INFINIDAT

WEBINAR REPORTS

事例から学ぶ大手製造業のランサムウェア対策
大容量データを確実に保護する
「Veeam + Infinidat」の最強コラボのご紹介

MSYS 丸紅情報システムズ

veeam

INFINIDAT

丸紅情報システムズ株式会社
IT基盤ソリューション事業本部
事業推進部　浦川 隆弘 氏

ヴィーム・ソフトウェア株式会社
シニア・システムズ・エンジニア
山田 隆紀 氏

Infinidat Japan合同会社
ソリューション・アーキテクト
橋口 慎一 氏

開催概要

近年、多くの企業がDX推進に取り組む中、ペタバイト級さらにはゼタバイト級のデータ管理の必要性と重要性が叫ばれるようになり、データストレージ技術への注目度が再び高まっている。

一方で昨今テレワークの普及を背景に、企業規模の大小にかかわらずランサムウェアによる被害が拡大し、堅牢かつ革新的なセキュリティ対策と包括的なデータ保護ソリューションが求められる時代となった。

そうした中で開催された今回のウェビナーでは、データ管理のトレンドや事例をはじめ、データとITシステムを保護するための効果的なランサムウェア対策を紹介した。

開催日時　：　2月8日（木）16:00-17:00 （日本時間）
主　　催　：　Infinidat Japan合同会社
協　　賛　：　丸紅情報システムズ株式会社、ヴィーム・ソフトウェア株式会社

CONTENTS

SESSION 1
大容量ストレージ/サーバーのランサムウェア対策
丸紅情報システムズ株式会社　IT基盤ソリューション事業本部　事業推進部
浦川 隆弘 氏

SESSION 2
ランサムウェア対策を実現したバックアップシステムとVeeamセキュリティ機能ご紹介
ヴィーム・ソフトウェア株式会社　シニア・システムズ・エンジニア
山田 隆紀 氏

SESSION 3
大容量データをサイバー犯罪から守る次世代ストレージInfiniBoxのご紹介
Infinidat Japan合同会社　ソリューション・アーキテクト
橋口 慎一 氏

SESSION 1

大容量ストレージ/サーバーのランサムウェア対策

SPEAKER

丸紅情報システムズ株式会社
IT基盤ソリューション事業本部　事業推進部
浦川 隆弘 氏

IPA（独立行政法人情報処理推進機構）が発表した「情報セキュリティ10大脅威 2024」で、2021年から4年連続1位となったのが「ランサムウェアによる被害」である。なかでもターゲットとされる傾向が高まっているのが製造業だ。デジタル技術を活用した工場のスマート化に伴ってアタックサーフェス（攻撃対象領域）が拡大していることが背景にあり、サプライチェーンでつながる企業の脆弱な部分から侵入し、"本丸"の企業を攻撃するケースも増えている。

ある半導体関連企業がランサムウェア対策に乗り出したきっかけも、そういった近年の被害の拡大にある。実際に同業者にもサイバー攻撃が広がっている中で、危機感をもった経営陣から号令がかけられた。

ランサムウェア対策でまず基本となるのはバックアップだが、ペタバイト級の大規模なデータを所有するこの企業は、これまでどんな体制をとっていたのだろうか。

当然、従来からもバックアップは行っていたものの目的としては災害対策を主眼としており、主にストレージレプリケーションを実施していたが、1週間分のスナップショットしか保存されていなかった。しかもそれらのバックアップデータは、イミュータブル（変更不能）ではなかった。

そこでこの企業が打ち出したのは、「データコピーを3つ取り、2種類のメディアで保存し、そのうち1つを違う場所で保管する」を基本とした、いわゆる「3-2-1ルール」を要件とするバックアップの整備計画だ。加えて単なるバックアップはランサムウェア対策にならないため、イミュータブルで保護するとともに、最低でも90日以上のデータを保管する必要があると考えた。

上記のような基本方針を受けてソリューション提案にあたった丸紅情報システムズの浦川 隆弘氏は、**「現時点ではランサムウェア攻撃を100%完全に防ぐ方法は存在しないだけに、万一被害が発生した際に業務停止による損失をいかに最小化するかがポイントとなります。したがって確実にデータを保護し、本番環境に素早く復旧できる仕掛けの準備が重要です」**と語る。

そして策定されたのが、ヴィームのバックアップソフト「Veeam」と、Infinidatの大容量ストレージ「InfiniBox」を組み合わせたランサムウェア対策である。

