ベリタスと NEC iStorage HSが ランサムウェア攻撃への回復力を強化

Veritas Enterprise Data Services Platform と NEC 改ざん防止テクノロジー搭載のiStorage HSでデータを保護し、攻撃から速やかに回復

VERITAS | Orchestrating a brighter world NEC

概要

データ主導の世界となった今日、ランサムウェア攻撃によって壊滅的な影響を受けることが増えています。その脅威の数は増加の一途をたどっているという調査結果も出ています。サイバー犯罪による被害総額は、2021 年までに世界全体で年間 6 兆ドルに達すると予想されており[1]、その中でもランサムウェアが占める割合は非常に高くなっています。では、企業がデータ保護を強化し、攻撃を受けても確実に回復できるようにするにはどうすればよいでしょうか。

ベリタスと日本電気株式会社 (NEC) は、ランサムウェア攻撃の増加と巧妙化に対するお客様の懸念を共に認識しており、ランサムウェア攻撃に対する回復力を高めるために、強力で信頼性の高いソリューションを提供するという両社の取り組みに基づき、NEC iStorage HS シリーズ(HS3/HS8) (以降、iStorage HS) の改ざん防止テクノロジを採用した、Veritas NetBackup 統合型 Open Storage Technology (OST) APIソリューションを新たに提供します。

NETBACKUP と NEC ISTORAGE HS (改ざん防止テクノロジー搭載) による保護の強化

iStorage HS に格納したデータに対するランサムウェアからの保護を、NetBackup™ から iStorage HS の改ざん防止機能を使用し透過的に統合管理することができます。管理者はファイルシステムを作成するときに、そのファイルシステムに対し、WORM (Write Once, Read Many) の指定をすることができます。

iStorage HS に搭載されている 改ざん防止機能は、WORM テクノロジのエンタープライズモードとコンプライアンスモードを使用して偶発的または意図的な情報の消去や改ざんを防止することで、重要なデータの信頼性を確保し、データを追跡管理して、ストレージ管理を簡素化します。

NetBackup と NEC の iStorage HS に搭載された改ざん防止 テクノロジを組み合わせて OST API を活用することで、iStorage HS ストレージに対し、NetBackup で改ざん不可能なポリシーとバックアップイメージを作成、管理できるようになります(図 1 を参照)。NetBackup 管理者は、iStorage HS の改ざん不可能なストレージにバックアップされたファイルの保持期間を設定、確認できます。iStorage HS は NetBackup に統合された保持ロックで OST API を利用します。API セットを使用すると、iStorage HS プラットフォームにバックアップされたファイルの保持期間を設定および取得できます。また、NetBackup インターフェースを使用して、iStorage HS にあるロックされたファイルの保持期間を追跡することもできます。この機能は、保持ロックのコンプライアンスモードとガバナンスモードに対応しています。

