

ランサムウェア対策に充実の選択肢 NECのストレージソリューション

高速ストレージからディスク・テープまで完備、サポートもワンストップで提供

ランサムウェア攻撃の手法は日々巧妙化し、もはや従来のソフトウェアに軸足を置いたセキュリティ対策だけでは被害を防ぐことは難しい。そのような脅威に対応するためには、実際にデータが保存されているストレージ製品自体にも目を向け、データの窃盗やランサムウェアによる暗号化被害を防ぐための仕組みを備えていく必要がある。ランサムウェア対策に効果的なストレージ製品と対策のポイントを、NECのiStorageシリーズの担当者に聞いた。

脅迫の手口は日々巧妙化し 中小企業の被害が増加

金銭搾取を目的としたランサムウェア攻撃が猛威を振るっている。脅迫の手口も巧妙化し、特定の組織を狙った標的型攻撃が侵入時の主流となっている。さらに、侵入後は身代金の要求に加え、「支払わなければ窃取したデータを公開する」と要求する二重脅迫、さらには取引先や顧客への攻撃やDDoS攻撃を絡めた三重・四重脅迫の手法も登場するなど、状況は悪化する一方だ。

被害の規模もどんどん拡大し、国内では業種問わずさまざまな企業が被害を受け、さらに公共機関や医療機関などの組織も標的となっている。警察庁が発表している「令和6年におけるサイバー空間をめぐる脅威の情勢等について」によると、ランサムウェア被害件数を組織規模別に比較したとき、前年度と比べて大企業の被害件数が減少しているものの、中小企業の被害件数が37%増加している。組織規模の大小を問わず攻撃が行われているこの状況について同資料では、「ランサムウェアの開発・運営を行う者が攻撃者にツールを提供し、その見返りとして身代金の一部を受け取るRaaS (Ransomware as a Service) による裾野の広がりが、対策が手薄な中小企業の被害増加につながっている」と分析しており、全ての企業・組織にしっかりと対策が必須な現状を示唆している。

安全な仕組みを備えたストレージ群で セキュアな構成を実現

では実際に、攻撃を受ける側はどのような対策を講じるべきなのか。具体的には、感染を防ぐ事前の対策と、被害を抑えるための事後の対策が必要になる。NECインフラ・テクノロジーサービス事業部門 データストレージ統括部の畠中輝義・プロフェッショナルは「ランサムウェアを使った攻撃は、従来のセキュリティ製品による対策だけでは防げない。被害を受けてしまうとその後の対応が困難を極めることも踏まえて、標的になる入り口とデータを保管しているストレージの双方での対策が重要だ」と指摘する。

ただし現在、多くの企業・組織ではストレージ領域の対策がまだ十分に行われていないのが実情だ。ストレージ領域で対策を行う際には、単にバックアップを取るだけでは不十分で、「ランサムウェアの特徴を

踏まえた上での安全な仕組みを備えた製品、あるいはセキュアな構成を考えてストレージシステムを導入する必要がある」と、畠中氏は指摘する。NECは高速なプライマリストレージ製品からバックアップ用の製品まで、「iStorageシリーズ」として企業・組織の規模や目的に応じた幅広い製品群を提供している。「3つのコピーを常に持ち、2つの異なるメディアで保存し、さらに1つは物理的に別の場所で保管する」というバックアップの基本姿勢、つまり「3-2-1ルール」も同社ソリューションで実現可能だ。

「市場のニーズを踏まえつつランサムウェア対策に有効な機能を随時実装し、ユーザーのデータ保護を支援するための製品開発を行っている」(畠中氏)。

プライマリ領域で有効な スナップショット機能

NECはオンプレミス向けのプライマリストレージ領域で、HDDとSSDのハイブリッド構成が可能な「iStorage Vシリーズ」を提供中だ。エントリー向け「V10e」、中規模向け「V110」、大規模向け「V310」、オールフラッシュの「V310F」の4種類をラインアップしており、それぞれのクラスに応じたかたちで、ランサムウェア対策に有効な複数のバックアップ機能が備わっている。

その中で同社が特に有効とするのが、V110、V310、V310Fが備える「スナップショット機能」である。「差分でバックアップを管理するため、高い容量効率で多数世代のバックアップを取得できる。そこがランサムウェア対策



畠中輝義
プロフェッショナル

と相性が良い。スナップショット取得時にはリダイレクト・オン・ライト (RoW) 方式を採用しているため、ストレージ性能への影響も小さい」と、NECデータストレージ統括部の鈴木淳平・プロフェッショナルはメリットを説明する。また、ランサムウェアや悪意のあるユーザーの不正操作からデータを保護するための「Secure Snap」機能も搭載されている。データ保護期間中はスナップショットの更新や削除ができない仕組みを備え、

「スナップショットを一定期間ロックすることで、悪意のある第三者や管理者権限を乗っ取るようなランサムウェアが現れた際も、バックアップデータが失われずに済む」と鈴木氏は話す。

そのほか、オプション機能として「筐体内コピー」「筐体外コピー」「暗号化機能」なども備えており、Vシリーズの外部ストレージ接続機能と筐体内コピー機能を利用して、パブリッククラウドサービス「AWS Storage Gateway」に二次バックアップを取ることもできる。これらを組み合わせることで、まずはプライマリストレージ側で柔軟かつ有効な対策を行うことが可能だ。



鈴木淳平
プロフェッショナル

アップソフトとも連携可能な改ざん防止 (WORM) 機能による2種類のランサムウェア対策が行えるようになっている。運用の容易性を重視する場合は前者、データの保護強度を重視する場合は後者、との使い分けも可能だ。