「まず『イミュータブルなバックアップデータの保管およびその保護』に向け、Veeamの強化型Linuxリポジトリを活用することで一定期間変更不可の状態とします。テープバックアップにもVeeamで対応することが可能です。さらにInfiniBoxのイミュータブルスナップショット機能により、99.99999%の可用性でデータを確実に保護します。次に『高速なリストア』について、Veeamのファストクローン機能により増分バックアップの合成処理を高速化するとともに、InfiniBoxによる200万IOPS、25GB/秒の卓越したストレージ性能を最大限に活用します。また『バックアップデータの大容量化』という問題についても、InfiniBoxであれば最大7ペタバイトまでデータをまとめて格納することが可能です」と浦川氏は、提案したソリューションの概要を示す。

ユーザーサイドでITシステム運用管理を担っている責任者も、**「製品選定に際して、やはり容量単価や性能単価は重要な判断基準となります。他社のアプライアンス製品も検討しましたが、InfiniBoxと同程度の大容量を確保するには、かなり高価になってしまいます。またテープとストレージを併用するなど、Veeamによって可能となるシステムの柔軟性も重視しました」**と語る。

VeeamとInfiniBoxを効果的に組み合わせたソリューションによって、セキュアかつ高速なバックアップ環境を構築できたのである。

SESSION 2

ランサムウェア対策を実現したバックアップシステムとVeeamセキュリティ機能ご紹介

SPEAKER

ヴィーム・ソフトウェア株式会社
シニア・システムズ・エンジニア
山田 隆紀 氏

前項で紹介した半導体関連企業が新たに構築したバックアップ環境において、Veeamコンポーネントは、仮想基盤やファイルサーバー、NASといったソースのすべてに対応。強化型Linuxリポジトリを介して大容量のバックアップデータをInfiniBoxに格納するとともに、DR（災害対策）を意識した遠隔地保管用のバックアップデータをテープライブラリに保管する役割を担っている。

これによりVeeamが提供しているのが、次の3つのベネフィットだ。

まずは「複数のバックアップソースに対する一元的な対応」である。ヴィームの山田 隆紀氏は、**「ソースごとにサイロ化したバックアップシステムが少なくありませんが、Veeamはバックアップ/リストア運用を統一化することで省力化を図ります」**と語る。

次に「柔軟なバックアップシステムの構成」である。システム拡張・変更を行う際にも、それに合わせてVeeamコンポーネントを配置し直すだけで対応できるのだ。なおVeeamはインスタンス単位で課金を行っており、ライセンスのモビリティ（移動）も可能だ。**「システムを変更してもインスタンス数の増加がなければライセンスを付け替えるだけで済むため、追加コストを抑制できます」**と山田氏は言う。

さらに「セキュアなバックアップデータ保管」の実現である。**「今回は特にInfiniBoxとの連携によって、大容量データ保管やスナップショット機能の活用といったシナジーのメリットを提供することができました」**と山田氏は強調する。

そしてVeeamの真価が発揮されるのが、安全・確実・高速にデータを戻すことができるリストアだ。山田氏は、多くの企業で起こりがちな次の3つのケースに対応したVeeamの機能の特徴を説明する。

1つ目は、バックアップデータが破損して読み込めないというケース。これに対してVeeamでは、自動リストア検証をクリアしたバックアップデータのみを保持する。**「Virtual Labと呼ばれる本番環境に影響されない隔離環境で実際にバックアップデータを起動させ、データの整合性が保たれているかどうかを確認します」**と山田氏は語る。

2つ目は、ランサムウェアに感染したマシンのデータをバックアップデータから復旧しようとしたが、バックアップデータ自体も感染していたというケース。これに対応するのが前述した強化型Linuxリポジトリで、バックアップデータの不変性を確保してランサムウェアによる改ざん（暗号化）を防止する。**「加えてVeeamはセキュアリストアという機能も搭載しており、サードパーティーの主要なウイルス対策ソフトウェアを使ってマシンデータのスキャンを行ってから復元します」**と山田氏は補足する。Windowsの仮想マシンだけでなく、Linuxの仮想マシンに対しても、YARAと呼ばれる機能を使ったスキャニングによりマルウェアを検知することが可能だ。

3つ目は、必要なデータを決められた時間内に戻せないケース。これに対してVeeamではすべてのデータを戻す必要はなく、優先度の高いデータを選択してリストアできる機能を提供している。**「アプリケーションやファイル単位での選択も可能で、なおかつエクスプローラー上で操作できるため、誰でも簡単にリストアを行えます」**と山田氏。さらに特筆すべきがインスタントリカバリ機能で、バックアップデータをホストのデータストアとしてマウントすることで、直接仮想マシンを起動することができる。これなら数分単位で目的のシステムを再開することが可能だ。