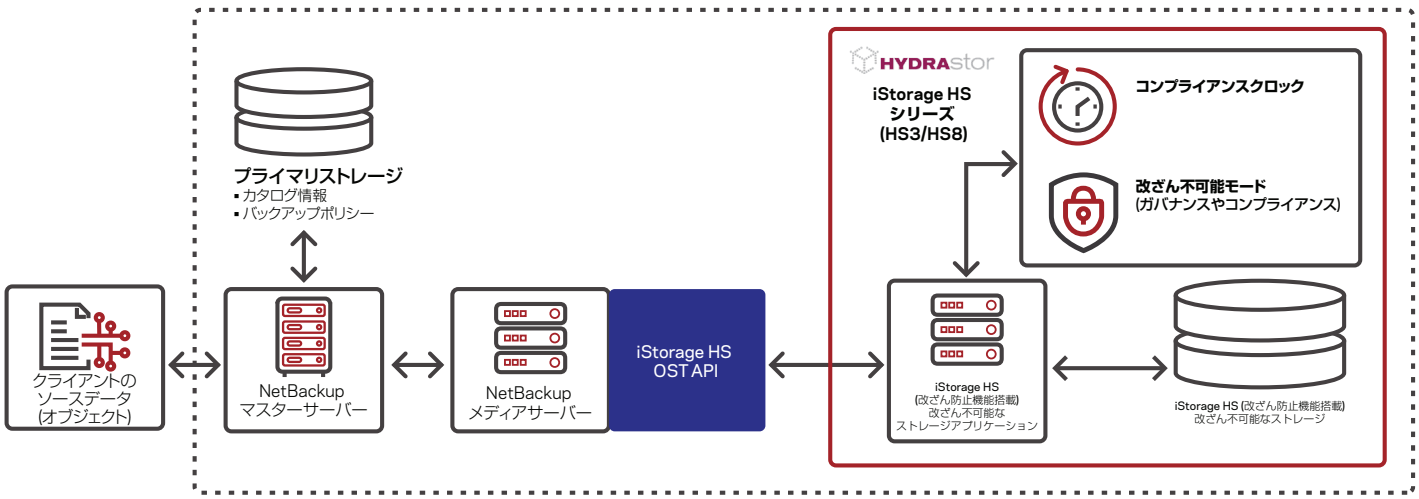

図 1. NetBackup と iStorage HS OST 論理アーキテクチャ対応の改ざん不可能なストレージ

Veritas Enterprise Data Services Platform と iStorage HS を組み合わせることで、米国サイバーセキュリティインフラストラクチャセキュリティ庁が推奨する「3-2-1」バックアップ戦略 (データのコピーを 3 つ以上用意、2 種類以上のメディアに保存、1 つをオフサイトに保存) を簡単に維持できます。データの複数のコピーを作成してから、改ざん不可能なクラウドまたはテープなどの代替メディアに追加のバックアップを保存できます。この「3-2-1」バックアップ戦略のアプローチを実現するには、組み込みのレプリケーション機能を提供する NetBackup Auto Image Replication (AIR) と、必要に応じて自動化され、統合された方法で大規模なリカバリをサポートする Veritas Resiliency Platform を使用して、データ保護を 2 つの階層で行います(図 2 を参照)。

「3-2-1」バックアップ戦略

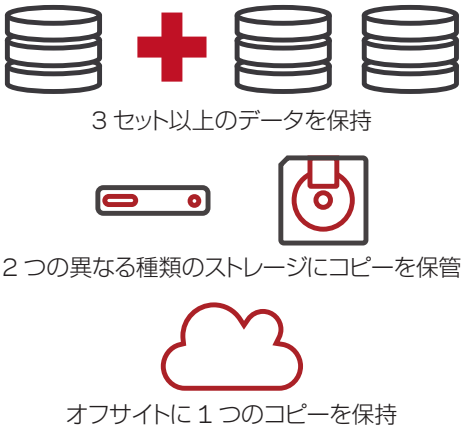

図 2.「3-2-1」バックアップ戦略 (データのコピーを 3 つ以上用意、2 種類以上のメディアに保存、1 つをオフサイトに保存)

悪質な活動の検知と特定

ランサムウェアに対する最初の防御は、所有しているデータ、保存場所、アクセスできるユーザー、アクセスしたユーザーを知ることです。iStorage HS と Veritas Enterprise Data Services Platform を統合することで、インフラをエンドツーエンドで把握し、データを実用的に可視化できます。こうしたベリタスのツールを利用することで、監査ログ、ファイルタイプ、アクセス権限、読み取り/書き込みなど、システム全体のデータやインフラ情報を、単一のカスタマイズ可能なユーザーインターフェースで明確に把握することができます。

ビジネスの回復にはデータの迅速なリストアが不可欠

効果的かつ効率的で多層的なバックアップおよびリカバリ戦略を策定すれば、自然災害や人的エラーなどの日常的な危険からデータを保護できます。iStorage HS は、NetBackup 単独での保護に防御層を追加し、ダウンタイムを最小限に抑え、回復力を維持します。Veritas Enterprise Data Services Platform と iStorage HS を活用することで、データの保存場所に関わらず、大規模な統合データリカバリを提供するという共同ソリューションの真価を実現できます。

実績ある回復力

バックアップおよびリカバリ戦略の中核に NetBackup と NEC iStorage HS (改ざん防止機能搭載) を据えることで、ランサムウェア攻撃などの最悪のシナリオが発生した場合でも、コストを最小限に抑え、リカバリを最適化し、リスクを評価して軽減できます。

ベリタスと NEC のパートナーシップと価値ある統合ソリューションについては、Veritas.com をご覧ください。ハードウェアおよびクラウドストレージ互換性リスト (HCL) については、ベリタスサポートページを参照してください。また、NEC iStorage HS については NEC.com をご覧ください。

1. https://cybersecurityventures.com/cybersecurity-almanac-2019/

ベリタスについて

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、ベリタスのソリューションを導入しています。ベ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。ベ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。ベリタステクノロジーズ合同会社は、Veritas Technologies の日本法人です。

〒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

各国オフィスとお問い合わせ先については、
弊社の Web サイトを参照してください。
www.veritas.com/ja/jp/company/contact

VERITAS | Orchestrating a brighter world NEC

V1281 03/21