Tシリーズでは、1Uラック型で9巻搭載可能な「T09A」、LTO-9世代のテープにより最大5PBまで増設できるスケーラブル型の「T280」を用意。テープ媒体への保存によって物理的なエアギャップを確保してバックアップを運用できることに加え、ネットワークにつながった場所でもWORM媒体を使つていれば改ざんが防止できるようになっている。「テープは持ち運びが可能なバックアップ媒体であるためオフサイト保管が可能というわかりやすさがある。昨今は大容量低成本でバックアップできるため、病院などの医療分野でも支持されている」と市川氏は説明する。

25年の実績を持つiStorage サポート網も全国に

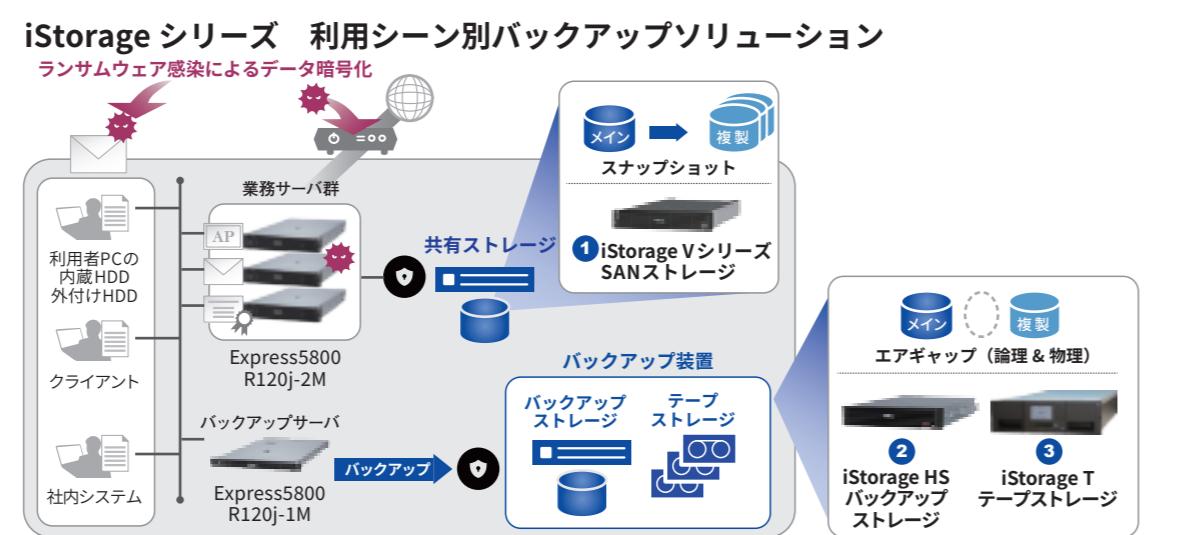
このようにiStorageシリーズを活用することで、プライマリストレージからバックアップ領域まで複数のラインアップを組み合わせて効果的なランサムウェア対策の仕組みを講じ、自社の状況に応じて安全にデータを保護できるようになる。「ランサムウェア対策としてストレージに求められるバックアップ機能を提供している。各種ストレージ製品に加えてバックアップソフトも取り扱っているので、ワンストップで対応できるところがNECの強みだ」と鈴木氏は語る。

iStorageシリーズは2025年で誕生25周年を迎えた。これまでTシリーズを7000台以上、HSシリーズを9000ノード以上出荷し、発売からまだ4年ほどしか経っていないVシリーズもすでに1200台以上が導入されている。製品ラインアップの幅広さと導入実績、そこで培った技術力と開発リソース、さらには全国に組織されているサポート網も含めた総合力がNECのストレージ製品の強みで、ユーザーが製品を選択するに際しての差別化ポイントになっている。

また、製品を販売するパートナーに対しても、提案時にセキュアなストレージ構成のサポートを行うほか、「ユーザーからの要望を製品開発に優先的に反映させる体制も整っている」(畠中氏)のことだ。現在iStorage25周年の特設サイトが用意され、最新情報などが紹介されている。IT商材を販売する企業にとって、提案時の参考になるだろう。

iStorage25周年 特設サイト

<https://jpn.nec.com/istorage/25th-anniversary/index.html>



iStorage ランサムウェア対策ソリューション

解決可能なお客様の課題	iStorage のランサムウェア対策で解決	製品・サービスの概要
低コストでバックアップ対策をしたい	<input checked="" type="checkbox"/> 標準機能かつ高い容量効率でバックアップデータを保護	iStorage Vシリーズ ① 改ざん不可なSnapshotによるデータ保護
万が一ウイルス感染してもデータを守りたい 素早く復旧したい	<input checked="" type="checkbox"/> 改ざん防止機能によりランサムウェア感染時にもデータを保護し、クリーンなデータから素早く復旧	iStorage HSシリーズ ① クローン機能による論理的なデータ隔離 ② 改ざん防止機能によるデータ保護 (WORM: Write Once Read Many)
ランサムウェア対策で推奨されている「3-2-1ルール」で確実にデータを保護したい	<input checked="" type="checkbox"/> バックアップデータをオフサイト保管することでより確実なデータ保護が可能	iStorage Tシリーズ ① テープ媒体の外部保管による物理的なデータ隔離 ② WORM 媒体によるデータ改ざん防止

(この特集記事は、週刊BCN 2025年6月23日発行vol.2064に掲載したもの)