ランサムウェアの被害は年々拡大しているだけに、バックアップデータの重要性はますます高まっている。そうした中で、ただデータを戻せるだけではなく、非常に高度なレジリエンス（回復力）を備えたバックアップシステムとしてVeeamは存在感を増しており、多くの企業から注目されているのである。

SESSION 3

大容量データをサイバー犯罪から守る 次世代ストレージInfiniBoxのご紹介

SPEAKER

INFINIDAT

Infinidat Japan合同会社
ソリューション・アーキテクト
橋口 慎一 氏

InfinidatのInfiniBoxは、「高いパフォーマンス」「高い可用性」「強固なセキュリティ」「コストの抑制」といった特徴を持つことからプライマリストレージとして広く利用されている。さらに容量単価でみてもリーズナブルであるため、バックアップ用途やセカンダリストレージとして利用されるケースも多い。

このInfiniBoxの数ある特徴の中で、Infinidat Japanの橋口氏がフォーカスするのがランサムウェア対策だ。サイバー犯罪向けのソリューションをInfinidatは『InfiniSafe』と名付けて展開しており、そこには大きく3つのピースがある。

1つ目は「改ざん防止スナップショット」。サイバー犯罪によって本番データの暗号化や削除が行われた場合でも、健全なデータから迅速に復旧できるようにするもので、InfiniBoxはペタバイト級の大容量データも瞬時にバックアップできる。こうして取得したスナップショットに対して改ざん防止期間を設定すると、その期間内はストレージの管理者であっても削除できないのだ。**「仮にストレージの管理者権限が乗っ取られたとしても、バックアップデータを保護することができます」**と橋口氏は語る。

さらに改ざん防止機能はバックアップ領域だけでなく、プライマリ領域に対しても適用することが可能だ。これが2つ目のピースとして提供している「改ざん防止ファイルシステム」である。InfiniBoxをNASとして使用している場合、ファイルシステム全体あるいは個々のファイルに対して一定期間の改ざん防止期間を設定することで、暗号化や削除ができないようにロックをかけることができる。**「InfiniBoxではこの機能についても追加ライセンスを支払うことなく、標準でご利用いただけます」**と橋口氏は訴求する。

3つ目のピースは「サイバー犯罪の検知」だ。Cyber Detectionと呼ばれる機能を活用するもので、サイバー犯罪を早期に検知し、復旧することで被害を最小化する。

「InfiniBoxで改ざん防止スナップショットを取得すると同時に、書き込み可能なスナップショットも取得し、こちらをスキャンサーバーにマウントして分析します。これによって異常を検知した場合、即座にアラート通知するとともに直近の健全なバックアップを提示します」と橋口氏は説明する。他社ストレージの類似ソリューションで見られるようなメタデータだけでなく、ヘッダーやコンテンツを含めた解析を行うことで、巧妙化するサイバー脅威をより高度な精度で検知するのがCyber Detection機能の強みだ。

こうしたInfiniBoxの特徴を生かしたサイバー犯罪対策の取り組みとしては、国内大手光学機器メーカーの事例もある。**「コストを抑えながらも安心して大容量データを保管できるアーキテクチャーに加えて、改ざん防止スナップショット機能を標準で利用できることが採用の決め手となり、画像データの保管およびバックアップのリポジトリとしてInfiniBoxをご利用いただいています。なお、このお客様でもバックアップソフトにはVeeamを採用しており、InfiniBoxとの相乗効果によりセキュリティを強化しています」**と橋口氏は語る。

さらに金融業界に目を向けると、国内大手銀行の事例もある。バックアップシステムの統合によるコスト削減と運用の簡素化、セキュリティレベルの向上を背景としたもので、こちらでも改ざん防止スナップショットならびに改ざん防止ファイルシステムといった機能を標準で利用できることが採用の決め手となった。その後もInfiniBoxは安定した稼働を続けており、当初のファイルサーバーやバックアップレポジトリだけでなく、現在ではIA統合基盤上でも導入が拡大しているという。

データの保管先であるストレージ層だからこそ実現できる技術によってInfiniBoxは、ランサムウェア対策に最適なソリューションとして高い評価を獲得しているのである。

INFINIDAT

INFINIDAT

jp_sales@infinidat.com | 03-4243-6343

© Infinidat 2024