数時間から数日かかっていた回復処理が、わずか数分または数秒にまで短縮され、事業継続性が損なわれません。

### Veritas NetBackup がもたらす確信

壊滅的な損害をもたらす可能性があるランサムウェア攻撃に、NetBackup なら備えることができます。世界トップクラスのデータバックアップおよびリカバリソリューションである NetBackup は、すべてのワークロード、すべてのクラウド、すべてのアーキテクチャをサポートできる単一のプラットフォームにより、規模に対応してビジネスクリティカルな回復力を提供します。

データを破壊する悪質な攻撃に対処するために、NetBackup には保護、検出、および回復ツールと、データとインフラを強化する回復力戦略が用意されており、ランサムウェア攻撃から確実に防御できます。

ランサムウェア攻撃に対する最大限の回復力の維持に Veritas NetBackup がどのように役立つかを、[www.veritas.com/ja/jp/protection/netbackup](http://www.veritas.com/ja/jp/protection/netbackup) でご確認ください。

1. Cybercrime Magazine, 「Global Ransomware Damage Costs Predicted To Exceed \$265 Billion By 2031 (全世界のランサムウェアによる被害額が 2031 年までに 2,650 億ドルを超える見込み)」, 2021 年 6 月 3 日
2. PurpleSec 社, 「10 Cybersecurity Trends You Can't Ignore In 2021 (2021 年に無視できない 10 のサイバーセキュリティ傾向)」, 2021 年 4 月 29 日

### ペリタスについて

Veritas Technologies はデータの可用性および保護のグローバルリーダーです。複雑化した IT 環境においてデータ管理の簡素化を実現するために、Fortune Global 500 の 87% を含む、先進企業 50,000 社以上が、ペリタスのソリューションを導入しています。ペリタスのエンタープライズ・データサービス・プラットフォームは、お客様のデータ活用を推進するため、データ保護とデータリカバリのオーケストレーションを実現して、ビジネスに不可欠なアプリケーションの可用性を常に確保し、複雑化するデータ規制対応に必要なインサイトを提供します。ペリタスのソリューションは信頼性とスケーラビリティに優れ、500 以上のデータソースと 60 のクラウドを含む 150 以上のストレージ環境に対応しています。ペリタステクノロジーズ合同会社は、Veritas Technologies の日本法人です。

## VERITAS

〒107-0052 東京都港区  
赤坂 1-11-44  
赤坂インターシティ 4 階  
[www.veritas.com/ja/jp](http://www.veritas.com/ja/jp)

世界各地の連絡先については、  
以下をご覧ください。  
[veritas.com/ja/jp/company/  
contact](http://veritas.com/ja/jp/company/contact)